CEPT ECC
Electronic Communications Committee

ECC Recommendation (23)03

Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers

approved 28 November 2023

Edition 28 November 2023

LIST OF ABBREVIATIONS

Abbreviation	Explanation
BSC	Base Station Controller
CEPT	Conference of European Postal and Telecommunications Administrations
CgPN	Calling Party Number
CdPN	Called Party Number
CLI	Calling Line Identification
EECC	European Electronic Communications Code
ECC	Electronic Communications Committee
ET	Extraterritorial
EU	European Union
FTN	Forwarded-to Number
GMSC	Gateway Mobile Switching Centre
HLR	Home Location Register
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber ISDN number
MSRN	Mobile Subscriber Roaming Number
OTT	Over-The-Top
PBX	Private Branch Exchange
PRN	Provide Roaming Number
PSTN	Public Switched Telephone Network
SIP	Session Initiation Protocol
SRI	Send Routing Information
TMSI	Temporary Mobile Subscriber Identity
VLR	Visitor Location Register

INTRODUCTION

Much work has already been done in the past with the goal of safeguarding the reliability of the Calling Line Identification (CLI). This has resulted in, among other things, the ECC Recommendation (19)03 [1] on Measures for Increasing Trust in Calling Line Identification and Originating Identification.

CLI spoofing has been increasing during the last years with a very negative impact for end-users and has become a significant problem. ECC Report 338 on CLI spoofing [2] adopted in June 2022 defines CLI spoofing as a technique that enables the originating party and/or any network operator handling the call or message to manipulate the information displayed in the CLI field with the intention of deceiving the receiving party or the network operators intervening in the handling of the call or message into thinking that the call or message originated from another person, entity or location. It also contains in the conclusion, under the form of six points, possible policy actions to mitigate or stop CLI spoofing. This ECC Recommendation implements the fourth possible policy action[1] mentioned in the conclusion of the ECC Report 338 and is complementary with ECC Recommendation (19)03.

The largest share of calls with spoofed numbers is caused by incoming calls with national phone numbers over the international network interfaces. End users get the impression that they are dealing with reliable parties (e.g. banks of which they are customers) and are thus misled. This ECC Recommendation puts forward measures to handle such incoming international voice calls with suspected spoofed national E.164 numbers as CLI. These measures could include that such voice calls would be either blocked, or at least the CLI is removed.

The ambition of this ECC Recommendation is to introduce some good practices and to move as far as possible towards a common approach in the CEPT countries, in particular for national fixed/geographic and mobile E.164 numbers. Also, the question which operator in handling the call should be responsible for the blocking of the call, or the removal of the CLI, is addressed.

The ECC Recommendation starts from the principle that, in general, it cannot be justified that calls originating from abroad can be associated with national fixed/geographic numbers. However, available CLI manipulation techniques enable the possibility for incoming voice calls to appear over international network interfaces with national fixed/geographic numbers. This leads to the conclusion that, unless there are justified and allowed exceptions for such CLI manipulation techniques, these numbers can be unambiguously considered as spoofed.

For national mobile numbers, the situation is more complex as national users can roam[2]. When an operator receives calls on the international network interfaces in which the calling party number is a national mobile number, the operator should ensure that either the number belongs to a user of an operator with domestic activities and the concerned user is abroad and can therefore be assumed to be making the call, or the call corresponds to another type of legitimate exception.

Annex 1 gives examples of scenarios of calls where the flow would result in incoming voice calls with national numbers as CLI over the international network interfaces, including some possible solutions which CEPT administrations can decide to impose as measures to handle cases of legitimate calls with a national number as CLI coming from abroad.

For the monitoring of the implementation of the ECC Recommendation, CEPT administration should hold a list of national operators that operate international network interfaces and therefore directly handle incoming international voice calls.

[1] "to consider an ECC Recommendation on blocking mechanisms implemented at international gateways for incoming traffic originated from suspected spoofed national E.164 numbers;"

[2] in this ECC Recommendation, roaming is considered as a technique enabling a mobile subscriber to attach to a foreign network (whilst abroad) and both originate and receive calls.

ECC RECOMMENDATION (23)03 OF 28 NOVEMBER 2023 ON MEASURES TO HANDLE INCOMING INTERNATIONAL VOICE CALLS WITH SUSPECTED SPOOFED NATIONAL E.164 NUMBERS

“The European Conference of Postal and Telecommunications Administrations,

considering

a) the ECC Report 338 on CLI spoofing [2];

b) that in many cases fraud (e.g. phishing) is facilitated by CLI spoofing and causes a lot of damage to users and society and consequently reduces the overall trust in numbering and electronic communications;

c) the damage caused by CLI spoofing is so extensive that the introduction of additional obligations for operators is justified;

d) the Recommendation ITU-T E.157 on International calling party number delivery [3];

e) the ECC Recommendation (19)03 on Measures for Increasing Trust in Calling Line Identification and Originating Identification [1];

f) that the origination of voice calls may take place in foreign jurisdictions through Over-The-Top (OTT) providers, which may either use numbers directly assigned to them, numbers sub-assigned to them by other providers, or specific numbers belonging to their end-users who avail of decoupling, as discussed in ECC Report 248 [4];

g) the Technical Report ITU-T TR.spoofing - Countering spoofing [7];

h) that the solutions CEPT recommends could also apply to the network provided calling party number and not only to the number to be presented as CLI.

recommends

that CEPT administrations should:

1. ensure that operators when directly handling incoming international voice calls over their international network interfaces adopt measures:

   a) to block incoming international voice calls which do not respect Recommendation ITU-T E.157 [3];

   b) for national geographic/fixed E.164 numbers: to preferably block incoming international voice calls, or at least to suppress the CLI of incoming international voice calls with a national geographic/fixed E.164 number, except in justified cases. Any exception should be carefully considered and justified, since exceptions may be particularly attractive for spoofers. If exceptions are allowed, a mechanism to securely manage the exceptions should be adopted (e.g. secure whitelist between providers);

   c) for national mobile E.164 numbers: to preferably block incoming international voice calls, or at least to suppress the CLI of incoming international voice calls with a national mobile E.164 number as CLI after checking and verifying that the user is not roaming abroad, except in justified cases. Checks on roaming status should be carried out while respecting relevant privacy provisions.

2. ensure that any measures adopted do not jeopardise the handling of legitimate incoming international voice calls or block nationally permitted exceptions (as further discussed in the informative Annex 1);

3. facilitate the cooperation between operators to implement in particular 1.c and 2 above.

Note:

Please check the Office documentation database https://docdb.cept.org/ for the up to date position on the implementation of this and other ECC Recommendations.

ANNEX 1: EXAMPLES OF SCENARIOS TO BE CONSIDERED FOR THE APPLICATION OF THIS ECC RECOMMENDATION (INFORMATIVE)

There are a few scenarios to be considered for the application of this ECC Recommendation. More precisely, the scenario (scenario n. 1) of incoming voice calls associated with national mobile E.164 numbers as CLI and the scenarios (scenario n. 2-5) where legitimate incoming voice calls appear over international network interfaces with national fixed/geographic or mobile numbers. The purpose of this Annex is to illustrate examples of such scenarios and to indicate where logic is to be implemented within the network to prevent the blocking of legitimate calls with possible considerations for combating CLI spoofing in such cases. The figures only show the main elements involved in the call flows, and the names of these elements could change with the different technology in use, i.e. 2G, 3G, 4G and 5G.

A1.1 SCENARIO 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”).

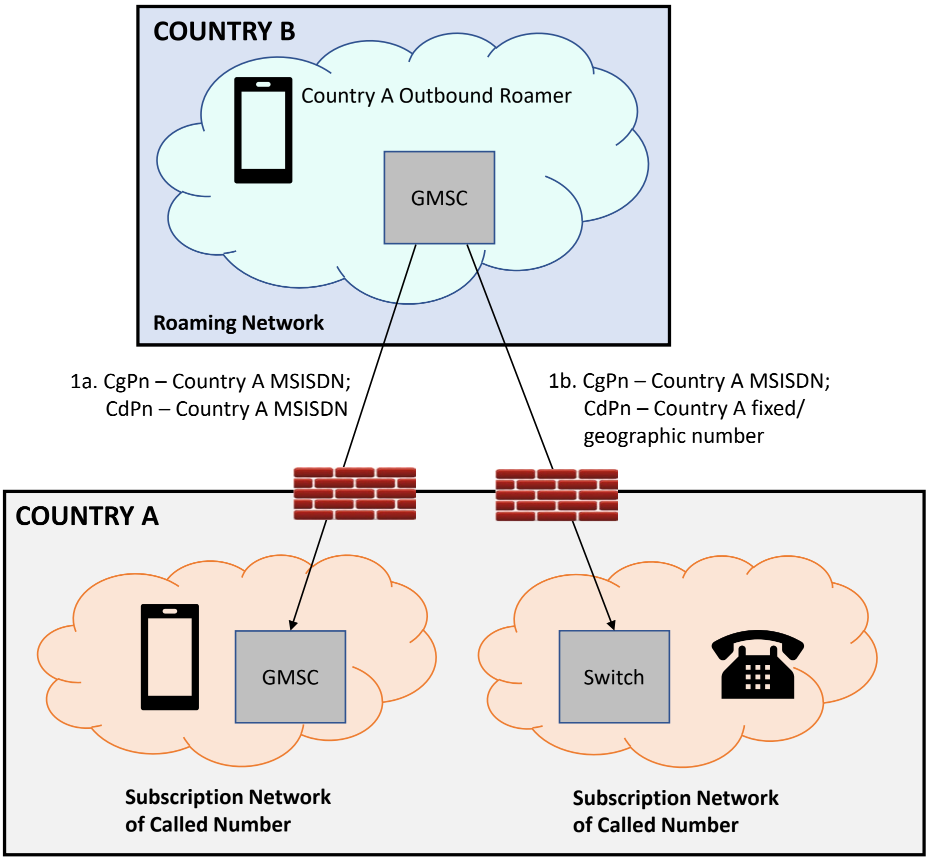
COUNTRY B
Country A Outbound Roamer
GMSC
Roaming Network
1a. CgPn – Country A MSISDN; CdPn – Country A MSISDN
1b. CgPn – Country A MSISDN; CdPn – Country A fixed/ geographic number
COUNTRY A
GMSC
Switch
Subscription Network of Called Number
Subscription Network of Called Number

Figure 1: Call from a national outbound roamer

Figure 1 shows the main steps involved in order for an outbound roamer of Country A to reach a national number of Country A while the caller is roaming in Country B. For each call leg, the calling party number (CgPn) and called party number (CdPn) are indicated. On the basis of the CdPn, the call is routed towards the subscription network of the called number in Country A (Step 1a or Step 1b, depending on whether the called number is a mobile number or fixed/geographic number respectively).

In order to avoid blocking such calls at the international network interfaces, operators should check and verify that the end-user is roaming abroad while respecting relevant privacy provisions. This check could also be done through a centralised neutral entity (roaming check proxy), or through a distributed solution, to ensure that the querying operator does not get more information than needed and has no direct access to the other operator’s Home Location Register (HLR).

A1.2 SCENARIO 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).

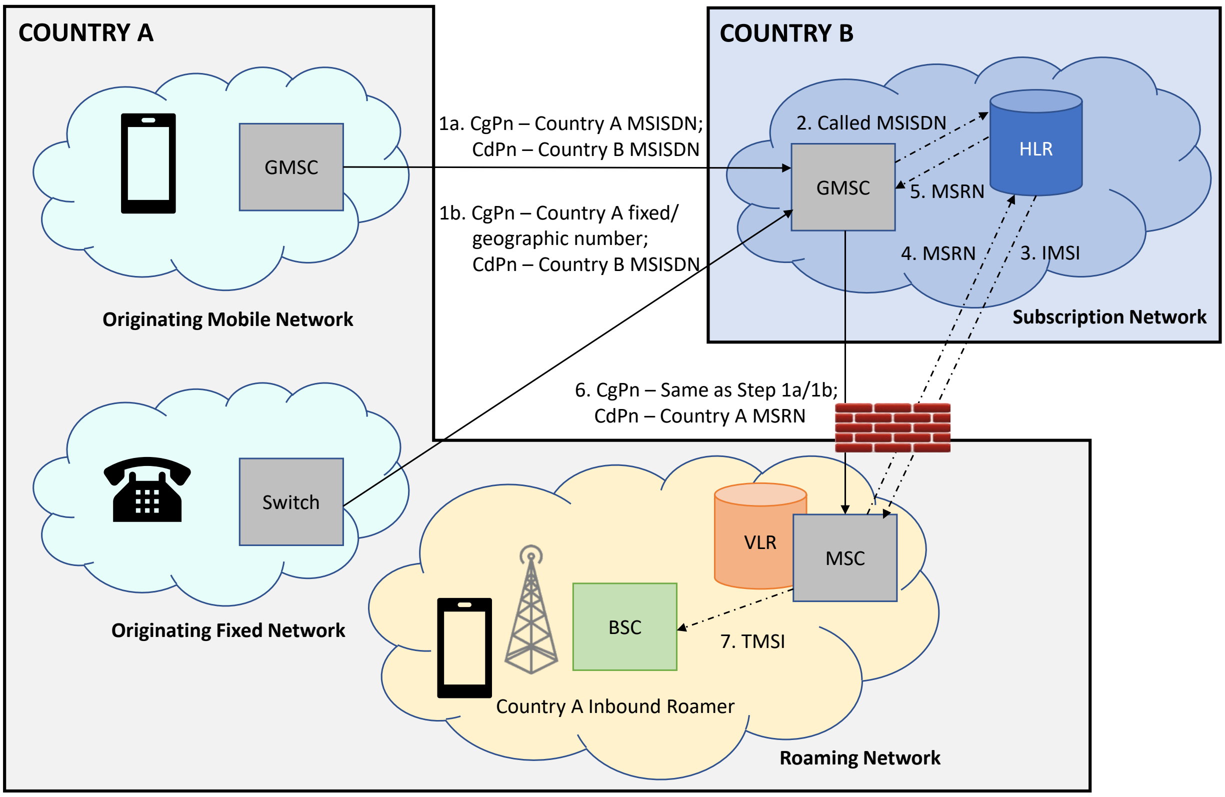
COUNTRY A
GMSC
Originating Mobile Network
Switch
Originating Fixed Network
1a. CgPn – Country A MSISDN; CdPn – Country B MSISDN
1b. CgPn – Country A fixed/ geographic number; CdPn – Country B MSISDN
COUNTRY B
2. Called MSISDN
HLR
GMSC
5. MSRN
4. MSRN
3. IMSI
Subscription Network
6. CgPn – Same as Step 1a/1b; CdPn – Country A MSRN
VLR
MSC
BSC
7. TMSI
Country A Inbound Roamer
Roaming Network

Figure 2: Call to an inbound roamer

Figure 2 shows the main steps involved in order to reach the inbound roamer and for each call leg, the calling party number (CgPn) and called party number (CdPn) are indicated. On the basis of the called Mobile Subscriber ISDN number (MSISDN), the call originating in a mobile or fixed network in Country A is routed towards the Gateway Mobile Switching Centre (GMSC) of the called party's subscription network in Country B (Step 1a or Step 1b respectively). Before proceeding with the call set-up, the GMSC then sends a Send Routing Information (SRI) query for the called MSISDN to the HLR (Step 2). The HLR then sends a Provide Roaming Number (PRN) request, including the International Mobile Subscriber Identity (IMSI) associated with the called MSISDN, to the Mobile Switching Centre/Visitor Location Register (MSC/VLR) in the roaming network in Country A (Step 3). The MSC/VLR responds to the HLR and includes the Mobile Subscriber Roaming Number (MSRN) in the response (Step 4). The MSRN would be a national mobile number from a numbering block assigned to the roaming network operator in Country A. The HLR would send the MSRN to the GMSC in the SRI (Step 5). The GMSC then uses the MSRN to route the call towards the MSC/VLR of the roaming network in Country A (Step 6). In turn, the MSC/VLR of the roaming network makes use of a Temporary Mobile Subscriber Identity (TMSI) to terminate the call towards the inbound roamer, thus ensuring the subscriber's confidentiality (Step 7).

In order not to impact legitimate voice calls as described in this scenario, operators should not block, or suppress the CLI of incoming international voice calls where the called party number (B-number) for the call is a national mobile number assigned for use as an MSRN. This measure requires that operators that operate international network interfaces and therefore directly handle incoming international voice calls are to be informed of the national numbering sub-blocks used by mobile network operators for MSRNs.

A1.3 SCENARIO 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:

- Scenario 3.1 - 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 (Figure 3);
- Scenario 3.2 - 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 (Figure 4).

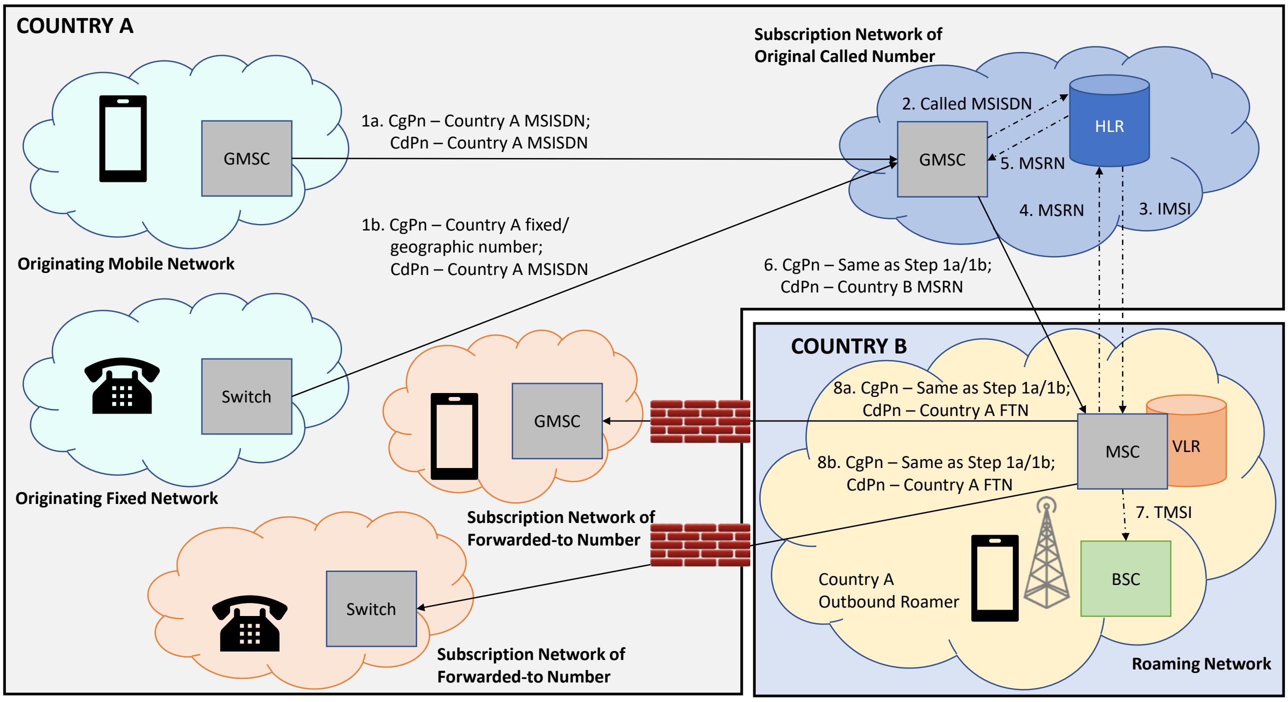
COUNTRY A
Subscription Network of Original Called Number
2. Called MSISDN
HLR
GMSC
1a. CgPn – Country A MSISDN; CdPn – Country A MSISDN
GMSC
5. MSRN
4. MSRN
3. IMSI
1b. CgPn – Country A fixed/ geographic number; CdPn – Country A MSISDN
Originating Mobile Network
6. CgPn – Same as Step 1a/1b; CdPn – Country B MSRN
COUNTRY B
Switch
8a. CgPn – Same as Step 1a/1b; CdPn – Country A FTN
GMSC
MSC
VLR
8b. CgPn – Same as Step 1a/1b; CdPn – Country A FTN
Originating Fixed Network
7. TMSI
Subscription Network of Forwarded-to Number
Country A Outbound Roamer
BSC
Switch
Subscription Network of Forwarded-to Number
Roaming Network

Figure 3: Call to a national outbound roamer with late call forwarding to a national number

Figure 3 shows the main steps involved for Scenario 3.1 and for each call leg, the CgPn and CdPn are indicated. On the basis of the called MSISDN, the call originating in a mobile or fixed network in Country A is routed towards the GMSC of the subscription network of the original called number in Country A (Step 1a or Step 1b respectively). Before proceeding with the call set-up, the GMSC then sends an SRI query for the called MSISDN to the HLR (Step 2). The HLR then sends a PRN request, including the IMSI associated with the called MSISDN, to the MSC/VLR in the roaming network in Country B (Step 3). The MSC/VLR responds to the HLR and includes the MSRN in the response (Step 4). The MSRN would be a national mobile number from a numbering block assigned to the roaming network operator in Country B. The HLR would send the MSRN to the GMSC in the SRI (Step 5). The GMSC then uses the MSRN to route the call towards the MSC/VLR of the roaming network in Country B (Step 6). In turn, the MSC/VLR of the roaming network makes use of a TMSI to terminate the call towards the inbound roamer, thus ensuring the subscriber's confidentiality (Step 7).

When the MSC/VLR establishes that the call cannot be set up towards the original called party (e.g. due to no reply from the called party, called party is busy, etc.) in Step 7, the MSC/VLR would make use of the call forwarding information stored in the called party's profile in the VLR. As in this case the forwarded-to number (FTN) would be a national number pertaining to the national numbering plan of Country A, the MSC/VLR would forward the call towards the subscription network of the FTN in Country A (Step 8a or 8b, depending on whether the FTN is a mobile number or fixed/geographic number respectively). The CgPn of the forwarded leg in Step 8a/8b would be the same national number of Country A which appears as the CgPn in Step 1a/1b and Step 6. The forwarding number would correspond to the number doing the forwarding which in this case is the national number of Country A assigned to the outbound roamer.

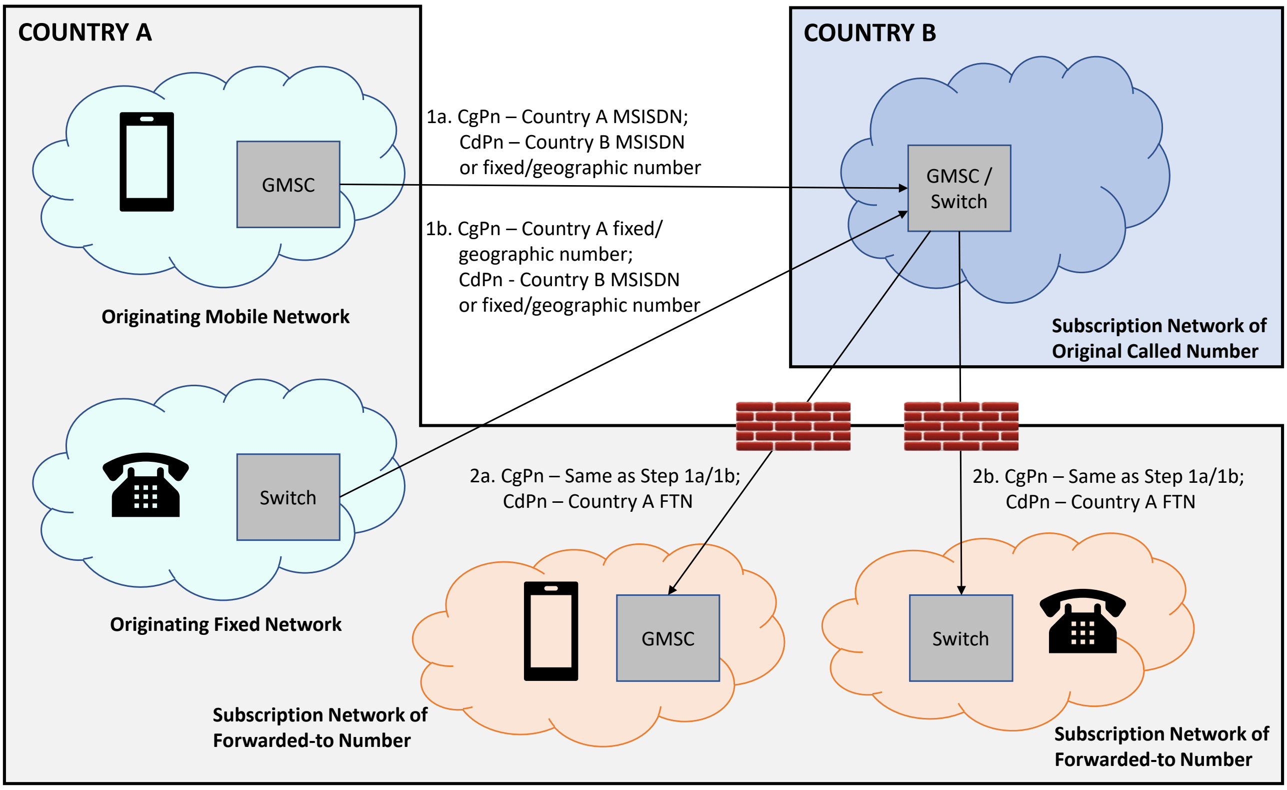
COUNTRY A
COUNTRY B
GMSC
1a. CgPn – Country A MSISDN;
CdPn – Country B MSISDN
or fixed/geographic number
1b. CgPn – Country A fixed/
geographic number;
CdPn - Country B MSISDN
or fixed/geographic number
GMSC / Switch
Originating Mobile Network
Subscription Network of Original Called Number
Switch
Originating Fixed Network
2a. CgPn – Same as Step 1a/1b;
CdPn – Country A FTN
2b. CgPn – Same as Step 1a/1b;
CdPn – Country A FTN
GMSC
Switch
Subscription Network of Forwarded-to Number
Subscription Network of Forwarded-to Number

Figure 4: Call to a foreign number with call forwarding to a national number

Figure 4 shows the main steps involved for Scenario 3.2 and for each call leg, the CgPn and CdPn are indicated. On the basis of the called foreign number, the call originating in a mobile or fixed network in Country A is routed towards the subscription network of the original called number in Country B (Step 1a or Step 1b respectively). The subscription network establishes that the call is to be forwarded due to unconditional or conditional call forwarding. The steps involved may vary depending on the call forwarding reason and are not being shown in detail in the Figure 4. The subscription network would then forward the call towards the FTN which in this scenario is a national number pertaining to the national numbering plan of Country A (Step 2a or 2b, depending on whether the FTN is a mobile number or fixed/geographic number respectively). The CgPn of the forwarded leg in Step 2a/2b would be the same national number of Country A which appears as the CgPn in Step 1a/1b. The forwarding number would correspond to the number doing the forwarding which in this case is the foreign number from the national numbering plan of Country B.

In order not to impact legitimate voice calls as in Scenario 3.1 and Scenario 3.2, operators should not block, or suppress the CLI of incoming international voice calls where the forwarding number is checked and verified as being assigned to a user who is roaming abroad (as in Scenario 3.1) or the forwarding number is a foreign number (as in Scenario 3.2).

A1.4 SCENARIO 4

A call from a national service provider implemented in a cloud solution and destined to a national number using the international network interface.

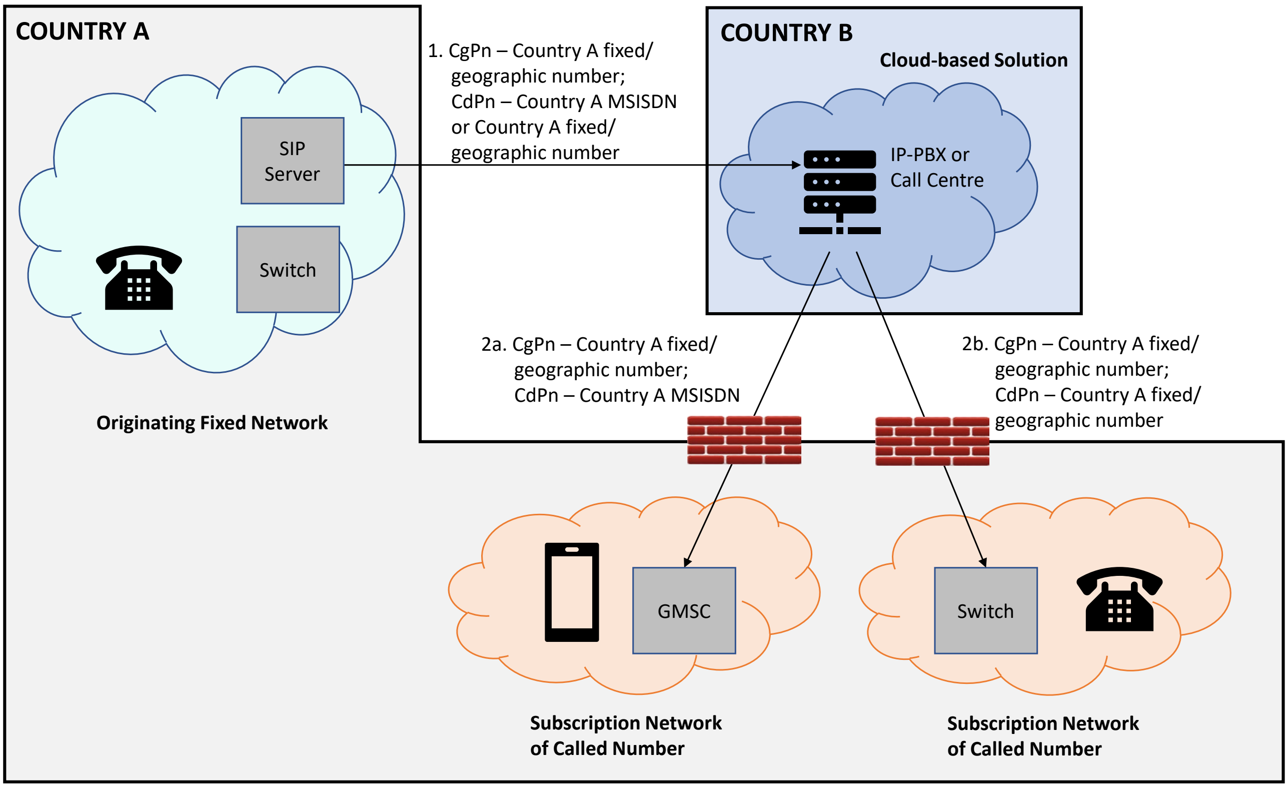
COUNTRY A
SIP Server
Switch
Originating Fixed Network
1. CgPn – Country A fixed/ geographic number; CdPn – Country A MSISDN or Country A fixed/ geographic number
COUNTRY B
Cloud-based Solution
IP-PBX or Call Centre
2a. CgPn – Country A fixed/ geographic number; CdPn – Country A MSISDN
2b. CgPn – Country A fixed/ geographic number; CdPn – Country A fixed/ geographic number
GMSC
Switch
Subscription Network of Called Number
Subscription Network of Called Number

Figure 5: Call from an end-user of a national service provider implemented in a cloud solution using a fixed/geographic number as CLI

Figure 5 shows the steps involved for the conveyance of a call originating by an end-user of a service provider in Country A, where the service provider in question opts to provide the service through a cloud-based solution in Country B. The call is routed towards the subscription network of the called number in Country A (Step 2a or Step 2b, depending on whether the called number is a mobile number or fixed/geographic number respectively).

In order not to impact legitimate voice calls, CEPT administrations may consider solutions to verify that the call is actually originated in Country A. To that end, in order to identify a voice call that should not be blocked, it could be useful to:

- Either introduce a whitelist to include the fixed/geographic numbers pertaining to Country A which are permitted to be used over such cloud-based solutions as CLI for incoming international voice calls. In such a case, operators should not block, or suppress the CLI of incoming international voice calls where the CgPn is included in a whitelist; or
- Impose an obligation on, or recommend to providers of cloud-based solutions to implement a dedicated interface[3] in Country A such that calls originated by an end-user in Country A with a national number from Country A as CLI would be received through this dedicated interface which could be the same connection used to convey calls originating from the national service provider. The call flow shown in Figure 5 would no longer be applicable if such a dedicated interface in Country A is implemented.

  By opting for the establishment of a dedicated interface in Country A, cloud-based solution providers would also become subject to the regulatory oversight of the respective CEPT administration responsible for the national numbers. Such oversight may also imply that, if malicious activity is detected, the CEPT administration may be able to take more direct action, (e.g. for EU Member States, action under Article 97(2) of the EECC), when compared with a situation without such dedicated interface.

[3] In this ECC Recommendation, a dedicated interface means the implementation by an undertaking of a dedicated SIP interface or alternative trunk type interface to serve another undertaking to ensure that calls from end-users of the latter undertaking originate on the national network.

A1.5 SCENARIO 5

A call from a number of Country A, which is assigned for extraterritorial (ET) use in Country B in accordance with ECC Recommendation 16(02) "Extraterritorial Use of E.164 Numbers - High level principles of assignment and use" [5], is destined to a national number of Country A.

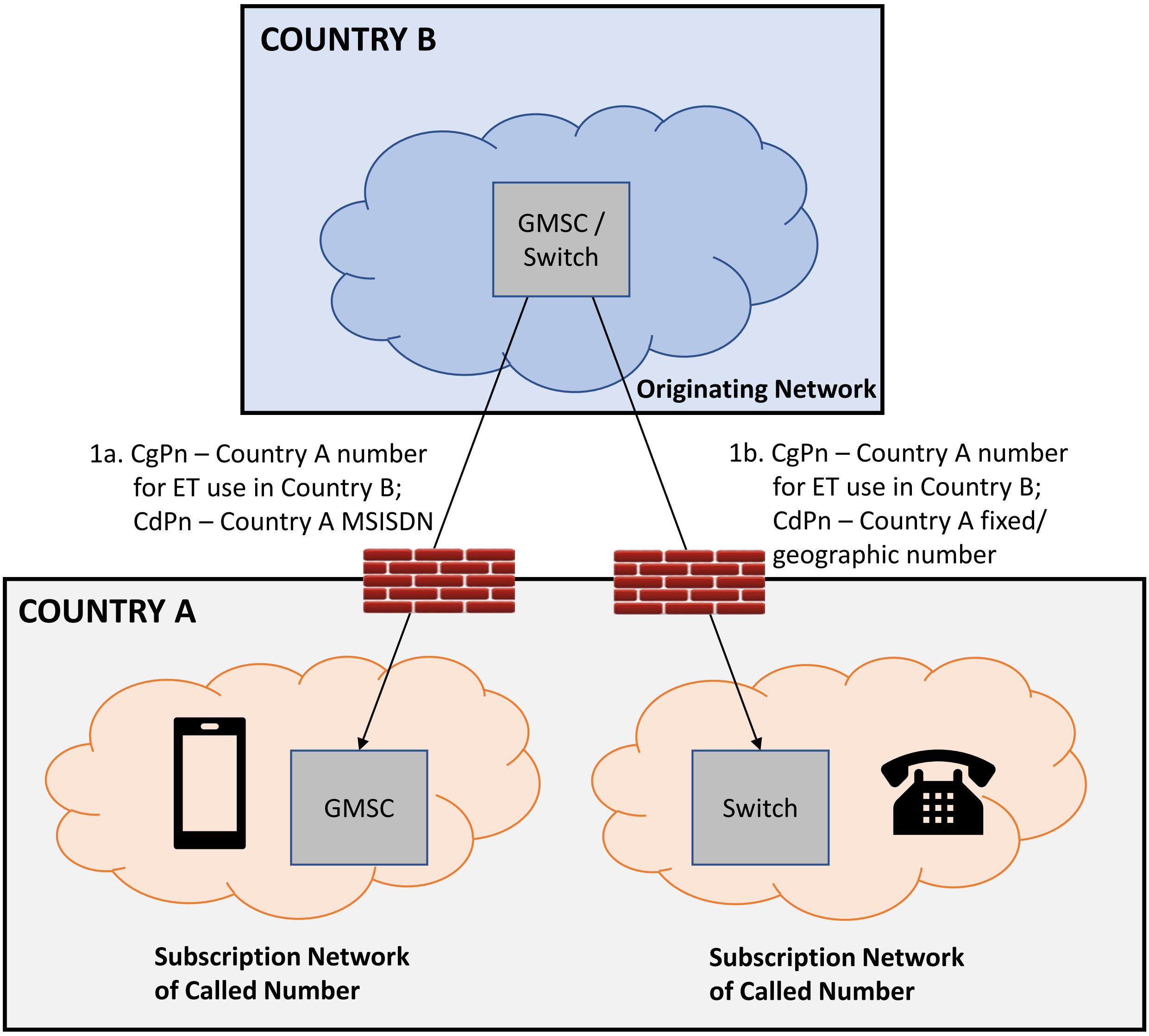
COUNTRY B
GMSC / Switch
Originating Network
1a. CgPn – Country A number for ET use in Country B; CdPn – Country A MSISDN
1b. CgPn – Country A number for ET use in Country B; CdPn – Country A fixed/ geographic number
COUNTRY A
GMSC
Switch
Subscription Network of Called Number
Subscription Network of Called Number

Figure 6; Call originating from a number of Country A, which is assigned for extraterritorial use in Country B, towards a called number in Country A

Figure 6 shows that the call originating from a number of Country A, which is assigned for extraterritorial use in Country B, is routed towards the subscription network of the called number in Country A (Step 1a or Step 1b, depending on whether the called number is a mobile number or fixed/geographic number respectively).

In order not to impact legitimate voice calls as in Scenario 5, operators should not block, or suppress the CLI of incoming international voice calls where the CgPn is a number assigned for extraterritorial use. However, the identification of measures intended to distinguish legitimate calls from calls spoofing such numbers with rights for extraterritorial use requires further study. Without such measures in place, the risk of allowing such a practice may outweigh the benefits.

A1.6 SCENARIO 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’ was addressed in detail in the ECC Report 248 on Evolution in CLI Usage [4], whereby it was shown that this 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.

Figure 7 shows two different call flows:

- Steps 1a and 1b (in blue): A normal call origination, whereby the caller makes use of the access (e.g. Session Initiation Protocol (SIP) trunk) from the original subscription network serving the E.164 number (i.e. for a non-ported number, the block operator which assigned the number; for a ported number, the recipient operator);
- Steps 2a and 2b (in red): An alternative call origination through an OTT application with an Internet Protocol (IP)/ Public Switched Telephone Network (PSTN) Gateway located in Country B, whereby the caller makes use of the broadband access. In this case, the caller and/or the OTT provider has associated the OTT subscription with the same E.164 number being served by the original subscription network).

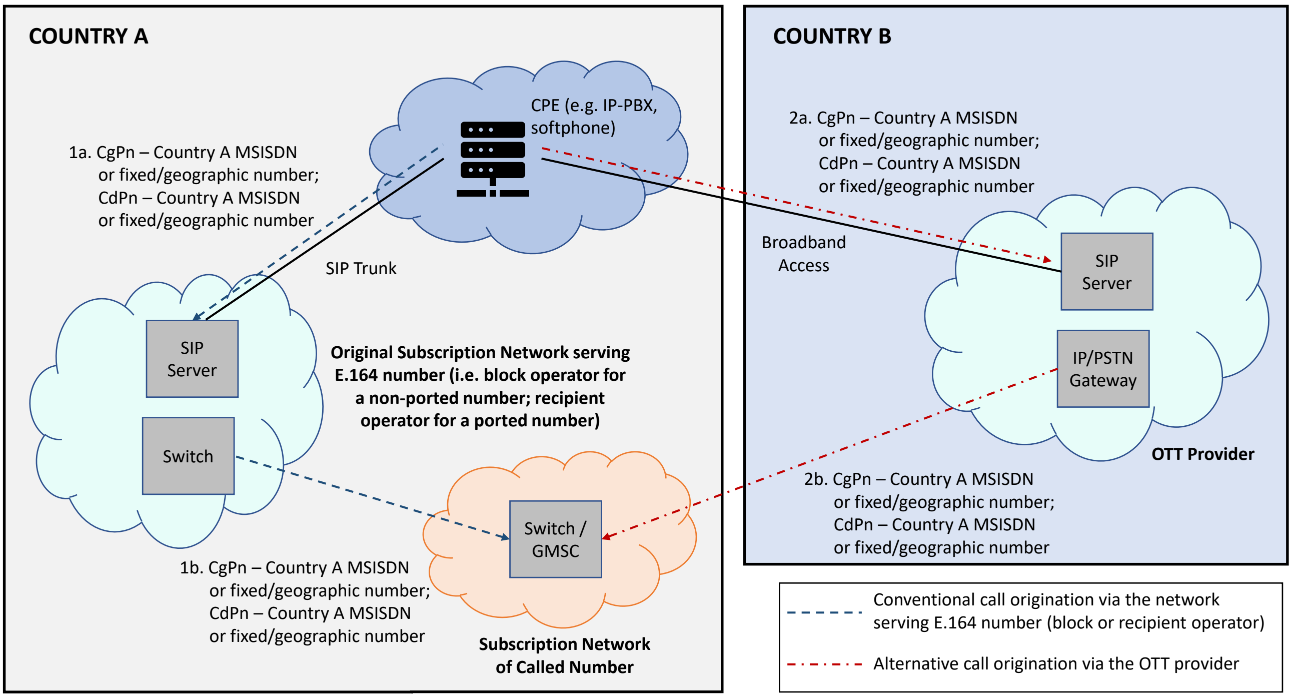
COUNTRY A
COUNTRY B
CPE (e.g. IP-PBX, softphone)
1a. CgPn – Country A MSISDN or fixed/geographic number; CdPn – Country A MSISDN or fixed/geographic number
SIP Trunk
SIP Server
Switch
Original Subscription Network serving E.164 number (i.e. block operator for a non-ported number; recipient operator for a ported number)
Switch / GMSC
1b. CgPn – Country A MSISDN or fixed/geographic number; CdPn – Country A MSISDN or fixed/geographic number
Subscription Network of Called Number
2a. CgPn – Country A MSISDN or fixed/geographic number; CdPn – Country A MSISDN or fixed/geographic number
Broadband Access
SIP Server
IP/PSTN Gateway
OTT Provider
2b. CgPn – Country A MSISDN or fixed/geographic number; CdPn – Country A MSISDN or fixed/geographic number
Conventional call origination via the network serving E.164 number (block or recipient operator)
Alternative call origination via the OTT provider

Figure 7: Calls originating from a number of Country A towards a called number in Country A through the original subscription network and through an OTT provider in Country B

In practice, this decoupling could severely limit the effectiveness of any measure being implemented which rests on restrictions or exceptions tied to specific numbering ranges. Such cases should be addressed by CEPT administrations imposing an obligation for such OTT providers to implement a dedicated interface in Country A if they would be allowing outgoing calls to make use of national numbers from Country A as CLI. Such an approach would make calls originated from such OTT providers outside of the scope of the measures being adopted, as the resulting voice traffic would not appear to be incoming calls over the international network interfaces. Furthermore, this approach would have no negative impact on the continued validity of the conclusions drawn in both ECC Report 248 on Evolution in CLI Usage [4] and ECC Report 273 on E.164 Numbering in OTT Communications Services [6].

ANNEX 2: LIST OF REFERENCES

[1] ECC Recommendation (19)03: “Measures for increasing Trust in Calling Line Identification and Originating Identification”, approved November 2019

[2] ECC Report 338: “CLI spoofing”, approved June 2022

[3] Recommendation ITU-T E.157: “International calling party number delivery”

[4] ECC Report 248: “Evolution in CLI usage – decoupling of rights of use of numbers from service provision”, approved April 2016

[5] ECC Recommendation 16(02): “Extra-Territorial Use of E.164 Numbers - High level principles of assignment and use”, approved April 2016, amended June 2023

[6] ECC Report 273: “E.164 Numbering in OTT Communications Services”, approved May 2018

[7] Technical Report ITU-T: “TR.spoofing - Countering spoofing”