SWISS TSP ANTI-SPOOFING AGREEMENT

TECHNICAL SPECIFICATION

(SPECIFICATION HOW SWISS OPERATORS MUST WORK TOGETHER TO PREVENT CALLER ID SPOOFING FOR CALLS INCOMING FROM ABROAD)

Document Information

Date of issue	01.07.2026
Replaces Version	1.2
Version Number	2.0
Last changes	29.06.2026
Status	Final
Comes into force on	01.07.2026

Document Release History

Version No.	Release Date	Purpose
1.0	30.10.2024	Initial Version elaborated and agreed by a TSP working group
1.1	04.03.2025	Update
1.2	01.04.2025	Update (Final)
2.0	29.06.2026	Update Clarifications and mobile rules (Final)

1. INTRODUCTION 3

1.1 Summary 3

1.2 Motivation 4

1.3 Scope 6

1.4 Definitions 6

1.5 Terminology 8

1.6 References 8

2. Solution to mitigate the spoofing issue 8

2.1 Idea and Challenge 8

2.2 Examples 9

3. Solution Rules 13

3.1 Marking incoming calls from abroad 13

3.2 Anonymizing Caller IDs 13

3.3 Blocking calls due to a spoofed Caller ID 14

3.4 Recognizing exceptions 14

4. List of Acronyms 16

1. INTRODUCTION

1.1 Summary

1.1.1 Technical Abstract

Every Swiss TSP shall mark calls from abroad with a P-CH-Origin header. This header allows a subsequent terminating TSP to recognize that the call came from abroad and apply their Anti-Spoofing rules accordingly.

The rule is: a P-CH-Origin header shall be added in the INVITE message for calls from abroad* (in general or at least in case the Caller ID contains a Swiss number)

*abroad => see definition in chapter 1.4

The format of the header is as follows:

P-CH-Origin: intl=<vsp>; tsp-id=<TSP ID>

Example: *P-CH-Origin: intl=sunrise; tsp-id=2251011*

The value of <vsp> of the “intl” parameter shall designate the TSP which added the P-CH-Origin header, e.g. *bics*, *lightup*, *salt*, *sunrise*, *swisscom*, *verizon*, etc.

For the TSP IDs please refer to:

www.uvek.egov.swiss => Telecom services => Service provider => Search for a TSP => Start Service

Both the parameters “intl” and “tsp-id” shall help to trace in case of failures or complaints. They have no relevance regarding Anti-Spoofing handling.

Note regarding the P-CH-Origin header (PCHO) and its parameters:

- According to RFC 3261, chapter 7.3.1, page 31:
  - The PCHO header field is case-insensitive. The recommended variant is camel-back like, considering CH usually written upper-case: “P-CH-Origin”
  - The “intl” and the “tsp-id” parameter as well as its values are case-insensitive.
- In the context of this PCHO header, the spaces in front of or after semicolons are allowed but optional (as described in RFC 3261, chapter 15.1, page 221)

Anti-Spoofing processing provides recognition of spoofed Caller IDs and applying a “spoofing protection measure”.

The combination of Swiss Caller ID and present P-CH-Origin header indicates that a Caller ID is spoofed. Although, there are some exceptions, where the Swiss Caller ID is legitimate also for calls from abroad. Beside some corner cases, calls from Swiss mobile users outbound-roaming in 2G or 3G networks abroad are an important exception.

Regarding the requirement to add the P-CH-Origin header there is an exception described in chapter 2.2.3.

1.1.2 Spoofing protection measure

This specification considers two measures to protect the called customer against Caller ID spoofing:

If spoofing is recognized,

- the Caller ID is anonymized (see chapter 3.2)

or

- the call is blocked (see chapter 3.3)

In the following text of this document both of these measures are referred to as "**spoofing protection measure**".

For the technical aspects of this topic, e.g. how to anonymize a Caller ID, refer to chapters 3.2 and 3.3.

It is clear that these two measures have different implications for the calls in question. For example, with regard to the tension between the "obligation to deliver calls" and the protection of "customers from abusive calls".

Examples (not exhaustive):

- Calls from Outbound-Roamers (OBR): In a conventional implementation, Caller IDs for calls made to Switzerland by OBR are evaluated as spoofed => false positive.
  It seems excessive and unfair to block these, whilst anonymisation appears justified in view of the spoofing problem, especially as there are ways to circumvent such a measure, such as VoLTE roaming or 2G/3G home routing.

- Calls with invalid or unassigned numbers: It is reasonable to block such calls, as there is no right to use such numbers, and blocking them therefore creates no false positive.

  Examples of such invalid Caller IDs:

  - Invalid format: e.g. +4131789 (too short, too long, invalid characters, . . .)
  - Number range not in use: e.g. +41397891234 (area code does not exist, 10k block is not used).
  - Number is not assigned to a subscription: only possible if the TSP is the NRH.
  - Art. 26a Absatz 5 FDV: Number is not allowed to be used as Caller ID: e.g. +41900… (https://www.fedlex.admin.ch/eli/cc/2007/166/de#art_26_a)

- Call transfer/forwarding case: Call from a Swiss TSP to a user abroad that the user abroad forwards/transfers to a user in Switzerland: The Caller ID is evaluated as spoofed in such a case. This is a false positive.
  Even if this concerns a very corner case it seems not reasonable to block such calls.

It is the responsibility of the TSP implementing the anti-spoofing measures to decide (per use case) which of these two measures is appropriate.

1.2 Motivation

1.2.1 Situation before implementing the rules described in this document

Swiss telephony customers suffer from unwanted marketing and scam calls. Sometimes they receive more spam calls than wanted calls. To counter this problem, TSPs are offering an

anti-spam service to filter out calls identified as spam. Some spammers started spoofing phone numbers (Caller ID) when calling our customers some time ago.

Calls with spoofed phone numbers

- makes it more difficult to detect the calls as spam
  (*unlike spam filters for mail, there is no content available to detect spam, only the possibly spoofed Caller ID and traffic patterns)*

- Make it appear as if the call is originating from a trusted source while the contrary is the case.

  and even . . .

- Spoofing Caller IDs from e.g. police, banks, insurance companies and with prior social engineering also private Caller IDs from e.g. relatives makes a scam even more credible.

- These involve a third-party victim: if the spoofed phone number exists and belongs to a customer, that customer will very often be called back because of missed calls and thus suffer from this additional kind of unwanted calls.

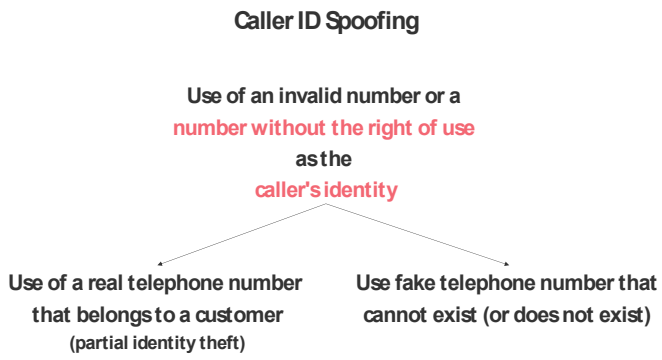

Figure 1-1: Definitions of spoofed number used in this document

Some Swiss TSPs implemented solutions to minimize spoofing cases. But there is little information available for detecting spoofed Caller IDs.

A real-time plausibility check has proven to be an effective tool in recent years. Simplified description: A TSP routes calls between their own customers within their network. So, in general, it is unlikely that the Caller ID of one of their own customers will be routed from outside into their own network.

Note: The best known and most occurring exceptions are calls from 2G and 3G outbound roamers. See chapter 3.4.

If a TSP recognised a spoofed number out of his own range, the TSP has the right and the obligation to apply a “spoofing protection measure” for this call.

With the above-described measures, the TSPs have achieved significant progress against spoofing. However, the spoofing parties started to use numbers from TSP X and TSP Y to setup calls with spoofed Caller IDs to TSP Z, the numbers of TSP X and TSP Z for spoofing against TSP Y, and so on. This happens automatically with the spoofing parties trying out different numbers towards the different TSPs.

1.2.2 Proposed solution

The TSPs have discussed how anti-spoofing mechanisms can be improved. At the same time, OFCOM Switzerland has discussed the matter with BNetzA and RTR.

The discussion has led to a solution, in which we consider Switzerland as an “island”, where calls from Swiss customers to other Swiss customers are routed only within Switzerland. Hence, there are (almost) never calls with legitimate Swiss Caller IDs incoming from abroad. Or vice versa, if incoming calls from abroad are made with a Swiss Caller ID, these Caller IDs are spoofed, unless it is an exceptional case.

This anti-spoofing model has also been introduced in other countries with great success, for example in Germany at the end of 2022. And the Swiss TSPs consider the solution to be the one with the best cost-benefit ratio and one that can be implemented quickly.

1.3 Scope

This document and the requirements and rules enclosed are valid for all Swiss TSPs.

The anti-spoofing rules and procedures specified in this document are:

1) meant as an add-on to the anti-spoofing measures already in place today.
2) are related to measures which Swiss TSPs cannot implement on their own.

Example: Using a premium number 090x as Caller ID is not allowed in Switzerland. A Swiss TSP may already block such calls today (point 1 above) and is able to implement this blocking on their own, without the co-operation with other Swiss TSPs (point 2 above).

1.4 Definitions

- **ASUT**: Association Suisse des Télécommunications
  The Swiss Telecommunications Association is in charge of gathering the TSP signature and contacts.
- **Caller ID**: The telephone number that is eventually presented to the called party.
  That information is usually taken from the SIP From header and in some cases from the PAI header.
  - In most cases the Caller ID Number and Display Name are taken from the SIP From header. Furthermore, there are also cases where the P-Asserted-Identity header (PAI) is displayed to the user, e.g. after SIP/ISUP interworking, when the From header does not contain a valid telephone number.
  - In this document, a **valid** Caller ID is a correctly formatted subscriber number that is actually assigned to a subscriber or at least to an NRH, while an **invalid** Caller ID is not assigned to an NRH or, if it can be determined, to a subscriber.
    Also see chapter 3.3.
- **Caller ID Anonymization** see chapter 3.2
- **From** header (according to SIP related RFC 3261)
  indicates the logical identity of the initiator of the call.
  In most cases the From header contains the telephone number that will pe presented to the callee as the Caller ID.
  In addition, the From header may contain a Display Name, that is also presented to the Callee.

- **Calls from abroad**: = Calls from non-Swiss TSPs
  Calls from abroad are (by definition) calls received from non-Swiss TSPs, i.e. from foreign network operators that are, by definition, non-compliant TSPs.

  It is irrelevant where the non-Swiss TSP's network functions are located (in Switzerland or abroad), nor is the caller's actual geographical location relevant.

- **IMRN**:
  The IP Multimedia Number (IMRN) is used to route the originating leg of a call from an outbound-roaming subscriber in a 2G or 3G network (VPLMN) to the home network.

- **Mobile Home Routing**:
  When Swiss subscribers use roaming abroad and make a call to a number in Switzerland, the call is marked as coming from abroad. As a result, the Swiss Caller ID of this roaming subscriber is anonymised (or the call may even be blocked), although the Caller ID would be valid for this use case.
  To prevent this false positive rating of OBR calls, the mobile TSP has the option to home route calls from outbound roamers. Home routing means the (originating leg of the) call is routed to the NRH who can validate the Caller ID. Such home routing is carried out using an IMRN. It is in the responsibility of the mobile TSP to implement home routing or not.

- **MSRN**:
  The Mobile Station Routing Number (MSRN) is used to route a call from the home network (HPLMN) to a subscriber roaming in a 2G or 3G VPLMN.

- **NH**:
  A TSP is the Number Holder (NH) of a number if either the TSP is the NRH and the Number is non-ported or if the number is in-ported to this TSP.

- **Non-compliant TSP**:
  A non-Swiss TSP is, by definition, a non-compliant TSP.

  Furthermore, a Swiss TSP (as defined above) that fails or refuses to comply with the agreements and requirements described and defined in this document is also a non-compliant TSP. Calls from such a non-compliant Swiss TSP are handled equally to calls from abroad.

- **NRH**:
  A TSP is the Number Range Holder (NRH) of a number if the number lies within the number range assigned to this TSP by OFCOM Switzerland.

- **PAI header** (P-Asserted-Identity header according to SIP related RFC 3325)
  to pass a Caller ID that is (should be) asserted by the caller's network operator.

- **Privacy header** (according to SIP related RFC 3325 and RFC 3323)
  to pass information about the caller's request whether the Caller ID shall be presented or not. The model with separate Caller ID (PAI) privacy indication allows to pass the Caller ID transparently through the networks and at the same time to ensure that the Caller ID is concealed from the callee.

- **Spoofed number**:
  A number is considered to be spoofed if the caller does not have the right to use that number or this right to use cannot be verified.

  Consequently, a subscriber can only claim their right of use for their number if they use a line provided by a Swiss TSP.

- **Spoofing protection measure**:
  An action like deleting a presumably spoofed Caller ID or blocking/intercepting a call with a spoofed Caller ID. For more information see chapter 1.1.2.

- **Swiss TSP**: A TSP registered with OFCOM and holding a license to provide telecommunications services in Switzerland.

  A Swiss TSP is presumed to comply with the agreements and requirements described and defined in this document.
  In this document, a Swiss TSP that does not fulfil these requirements is referred to as a non-compliant TSP.

- **TSP-ID**
  The TSP ID value is an identification number assigned by OFCOM Switzerland to each TSP. For the TSP IDs, please refer to the corresponding web page:

  www.uvek.egov.swiss => Telecom services => Service provider => Search for a TSP => Start Service

- **Teldas**: Company in charge of Operator Number Portability (ONP) and Individual Number Allocation (INA).

This section only contains abbreviations that are closely related to this document and are necessary for understanding the content. For a complete list, including common acronyms, see chapter 4.

1.5 Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [2] and indicate requirement levels for compliant SIP implementations.

1.6 References

[1] SR 784.10, Fernmeldegesetz (FMG) / Telecommunications Act (TCA)

[2] SR 784.101.1, Verordnung über Fernmeldedienste (FDV) / Ordinance on Telecommunication Services (OTS)

[3] SR 784.101.113/1.7, Identifikation des anrufenden Anschlusses / Calling-line identification

2. SOLUTION TO MITIGATE THE SPOOFING ISSUE

2.1 Idea and Challenge

All calls with a Swiss Caller ID originating from abroad are considered spoofed calls.

The challenges this involves are:

- Detecting when a call is incoming from abroad
- Recognizing exceptions, i.e. the legitimate use of a Mobile Swiss Caller ID roaming abroad. See chapter 3.4.
- Executing the “spoofing protection measure”.

2.1.1 Recognizing and marking of calls incoming from an untrusted network

Because in many cases, calls are routed by the international carrier not to the actual terminating TSP's network but to another TSP's transit network, the terminating TSP does not know whether the call in question was originated abroad or within Switzerland. Rather, the TSP sees the Swiss Caller ID and concludes that the call must have been originated in Switzerland.

To overcome this issue, the Swiss TSP receiving the call from abroad must mark the call so that this call can be recognised as a call originating from abroad later by any other transit Swiss TSP or terminating Swiss TSP.

All calls containing a Swiss Caller ID in the From header or the P-Asserted-Identity header must be marked. If this marking is (technically) not feasible the TSP shall anonymize the calls instead as described in the example of chapter 2.2.3.

As an option, any calls from abroad may be marked regardless of whether the Caller ID is Swiss or foreign.

2.2 Examples

In this chapter the agreed approach is explained with the help of several examples.

The actual rules are defined in chapter 3, Solution Rules.

2.2.1 Example 1: Call from abroad incoming from a (non-Swiss) carrier to a Swiss TSP terminating network (this TSP is able to mark the calls with the P-CH-Origin header).

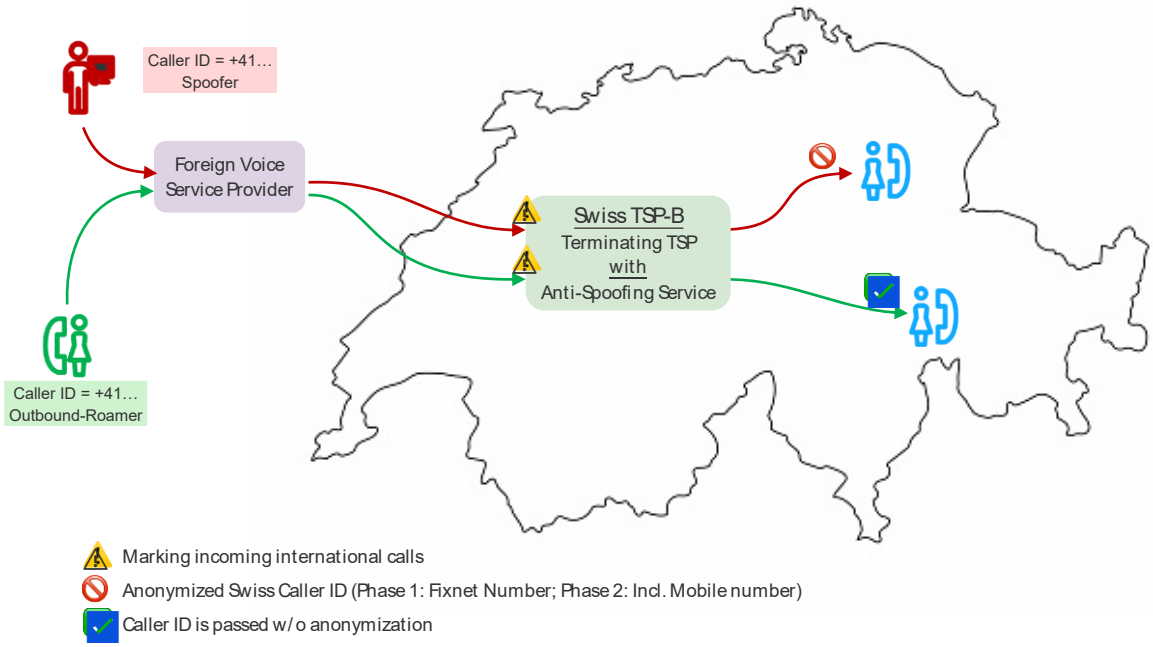

Figure 2-1: Call from abroad incoming from (non-Swiss) carrier to a Swiss TSP terminating B network

- Incoming call from abroad to Swiss TSP-B
- The terminating TSP-B must* mark the call as call from abroad (add P-CH-Origin header)
  - TSP-B can do this generally for all incoming calls from abroad (preferred option) or only if the Caller ID is a Swiss number.

    * *If the call remains within the TSPs network, it is optional to add the header.*
- The terminating TSP-B must check the P-CH-Origin header and, if present, evaluate the Caller ID:
  if it is a Swiss Number the terminating TSP-B must execute a “spoofing protection measure”.
- The terminating TSP-B may run further anti-spoofing checks and counter measures before terminating the call towards the callee (as today): e.g. check if the Caller ID contains an invalid or prohibited value.

2.2.2 Example 2: Call from abroad incoming from a (non-Swiss) carrier to a Swiss terminating TSP-B network via a Swiss transit TSP (regular case; TSP has capability to add the P-CH-Origin header)

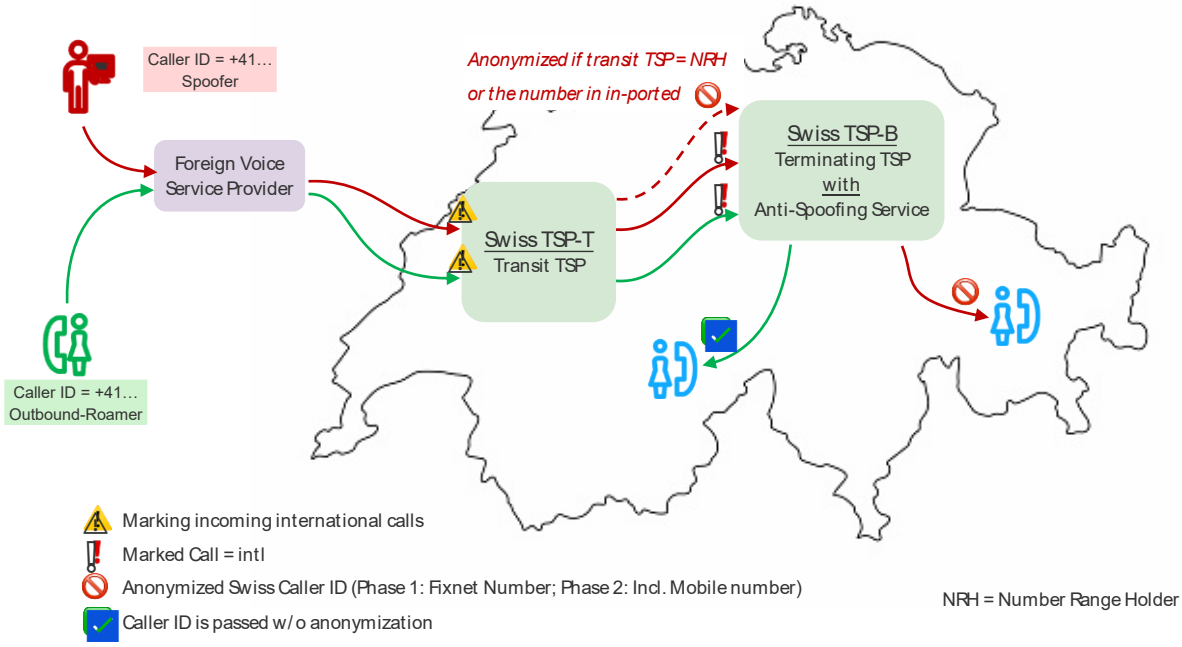

Figure 2-2: Call from abroad incoming from international carrier via Swiss transit TSP to Swiss terminating TSP-B (regular case)

- Incoming call from abroad to Swiss transit TSP-T
- The TSP-T must mark* the call as coming from abroad (add P-CH-Origin header)
  - TSP-T can do this generally for all incoming calls from abroad (preferred option) or only if the Caller ID is a Swiss number.

    *or exceptionally anonymize the Caller ID as described in chapter 2.2.3.
- TSP-T may apply its “spoofing protection measure” if TSP-T is the NH of the Caller ID.
- TSP-T shall route the call towards the terminating network of TSP-B.
- The terminating TSP-B must check the P-CH-Origin header and, if present, evaluate the Caller ID:
  if it is a Swiss Number the terminating TSP-B must execute a “spoofing protection measure”.
- The terminating TSP-B may run further anti-spoofing checks and counter measures before terminating the call towards the callee (as today): e.g. check if the Caller ID contains an invalid or prohibited value.

2.2.3 Example 3: Call from abroad incoming from a (non-Swiss) carrier to a Swiss terminating TSP-B network via a Swiss transit TSP-T: TSP-T cannot set the P-CH-Origin header

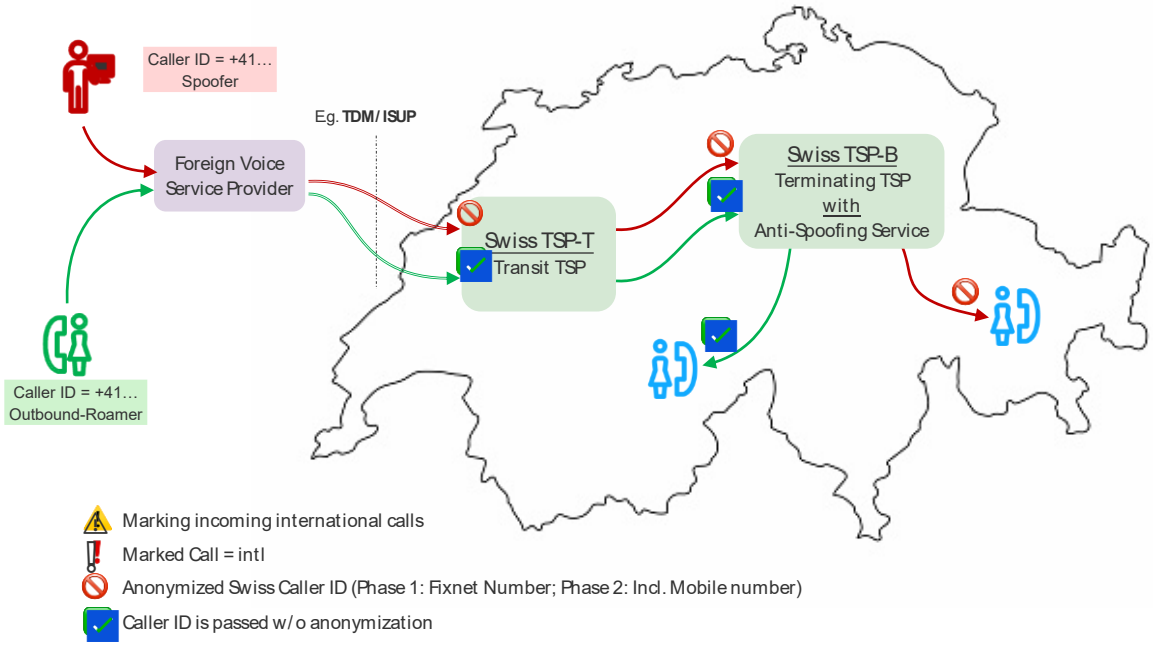

Figure 2-3: Call from abroad incoming from int'l carrier to Swiss TSP-B network via TSP-T that cannot set the P-CH-Origin header

- Incoming call from abroad to Swiss transit TSP-T
- If a TSP-T is technically not able* to mark the call with the P-CH-Origin header (because the call is incoming via circuit-switched trunks), this TSP-T shall check the Caller ID and the Called Party Number:
  - If the Called Party Number contains a Swiss TSP's IMRN or MSRN, the Caller ID shall be ignored and passed transparently. See chapter 3.4.1.

    The mobile TSPs inform the TSP-T of the IMRN/MSRN number ranges in use and such TSP-T is obliged to whitelist (called party number) the IMRN/MSRN range of mobile TSP.

  Else, if the Called Party Number does not contain an IMRN/MSRN:

  - If the Caller ID is a Swiss Number (i.e. starting with "+41") the TSP-T must execute a "spoofing protection measure".

  * This exception only applies to ISUP signalled connections. To anonymize the Caller ID means to set the "Address presentation restricted indicator" to '01' (presentation restricted) in the "Calling Party Number" and (if present) in the Additional Number delivered in the Generic Number field.

- The TSP-T shall route the call towards the terminating network of TSP-B directly or via another national transit TSP.

Note: In this case the P-CH-Origin header will not be present.

3. SOLUTION RULES

While the previous chapters are mainly informative, the rules are formally defined here.

The goal of this chapter is to establish rules that are defined in such a way that the ‘system’ works when these rules are followed.

3.1 Marking incoming calls from abroad

The information “call is originating from abroad” is an important criterion to determine whether a Caller ID shall be considered spoofed.

First, it must be clearly defined what we consider as call from abroad. This is defined above in chapter 1.4 Definitions.

Hence, it is agreed on a common understanding about marking criteria and how we mark the calls.

3.1.1 Marking criteria

A Swiss TSP shall mark calls with Swiss Caller ID or generally mark incoming calls from abroad as described above in chapter 2.1.1.

In case a Swiss TSP maintains circuit-switched (ISUP) equipment, it is not possible to add SIP headers. In this case the Swiss TSP must anonymize Swiss Caller IDs of such calls as described in chapter 2.2.3 above and defined in chapter 3.2 below.

3.1.2 Marker to indicate the origin of the call from abroad

Marking of calls matching criteria mentioned in the chapter above shall be performed by adding the SIP header as described in chapter 1.1.

3.1.3 Transparent forwarding of the P-CH-Origin header only between Swiss TSPs

The P-CH-Origin header must be passed transparently between compliant Swiss TSPs.

P-CH-Origin header shall be deleted at the UNI towards customers and at the NNI towards non-compliant Swiss TSPs.

3.2 Anonymizing Caller IDs

One of the “spoofing protection measures” outlined in chapter 1.1.2 is to anonymize the Caller ID.

To anonymize a Caller ID means:

- Delete the URI user and host part of the From header and to replace it by an appropriate value, e.g. sip:unavailable@unknown.invalid (recommended) or sip:anonymous@anonymous.invalid.

AND

- Replace the content of the From header’s "display name" by “anonymous”, “unavailable” or delete it.

AND

- Set the Privacy header with the value "id" (if not already present): Privacy: id

A terminating Swiss TSP must anonymize a Caller ID if

- a call is delivered to the customer (UNI)

AND

- a call is marked as call from abroad (i.e. the P-CH-Origin header is present)

AND

- the Caller ID is a valid Swiss telephone number or an invalid telephone number.

A transiting Swiss TSP that is the NH of a Caller ID can act like a terminating TSP and perform the “spoofing protection measure”.

3.3 Blocking calls due to a spoofed Caller ID

One of the “spoofing protection measures” outlined in chapter 1.1.2 is to block the call.

A call may be blocked by rejecting it with an appropriate response code (e.g. 606…608) or by intercepting it and playing an announcement.

Forwarding such calls to an announcement or even to a “honey pot” seems to be a more effective measure, since most calls with spoofed Caller IDs are made intentionally. The spoofing attacker has to spend more time (and money) on incoming calls than if they were to receive the “convenient” response code.

A transiting Swiss TSP that is the NH of a Caller ID can act like a terminating TSP and perform the “spoofing protection measure”.

3.4 Recognizing exceptions

There may be exceptions, where using a Swiss Caller ID when calling from abroad is legitimate. Furthermore, there are cases that lie in a grey area.

Most frequent legitimate case that can be solved with mobile home routing:

- Swiss 2G/3G outbound roamer calling a Swiss destination.

A less common legitimate use case that cannot be recognized as an exception is:

- A Swiss subscriber calls a subscriber abroad who has set up call forwarding or call transfer to a Swiss destination number.

Further use cases that are defined as illegitimate use cases:

- Usage of foreign telephony service allowing to send a Swiss Caller ID (even if there was some validation between the subscriber and the foreign service provider).

- Operating a call center using Swiss Caller IDs with a foreign operator.

3.4.1 Use case mobile Outbound Roaming: informal

Swiss mobile subscribers outbound roaming in a 2G/3G network, calling a Swiss destination

4G (and later generations) outbound roamers will not face this issue, because in their case home routing applies natively (S8HR). I.e. the caller origin from a telephony point of view will be the mobile operator in Switzerland and not the roaming operator abroad.

For 2G/3G, the simplest solution to handle this use case is home routing, too. Home routing in this case would be done with a special number, the so called IMRN (IMS Routing Number). The IMRN number range is defined per mobile TSP.

Calls addressed to an IMRN mean the originating leg of a call and are always routed to the TSP that is the NRH of the subscriber owning the caller ID. Because of that and because the IMRN is signalled from the home network to the visited network via alternative signalling path (SS7) the NRH (= mobile home network) can distinguish between legitimate from illegitimate cases.

4. LIST OF ACRONYMS

2G	2nd Generation Mobile Network
3G	3rd Generation Mobile Network
4G	4th Generation Mobile Network
BCP	Best Current Practises by IETF
BNetzA	Bundesnetzagentur (Germany)
CLI	Calling Line Identity
DETEC	Federal Department of Environment, Transport, Energy and Communications (German: UVEK)
FDV	Fernmeldedienstverordnung in German
FMG	Fernmeldegesetz in German => TCA
HPLMN	Home Public Land Mobile Network
I-SBC	Interconnect Session Border Controller (placed at NNI)
ID	Identity
IETF	Internet Engineering Task Force
IMRN	IP Multimedia Routing Number
IMS	IP Multimedia System
INA	Individual Number Allocation
NNI	Network to Network Interface, i.e. SIP trunk interfaces between TSPs
NH	Number Holder (see chapter 1.4, Definitions)
NRH	Number Range Holder (in the sense as used by Teldas/OFCOM)
OBR	Outbound Roaming / Outbound Roamer
OFCOM	Federal Office of Communications
ONP	Operator Number Portability
PAI	P-Asserted-Identity header
RFC	Request for Comment Standard by IETF
RTR	Rundfunk und Telekom Regulierungs-GmbH (Austria)
S8HR	S8 Home Routing
SIP	Session Initiation Protocol by IETF
UVEK	Eidgenössisches Department für Umwelt, Verkehr, Energie und Telekommunikation (English: DETEC)
TCA	Telecommunication Act
TSP	Telecommunications Service Provider
UNI	User to Network Interface, i.e. the interface to the customers
URI	Uniform Resource Identifier
VPLMN	Visited Public Land Mobile Network