Bern, October 2025

Swiss TSP Anti-Spoofing Agreement
Technical Specification (Version 1.2)

Within the framework of an industry «Anti-Spoofing Working Group», multiple Swiss Telecommunication Service Providers (TSPs) have reached a consensus about the present specifications as a proactive measure to fight the issue of spoofing calls originating from abroad.

This initiative is an important move to protect Swiss telecommunications networks and the consumers against the growing problem of Spoofing, where callers hide their identity by using fake phone numbers. Such calls often aim to defraud individuals or organizations, posing not only significant security threats but also economic risks.

The specifications outlined by the Working Group represent a comprehensive and collaborative effort to standardize processes across the industry, ensuring all parties involved adhere to best practices for managing calls effectively. The key element of the solution is the marking of calls originating from abroad to enhance Swiss TSPs ability to intercept and manage potentially malicious calls before they reach consumers. Whether to anonymize such marked calls or not is not part of these specifications as this will remain in the responsibility of each terminating Swiss TSP.

Several TSPs of the «Anti-Spoofing Working Group» are member of the Swiss Telecommunication Association (asut). Therefore asut was asked to coordinate the publication of the specifications. To this end, asut formally requested an assessement from the Swiss Federal Office of Communications (OFCOM) whether these specifications meet the requirements outlined in Art. 26a of the Ordinance on Telecommunications Services. OFCOM not only confirmed the appropriateness and admissibility of the specifications but – recognizing its importance – decided to refer in its regulatory framework (TAV) starting 1st January 2026 to these Anti-Spoofing Specifications.

Future efforts of the Working Group may include ongoing assessments of the effectiveness of these measures, updates to technical standards, and further collaboration to expand Anti-Spoofing strategies in Switzerland.

asut
Schweizerischer Verband der Telekommunikation
Hirschengraben 8
3011 Bern

+41 (0)31 560 66 66
info@asut.ch
www.asut.ch

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	01.04.2025
Replaces Version	1.1
Version Number	1.2
Last changes	01.04.2025
Status	Final
Comes into force on	According to the “Anti-Spoofing" Agreement”

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	Updated acc. to Feedback from Sunrise, Verizon and Swisscom
1.2	01.04.2025	Updated acc. to Feedback from Verizon (editorial changes)

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 that the use of upper and lower case in the header name ‘P-CH-Origin’ is easier for human readers and therefore a camel-back notation has become established for these names. However, acc. to RFC 3261, chapter 7.3.1 when comparing header fields, field names are always case-insensitive.

I.e. **P-CH-Origin** is equivalent to e.g. **P-Ch-Origin** is equivalent to e.g. **p-ch-origin**

Anti-Spoofing processing provides recognition of spoofed Caller IDs and anonymizing of the spoofed Caller ID (considered as the normal case here) or even blocking of calls with a spoofed Caller ID (e.g. invalid number).

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.

Therefore, the Anti-Spoofing measures are implemented in phases.

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

1.1.2 Phased Implementation

The first step that can be done immediately, is to mark* calls from abroad. This step only allows to anonymize calls. For the marking of calls the only criteria is “call is incoming from abroad”.

* *The requirements for how and when calls are to be marked are described in chapter 2.1.1 and chapter 3.1.1.*

Phase 1: Considering Swiss numbers except mobile numbers

Regarding the anonymizing of spoofed numbers, mobile numbers may not be anonymized (or blocked) in Phase 1 – except by the number range holder.

Reason: when mobile outbound roamers call Switzerland from abroad, Swiss Caller IDs are legitimately displayed.

Phase 2: Considering all Swiss numbers, incl. mobile numbers

It is also planned to anonymize mobile phone numbers as soon as we are able to reliably distinguish spoofed cases from 2G/3G outbound roaming cases or if the number of such calls will not be significant anymore. This document refers to this as Phase 2.

The steps required and the roadmap for achieving Phase 2 have yet to be discussed and developed.

1.2 Motivation

1.2.1 Today’s situation

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.

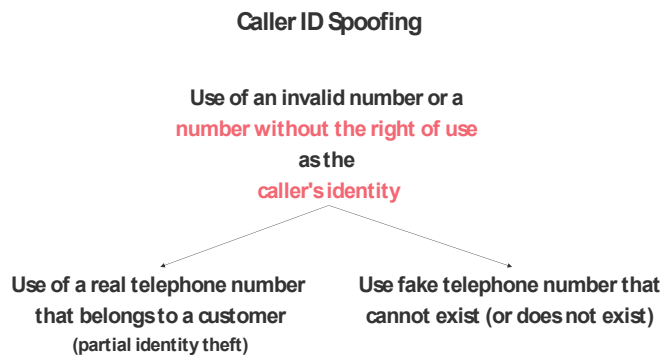

Figure 1-1: Definitions of spoofed number used in this document

Some Swiss TSPs implemented solutions to minimize spoofing cases. But regarding spoofed Caller IDs there is little information to detect 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, apart from some exceptions, 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, Recognizing exceptions.

If a TSP recognised a spoofed number out of his own range, the TSP has the right and the obligation to block the call or to anonymize the Caller ID for this call.

To block a call, there must be a 100% certainty that the Caller ID is spoofed. Every exception must be ruled out. To exclude (almost all) exceptions, the TSP must make a major effort and there still is some residual risk.

Therefore, TSPs are encouraged to opt for the weaker form of defence: “Anonymization of the Caller ID”.

Another verification that a TSP can perform is to check whether a Caller ID is completely invalid, e.g. from a number block not assigned to a TSP.

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 will happen even without big investigation in number ranges, but just as an evolution of trial and error with different numbers towards the TSPs.

1.2.2 Proposed solution

The TSPs have discussed, how anti-spoofing mechanisms can be improved. 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.

Beside the exceptions, where Swiss Caller IDs incoming from abroad, are legitimate use cases, to recognise whether a call is coming from abroad was identified as a challenge.

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 3.1.3.
- **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 abroad are primarily calls from non-Swiss TSPs, i.e. from foreign network operators that are, by definition, non-compliant TSPs.

  In this document, calls from non-compliant TSPs are also referred to as calls from abroad, since the required treatment is the same.

Calls from abroad shall be marked by a Swiss TSP in accordance with the rules and descriptions below.

- **NH**:
  A TSP is the Number Holder (NH) of a number if it is non-ported and if it lies within the number range assigned to this TSP or if the number is in-ported to this TSP.

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

- **PAI 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.

- **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 the DETEC (UVEK) to each TSP (also known as TSP). For the TSP IDs please refer to the corresponding UVEK web page:

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

- **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.

- **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) / Decree concerning Telecommunication Services

[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 imposes are:

- Recognizing, if a call is incoming from abroad
- Recognize the exceptions, i.e. legitimate use of a Swiss Caller ID from abroad.
- Anonymizing the Caller ID accordingly

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, if the call in question was originated from abroad or from 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).

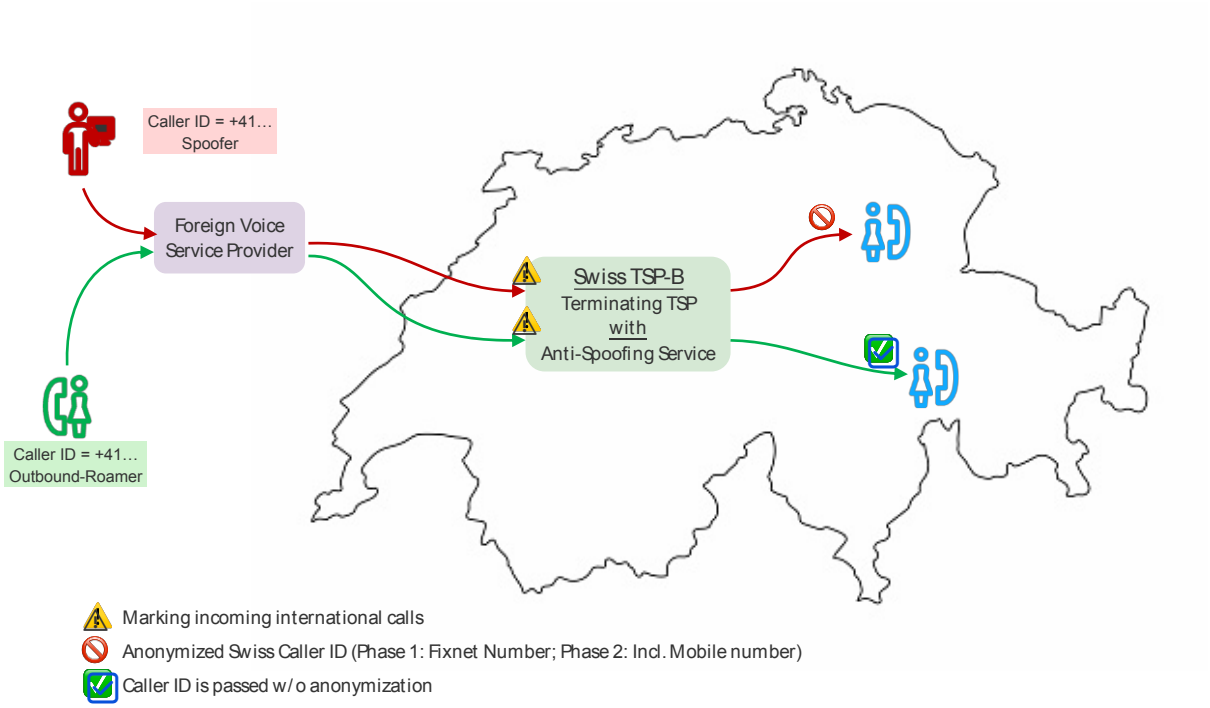

Figure 2-1: Call from abroad incoming from (non-Swiss) carrier to a Swiss TSP terminating B network

- 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 valid Swiss Fixnet Number the terminating TSP-B must anonymize the Caller ID.
  - an invalid number the terminating TSP-B must anonymize the Caller ID or may even block the call.
  - a valid Swiss Mobile Number the terminating TSP-B must pass the mobile Caller ID (for phase 1) unless the terminating TSP-B is the NH and has further information to detect a case of spoofing.
- 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)

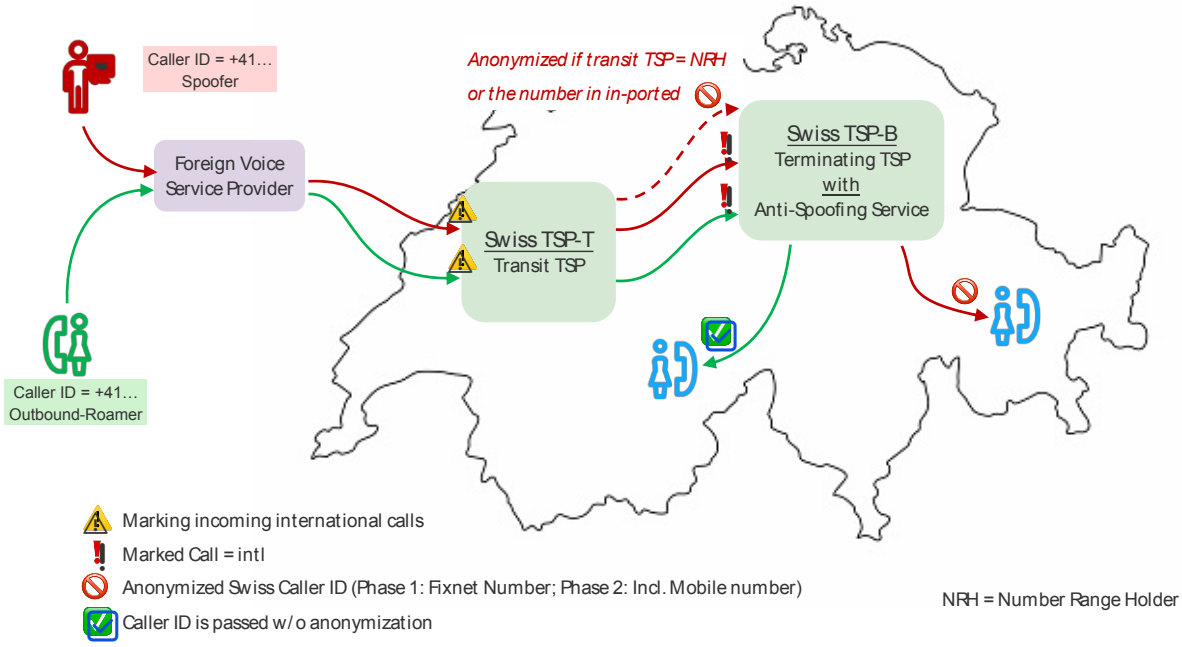

Figure 2-2: Call from abroad incoming from international carrier via Swiss transit TSP to Swiss terminating TSP-B (regular case)

- 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 anti-spoofing rules 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, must check the Caller ID and
- The terminating TSP-B must check the P-CH-Origin header and, if present, evaluate the Caller ID and proceed as described in chapter 2.2.1. above (from the third bullet point).

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

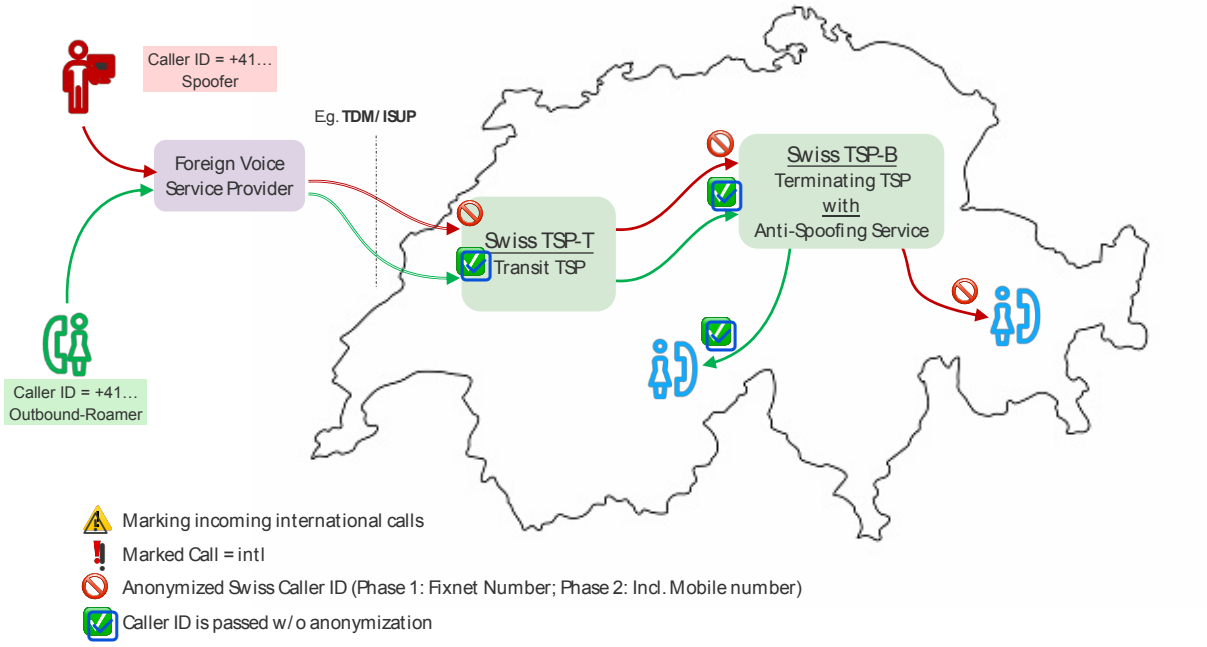

Figure 2-3: Call from abroad incoming from int'l carrier to Swiss TSP-B network via TSP-T that cannot set the P-CH-Origin header

- 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 – that might be if the call is incoming via circuit-switched trunks, this TSP-T shall check the Caller ID: if it is
  - a valid Swiss Fixnet Number the TSP-T must anonymize the Caller ID.
  - an invalid number the TSP-T must anonymize the Caller ID or may even block the call.
  - a valid Swiss Mobile Number, it must pass the mobile Caller ID (for phase 1)
- 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 it is not possible for a Swiss TSP to mark the calls from abroad, this 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.

Remark: a reason being not able to mark calls from abroad as required might be, that the call ingress is circuit-switched based.

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

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

If Caller ID spoofing is detected, the Swiss TSP may block the call or pass the call with an anonymized Caller ID.

The anti-spoofing measures described in this document do not guarantee a 100% reliability. It may happen that a Caller ID is incorrectly identified as spoofing. If the main indicator for detecting spoofing is the P-CH-Origin header, the resulting action should therefore be to anonymize the Caller ID rather than to block the call.

To anonymize a Swiss 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. P-CH-Origin header is present)

  AND

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

In case the Caller ID is a valid Swiss Mobile telephone number, it shall neither be anonymized nor blocked.

A transit or terminating Swiss TSP that is the NH of a Caller ID can also anonymise this Caller ID in other cases and on the basis of other criteria than those listed above.

3.3 Blocking calls due to a spoofed Caller ID

The normal measure to treat calls with a spoofed Swiss Caller ID (suspicion) is to anonymize the Caller ID as described in the previous chapter.

However, a stricter measure is to block such calls. When they block a call, however, they should be sure that the Caller ID is spoofed, as is the case with an invalid Caller ID.

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.
- Special case: Number is not allowed to be used as Caller ID: e.g. +41900…

Blocking such calls seems appropriate and might be responded with a 60x response.

However, 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 spoofer must invest more time (and money) for answered calls.

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 often legitimate case:

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

Less common legitimate use case:

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

Further use cases – unclear if legitimate or not – are:

- Usage of foreign telephony service (like Skype) allowing to send a validated Swiss Caller ID.

- Operating a call center from abroad using Swiss Caller IDs.

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

4G (and later generations) outbound roamers we 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 (i.e. an IMRN) of a pre-defined number range, i.e. with a well-known number. Calls from abroad routed to an IMRN will contain a legitimate Swiss Caller ID and this case can be easily recognized by the IMRN. This kind of home routing is not yet introduced by all Swiss mobile TSPs, and its introduction requires some significant efforts. Due to home routing being the standard for 4G and 4G steadily replacing 2G/3G, the agreed scenario is:

Phase 1 – exclude mobile Caller ID from anonymization:

- Allow Swiss Caller IDs for calls from abroad containing mobile numbers (Caller ID whitelist) from the mobile number ranges +4175*, +4176*, +4177*, +4178*, and +4179* as well as the new IoT number ranges +4168*, +4169*, +4172* and +4173*.

- Let's make time work for us. As 4G network coverage increases and 2G/3G usage decreases (including abroad), we will reach the point where an exception for mobile Caller ID is less relevant.

Phase 2 considerations:

In phase 2, when also the anonymization of mobile Caller ID is allowed or required, still some roles should be considered.

- Allow exceptions by check of the called address => called address whitelist containing IMRN.
  With this measure home-routing cases may be easily and reliably recognized and excepted from Caller ID anonymizing.

- Allow exceptions by check of the Caller ID=> Caller ID whitelist containing special mobile number ranges, e.g. used by M2M/IoT devices. For these devices the presentation of the Caller ID might be a significant part of the service.

Other exceptional use cases

It is very difficult to solve exceptional use cases in real time and across TSPs.

The solution the TSPs have agreed on, suggests a Swiss TSP maintains whitelists (for A- and B-numbers) and for customers to be able to have their numbers entered in these lists.

The drawback of this approach is, that a customer needs to decide whether the Caller ID is protected against spoofing or not.

4. LIST OF ACRONYMS

2G	2nd Generation Mobile Network
3G	3rd Generation Mobile Network
4G	4th Generation Mobile Network
A-SBC	Access Session Border Controller (placed at UNI)
BCP	Best Current Practises by IETF
CLI	Calling Line Identity
DETEC	Federal Department of Environment, Transport, Energy and Communications (German: UVEK)
FDV	Fernmeldedienstverordnung in German
FMG	Fernmeldegesetz in German => TCA
I-SBC	Interconnect Session Border Controller (placed at NNI)
ID	Identity
IETF	Internet Engineering Task Force
IMRN	IP Multimedia Routing Number
INA	Individual Number Allocation
IoT	Internet of Things
NNI	Network to Network Interface, i.e. SIP trunk interfaces between TSPs
M2M	Machine-to-Machine
NH	Number Holder (see chapter 1.4, Definitions)
NRH	Number Range Holder (in the sense as used by Teldas/OFCOM)
OFCOM	Federal Office of Communications
ONP	Operator Number Portability
PAI	P-Asserted-Identity header
RECIP	Recipient (of a ported number)
RFC	Request for Comment Standard by IETF
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