

**Diretoria de Tecnologias e Plataformas de Serviços**

Gerência de Estratégia de Tecnologia e Integração de Serviços

Recomendação Técnica de Tecnologia

RTT N°: 007-2021

Version: 1.0

Date: 09/27/2021

Estado(s): Todas UFs

Title: Technical Requirements for Call Spoofing Prevention in Oi Fixed Network

Projeto de Investimento: N/A

Área de Negócio: N/A

Posição IM: N/A

Valor Orçado: N/A

Meta de Ativação: -

Impacto da Não Implantação:

Author:
Laércio SerikavaTel.:
+55 21 98766-8124E-mail:
laercio.serikava@oi.net.br**Distribution List**

- Ger. Planej./Proj. Comutação e NGN
- Ger. Atacado/Roaming Internacional
- Gerência de Regulamentação

Approved by:

Mauro Fukuda



Alberto Boaventura



Call Spoofing Prevention in Fixed Network

Document Title:
Technical Requirements

Author:
Laércio Takeshi Serikava

Reviewed by:

Version:
1.0

Confidential

Change History			
Revision	Date	Author	Revision Description
1.0	09/24/2021	Laercio Serikava	Initial version



1 INTRODUCTION

1.1 Document Purpose and Scope

This Technical Requirements Specification document provides the technical requirements implemented in the fixed voice network towards the prevention of fraud and call spoofing. The intent of this document is to make aware to the Oi's interconnecting Carriers and partners that the company is engaged to mitigate illegal robocalling and call spoofing from its subscribers and it has been implemented structure for Calling Line Identification Validation service in the current TDM based voice network as well as in the SIP/VoIP technology. Such best practices have already been adopted pretty earlier to the creation of STIR/SHAKEN framework.

1.2 Overview

Telecommunications fraud is on the rise and costing operators a huge amount of money each year. Statistics show that the occurrence of wireless and wireline fraud has not only increased, but the value of those losses has increased as well. Operators are vulnerable to fraud attacks on many fronts. As new technologies are introduced into the network, they are finding it increasingly difficult to proactively protect their bottom line using traditional fraud detection tools.

As networks begin their evolution to IP-based technologies, fraud will continue to increase. Voice over IP (VoIP) technology introduces an entirely new set of problems, and most fraud systems are not IP-enabled. Likewise, wireless technologies such as 3G and 4G raise the same concerns. Operators need visibility to these networks without the expense and resource allocation of traditional fraud management systems.

Combating fraudsters, who are proving to be extremely innovative and technically astute, requires preventive solutions rather than reactive measures that are implemented after largescale incidents have occurred. Fraud erodes margins, consumes network capacity, increases network errors and jeopardizes customer relationships. Operators simply cannot afford to write off these losses and allow fraud to erode their bottom line.

2 FRAUD PREVENTION TECHNIQUES IN THE FIXED NETWORK

Majority of fraud occurrence in the fixed voice network comes from interconnection routes and PBX connections where subscriber intends to spoof the identity by using fake caller ID information to mask the true source in order to make such call not chargeable due to the discrepancy in the call detailed record [CDR].

2.1 Screening the Threats

Oi network which currently comprises the former Telemar and Brasil Telecom network operators has deployed SS7 signaling network back 2002 by deploying INFusion STP from Alcatel to support 25 million fixed voice subscribers, those STPs were capable to perform call screening service to detect and prevent fraud as well as block unwanted traffic through Call Type Blocking service. As the Call Screening Service does not require any trigger from the TDM switch, it is also called Triggerless Screening Services, quite different form de usual solution based on Intelligent Network [IN] with INAP protocol and specialized SSP switches to trigger the service.

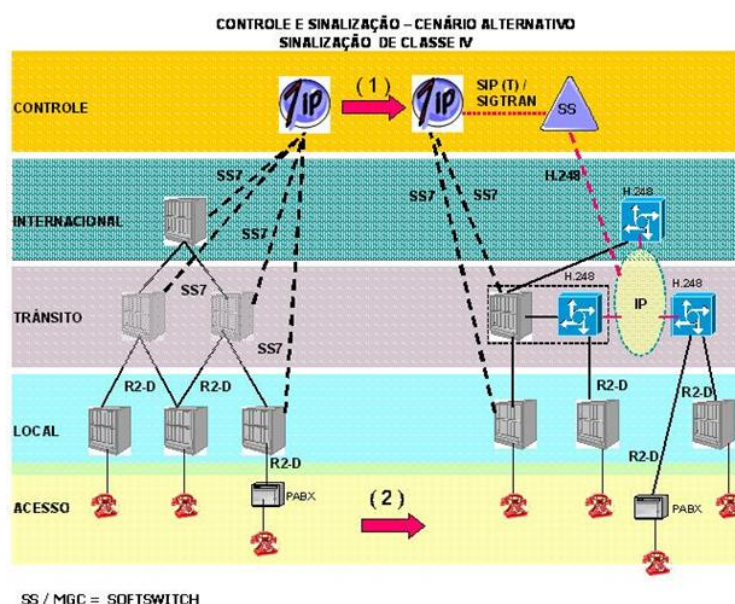


Figure 1 – SS7 Signaling Network

Few years later Oi has enhanced the signaling network with deployment of new STPs generation which added capability of generating accurate CDRs in real time based on the call related signaling MSUs, where every single raw SS7 message is correlated to build a CDR related to a calling session, additionally enriched features such Calling Line Identity Validation for Payphones and PBX subscribers, INAP/CAMEL trigger manipulations for prepaid subscribers and eventually Local Number Portability. Those STPs have been provided by Tekelec (EAGLE5) and Tropico [Vectura Signaling Server aka "7IP"].

Such STP technology enabled the implementation of call screening service based on deep analysis of ISUP messages used during call setup.

Call Screening Services provides Oi the ability to screen calls based on a variety of options:

- Detect fraud by blocking calls by fraudulent subscribers or applying Caller ID enforcement.
- Block traffic originating/terminating by/to an unfriendly network
- Prevent unwanted / unsolicited call traffic

- Manage Delinquent Accounts by blocking calls originated by / terminating to delinquent or suspect accounts
- Flexible Screening Management:
 - Group Screening: Block calls to certain destinations. [e.g. block all calls to a particular country].
 - Specific Screening: Control calls based on a combination of Calling / Called subscriber.

Call Screening Service compares various parameters of the call setup messages (ISUP IAM/TUP IA) with provisioned values to allow or release the call and eventually change some parameter of the message [CgPN or CdPN].

2.1.1 Fraud Prevention in PBX Connection in TDM Network

Oi has implemented Calling Line Identification Validation feature in the SS7 network to validate the identity of its PBX subscribers. This feature checks the subscriber calling party identity within ISUP message during the call setup phase, in case of identity violation the application changes the Calling Party ID originally informed by the PBX to the actual assigned one based on the provisioned entry in the DB. Thus, the called party will get the proper Calling Party number and the CDR will keep the enforced caller ID since it is build based on all correlated SS7 messages.

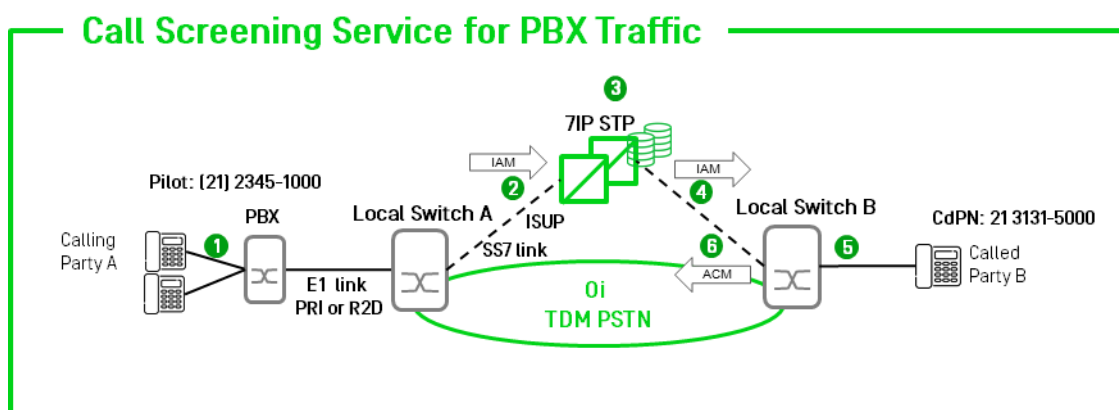


Figure 2 – Calling Line Identification Validation (CLIV) in SS7 Network

Figure 2 shows the Screening Services & CLIV permitting the call in the network.

1. PBX subscriber places an outgoing call to [21] 3131-5000
2. At call setup, Switch A sends an IAM to STP for routing to next node, in that IAM it is added Digit String correspondent to a specific PBX identification related to the PBX-CLIV application.
3. STP screens the call and performs the validation of caller ID based on the digit string and also decides if the call is allowed according to the destination. If the CgPN matches the DB entry [Pilot #], then goes to the next step, otherwise CLIV enforces the CgPN according to the DB Entry.
4. STP routes the IAM to the next node [Switch B] based on DPC.
5. Terminating node receives IAM, recognizes DPC as its own, examines the CdPN and proceeds the termination to called party.
6. Terminating node sends ACM back to originating switch.

Oi has customers using PBX type connection with active dialers for campaigns who generates massive traffic. Those dialers have assigned numbering plan that are checked and eventually the caller ID is enforced with the assigned ones during call setup in order to prevent call spoofing originated by owned customers.

This application known internally as TAR DDR has initially been deployed to prevent revenue leakage by call ID spoof from PBX users. The acronym stands for charge individual DID extension.

2.1.2 Caller ID Validation and Enforcement Policy for IP-PBX in VoIP Network

Oi provides an IP-PBX connection to the network which is well known as SIP Trunking service. Currently this service is provided through IMS VoIP framework and prevention of call spoofing mechanism has also been implemented to mitigate spam and fraud issues. Hereunder is described the details of that implementation.

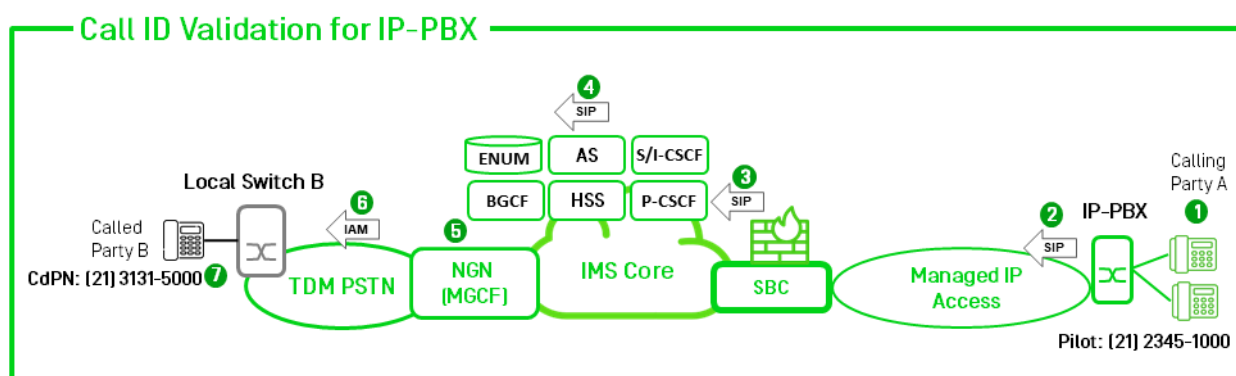


Figure 3 – Calling Line Identification Validation [CLIV] for IP-PBX in IMS VoIP Network

Figure 3 shows the CLIV for IP-PBX connected to the Oi VoIP/IMS network.

1. IP-PBX extension places an outgoing call to [21] 3131-5000.
2. At call setup, IP-PBX sends SIP message to the SBC.
3. SBC forward SIP INVITE message to the IMS P-CSCF which screens the originating call and performs the validation of caller ID based on provisioned IMS subscriber data. If the CgPN matches the DB entry [Pilot #], then goes to the next step, otherwise P-CSCF enforces the CgPN [Pilot #] in the SIP Header changing the value of P-Asserted Identity field with respective Pilot number of IP-PBX.
4. After ENUM lookup SIP Message goes to the IMS Application Server which inserts the correct Pilot Number in the "From" Header of SIP message.
5. Session is forwarded to the MGCF which sends ISUP IAM to the terminating Switch in the TDM PSTN.
6. Terminating node receives IAM, recognizes DPC as its own, examines the CdPN and proceeds the termination to called party.
7. Terminating node sends ACM back to MGCF.

Similar to the TDM network, Oi has also connected customers through SIP Trunking service, the IP-PBX type connection to the IMS network, where the originators are active dialers for

marketing campaigns. Those dialers have assigned originating numbers in the IMS network that are checked and validated and eventually the caller ID is enforced with the assigned ones during call setup in order to prevent call spoofing originated by owned customers.

2.1.3 Strong Authentication for VoIP FTTH Subscribers

Oi delivers VoIP service to the GPON FTTH subscribers which employs the NASS Bundled Authentication according to the ETSI TISPAN TS 187003 specification. It allows the use of authentication information obtained at the Transport and Network Layers by the Service Layer.

The TISPAN Network Attachment Subsystem (NASS) maintains information about IP-connectivity access sessions. The information is stored in a Connectivity Session Location and Repository Function (CLF). The information is accessible by other subsystems such as IMS.

2.1.3.1 Authentication at Access Layer (L2 and L3)

The SIP REGISTER procedure of the UE [user equipment] to the IMS will be established after the authentication of the access to the network that takes place between the Residential Gateway (RG) and the NASS.

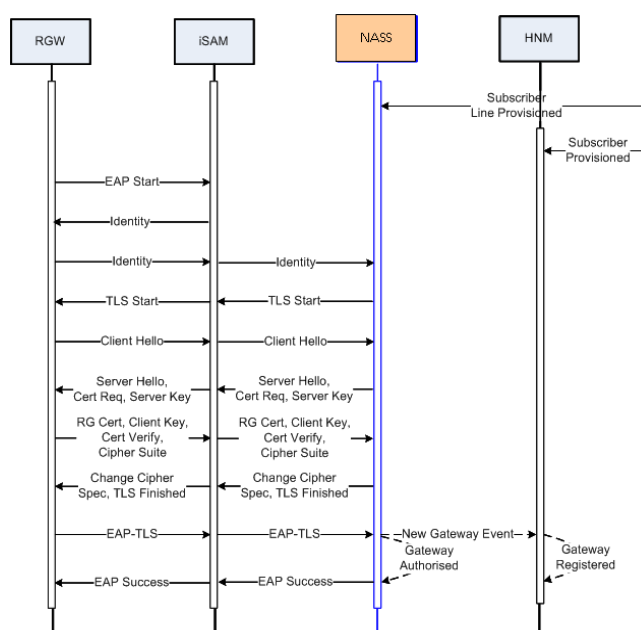


Figure 4 – Access Layer Authentication

The initial phase of UE authentication comprises the RG attachment to the access network that is performed through EAP over Ethernet [802.1X] by NACF [Network Access Configuration Function].

2.1.3.2 DHCP Network Attachment

In the next step shown in Figure 5 is achieved the DHCP Network Attachment: the subscriber identification comprised by the Line ID is inserted in the IP Address request [DHCP Op.82], the NACF allocates an IP address to the RG and configures the subscriber profile in layer 3 [in the BNG]. The NACF also retains the information about user identification Line ID [L2] and IP address [L3].

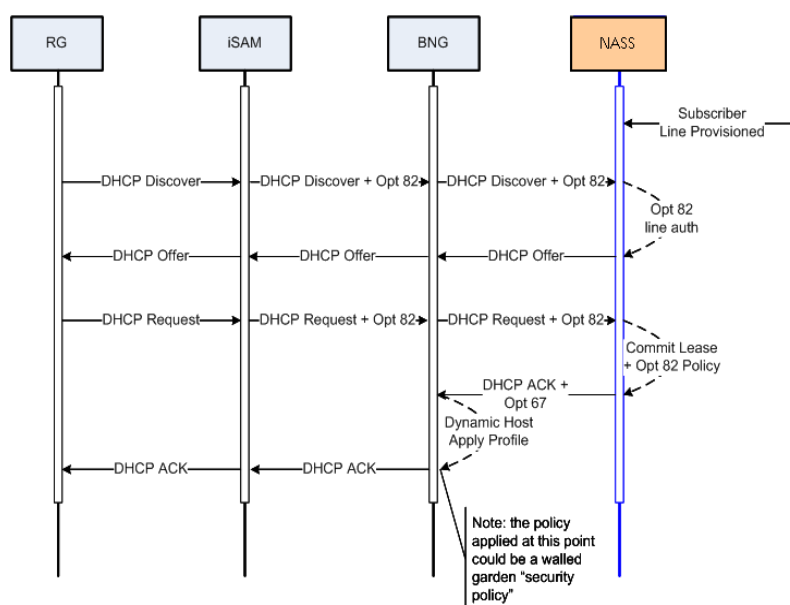


Figure 5 – DHCP Network Attachment

The final RG configuration process can be started by notifying the installer technician to the OSS Activator and the Auto Configuration Server [TR-069 platform a.k.a. Home Device Manager] will configure the its VoIP Client with the respective subscriber credentials to access IMS network. Details depicted in the Figure 6.

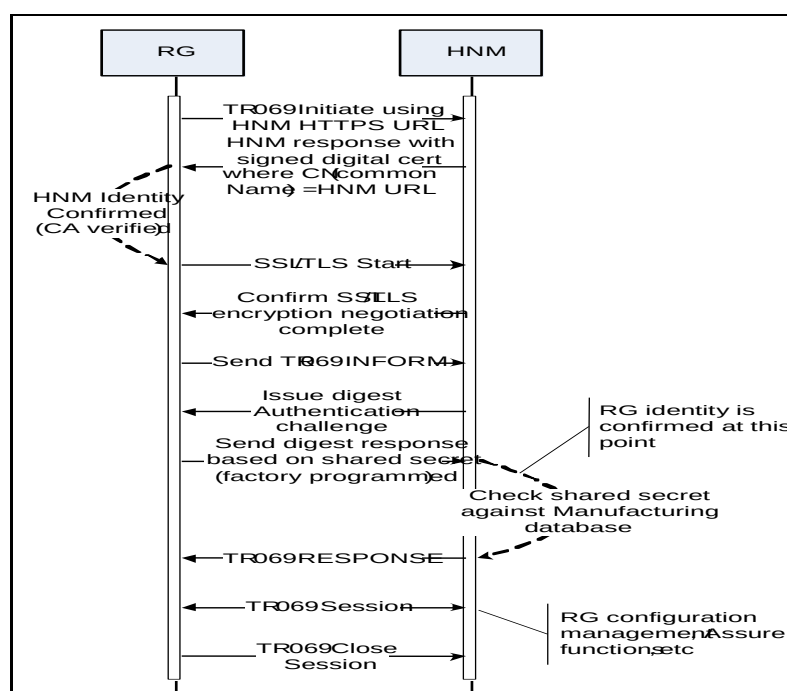


Figure 6 – VoIP Credential Load at RG

2.1.3.3 NASS Bundled Authentication

Once the SIP UE is configured in the RG, the SIP Registration process starts. The UE sends a SIP REGISTER message with IP address obtained from NACF.

The P-CSCF sends a DIAMETER UDR message to the NACF to obtain the location information [Line ID].

CLF proceeds lookup of the Line ID info with the IP address.

The CLF returns the respective Line ID to the P-CSCF via DIAMETER UDA, which inserts it in the SIP REGISTER message as PANI [P-Access Network Info].

The Figure 7 shows RG's SIP client request registration to the IMS core. As part of the registration process, the IMS core queries the NASS CLF entity to obtain the line ID used by the subscriber. This line ID is compared with line ID provisioned in HSS for that subscriber. If the line ID query matches the provisioned entry in the HSS, then IMS authorizes the user registration.

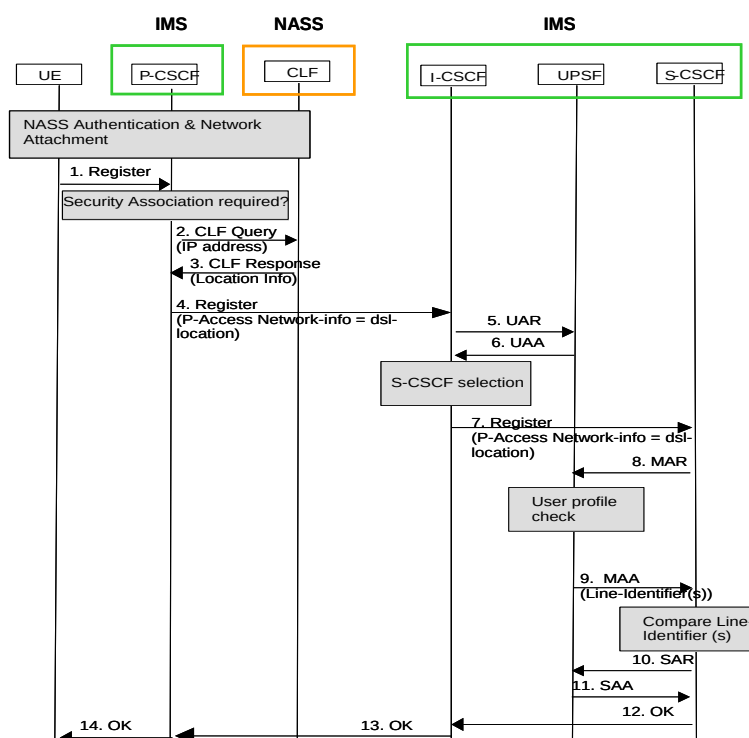


Figure 7 – IMS NASS Bundled Authentication

Notice the NASS Bundled Authentication restricts the RG nomadicity, and so it cannot be attached to the access network from another different location since Line ID it is tied to the GPON/OLT physical port. Likewise, the RG cannot be registered to the IMS network by using different Line ID or not assigned SIP credential to that subscriber e.g. the IMS Public ID [respective phone number]. If the subscriber hacks the RG to change the VoIP credential e.g. subscriber number, during SIP register procedure IMS will not authorize the authentication due to the mismatch in that subscriber entry.

3 CONCLUSIONS

Oi has been implementing along the years customized applications and mechanism to prevent real time fraud and call spoofing in both TDM and IMS/VoIP network.

4 Acronym

- ANI – Automatic Number Identification
- AS – Application Server
- CDR – Call Detail Record
- CED – Caller Entered Digits
- CdPN – Called Party Number
- CDR – Call Detail Record

- CgPN – Calling Party Number
- CLF – Connectivity Session Location and Repository. Function
- CO – Central Office
- CSCF – Call Session Control Function
- DHCP – Dynamic Host Configuration Protocol
- DID – Direct Inward Dialling
- DPC – Destination Point Code
- DTMF – Dual Tone Multi-frequency
- FTTH – Fiber to the home
- GPON – Gigabit-capable Passive Optical Network
- HSS – Home Subscriber Server
- IAM – Initial Address Message
- I-CSCF – Interrogating-Call Session Control Function
- IMS – IP Multimedia Subsystem
- IN – Intelligent Network
- INAP – Intelligent Network Application Part
- IP – Internet Protocol
- IP-PBX – IP Private Branch Exchange
- ISUP – ISDN [Integrated Services Digital Network] User Part
- MGCF – Media Gateway Control Function
- MTP – Message Transfer Part
- NASS – Network Attachment Subsystem
- NGN – Next Generation Network
- NP – Number Portability
- OAMP – Operations, Administration, Maintenance and Provisioning
- OBCM – Outbound Call Management
- OLT – Optical Line Terminal
- ONT – Optical Network Terminal
- OPC – Originating Point Code
- OSS – Operating Support System
- PBX – Private Branch Exchange
- P-CSCF – Proxy Call Session Control Function
- PIN – Personal Identification Number

- POTS Plain Old Telephony Service
- PSTN Public Switched Telephony Network
- RG – Residential Gateway
- SBC Session Border Controller
- S-CSCF Serving Call Session Control Function
- SCP – Service Control Point
- SGW Signaling Gateway
- SIP Session Initiation Protocol
- SS7 – Signaling System #7
- SSP – Service Switching Point
- STP – Signal Transfer Point
- TAS Telephony Application Server
- TCAP – Transaction Capabilities Application Part
- TDM Time Division Multiplexing
- UE User Equipment

End of Document