



INTERNATIONAL INTERCONNECTION FORUM
FOR SERVICES OVER IP

CLOUD NUMBERS USE CASES

INDEX

	1
1. Introduction	4
2. What is a cloud number?	5
3. CLI use by Cloud numbers	6
A) Generate destination calls	6
B) Receive originating calls	7
C) Exceptions	9
4. VOICE CARRIER ROLE	10
4.1 - Voice Management	10
4.2 - DID's management	10
4.3 – Regulatory	10
4 – Connectivity	10
4.5 – Security	10
5. TECHNICAL DESCRIPTION	12
6. USE CASES	13
6.1 Corporate Telephony	14
6.2 Cloud Contact Center	15
6.5 Call Forwarding	18
6.6 DIDs for remote device	19
6.7 Conferencing Platform	20
Other possible cases:	21
6.8 Calling App / OTT – in and outbound dialing Contact	21
6.9 ONLINE-Ads	21
6.10 MO (Mobile-Originated)	21
7. REGULATORY REQUIREMENTS	22
8. FRAUDS	23
Social Engineering	24
Spoofed Identity (Spoofing)	24
Vishing (Voice + Phishing)	24
VoIP Phishing	25
Denial-of-Service (DoS) attacks	25

International Revenue Share Fraud	25
Unauthorized Access to Voice Systems	25
9. Summary and Conclusion	26
10. Glossary of acronyms and abbreviations	27

1. Introduction

Customers are experiencing an accelerated transformation as a result of digitalization and globalization.

Factors such as the explosion of eCommerce or the increase in B2C-C2B relationships through online channels is driving companies to demand value-added voice services.

More and more customers are asking for global solutions, in order to be able to offer their services to globally operating companies.

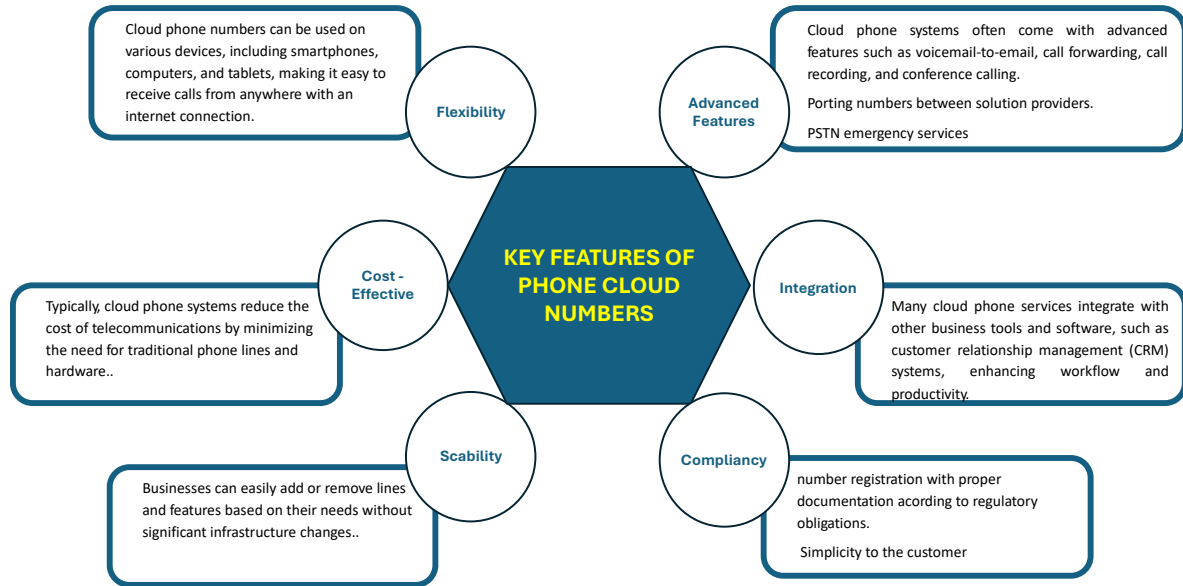
These services, such as Cloud Numbers or Freephone, emerge as the key to achieving excellence in customer service, triggering the best user experience, a factor considered a differentiating aspect in a digitized and hyperconnected world. Added to this is the rise of new customers who require a new type of interaction. Specifically, via portals through the end-to-end automated service, at the same time as they demand global coverage, not only geographically, but also for the different uses of the traditional services.

This document **“Cloud Numbers and Inbound Calls”**, tries to analyze and give visibility to the critical aspects to address the growing demand on new cloud communication through voice services, such as DiDs Geo&Mobile, share cost, ITFS and UIFN numbers and also PSTN enable full replacement, in a new world of digital services.

2. What is a cloud number?

A phone number that utilizes cloud-based technology to facilitate communication. Unlike traditional phone numbers tied to physical phone lines, cloud phone numbers are part of a Voice over Internet Protocol (VoIP) system, allowing users to make and receive calls over the internet.

Key features for the customer:



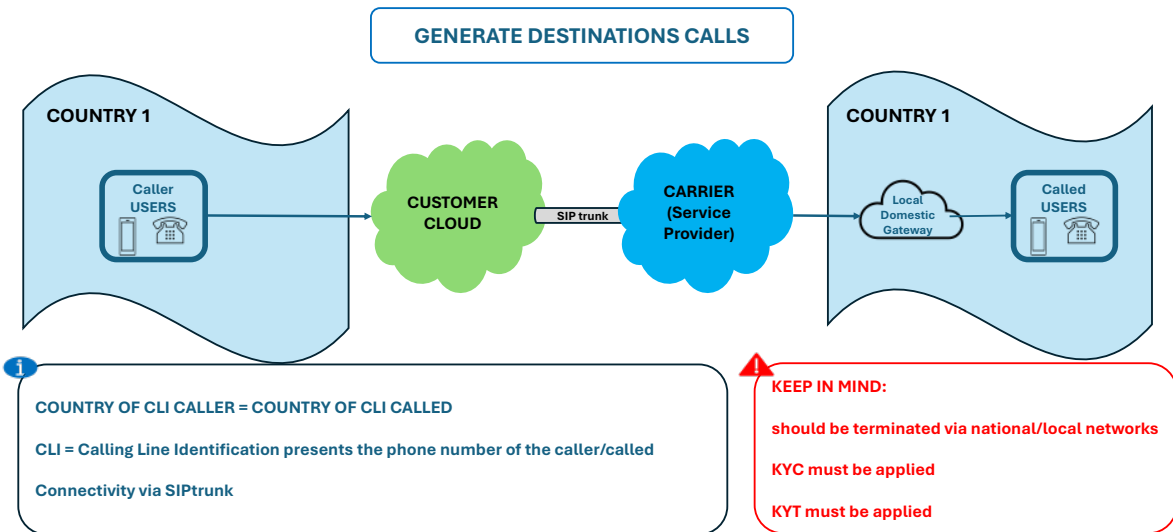
Overall, cloud phone numbers offer a modern solution for both businesses and individuals looking for efficient and versatile communication options.

3. CLI use by Cloud numbers

A) Generate destination calls

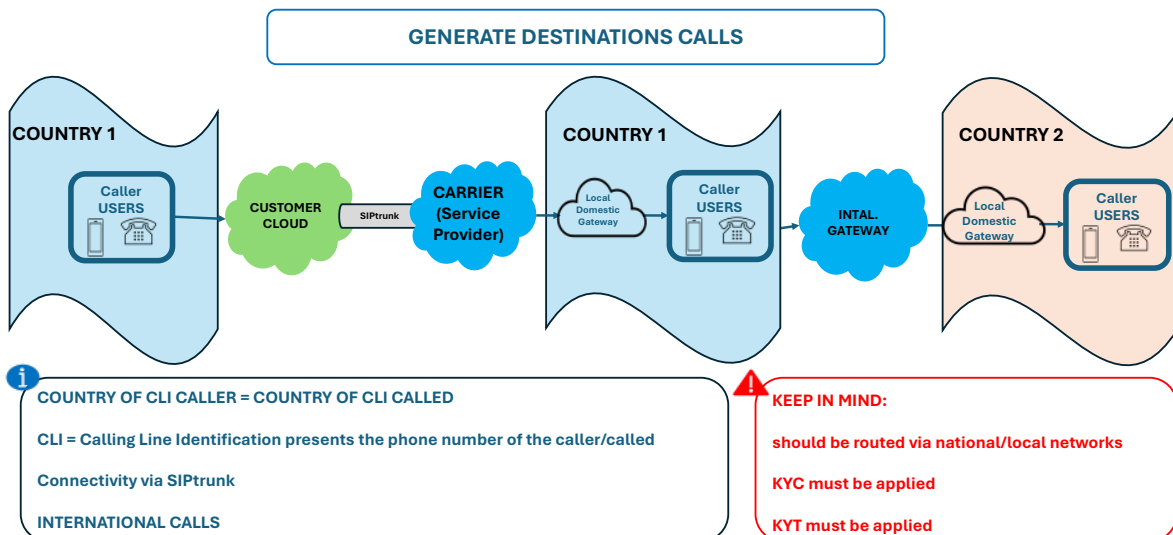
To National/local numbers

- (CLI country nA= CLI country nB= => should be terminated via national/local networks (usually SIPTRUNK interconnection).



To International numbers

- CLI country nA different from CLI country nB
- From DIDs provided by Carrier -> The provider carrier of the DID should terminate the international call made by this DID via the carrier's international network as this is regular voice traffic.



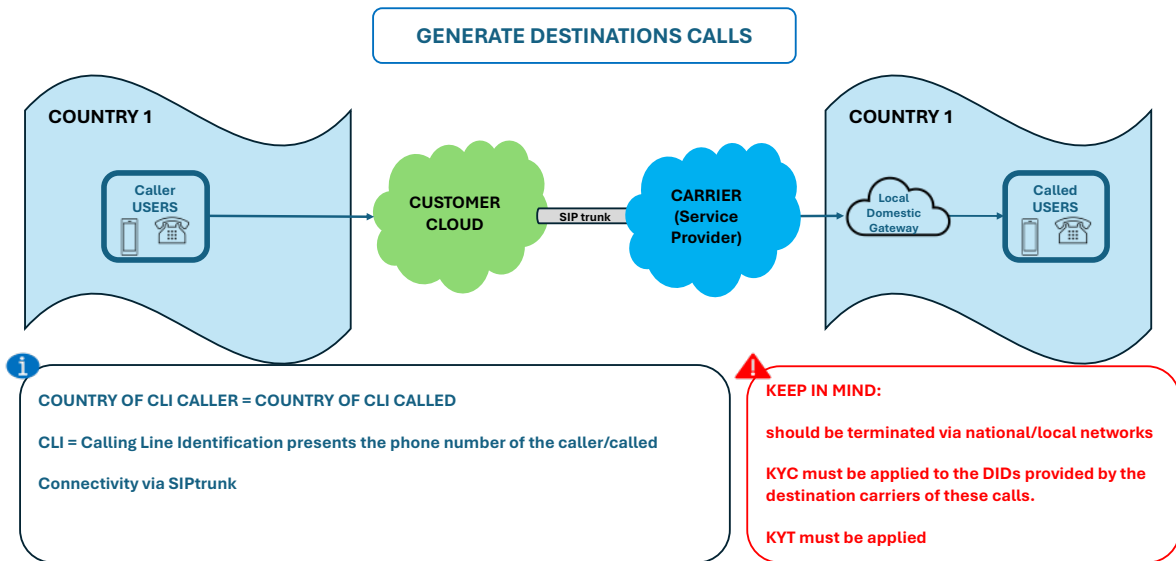
- There are DIDs not provided by the Carrier that are making international calls and are being carried on the international network as the rest of the international traffic and we do not know the origin of those numbers.

- CN traffic over ILD network of carriers (when carrier is not providing the numbers – therefore not offering the CN service to end user customer) Typical ILD
 - FMS monitoring
 - KYC not applied, lower-level attestation

B) Receive originating calls

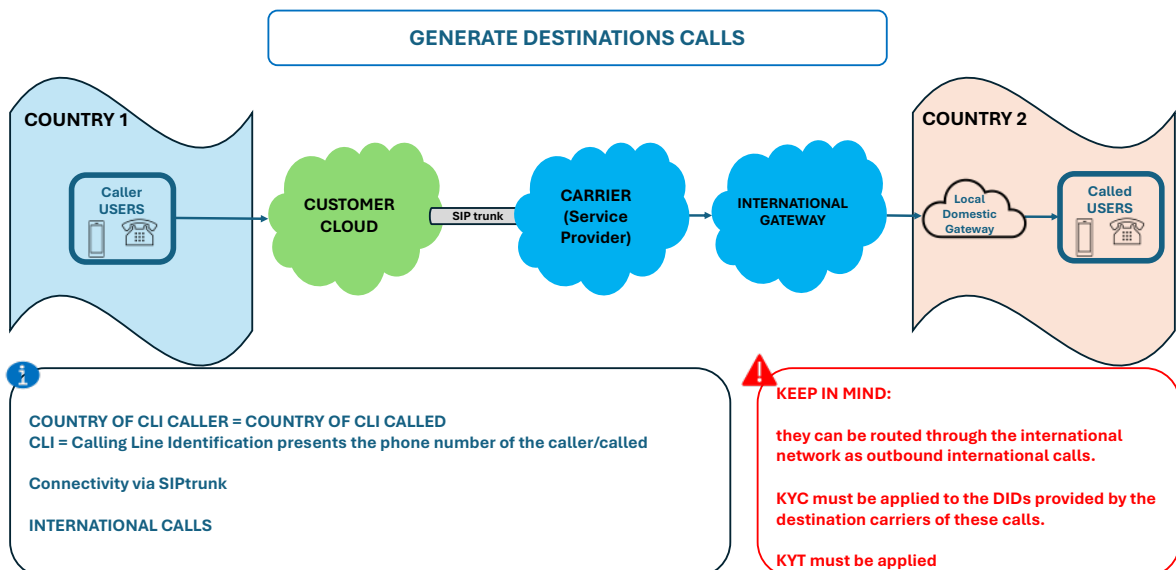
From National/local numbers

- (CLI country nA= CLI country nB)= => received via the provider of the number and terminated via the national/local networks.



From International numbers

- (CLI country nA different from CLI country nB), received via the provider of the number through the SIPTRUNK Interconnection



SUMMARY

KYT and KYC must be applied

Only our provide CLI's to be used

When country number A = to country number B (national call) must be terminated via local networks

When country number A different to country number B (international call) must be terminated via international networks

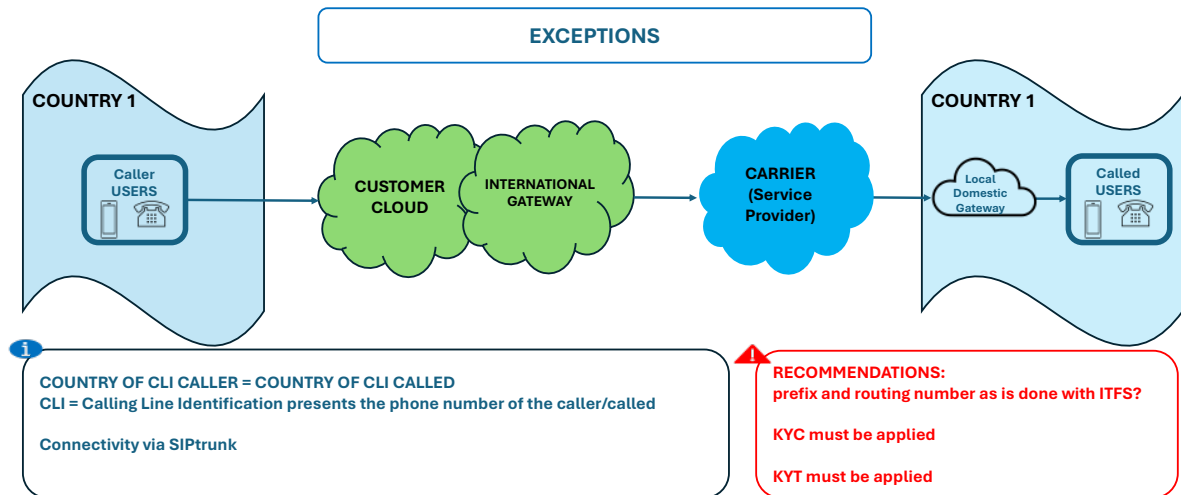
The appropriate documentation must be received

If the above conditions are met even if the calls are coming from international locations, it should be allowed to pass with the local CLI

C) Exceptions

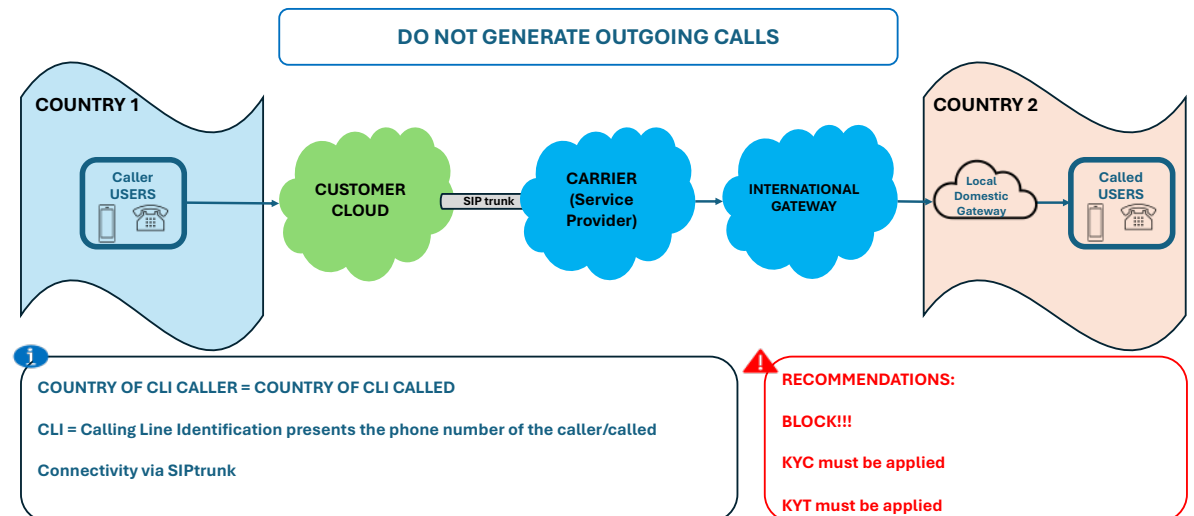
National incoming Calls arriving directly from International networks

- There are use cases (e.g. conference platform, cloud PBX...) that may result in:- a national CLI with national CLI destination (country nA = country nB), arriving via international networks.

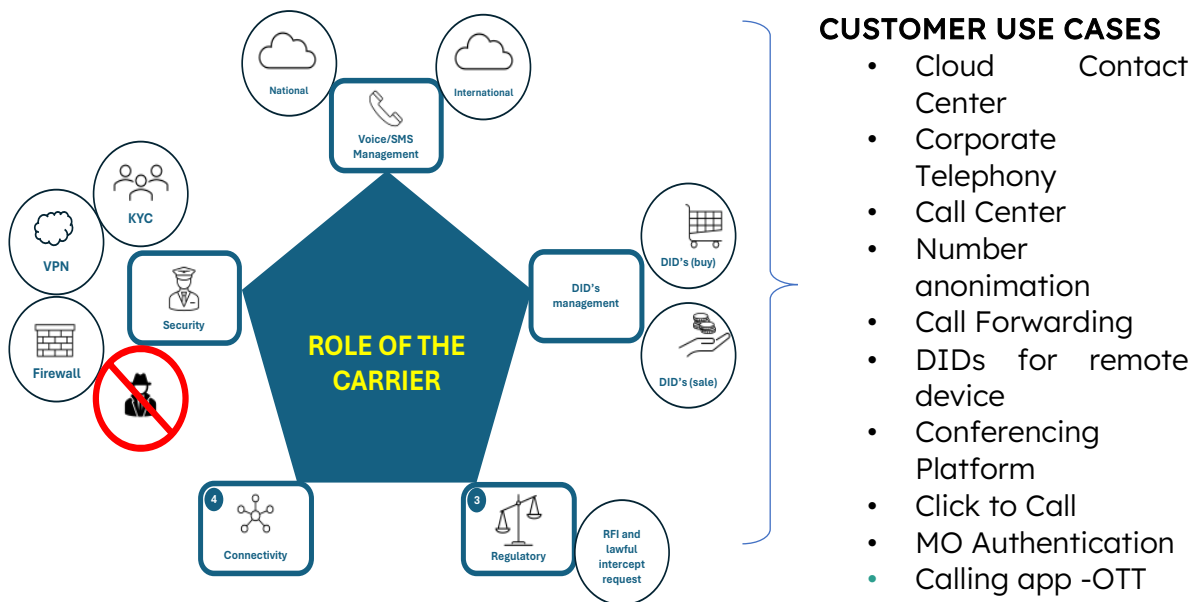


TOLL FREE generating outgoing calls

- It depends on the country regulation, in some countries it is allowed



4. VOICE CARRIER ROLE



4.1 - Voice Management

National (Inbound + outbound): The carrier must ensure that it delivers its customers' traffic nationwide.

International (Inbound + outbound): The carrier must ensure that it delivers its customers' traffic internationally.

4.2 - DID's management

DID's (buy): To provide the DID's to the customer, the operator will arrange the purchase of local numbers with the corresponding national operator.

DID's (sale): The operator will resell the specific DID numbering hired to the local operator to resell to the Customer.

4.3 – Regulatory

The regulation surrounding the DID's and Break-in/Break-out calls is very different in each country, which forces voice carriers to act differently and to adapt themselves on a case-by-case basis.

It is the operator's mission to be aware of any regulatory changes to comply with all applicable laws.

4 – Connectivity

The operator will provide the necessary national/international connections in order to guarantee the Customer's connectivity.

4.5 – Security

KYC (Know Your Customer): KYC applies only to numbers to DID's that we as carriers provide. KYC doesn't apply for carriers when carriers are not providing the DID's and calls are carried over international GWs. CN traffic over ILD

network of carriers (when carrier is not providing the numbers – therefore not offering the CN service to end user customer) Typical ILD:

- FMS monitoring
- KYC not applied, lower-level attestation

KYT (Know Your Traffic): must also be applied. Only the carrier's provided CLI's to be used.

The appropriate documentation must be received

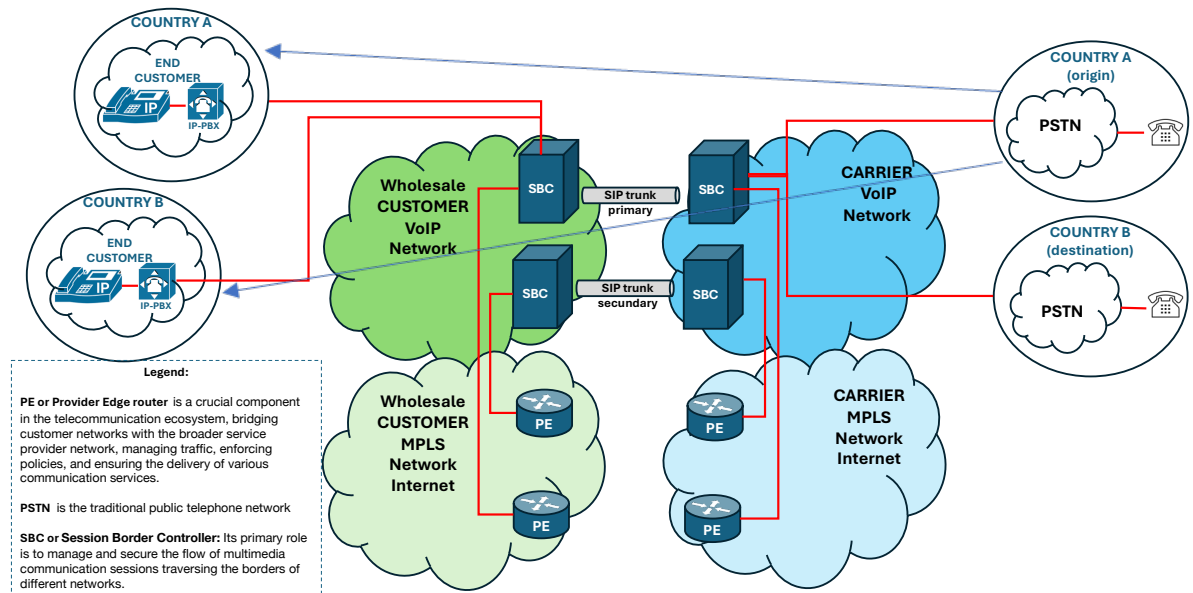
To resale DIDs, it is very important to collect certain information from the client to whom the DIDs are sold, to at least know where they will be located and the use to which they will be given. There are some countries in which certain proofs are even required to ensure the veracity of the data provided by the client.

VPN: Technology that creates a secure and encrypted connection over a less secure network, such as the internet. protect private web traffic from snooping, interference, and censorship. Key Features of a VPN: Encryption, Privacy, Remote Access, Bypass Restrictions, etc. Benefits: Enhanced Security, Improved Online Access, Anonymous Browsing, Safe File Sharing, etc.

Firewall: A firewall is a network security tool that acts as a barrier between an internal network and the outside, such as the Internet

STOP Fraudulent: Having the necessary tools to automatically monitor, control and block potentially fraudulent traffic.

5. TECHNICAL DESCRIPTION



6. USE CASES

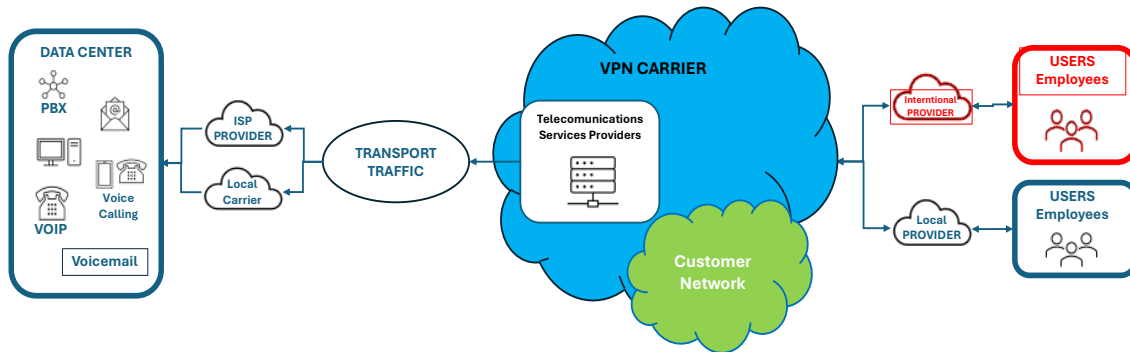
Use Case	Use Case Name	Use Case Description
1	Corporate Telephony	Corporate telephony refers to the telephony infrastructure used by companies to manage and enhance internal and external communications. It typically includes services such as voice calls, voicemail and other unified communications systems (e.g. VoIP, PBX systems). It is a replacement for the PSTN, which provides business telecommunications services over SIP trunks.
2	Cloud Contact Center	A Contact Center in the cloud is a system that is accessed through the Internet and from which all the company's communication channels with customers (Omnichannel - voice, chat, email) are managed. Some of these contact centers may be outsourced, being operated by third-party providers and may not even be located in the same country as the company they represent. Using local numbers from the customer's region, PAI (P-Asserted-Identity) and from headers in SIP signaling will differ to maintain compliance and ensure proper display of calling line identification.
3	Call Center	Customer communication platform, cloud numbers and inbound calls allow customers to access the contact center (typically inbound voice services only). But that can include CPaaS-type solutions where inbound and outbound numbers can be assigned to various services provided through the CPaaS platform that provides API integration and custom-coded call flows.
4	Number Anonymity	Service requiring a pool of numbers to anonymize caller identification. Identity mask is widely used by platforms that facilitate communication between users (e.g., users and service providers) without exposing their personal phone numbers. The service acts as an intermediary, ensuring that both parties can communicate while their real phone numbers remain hidden.
5	Call Forwarding	Service requiring a pool of numbers, for instance, call forwarding is used to route the call to a server to track and collect metrics regarding the profile of the calls (e.g., call duration, caller location, time of day, call volumes). This service is often used by businesses for marketing campaigns, customer service, or contact centers to monitor and optimize the performance of their communication channels.
6	IoT	There are some special projects that require case-by-case analysis. Niche cases related with remote devices where DIDs could complement IoT or mobile connection. Numbers provided for IoT (IP end points) devices (i.e. cars, eolic station, vending...)
7	Conferencing Platform	Audio conferencing allows users to join the audio portion of meetings from anywhere using a dial-in number or to invite anyone from anywhere using a dial-out number. Operators, apart from offering the termination of these calls, can offer numbering (DIDs). UC companies use this service; the platform calls participants using numbers that do not necessarily belong to the participants themselves and often may not support dialing back to the number that originated the call.
8	Online Ads	Click-to-Call services enable users to initiate a phone call directly from a web page or application by clicking on a button. It's a commonly used feature in online ads, user support platforms, or websites where users can quickly connect to businesses
9	MO Authentication	MO (Mobile-Originated) Authentication refers to the use of a mobile phone to authenticate users in various online services. This type of authentication is widely used for verifying a user's identity or confirming transactions by sending a one-time password (OTP) via SMS or voice call to the mobile number associated with the account.
10	Calling App / OTT – in and outbound dialing	OTT calling applications, which utilize actual phone numbers for voice services. In outbound dialing, the app server routes a user's call through a Carrier to a destination number (mobile or landline). Often these services validate the CLI using MO authentication Inbound dialing user receiving calls on an OTT app, where the call could originate from another VoIP service or a traditional phone line.

6.1 Corporate Telephony

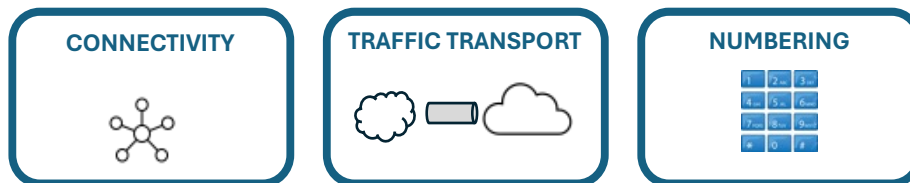
Use Case Definition

Corporate telephony refers to the telephony infrastructure used by companies to manage and enhance internal and external communications. It typically includes services such as voice calls, voicemail and other unified communications systems (e.g. VoIP, PBX systems). It is a replacement for the PSTN, which provides business telecommunications services over SIP trunks.

Commercial Diagram



WHAT'S THE CUSTOMER CONTRACTING IN THIS USE CASE TO THE CARRIER?



6.2 Cloud Contact Center

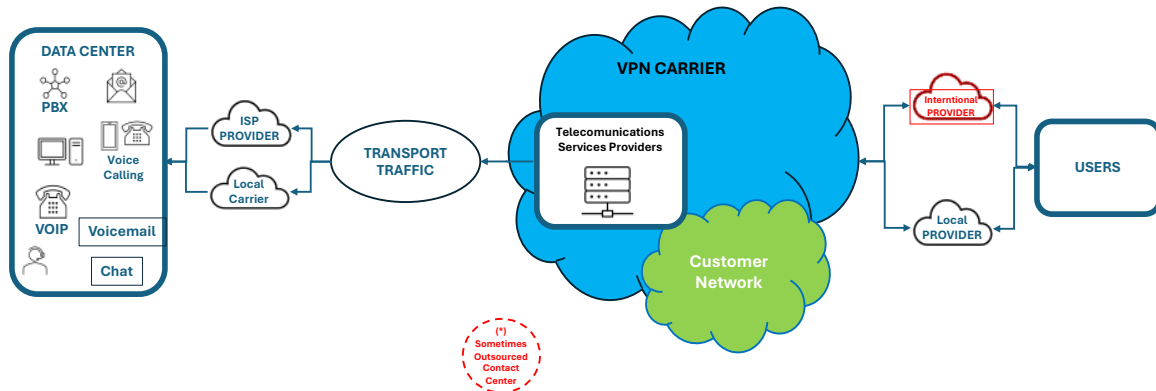
Use Case Definition

A Contact Center in the cloud is a system that is accessed through the Internet and from which all the company's communication channels with customers (Omnichannel - voice, chat, email) are managed.

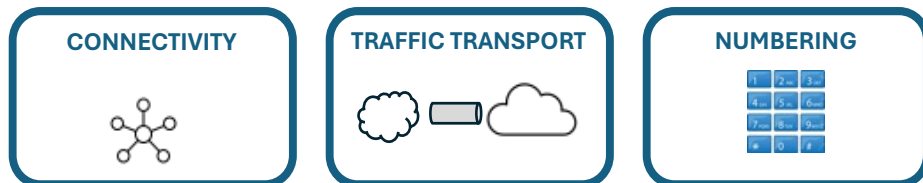
Some of these contact centers may be outsourced, being operated by third-party providers and may not even be in the same country as the company they represent.

Using local numbers from the customer's region, PAI (P-Asserted-Identity) and from headers in SIP signaling will differ to maintain compliance and ensure proper display of calling line identification.

Commercial Diagram



WHAT'S THE CUSTOMER CONTRACTING IN THIS USE CASE TO THE CARRIER?



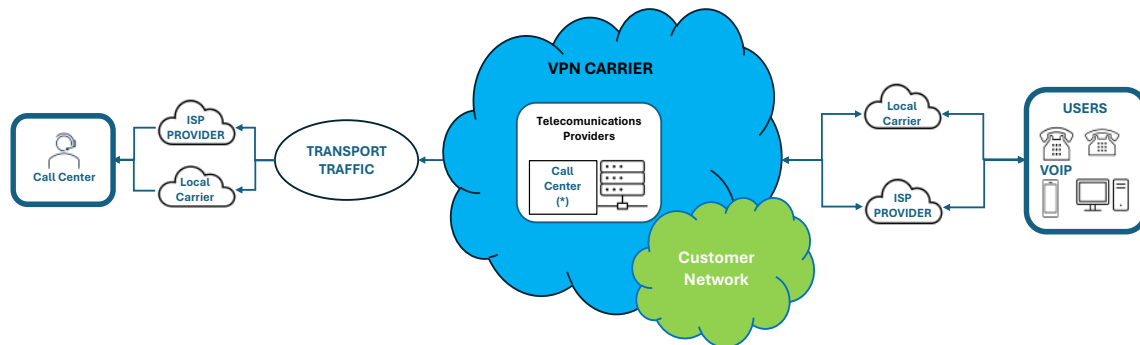
6.3 Call Center

Use Case Definition

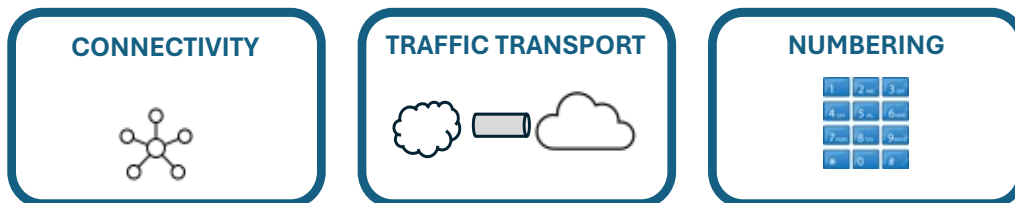
Customer communication platform, cloud numbers and inbound calls allow customers to access the contact center (typically inbound voice services only).

But that can include CPaaS-type solutions where inbound and outbound numbers can be assigned to various services provided through the CPaaS platform that provides API integration and custom-coded call flows.

Commercial Diagram



WHAT'S THE CUSTOMER CONTRACTING IN THIS USE CASE TO THE CARRIER?

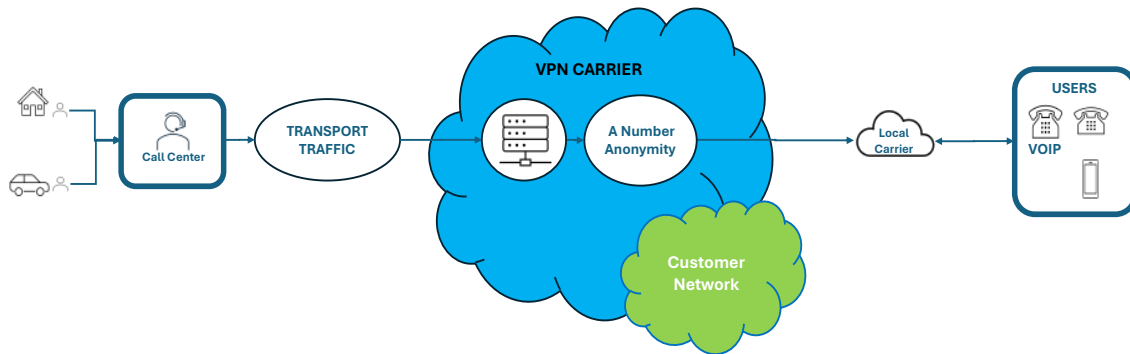


6.4 Number Anonymity

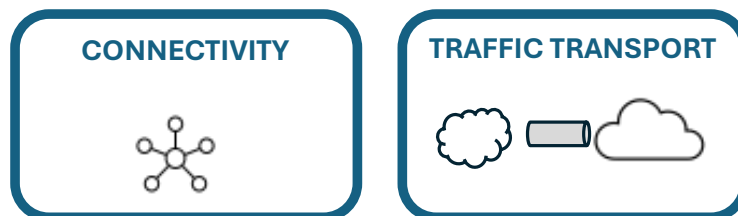
Use Case Definition

Service requiring a pool of numbers to anonymize caller identification. Identity masking is widely used by platforms and other services that facilitate communication between users (e.g., users and service providers) without exposing their personal phone numbers. The service acts as an intermediary, ensuring that both parties can communicate while their real phone numbers remain hidden.

Commercial Diagram



WHAT'S THE CUSTOMER CONTRACTING IN THIS USE CASE TO THE CARRIER?



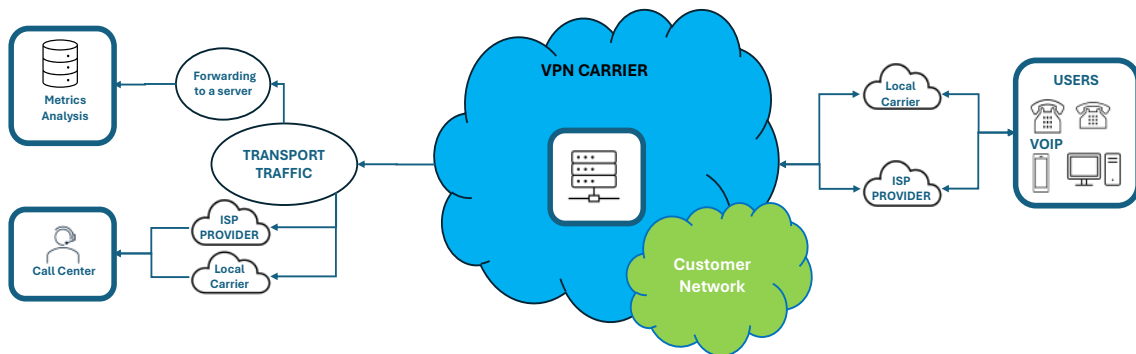
6.5 Call Forwarding

Use Case Definition

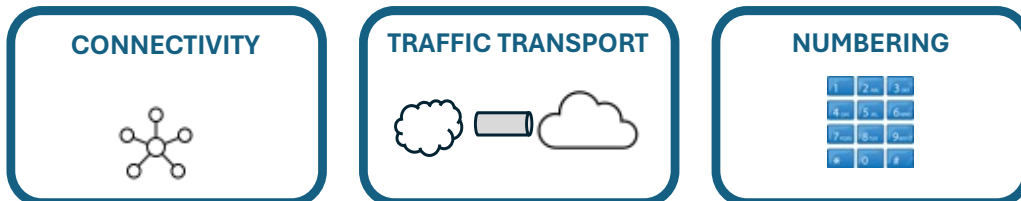
Service requiring a pool of numbers, for instance, call forwarding is used to route the call to a server to track and collect metrics regarding the profile of the calls (e.g., call duration, caller location, time of day, call volumes).

This service is often used by businesses for marketing campaigns, customer service, or contact centers to monitor and optimize the performance of their communication channels.

Commercial Diagram



WHAT'S THE CUSTOMER CONTRACTING IN THIS USE CASE TO THE CARRIER?



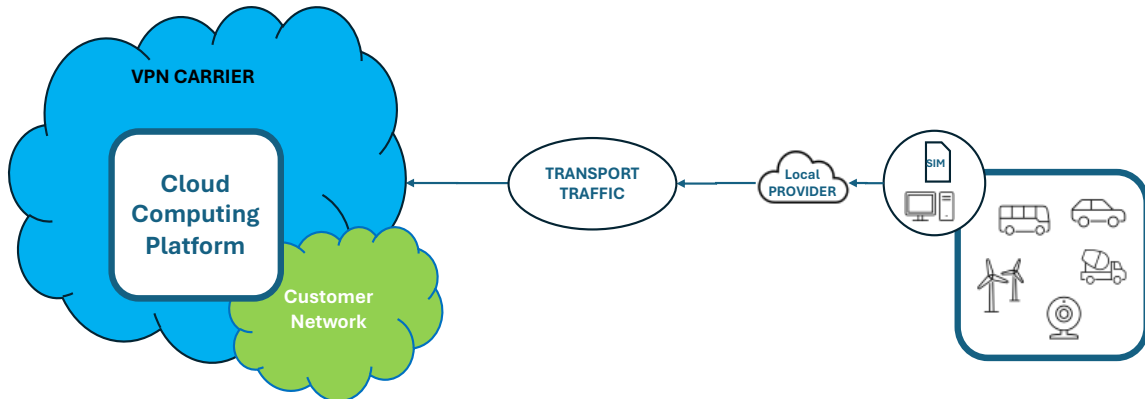
6.6 DIDs for remote device

Use Case Definition

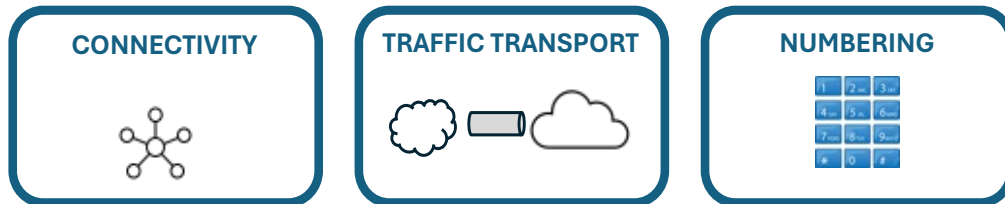
There are some special projects that require case-by-case analysis. Niche cases related with remote devices where DIDs could complement IoT or mobile connection.

Numbers provided for IoT (IP end points) devices (i.e. cars, eolic station, vending,)

Commercial Diagram



WHAT'S THE CUSTOMER CONTRACTING IN THIS USE CASE TO THE CARRIER?



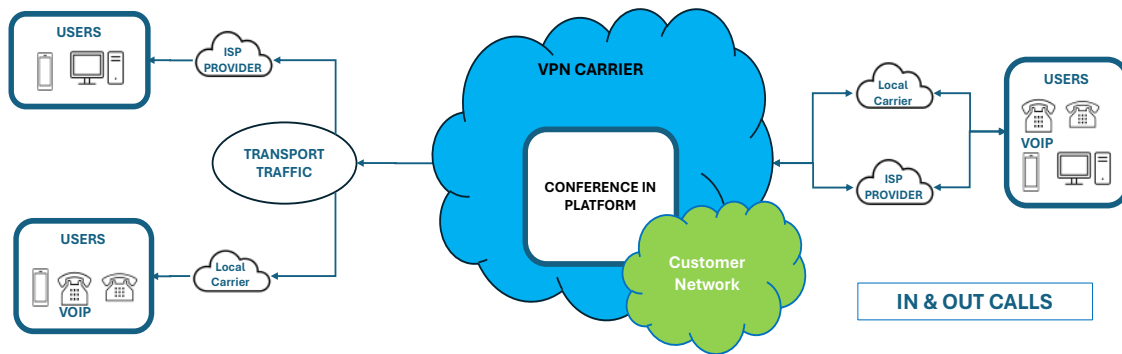
6.7 Conferencing Platform

Use Case Definition

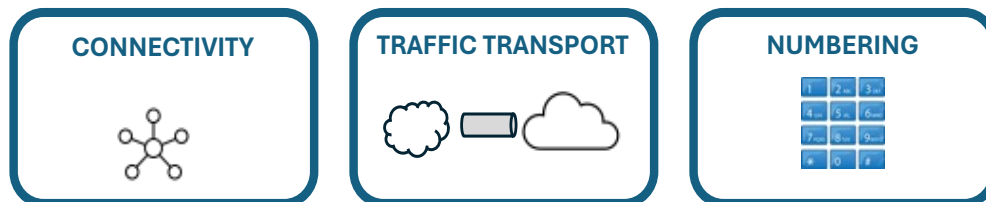
Audio conferencing allows users to join the audio portion of meetings from anywhere using a dial-in number or to invite anyone from anywhere using a dial-out number. Operators, apart from offering the termination of these calls, can offer numbering (DIDs).

UC companies use this service; the platform calls participants using numbers that do not necessarily belong to the participants themselves and often may not support dialing back to the number that originated the call.

Commercial Diagram



WHAT'S THE CUSTOMER CONTRACTING IN THIS USE CASE TO THE CARRIER?



Other possible cases:

6.8 Calling App / OTT – in and outbound dialing Contact

OTT calling applications, which utilize actual phone numbers for voice services.

In outbound dialing, the app server routes a user's call through a Carrier to a destination number (mobile or landline). Often these services validate the CLI using MO authentication

Inbound dialing user receiving calls on an OTT app, where the call could originate from another VoIP service or a traditional phone line.

6.9 ONLINE-Ads

Click-to-Call services enable users to initiate a phone call directly from a web page or application by clicking on a button. It's a commonly used feature in online ads, user support platforms, or websites where users can quickly connect to businesses.

6.10 MO (Mobile-Originated)

MO (Mobile-Originated) Authentication refers to the use of a mobile phone to authenticate users in various online services. This type of authentication is widely used for verifying a user's identity or confirming transactions by sending a one-time password (OTP) via SMS or voice call to the mobile number associated with the account.

7. REGULATORY REQUIREMENTS

The regulation surrounding the DIDs and Break-in/Break-out calls is very different in each country, which forces voice carriers to act differently and to adapt themselves on a case-by-case basis.

For those use cases of PSTN replacement, emergency calls or legal interception is required.

Resale is prohibited or very restricted in many Countries:

- Countries in which resale is not allowed: In some cases, a three-party agreement can be used to assign numbers directly to end customer.
- In these cases, in which resale is allowed, Regulator might require to get a reseller license to sub-assign numbers.

It is also very important for the resale of DIDs to collect certain information from the client to whom the DIDs are sold, to at least know where they will be located and the use to which they will be given. There are some countries in which certain proofs are even required to ensure the veracity of the data provided by the client.

For **outbound termination of international traffic**, should comply with the rules related with international traffic, it is important to have the carrier license that each local regulatory entity considers necessary. Also, different aspects must be considered in relation to CLI treatment and the delivery of national traffic over international networks, since in some countries there is regulatory pressure to prevent this.

In summary, it is crucial to liaise closely with the local regulator in each case to ensure that the service is provided or resold in accordance with the relevant regulations. If this is not possible, it is important to explain the legitimate use cases to the regulator to facilitate the approval of the service provision by the carrier

8. FRAUDS

The carrier community follows the guidelines of the Anti-Fraud Code of Conduct, developed by the Global Leaders' Forum together with the i3Forum, which sets out the principles to prevent and avoid fraud by monitoring and analyzing the profile of communications to prevent and combat fraud by stopping any fraudulent communications and preventing the fraudster from reaping the economic benefits of these activities.


The Global Leaders Forum link:

<https://glfcommunity.com/>

Link to Global Leader Forum's jointly with i3Forum antifraud Codes of Conduct:

<https://glfcommunity.com/our-work/fighting-fraud/code-of-conduct>

The Voice Code of Conduct:



Code of Conduct for International Carriers on the prevention of fraudulent traffic (Voice)

Principle 1 – Targets and Monitoring
Targets for prevention of fraudulent traffic to be included within management reporting
Carriers will include in their internal management reporting dashboards relevant metrics and targets to all top executives to understand, and oversee, all activity to reduce fraudulent traffic flows.

Principle 2 – Processes
Carriers to adhere to i3 Forum recommended processes to detect and avoid fraud
Carriers will adopt the definitions and recommendations to avoid fraudulent traffic specified in "Fraud Classification and Recommendations on Dispute Handling within the Wholesale Telecoms Industry – Release 3.0" and shall use reasonable efforts to support the investigation of suspected fraud.

Principle 3 – Destinations
Identified fraudulent number ranges and destinations to be blocked
Carriers will actively monitor their individual traffic patterns to identify fraudulent number ranges and destinations, and take appropriate measures individually to block fraudulent traffic as soon as technically feasible.


Principle 4 – Payment Flows
All reasonable action to be taken to avoid payment flows to the instigators of fraudulent traffic
Where the instigators of fraudulent traffic have been identified beyond reasonable doubt, carriers will individually seek to stop payment flows as soon as technically and commercially feasible subject to any relevant legal obligations. The originating carrier will remain responsible for the fraudulent traffic and financially liable in case the payment flows cannot be stopped by the downstream carrier(s).

Principle 5 – Reporting
Commitment to share information regarding fraudulent traffic flows with carrier peers
Carriers will actively share information on fraudulent traffic and its origination, where permissible, subject to anti-trust legislation, contractual and regulatory obligations and commercial constraints, with all potentially impacted peers.

Principle 6 – Contracting
Adoption of standard contracting terms addressing fraudulent traffic management
Carriers will adopt, once available, standard contracting terms developed by the i3 Forum for the management of fraudulent traffic and subsequent dispute resolution.

Principle 7 – Revenue Share Numbers
Providing clients with the option to opt-out from specific number ranges
Carriers who directly breakout special number ranges for revenue share purposes, including "special services" and audiotext (a typically higher rate destined for content related services), will clearly outline in their rate sheet that they contain such breakouts and offer customers the ability to "opt out" of such ranges prior to engaging in voice traffic. Intermediary operators will not be accountable if they are not aware of these breakouts.

The SMS Code of Conduct:



Commitment from international carriers to adhere to principles to combat SMS fraud

Principle 1 – Target and monitoring
Targets for prevention of fraudulent traffic to be included within management reporting.

Principle 2 – Processes
Carriers to adhere to i3Forum recommended processes to detect and avoid fraud.

Principle 3 – Blocking
Identified fraudulent numbers and ranges to be blocked.

Principle 4 – Payment flows
All reasonable action to be taken to avoid payment flows to the instigators of fraudulent traffic.

Principle 5 – Reporting
Commitment to share information regarding suspicious traffic flows with the upstream and downstream parties.

Also, **KYC (Know Your Customer)** must be established for customers to which the DiDs are provided by the carriers.

Fraud in cloud number services, also known as "VoIP fraud" (Voice over IP), has been a growing problem as more companies adopt this technology.

Fraudsters cause a decrease in customer service by dedicating a portion of their time to fraudulent calls. An economic cost due to increased unwanted operational costs, wasted business resources, congestion and denial of service, loss of customer satisfaction and confidence, etc.

To protect against fraud in cloud services, it is important to implement adequate security measures, such as multi-factor authentication, monitoring of unusual traffic, and staff education on security practices. On the carrier side, it is also very important

to require KYC because it helps to verify the customer's identity, which is essential to avoid impersonation, fraud or unauthorized access.

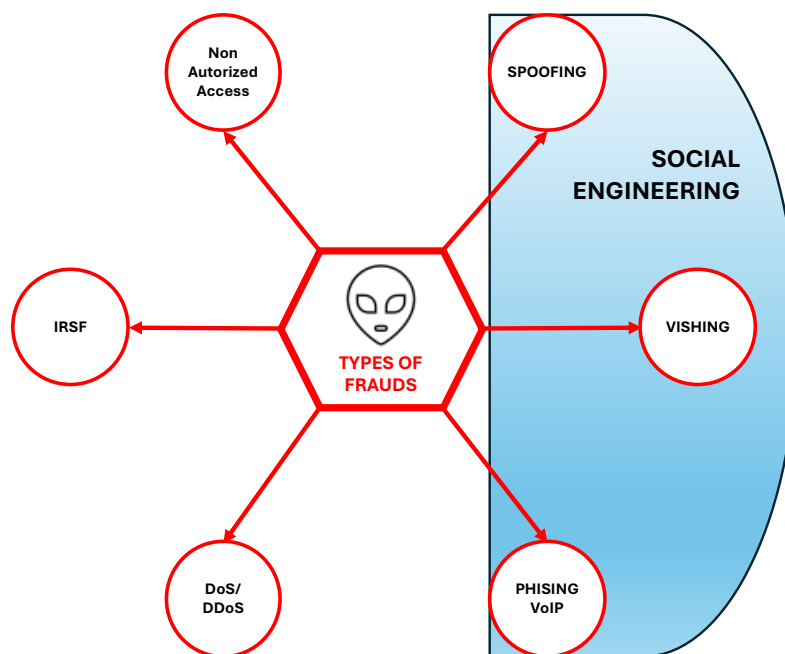
The type of frauds suffered by this type of number is the same as those suffered by any type of communication. These frauds are included in the i3Forum documents to be found in the following links:

LINK to **i3Forum** Fraud classification documents:

Voice: <https://i3forum.org/workgroups/voice-fraud/>

Messaging: <https://i3forum.org/workgroups/messaging-fraud/>

Of all of them, the most recurrent frauds to the customers hiring this type of service are shown below:



Social Engineering

These are practices carried out by fraudsters to obtain information, access and permissions directly from end customers that subsequently allow them to impersonate them and carry out scams using their credentials. The main modalities are:

Spoofed Identity (Spoofing)

Criminals can spoof the caller ID to make it appear that the call is coming from a trusted number. This can lead to the exploitation of confidential information or even money transfers.

There are different types of spoofing: IP, ARP, DNS (domain), Web, email, GPS, facial recognition, etc.

Vishing (Voice + Phishing)

Telephone scam to obtain customer data and steal from them (SPOOFING, identity theft).

Using technology, fraudsters make their calls look legitimate and impersonate trusted entities to trick employees into revealing sensitive information or compromising the

security of the company. They can also impersonate a customer in order to get employees to reveal personal data about that customer to defraud them later.

VoIP Phishing

Like traditional phishing, this fraud involves tricking users into revealing sensitive information through fraudulent phone calls that may appear legitimate.

Denial-of-Service (DoS) attacks

Fraudsters can flood a VoIP system with malicious traffic, causing service saturation and interruption.

There is a Distributed Denial-of-Service (DDoS) variant in which the fraudster launches the attack from multiple zombie machines that he has previously hacked.

This can lead to financial losses and damage to the company's reputation.

International Revenue Share Fraud

Fraudsters access the Company's Contact Center PBX system and take advantage of revenue sharing agreements with carriers by generating a large volume of international calls to high-cost premium rate numbers.

They often collaborate with fraudulent operators that charge high rates for call termination, and share the revenue generated by the traffic.

Unauthorized Access to Voice Systems

Fraudsters can exploit vulnerabilities in the cloud voice infrastructure or access PBXs (if certain outbound channels, ports, are left unprotected) to gain access and make calls, e.g. spam calls.

The following table shows the frauds that affect each of the use cases:

	Non Authorized Access	SPOOFING	VISHING	PHISING VoIP	DoS/ DDoS	IRSF
Cloud Contact Center	X	X	X	X	X	
Corporate Telephony	X	X	X	X	X	X
Call Center	X	X	X	X	X	
Number Anonymity		X	X	X		
Call Forwarding	X	X	X	X		X
IoT	X				X	
Retail Use (HCD)				X		
Conferencing Platform	X	X		X		
Calling App / OTT	X	X	X	X		X

9. Summary and Conclusion

The New World of Communications morphed into a 'fuzzy' world yet significantly dependent on the core telecom asset – “Numbers”

Moving from traditional services: pre-programmed and use cases with standard handshakes across global telecom community to “X-aas” services: custom and non-standard or programmable application/handshake needing complex management

The use of “Numbers” however has significantly evolved considering the changing market requirements:

Customer Transformation:

Rapid changes in Customer Business driven by digitalization and globalization.

Value-Addition:

Rapidly evolving eCommerce growth and online B2C, B2B & B2B2C relationships.

Global Solution Requirement:

Customers increasingly seek global solutions to cater to internationally operating companies.

New Use Cases & Experimentation:

Customers require new types of interactions, including end-to-end automated services via portals.

Regulatory compliances:

all of the above need to be conforming to global, regional and national regulations as applicable.

There are new use cases that offer legitimate solutions to end customers who demand Cloud numbers to offer the best customer experience.

As they are global customers, they are looking for a global solution provider, which is channeled through the figure of the carrier. It may happen that such services cannot be offered by carriers due to the impossibility of resale prohibited by local regulations in certain countries.

Therefore, it is crucial to liaise closely with the local regulator in each case to ensure that the service is provided or resold in accordance with the relevant regulations. If this is not possible, it is important to explain the legitimate use cases behind the service to the regulator to facilitate the approval of the service provision by the carrier.

The carrier offers the sale of the numbers, the transport of the communications linked to those numbers, security, and guarantees compliance with the legal and regulatory requirements of each country where the number is contracted.

The carrier establishes the mechanisms defined in the industry for the detection and prevention of fraud. And in the case of cloud numbers, it becomes crucial to comply with the Know your customer requirement (KYC), because it helps to verify the customer's identity, which is essential to avoid impersonation, fraud or unauthorized access.

10. Glossary of acronyms and abbreviations

API: Application Programming Interface, is a set of rules and protocols that allows different software applications to communicate with each other.

App: Application, software program designed to perform a specific function or set of functions on a computer, smartphone or Tablet.

ARP: Address Resolution Protocol, protocol used to map an IP address to a MAC (Media Access Control) address within a local network.

B2B: Business to Business, refers to commercial transactions, relationships or activities conducted between two business rather than between a business and individual.

B2B2C: Business to Business to Consumer is a business model where a company (the provider) partners with another business (the intermediary or distributor) to offer products or services directly to end consumers.

B2C: Business to Consumer, commercial transactions where a business sells products or services directly to individual consumers.

C2B: Consumer to Business, consumers offer products, services or information to businesses.

CLI: Calling Line Identification

CPaaS type: Communications Platform as a Service. Cloud-based platforms that enable business to integrate communication features -such as voice calls, messaging, and video calls- into their own applications via APIs.

DDoS: Distributed Denial of Service, is a type of cyberattack where multiple compromised computers or devices are used to flood a website or online service with excessive traffic.

DID: Direct Inward Dialing, service that allows callers to directly dial specific phone numbers within a company's phone system without going through a receptionist or an operator.

DNS: Domain Name System, system that translates human-readable domain names into numerical IP addresses that computers use to identify each other on the internet.

DoS: Denial of Service, cyberattack where a network or website is overwhelmed with excessive traffic or data, causing it to become slow, unresponsive, or unavailable to legitimate users.

FMS: Fraud Management System, Telefonica's traffic management tool that allows the prevention and detection of fraud, both in incoming and outgoing traffic flows.

GPS: Global Positioning System, a satellite-based navigation system that allows users to determine their exact location anywhere in the world in real time.

ILD network: Interconnect Long Distance is a telecommunications network that facilitates international long-distance calls between different countries or regions.

IMS: IP Multimedia Subsystem, framework used to deliver multimedia services over IP networks.

IoT: Internet of Things, refers to interconnected network of physical objects, devices, sensors, and systems that communicate and share data over the internet.

IP: Internet Protocol

IRSF: International Revenue Share Fraud

ITFS: International Toll Free Services, allows callers from different countries to make free calls to specific toll-free numbers, enabling international communication without charge to the caller.

KYC: Know Your Customer

KYT: Know Your Traffic

nA: Calling Number

nB: Called Number

OTP: One Time Password, it's a unique, temporary code used for authentication purposes, often sent via SMS or generated by a device to verify a user's identity during login or transactions

OTT: Over The Top, it refers to services or content delivered directly to users over the internet, bypassing traditional telecom networks.

PAI: P-Asserted-Identity) is a protocol used, particularly in VoIP and IMS networks. It allows a network element, such as SIP to assert or indicate the identity of the user who is actually requesting or initiating a call.

PBX: Private Branch Exchange, private telephone switching system used within an organization. It manages internal calls between employees and connects them to external phone lines for outgoing and incoming calls.

PSTN: Public Switched Telephone Network is the traditional global network of fixed-line telephones that connects calls through circuit-switched technology.

SIP: Session Initiation Protocol, a signalling protocol used to create, manage, and terminate communication sessions over IP networks. It's the primary technology in VoIP.

SIPTRUNK: Session Initiation Protocol Trunk, is a virtual connection that uses the SIP to provide voice and data communication services between a business and its telecom service provider over the internet or IP networks.

SMS: Short Message Service

UIFN: Universal International Free Number, is a type of international toll-free number.

VoIP: Voice over Internet Protocol, is a technology that allows voice communication and multimedia sessions to be transmitted over the internet or other IP networks.

VPN: Virtual Private Network, a service that creates a secure and encrypted connection between your device and a private network over the internet.

X-aas (está en el capítulo 9): Extended Automatic Signalling, protocol or system used within signaling networks to support advanced or extended signaling features beyond basics functions, related to routing, call setup, etc.