ECC Report 248

Evolution in CLI usage – decoupling of rights of use of numbers from service provision

Approved 28 April 2016

0 EXECUTIVE SUMMARY

E.164 numbers have been used as Calling Line Identification (CLI) for identifying the calling party and for routing and terminating calls in the case of location-based services. The most universally used signalling protocol stack to carry CLI parameters was, and still is, the ITU-T Signalling System No. 7 (SS7).

The origination, transit and presentation of CLI digits in the PSTN was traditionally the sole responsibility and custody of the network operators and the possibility of manipulating CLI digits was remote and required specialised equipment. This secure environment promoted trust in the CLI digits presented to end-users and the supply chain extended from the originating network, through a transit network if needed, to the terminating network.

The transition from legacy networks has transferred intelligence to the network edge and more sophisticated end-user devices and applications have empowered end-users to make use of the CLI capability in an increasingly flexible way thereby extending the supply chain well beyond the traditional players. This development, while broadly beneficial to calling parties, has created an environment where the inherent trust in CLI has been eroded and in some cases abused to perpetrate consumer harm through the manipulation of the E.164 number used as CLI. In 2009, the ECC published a report (ECC Report 133) which examined this issue and provided guidelines on how to increase trust in originating identifiers, including CLI. Striking a balance between maintaining and increasing trust in CLI, while also facilitating flexibility and service innovation is an interesting challenge for regulators.

This Report now identifies several ways in which CLI may be used in an increasingly flexible way and examines the regulatory issues and current regulatory practices associated with each type of use, including the need for validation mechanisms to retain and restore trust in CLI.

Chapter 4 provides examples of the use of E.164 numbers as CLI by service providers other than those to whom a number range was assigned by the NRA. The scenarios described include cases where the access network of the calling party's own service provider is used (i.e. the service associated with the number to be provided as CLI) as well as cases where alternative access networks are used.

Chapter 5 then describes CLI validation techniques and rules and summarises the advantages and disadvantages of the various approaches. This chapter also introduces future validation techniques which are currently being considered.

Chapter 6 then looks at the legal framework that exists around the use of CLI. This chapter introduces the provisions contained in the European Regulatory Framework and maps the obligations contained therein to the different CLI service functionalities. This chapter also describes the legal background for the assignment of numbers and the rights of use of end-users and service providers and considers the impact of more flexible use of CLI on those rights and on the implications for lawful interception.

Chapter 7 concludes that if the validation measures discussed in this report are implemented then the risk of consumer harm (e.g. Calling/Caller ID Spoofing) is minimised. Spoofing can occur only when you have a party in the calling chain that has malicious intent and this is independent of the flexible use of CLI.

In order to facilitate increased flexibility in CLI use, while promoting greater customer empowerment and ensuring regulatory framework compliance:

- CLI validation techniques should be made mandatory. The alternative service provider should provide validation measures ensuring that the end user has the right to use the number.

- When setting down the regulatory framework, the regulatory authorities should carefully consider which number types and under which criteria they consider can safely be used for flexible CLI purposes so that the risk of harm to consumers and other end-users is reduced.

- End users should have the right to use their number[1] in alternative services. Operators to whom numbers are assigned should not be able to restrict the use of those numbers as CLI for other services as long as the flexible use is in conformance with the regulatory framework.

[1] ECC Recommendation (07)02 "Consumer Protection Against Abuse Of High Tariff Services" recommends "*that it is not allowed to use a premium rate number in CLIP*" and ECC Recommendation (11)02 "Calling Line Identification And Originating Identification" recommends *"that premium rate numbers should be excluded as valid OI/CLI. The NRA decides what national number ranges could or could not be used as OI/CLI*";

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Abbreviation	Explanation
ACD	Automatic Call Distributor
3GPP	3rd Generation Partnership Project
BRI	Basic Rate Interface
BS	Base Station
CEPT	European Conference of Postal and Telecommunications Administrations
CLI	Calling Line Identification
DDI	Direct Dialling In
DNS	Domain Name System
DTMF	Dual-Tone Multi-Frequency
E.164	ITU-T Recommendation – “The international public telecommunication numbering plan”
EC	European Commission
ECC	Electronic Communications Committee
ENUM	Telephone Number Mapping
EU	European Union
HLR	Home Location Register
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU	International Telecommunication Union
ITU-T	ITU – Standardisation Sector
IVR	Interactive Voice Response
LCR	Least Cost Routing
MAP	Mobile Application Part
MCC	Mobile Country Code
MNC	Mobile Network Code
MNO	Mobile Network Operator
MSC	Mobile Switching Centre
MVNO	Mobile Virtual Network Operator
NAPTR	Name Authority Pointer

NGN	Next Generation Protocol
NRA	National Regulatory Authority
OI	Originating Identification
OTT	Over the Top
PBX	Private Branch eXchange
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PRI / PRA	Primary Rate Interface / Primary Rate Access
PSTN	Public Switched Telephone Network
SCCP	Signalling Connection Control Part
SIGTRAN	Signalling Transport
SIP	Session Initiation Protocol
SMS	Short Message Service
SMSC	SMS Centre
SS7	ITU-T Signalling System no. 7
URI	Uniform Resource Identifier
USD	Universal Service Directive
USSD	Unstructured Supplementary Service Data
VCC	Virtual Calling Card
VLR	Visitor Location Register
VoIP	Voice over IP
VoLTE	Voice over LTE (Long Term Evolution)

1 INTRODUCTION

For many years now, E.164 numbers have been used as Calling Line Identification (CLI) for identifying the originating calling party and for routing and terminating calls in the case of location-based voice services. The most universally used signalling protocol stack to carry CLI parameters was, and still is, the ITU-T Signalling System No. 7 (SS7) using several upper layer protocols including ISUP and MAP. In the SS7 protocols the originating E.164 number is mapped to the A-number and CLI parameter fields.

As the rollout of next generation networks (NGNs) and 4G mobile networks continues to gather momentum, standardisation bodies are adopting SIP as the main protocol to be used in voice-based electronic communications. In these new protocols the role of E.164 numbers has changed so that they can be used as names, addresses or other kinds of identifiers that can be converted, for sake of example, to IP addresses in order to route and terminate communications traffic. So even as new signalling systems (such as Diameter for VoLTE) are introduced, the CLI will continue to be relevant.

An increasing number of individuals and enterprises adopt services that use different network technologies and access paths. While the technologies may differ, the role of the E.164 number as an origination identifier remains critically important in order to identify a calling party and to return a missed call or communication. However, as the E.164 number may no longer be associated with a physical access path, using the CLI to validate the location of a calling party may no longer always be reliable. These developments do not apply to the use of numbers as connected line identification.

The transition from legacy networks has transferred intelligence to the network edge and more sophisticated end-user devices and applications have empowered end-users to make use of the CLI capability in an increasingly flexible way. This development, while broadly beneficial to calling parties, has created an environment where the inherent trust in CLI has been eroded and in some cases abused to perpetrate consumer harm through the manipulation of the E.164 number used as CLI.

This Report identifies several ways in which CLI may be used in an increasingly flexible way and examines the regulatory issues and current regulatory practices associated with each such type of use, including the need for validation mechanisms to restore and retain trust in CLI. The scope of this report is limited to the use of E.164 numbers as CLI and the various issues associated with this usage in modern day networks and applications.

The practice of some operators modifying or deleting the CLI in cases where there are differentiated wholesale termination charges depending on the origin of the call is not addressed in this Report.

2 DEFINITIONS

The terms defined below specifically relate to the use of these terms in this ECC Report.

Term	Definition
Bridge	Equipment with the facility within a service provider or carrier that connects two or more connections (legs) together and monitors the call session.
Callback	A call where the call originator sends a call request (e.g. via a normal telephone call, a smartphone app or through a USSD request) to an intermediary node. The intermediary node then calls the terminating number and the originating number and seamlessly connects both legs of the call. The called party will experience a normal call and the CLI of the originating caller may also be displayed.
Calling/Caller ID spoofing	A procedure that enables the calling party to manipulate the information displayed in the CLI field so that the called party thinks that the call originates from another person, entity or location.
Calling Line Identification Presentation	According to ITU-T Recommendation E.157, calling line identification presentation is a supplementary service offered to the called party which provides the calling party's number, with additional address information (e.g. calling party sub-address) if any, to the called party.
Connected Line Identification	Supplementary service where the network delivers the connected line identity to calling party on call acceptance regardless of terminal's ability to handle the information.
Dialler	An electronic device that is connected between a telephone line and terminal equipment to monitor dialled numbers and alter them to seamlessly provide services that otherwise require lengthy access codes to be dialled. A dialler automatically inserts and modifies the dialled numbers depending on conditional parameters such as time of day, country or area code dialled thereby allowing the user to avail of different services offering the most competitive rates.
Gateway	A technology that enables communication between networks that use different communications protocols (e.g. PSTN to/from IP).
On Top SIM or SIM Sticker	Electronic circuit slim board that is attached over the SIM card that includes an application to intercept the dialled digits in order to implement a dialler service or a callback service linked to a roaming or non–roaming scenario.
Roaming	A mobile communication originating or terminating on a visited network.
Proxy server	A server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service from a different server (e.g. SIP Proxy server).

3 COMMON SIGNALLING SYSTEMS AND SUPPLEMENTARY SERVICES

3.1 SIGNALLING SYSTEM NO. 7 (SS7)

The ITU-T Signalling System No. 7 (SS7) is a set of telephony signalling protocols which have been used for many decades in the public switched telephone network (PSTN) to set up and tear down telephone calls. SS7 is an “out-of-band” signalling system which means that the signalling information used to control the communications has its own dedicated data channels which are separate and distinct from the bearer channels used for the actual voice communications during a call. Over the years SS7 has been used effectively to provide additional functionality including number translation, number portability, prepaid billing, short message service (SMS), and the transmission of CLI information.

Supplementary services are provided in the upper layers (i.e. The User Part) of the SS7 protocol stack as illustrated in Figure 1:

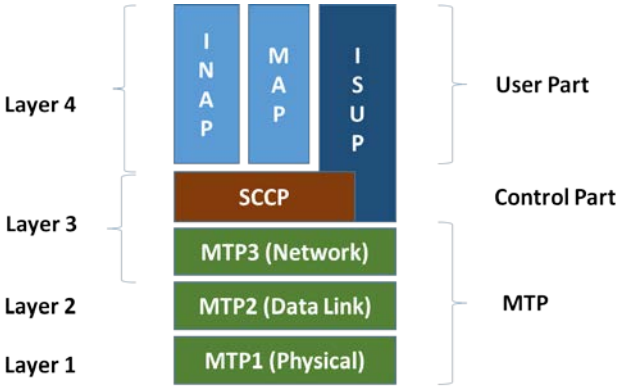

Figure 1: SS7 Protocol Stack

The ISDN User Part (ISUP) provides many messages and parameters that have been explicitly created for the support of supplementary services across the network. The introduction of ISUP has helped to greatly standardise widely used services and it has enabled interoperability across different networks provided by different vendors. ISUP provides the flexibility to accommodate these differences using a rich message set and a large set of optional parameters.

3.1.1 How Calling Line Identification (CLI) works in SS7

The ITU-T defines a core set of widely used ISDN services in the Q.730–Q.739 series of specifications using ISUP network signalling. This section provides an example as to how ISUP provides support for CLI.

Being able to identify the calling party allows the called party to make decisions before answering a call. For example, end-users can use the CLI to screen calls allowing them to choose which calls they wish to accept or a business might use the CLI to query a database for customer account information before a caller is connected to a call centre agent. Of course the CLI can be blocked and ITU-T Q.731.3 describes the terms Calling Line Identification Presentation (CLIP) and Q.731.4 describes Calling Line Identification Restriction (CLIR). ISUP contains parameters that, for each call, specify whether a calling party number should be presented or restricted. The number is delivered only if the value is set to presentation allowed. If the connection encounters non-SS7 interworking (i.e. where the call originates on a different network type or implementation) the address information may not be available for presentation. Furthermore if the call transits across one or more networks (e.g. an international call) the transit operator might not transport the information in some cases if it considers the source untrustworthy or if national regulatory policy prohibits the practice. While the actual display to the end-user varies depending on location, it is quite common to see restricted addresses displayed as "private", “unavailable” or “unknown”.

There are systems, such as ISDN that provide the calling party with the capability of choosing the CLI to be presented for a particular call. This is typically restricted to business users who have Private Branch Exchanges (PBXs) installed that are connected to the PSTN. In such cases, the public network operator may set down requirements concerning the CLI type or types that are permitted and/or may validate CLIs incoming from the PBX to ensure they comply with regulatory requirements.

3.2 SESSION INITIATION PROTOCOL (SIP)

In NGN networks, particularly in IMS systems, the signalling protocol used for end-to-end communication is SIP. Figure 2 describes one possible implementation of this stack (there are some applications that use UDP instead of TCP) in the protocol stack of SIP.

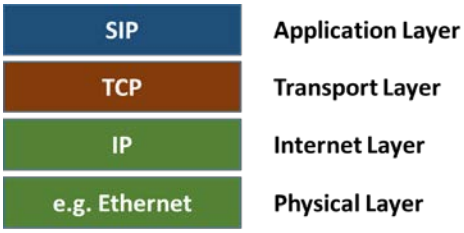

Figure 2: SIP Protocol Stack

Using SIP, the identification of the caller is also possible. SIP defines three different “header fields” for this purpose and a fourth related with privacy:

- The “From” header field contains the Originating Identification (OI) that the user wants to pass transparently through the network to the destination. This is comparable with a user-provided (i.e. a non-verified generic E.164 number) parameter in ISUP.
- The “P-Asserted-Identity” header field is designed to carry the network-provided identifier (in ISUP the corresponding parameter is the Calling-Party-Number parameter). This field should normally only be configurable by the originating service provider, but depending on the implementation, may be configurable also by the user and/or by intermediary service providers and, therefore, is not always reliable.
- The “P-Preferred-Identity” header field is designed to give to the user the possibility to input user-generated information. According to the relevant ETSI standard[2], the value input shall be checked by the network to see if it is one of a stored list of identifiers registered by the subscriber and authorised by the network. If the value is not in this list then it will be replaced by a default identifier.
- The “Privacy” header field gives users the possibility to restrict the presentation of their OI contained in the P-Asserted-Identity header.

As with SS7, supplementary services OI Presentation (OIP) and /OI Restriction (OIR) (equivalent to CLIP/CLIR) are also defined in the relevant ETSI standard.

3.3 INTERWORKING BETWEEN SS7 AND SIP

In heterogeneous networks, using ISUP (SS7) and SIP, there is a need to allow interworking of both protocols. A technical specification from ETSI[3] has standardised this specific interworking methodology. Figure 3 and Table 1 illustrate the mapping related with the identification of the caller between those protocols.

[2] ETSI TS 183 007 (v1.3.0 2008-01) - Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Protocol specification

[3] TS 129 163 (Interworking between the IP Multimedia Core Network),

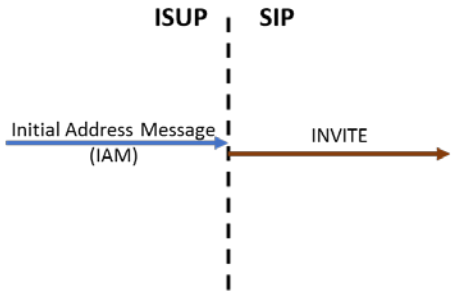

Figure 3: Interworking between ISUP and SIP

Table 1: CLI mapping between ISUP and SIP

ISUP protocol			SIP protocol		
Calling Party number parameter		Generic Number parameter (ACgPN)	P-Asserted-Identity header field	From header field	Privacy header field
Screening indicator	Address presentation restricted indicator	Address presentation restricted indicator			
UPVP or NP	PA	PA	Derived from address included in the CPN	Derived from address included in the GN	Not included
UPVP or NP	PR	PA	Derived from address included in the CPN	Derived from address included in the GN	Priv-value="id"
UPVP or NP	PA	-	Derived from address included in the CPN	SIP URI derived from address included in the CPN	Not included
UPVP or NP	PR	-	Derived from address included in the CPN	SIP URI with "*Anonymous*" address	Priv-value="id"
UPVP or NP	PA	PR	Derived from address included in the CPN	SIP URI derived from address included in the CPN	Not included
UPVP or NP	PR	PR	Derived from address included in the CPN	SIP URI with "*Anonymous*" address	Priv-value="id"
UPVF or UPNV	PA or PR	-	Not included	SIP URI with address "*Unavailable User Identity*"	Not included

Legend:

NP – Network provided
UPNV – User provided not validated
UPVF- User provided verified and failed
UPVP – User provide verified and passed
PA – Presentation allowed
PR – Presentation restricted
GN – Generic Number
CPN – Calling Party Number

3.4 TRUST IN CLI AND THE EXTENDED ELECTRONIC COMMUNICATIONS SUPPLY CHAIN

The origination, transit and presentation of CLI digits in the PSTN was traditionally the sole responsibility and custody of the network operators and the possibility of manipulating CLI digits was remote and required specialised equipment. This secure environment promoted trust in the CLI digits presented to end-users and the supply chain extended from the originating network, through a transit network if needed, to the terminating network.

The transition from legacy networks has transferred intelligence to the network edge and more sophisticated end-user devices and applications have empowered end-users with the ability to manipulate CLI digits thereby extending the supply chain well beyond the traditional players. This development, whilst providing some benefits to end-users in terms of increased flexibility, has its drawbacks and instances of consumer harm have occurred through fraudulent or misleading use of CLI. Such examples include call back services to high tariff numbers, unauthorised voicemail access and identity theft using fake CLI digits and use of numbers assigned to other parties (or use of unassigned numbers) as CLI, to facilitate malicious calls to emergency services, law enforcement and individual citizens. The extension of the supply chain has therefore resulted in an eroding of the inherent trust that existed in CLI.

As the supply chain has extended, the use of OI/CLI information has become largely based on trust. As calls pass country borders or break out from IP-based networks to the PSTN, the transiting and terminating operators have very little or no means to verify the authenticity of the parameters received and only the originating network (or entity/individual if user-provided) has knowledge of the CLI's authenticity.

ECC Report 133, published in 2009, analysed how the concept of Originating Identification (OI) provides users with capabilities similar to the CLI, but the OI extends the traditional CLI to new networks, such as NGNs which may use identifiers other than E.164 numbers. The Report provides 20 guidelines on how to increase trust in OI/CLI. The guidelines are useful for NRAs, operators and end-users.

Striking a balance between maintaining and increasing trust in CLI and facilitating flexibility and service innovation is a significant challenge for regulators. It should be noted that although some standardisation initiatives are taking place to provide additional security measures in future networks (such as within IETF-STIR – see sub-section 5.5) it is recommended that in critical applications meticulous security methods and validation techniques are used and all parties in the electronic communication supply chain should be required to follow the same principles. These principles should be based on international standards, regulations and guidelines. Chapter 5 provides further information on such validation techniques.

4 EXAMPLES OF CALL SCENARIOS WITH FLEXIBLE USE OF CLI

This section provides examples of the use of E.164 numbers as CLI by service providers other than those to whom a number range was assigned by the NRA. The scenarios described include cases where the access network of the calling party's own service provider is used (i.e. the service associated with the number to be provided as CLI) as well as cases where alternative access networks are used.

4.1 EXAMPLES USING THE ACCESS NETWORK OF THE CALLING PARTY'S OWN SERVICE PROVIDER – TWO-STAGE DIALLING

In a two-stage dialling scenario the calling party dials a number other than the destination number and an intermediate step takes place before connecting the call to the destination number. Two examples are provided in this section.

4.1.1 Virtual Calling Card Service

The call flow illustrated in Figure 4, describes the mechanism used by a virtual calling card service using a two-stage dialling process. In the first stage (or leg), the calling party dials an access number and the call is routed to a service platform. The calling party is then authenticated by the platform by the CLI digits or by inserting a PIN code. If the user has sufficient call credit the platform permits the user to enter the destination number. The second stage of the call then takes place where the destination number is dialled by the service platform and routed to the destination network. Both legs of the call are then connected and the CLI presented during the first leg of the call is also presented to the called party during the second leg of the call.

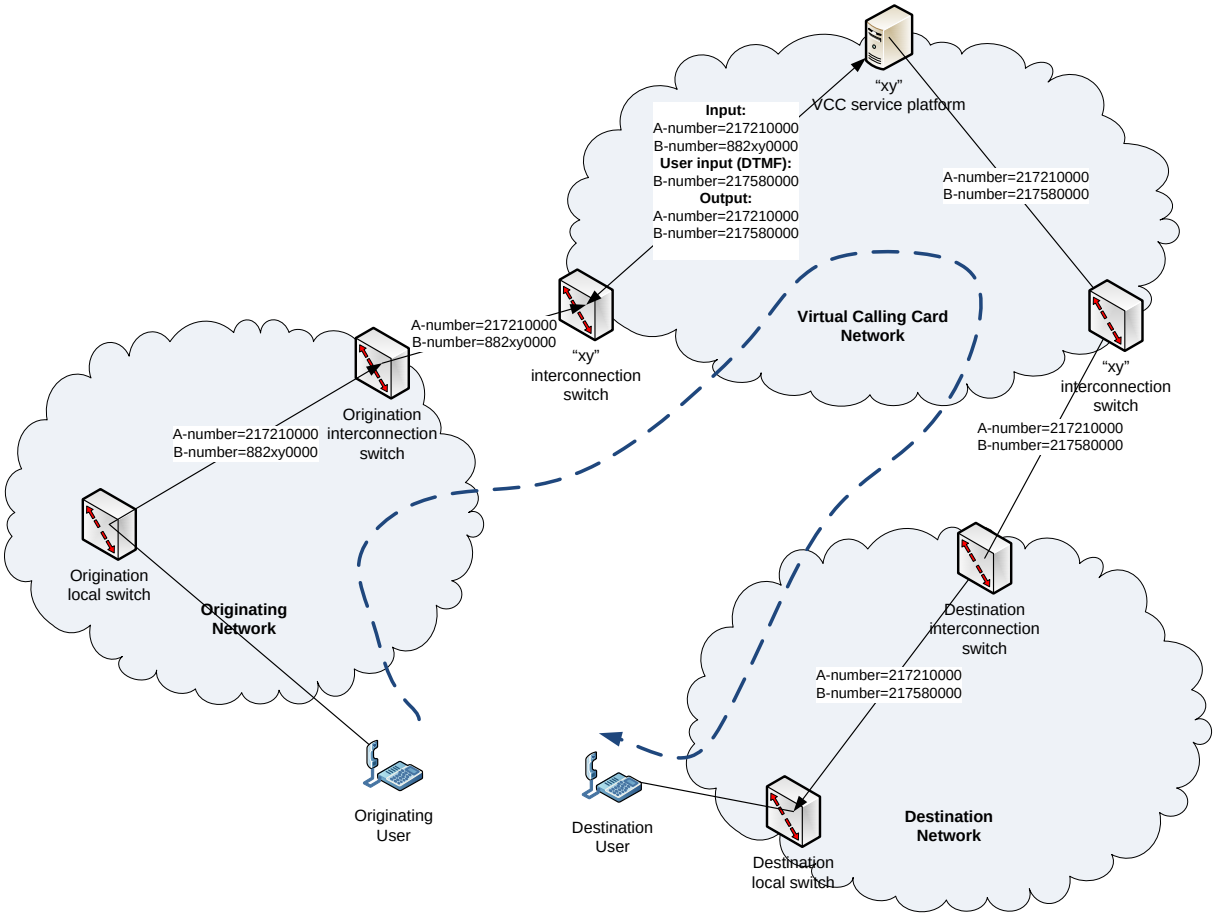

Figure 4: Virtual Calling Card service call establishment

4.1.2 On Top SIM / SIM Stickers

On Top SIM or SIM Stickers enable customers who wish to make international calls, even when roaming, from their mobile devices independent of the subscription they have with their mobile service provider. The service is activated by placing a foil chip on top of the existing SIM card. The SIM card is then reinserted into the phone and turned on. There is no visible difference to the user's existing service. When an international call is made the SIM Sticker intercepts the dialled digits and then dials the number of its own PSTN/IP Gateway Call Server. After establishing the connection with the Call Server, the initial dialled number is used to establish the connection to the destination user.

In order to achieve lower call prices on international calls to its customers, the SIM Sticker service provider will have most of the termination fees as national (instead of international), due to the fact that the international part of the connection is made mainly via the Internet and then breaks out locally in the destination country. The service provider can have its own international gateways or has an agreement with another carrier that uses the Internet as the international backbone for the communications.

The CLI presented when the SIM Sticker service is used is the number associated with the calling party's mobile subscription. So even if an alternative service provider is used for international calls the calling party has rights of use for the number displayed as CLI.

Figures 5, 6 and 7 illustrate how SIM Stickers work for:

1. International calls in a non-roaming scenario;
2. International calls in a roaming scenario with Callback.

4.1.2.1 International calls in a non-roaming scenario

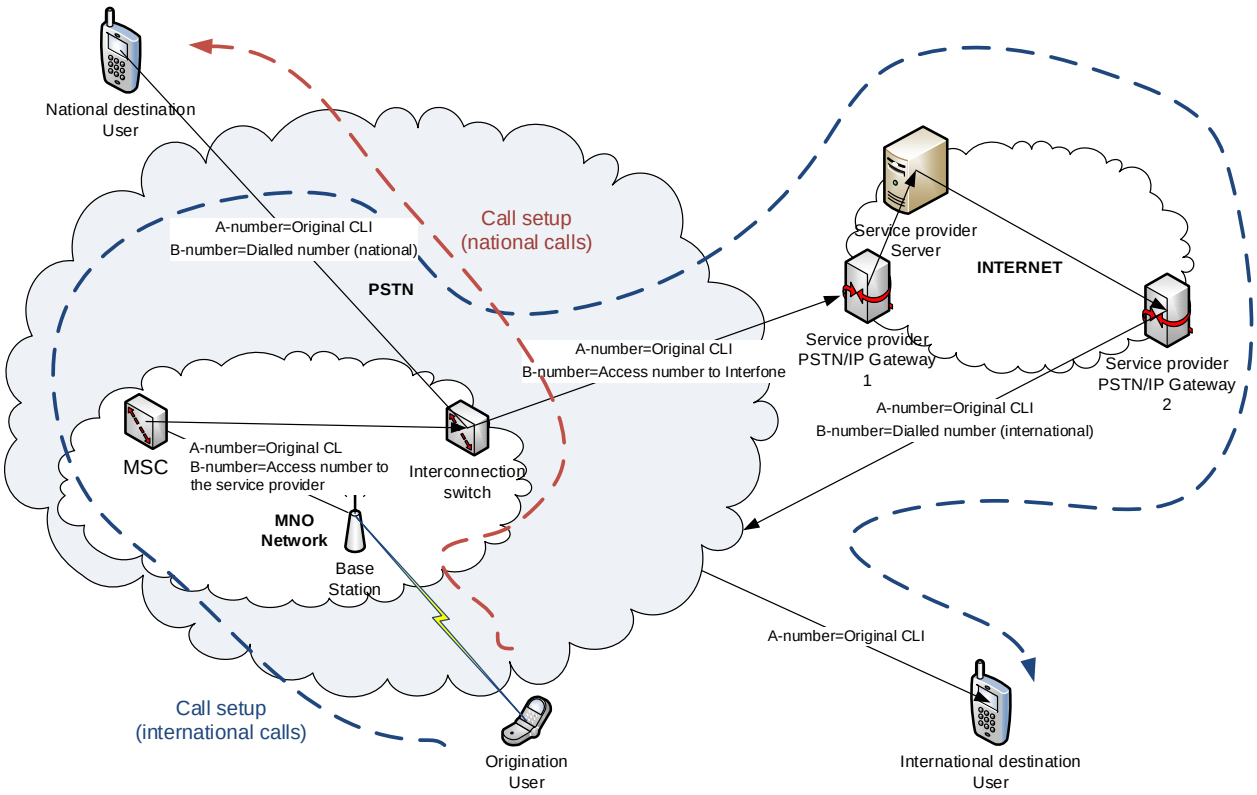

Figure 5: International call in a non-roaming scenario

- National setup call (red call flow)

- The service does not have an impact on this type of call. The calling party uses his existing mobile subscription to make the call.

- International setup call (blue call flow)

- The application that is in the SIM Sticker saves the dialled international number and dials the access number of the service provider platform (a local number);
- The mobile operator routes the call according with the number dialled by the application;
- The service provider platform validates the CLI (i.e. verifies if the CLI is associated with a customer of the SIM Sticker service provider) and collects the original dialled number by the user from the SIM Sticker and establishes a new communications leg to the destination number;
- Both legs of the call are connected in order to establish the communication between the calling party and the called party. The CLI in the second leg is, despite an independent connection/call, the original CLI from the first leg. All connections are performed in one step. For the user there is no significant delay by inserting the service provider node and for the automatic authentication procedure of the user.

4.1.2.2 International call in a roaming scenario with Callback

In this scenario the callback procedure is used.

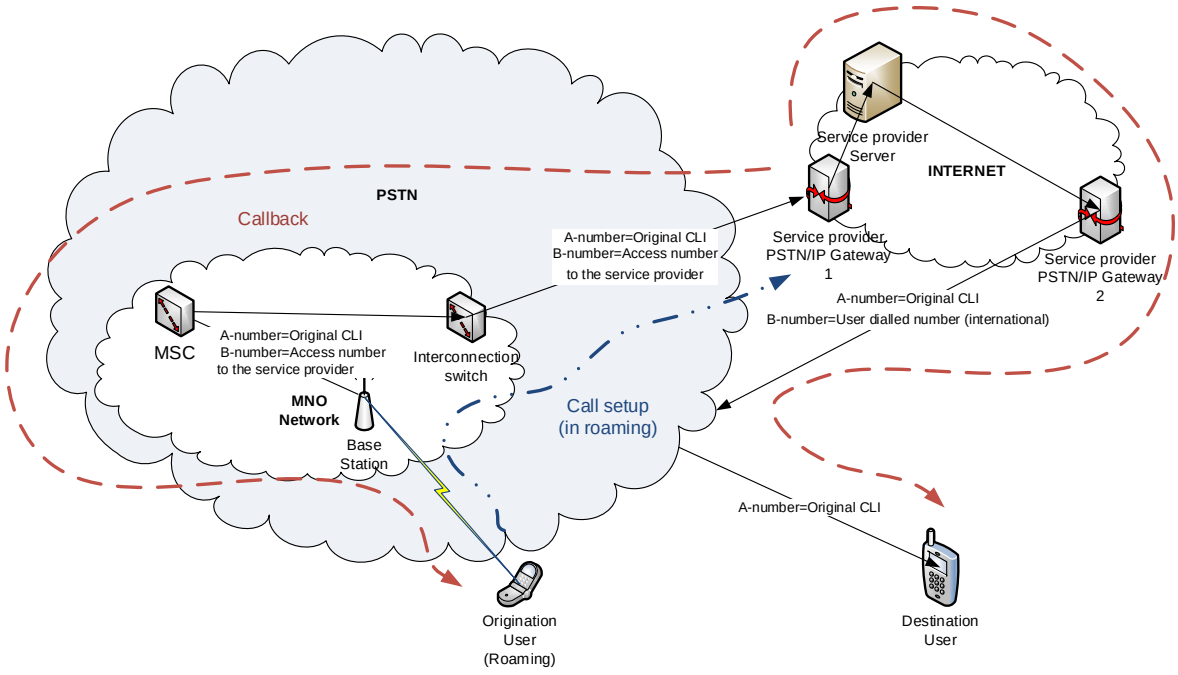

Figure 6: International call in a roaming scenario with Callback

Establishing a call in a roaming situation (1 and 2 is the blue call flow; 3 to 5 is the red call flow):

- The user dials any number when in roaming;
- The application that is in the SIM Sticker saves the dialled number and dials the access number of the service provider's platform;
- After receiving the CLI (setup phase), the platform releases the call and makes a return call to the calling party. In other words, it initiates a new call toward the user terminal (using the CLI – that was authenticated by the platform as a customer);

- After collecting the number dialled by the calling party, the SIM Sticker service provider's platform initiates a second leg to the destination number;
- After successfully establishing communications, the two legs are connected and communication between the calling party and the called party is possible. The CLI from the first leg of the call is presented to the called party in the second leg.

In order to clarify the model and also the market value, Figure 7 shows a hypothetical network spread over a few countries, using the Internet as the core for international interconnections.

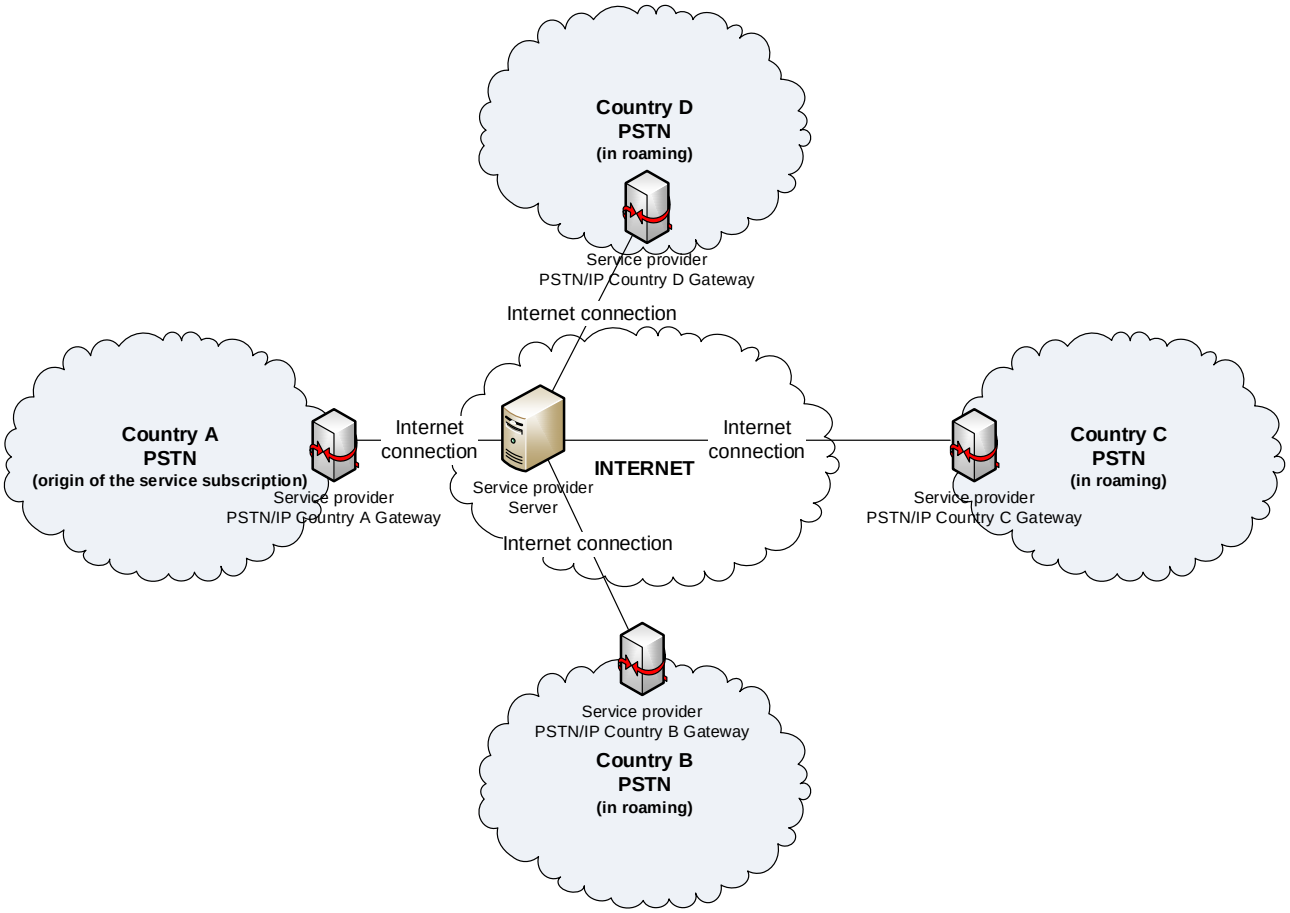

Figure 7: International call in a roaming scenario with Callback (multi-country)

4.2 EXAMPLES USING ALTERNATIVE ACCESS NETWORKS

This section describes use cases where an alternative access network is used. The use cases described in this section may not be allowed in some CEPT countries while in others it may be subject to regulatory approval on a case-by-case basis.

4.2.1 A PBX or ACD with services obtained from competing service providers using different PSTN access networks

A good example of this type of configuration is where a call centre operation contracts different services for inbound and outbound calling using different PSTN access networks. When a customer contracts two (or more) different operators to provide connectivity to its PBX or ACD each service will have an E.164 number (or number range) associated with it. In order to attract calls on the inbound service the CLI presented with outbound calls needs to be the same as that associated with the inbound service rather than the actual CLI associated with the line in use for the outbound call. Regulators often allow this type of arrangement on a case-by-case approval basis mainly because the subscriber has the rights of use for the number. Other examples also exist where the same number is used as CLI in both (all) connections from the PBX

independently of the access network used provided the service providers and the regulator support and agree with the approach. Figure 8 illustrates this scenario in an ISDN environment but this scenario could also be extended using a mobile access network for certain calls.

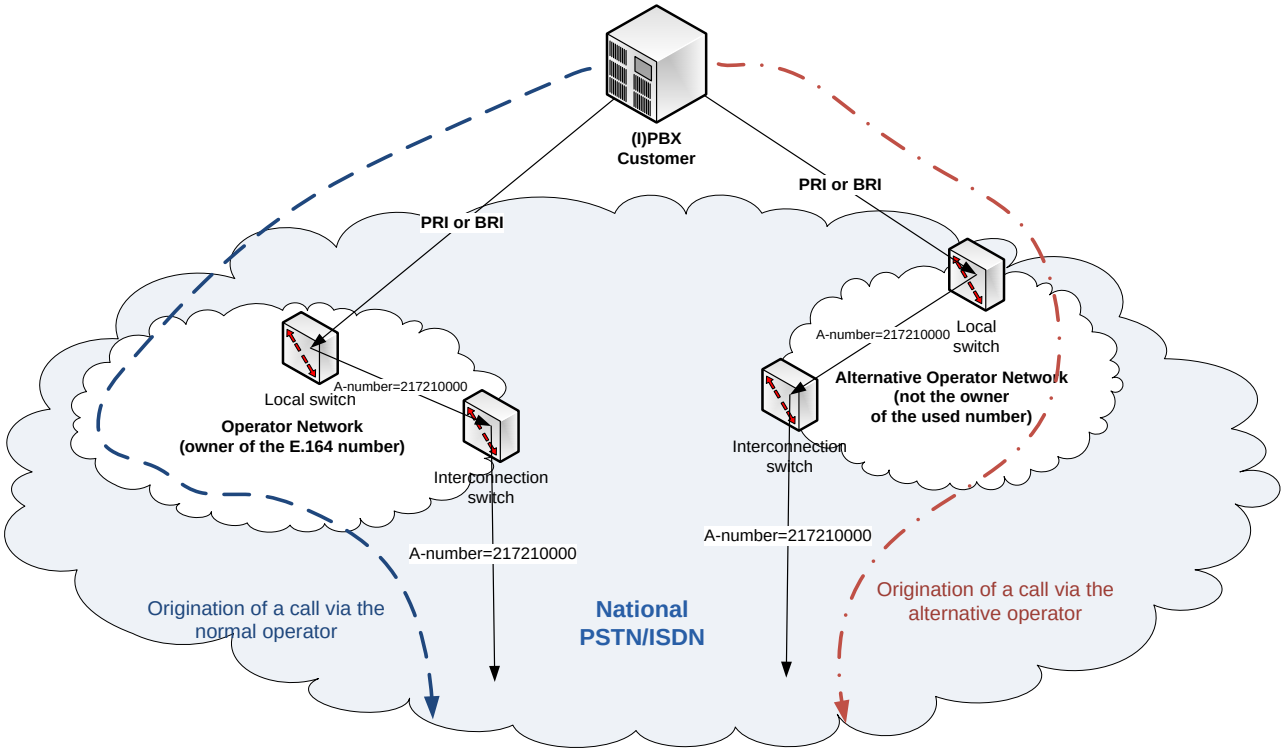

Figure 8: User equipment using two different PSTN/ISDN accesses

Figure 8: shows two different call flows:

- In **blue**: A normal call origination, using the access (PRI) from the owner of the DDI number;
- In **red**: An alternative call flow, using a second PRI of another operator. In this case the operator has programmed the access with the (same) number of the original operator i.e. using a number that was not assigned to him.

The two different accesses can be chosen, for example, based on a Least-Cost Routing (LCR) option programmed in the PBX. The same CLI is used in both cases.

This example could be also extended to cover a scenario where an end-user has two or more subscriptions (mobile or fixed) and wishes to use an E.164 number associated with one subscription as CLI in calls originating from another subscription. In this scenario the end-user has rights of use to the E.164 number associated with each subscription.

4.2.2 An IP-PBX with PSTN and Broadband Access

This type of set-up is becoming more common for business and some residential customers. The equipment is connected using two different access technologies i.e. broadband and PSTN and typically the number associated with the PSTN access is presented as CLI for all calls. Figures 9 and 10 below illustrate different implementations of this approach.

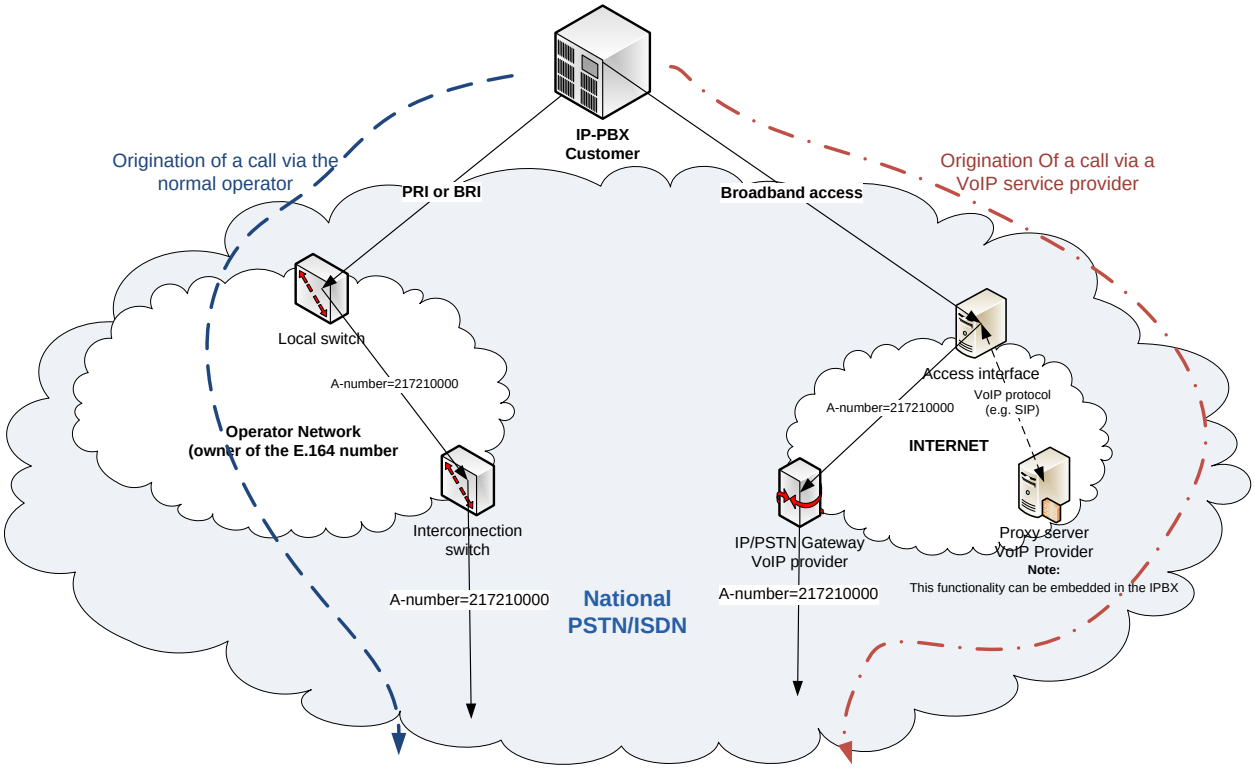

Figure 9: User equipment using an alternative IP access

Figure 9 shows two different call flows:

- In **blue**: A normal call origination, using the access (PRI) from the owner of the DDI number;
- In **red**: An alternative call flow, using the broadband access. In this case the user and/or the VoIP service provider has programmed the VoIP subscription with the same number as the original operator, using a number assigned to the user but to a different service and/or service provider.

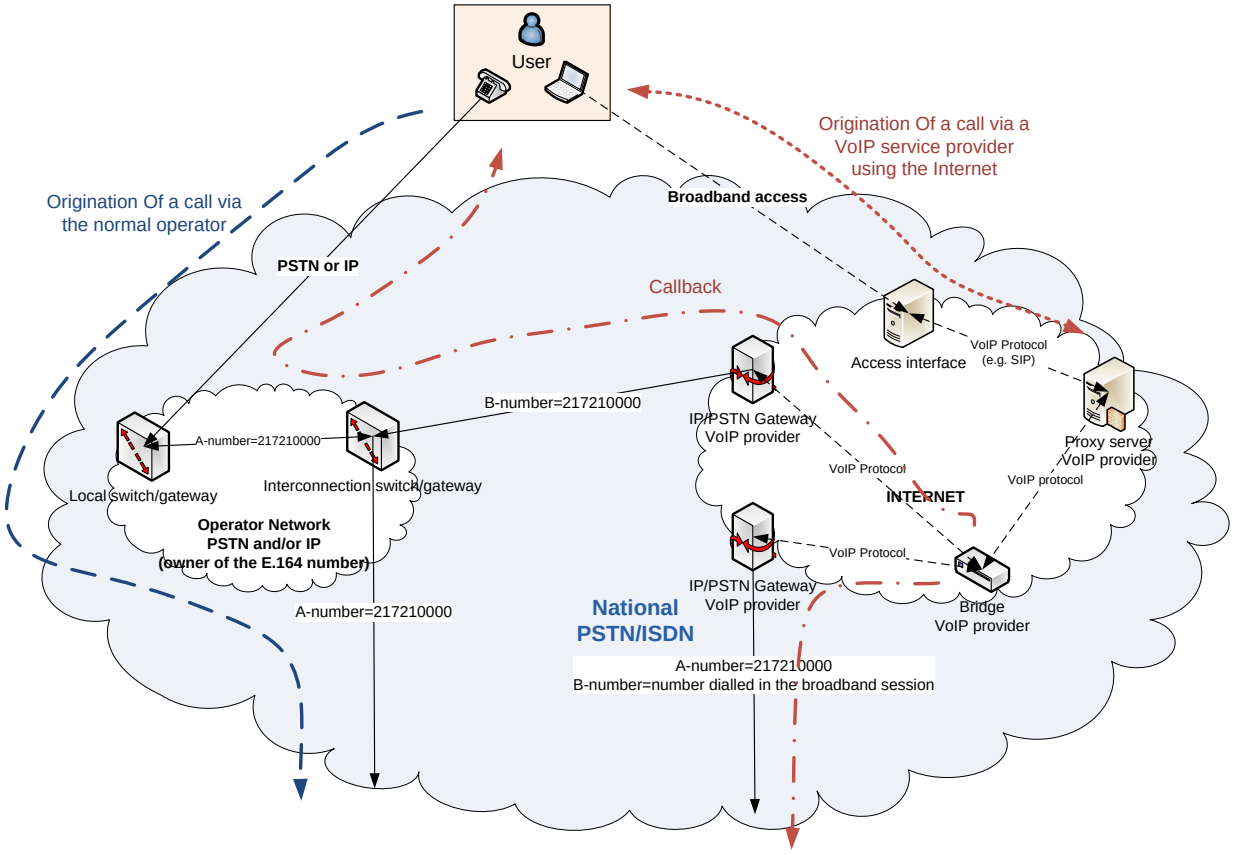

Figure 10: VoIP service provider using two different connection legs

The Figure 10 shows for the same scenario a different implementation approach:

- In **blue**: A normal call origination, using the access from the owner of the number;
- In **red**: An alternative call flow, using the broadband access. In this case the user and/or the VoIP service provider has programmed the VoIP subscription with the (same) number of the original operator, using a number assigned to the user but to a different service and/or service provider. The call flow is composed by two different communication legs:

1. Using the broadband access, the user establishes the communication login into the VoIP provider's application and sends the destination address information (Call control);
2. After validation of the profile of the user (e.g. credit) the VoIP service provider starts a communication leg from its network to the user's PSTN (or alternatively, its IP connection) access;
3. After the user answers, the VoIP service provider establishes the second communication leg to the destination address and, through special equipment (bridge), connects both communication legs.

In this example call control and media transportation is split into two different types of connections: the call control which uses the broadband access and the actual traffic which is transported through the Internet and terminated/originated in the PSTN accesses.

This scenario could be also extended to cover mobile connections.

4.2.3 Example of an independent SMS service provider

The use of mobile numbers (from the user) for identifying a SMS (as a CLI) is more and more used by SMS service providers or even by the mobile operator responsible for the number.

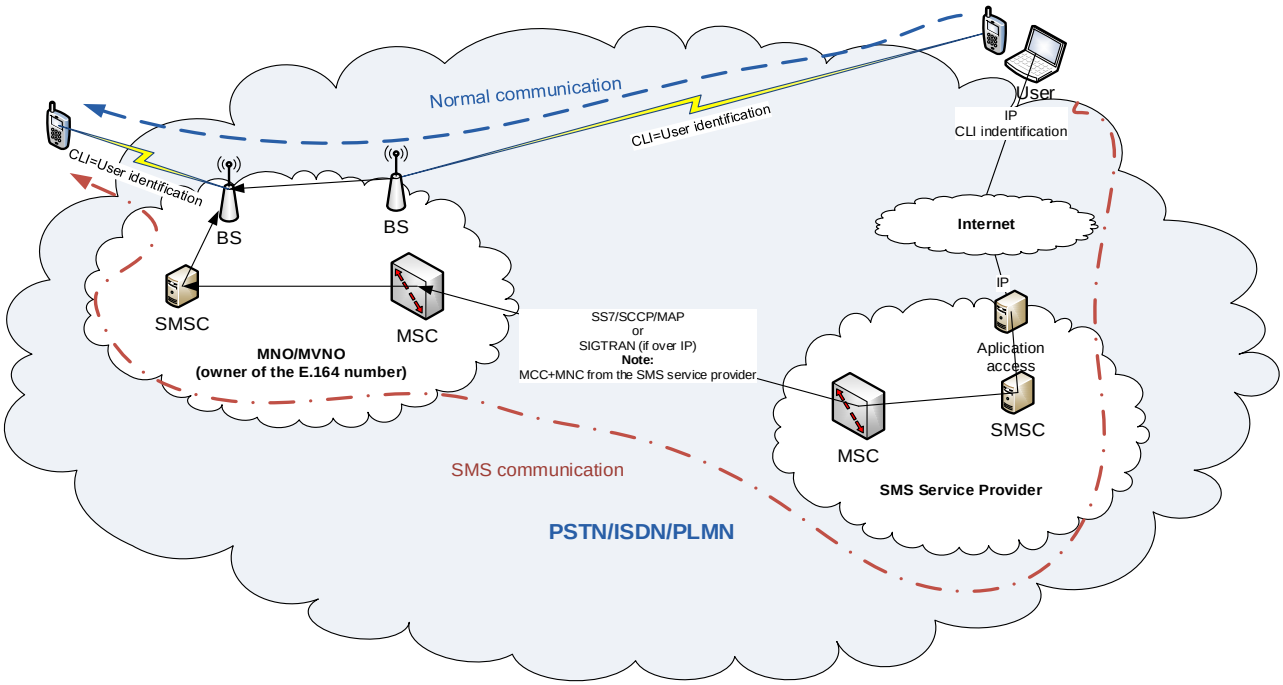

Figure 11: Scenario of an independent SMS service provider

The Figure 11 shows two different call flows:

- In **blue**: A normal communication, using the network related with the mobile subscription. Sending a SMS from the mobile device (through the radio interface) will have a similar communication flow;
- In **red**: An alternative call flow, using an independent SMS service provider. The Internet access can be used by the user to send a SMS;
- In both communication flows, the same CLI is used to identify the originating user.

4.2.4 Example of a Dual IMSI solution using the same E.164 number as CLI

The technique of Dual IMSI allows a mobile operator to take advantage of roaming agreements of another mobile operator. Typical case is when a small mobile operator (operator A) makes an agreement with another mobile operator (operator B) in order to use the roaming agreements of operator B when operator A's users are abroad. The two operators could be either of the same country or of two different countries.

This technique corresponds to having two IMSI numbers on the same SIM. Only one E.164 number is associated with the two IMSI numbers. This number is provided by operator A. Depending on the scenario, only one out of the two IMSI numbers is active at any time.

One of the IMSI (IMSI1) belongs to operator A and the other (IMSI2) belongs to operator B. Operator B reserves a sub range of its IMSI number space to be used in the service. In a roaming scenario, the visited network will only see the IMSI number that is active.

The following table shows which IMSI is active depending on where the SIM is, namely in which country. The table refers to the case where the two operators belong to two different countries. In case both operators belong to the same country the line referring to "Operator B country" is not present.

Table 2: Dual IMSI solution with the same E.164 number

Country	Active IMSI
Operator A country	IMSI 1 (Operator A)
Operator B country	IMSI 1 (Operator A)
Other countries	IMSI 2 (Operator B)

So, considering the CLI is always the same, there will be situations (see last row) in which from the roaming agreement in the other country it seems that the SIM belongs to operator B, while the serving operator is operator A. In other words, at first view (without considering the agreement between operator A and B) it seems that the CLI refers to one operator while the IMSI number is of another operator.

The use of the dual IMSI technique has an impact on the registration phase of the SIM. In the following figure, the three situations of the previous table are considered.

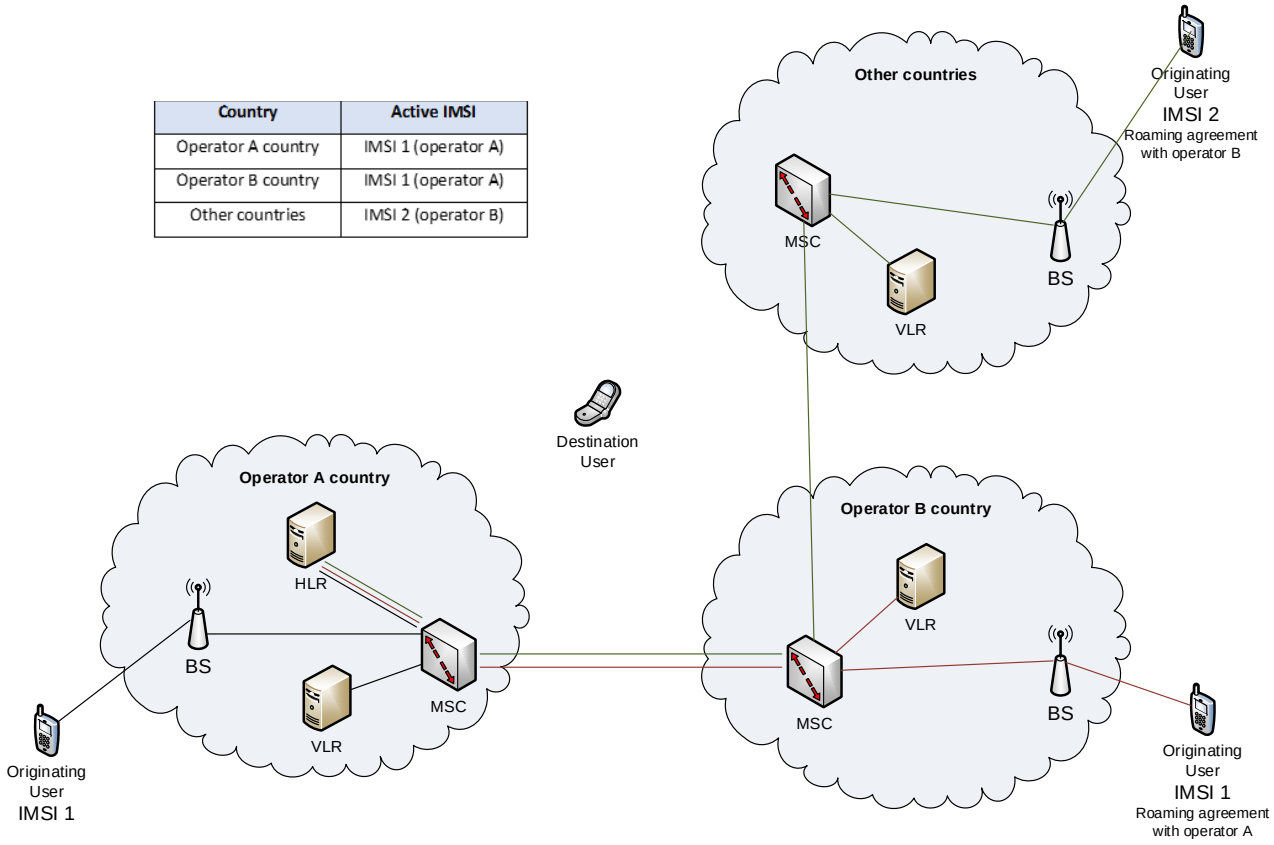

Figure 12: Scenario of Dual IMSI solution (Registration phase)

In Figure 12, the main involved network elements are shown. When the SIM is in the operator A country, the normal registration takes place (black lines). In case, the SIM is in the operator B country, the SIM is registered on the basis of the normal international roaming agreement between operator A and B (red lines). In case the SIM is in a country different from the operator A country and operator B country, from the point of

view of the operator in this last country, the usual international roaming agreement with the operator B takes place (green lines). Actually, when the signalling arrives to operator B, it could be transferred to operator A, since the real HLR is of the operator A. The real implementation could depend on the agreements between the two operators.

In the following figure, the call set-up phase is shown. The dashed line refers to signalling and the continuous line to the connection established.

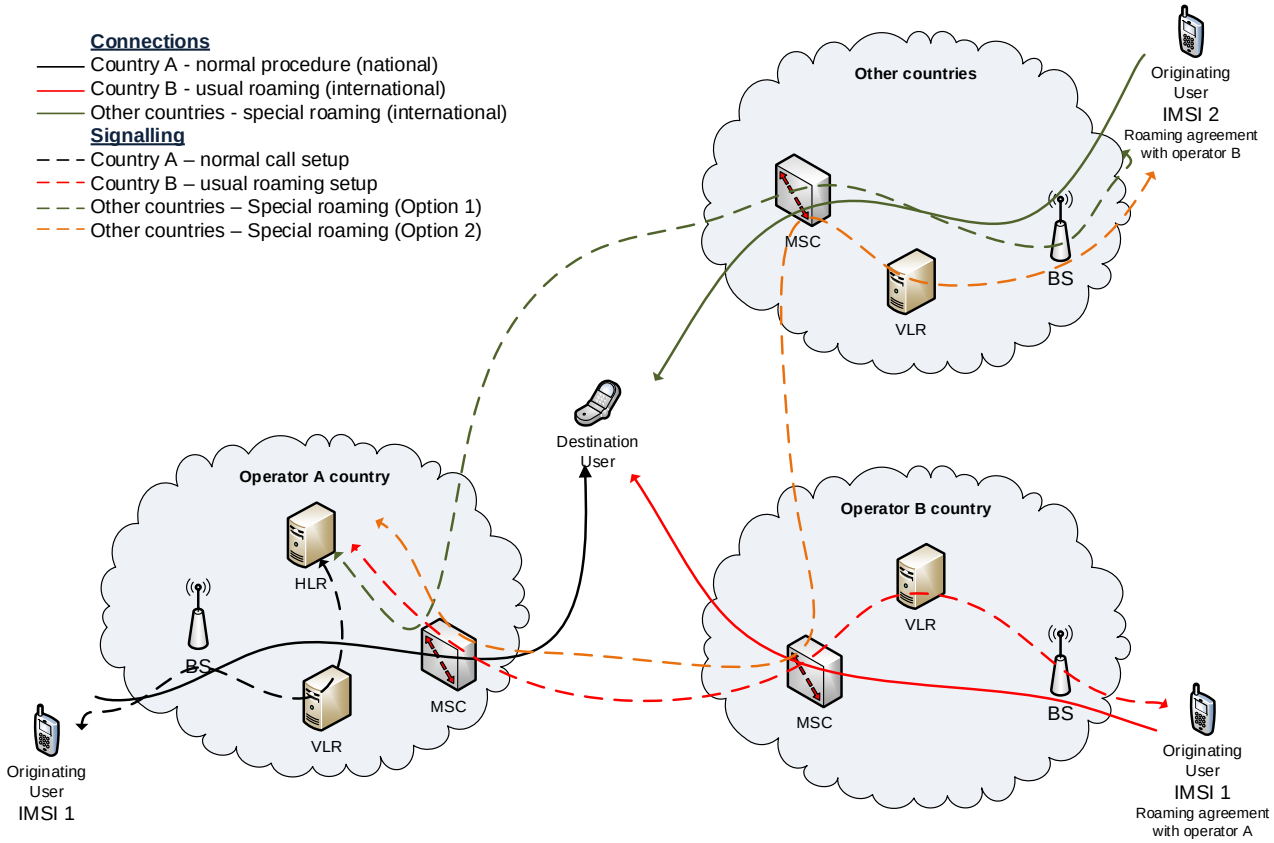

Figure 13: Scenario of Dual IMSI solution (Call Set-up phase)

In case the SIM is in the operator A country the normal set-up procedure takes place (black lines). In case the SIM is in the operator B country, the usual set-up procedure for international roaming agreement takes place (red lines). In case the SIM is in any other country, two possible signalling paths could take place depending on the agreements between operator A and operator B. In particular, in case the HLR of operator A is registered in the VLR, the signalling follows the green line. Otherwise, if the HLR of operator B is registered in the VLR, signalling follows the path of the orange line.

4.3 USING ALPHANUMERIC IDENTIFICATION FOR SMS

Using an alphanumeric string as the CLI for SMS/MMS services is technically possible and has been foreseen by the 3GPP standards, but could create a conflict of trust for the recipient unless there is a guide or a regulation that specifies rules for the use of this type of identification.

One of the most important characteristics of CLI is that it should identify the sender and be reliable.

An ECC questionnaire circulated during 2013 indicated that alphanumeric identification is not allowed or regulated, but in practice, it is used in most of the countries that answered the questionnaire.

In Italy, a first framework regulation has been published[4] for trialing rules on using alphanumeric strings as identifier for SMS/MMS calling parties (CLI).Only business users have the right to use Alphanumeric CLI (called Alias). A business user can ask to send SMS with its Aliases with more than one SMS service provider. The SMS service provider could be a mobile operator (including virtual ones) or any other entity that has a general authorisation.

The use of alphanumeric strings as CLI should help to increase end-user's confidence in origin identifiers. In order to maintain confidence in aliases, AGCOM considered it important that, in case of doubts, the following services are provided:

1. Information to end-users about who is using the specific alias;
2. Traceability of the real sender (traceability has to be guaranteed independently from what is written in the CLI field).

In order to accomplish the first item, the SMS service provider must register Aliases in a directory handled by the Italian NRA (AGCOM) before using them. The registration is in real time, namely the service provider immediately receives confirmation or rejection of the registration. Possible rejections could occur in case at least one field is empty or in the wrong format.

The mobile service provider can access AGCOM's directory to seek information about the users of a single Alias. A single user that receives a SMS with an Alias may ask the customer care of his own mobile service provider for information about the sender, including possible contact points.

More than one business user may use the same Alias, even if the general rule is that the Alias identifies the business user or its goods/services, and the regulation on brands has to be respected.

[4] Deliberation No. 42/13/CIR of June 2013

5 TYPES OF CLI VALIDATION AND RULES

The common situation is that an end-user has a contract for a service with an electronic communications service provider and is granted rights of use to a number with that service or access path. When an end-user wishes to use that number as CLI with another service provider, special validation procedures exist to ensure that the end-user has rights of use to that number. It is possible to categorize three different types of validations:

- Automatic validation;
- Manual validation;
- Alphanumeric identification.

5.1 AUTOMATIC VALIDATION

This is the most common practice by VoIP or SMS service providers. The following techniques are used:

- After a user signals that it intends to use a mobile number registered with the service provider, a code is sent by the service platform to the user's number by SMS. The user, after receiving the SMS, shall insert the received code in the validation field of the indicated number. The user is only allowed to use the mobile number as identification in the new application once this procedure is complete.
- For geographic numbers, this procedure is slightly modified. Instead of sending a SMS, the application generates an automatic voice call to the indicated geographic number and once the call is answered, an IVR (Interactive Voice Response) generates a code that the user shall enter in the validation field for the indicated number. The user is then able to use the geographic number as identification in the new application.

5.2 MANUAL VALIDATION

Manual validation is less used, because it increases the administrative burden of the validation process, risking human errors and/or mistakes. However, the right of the user may be validated in a more legal form, since it is possible to evaluate, via written documents, the subscription of the customer and the related numbers associated with the subscription. Some examples of documents that support validation are:

- Contract of the service provider who has originally been assigned the number;
- Invoice/Receipt from the subscription, with indication of the number assigned;
- Identification of the subscriber.

This procedure is often used for non-geographic numbers, since those numbers do not normally terminate in a user's equipment, as they are usually translation numbers.

5.3 ALPHANUMERIC IDENTIFICATION

When alphanumeric identification is used as CLI (e.g. in an SMS service) the following criteria could be considered:

- Alias identifies the business user or its goods/services;
- Alias that identifies (or is similar to) a public entity or an institution is reserved for potential use by that entity;
- Alias cannot be a number, in order to not be confused with a normal E.164 number;
- Alias must respect the regulation on brands;
- Utmost diligence must be used in assigning Aliases
- Alias should be traceable, allowing the identification of the SMS sender.

- Alpha-numeric character strings shall be limited to 11 characters in accordance with the relevant ETSI/3GPP standard[5].

For service providers, it is also convenient to maintain a database of all aliases with their associated information about the Alias business users, in order to support identification.

Also considering brands, the same Alias could be used by more than one business user.

Moreover, in order to increase competition, the business users can seek clearance to send SMSs with their own Alias or Aliases to more than one SMS service provider. Since each SMS service provider has to register Aliases that it handles, the same Alias of a specific business user may be used in several entries.

5.4 SUMMARY

The following table summarizes the pros and cons of the methodologies identified for the validation procedure described in the previous sections:

Table 3: Pros and Cons of Validation methods

Method		Pros	Cons
Automatic validation	Sending of a code via a SMS	• Simple procedure with an easy implementation process; • Procedure already used in validation procedures for number portability (e.g. sending the Porting Code); • It is reliable for most subscriptions.	• In the case of a corporate subscription, the user is not the owner of the number. • This restriction is also applicable for normal number portability.
	Sending of a code via a voice call	• Simple procedure with an easy implementation process. • It is reliable for some types of subscriptions.	• With fixed line telephony, there is no guarantee that the person initiating the authentication request and answering the call is the actual subscriber (e.g. in a corporate network with DDI).

[5] ETSI TS 123 040 (Technical realization of Short Message Service)

Method		Pros	Cons
Manual validation	Through documentation	• Very reliable procedure for all types of subscriptions.	• Complex procedure with a heavy administrative implementation process. • It increases the administrative burden of the validation process. • It allows human errors and/or mistakes.
Alphanumeric identification rules	Based on a database registry (could be unique, per authorized provider or could be multiple registries within the same provider)	• It will allow users to verify the origin of SMS identified by alphanumeric characters.	• May be possible that the same name identifies different entities • Limited to a maximum of 11 characters

In cases there is no control or validation, contractual requirements may be necessary between the customer and the service provider to prevent unauthorised use of telephone numbers as CLI.

5.5 POSSIBLE FUTURE VALIDATION TECHNIQUES FOR END-TO-END SIP CALLS

The Internet Engineering Task Force (IETF), through its working group Secure Telephone Identity Revisited (STIR), is studying a mechanism that will specify a SIP header-based mechanism for verification that the originator of a SIP session is authorized to use the claimed source telephone number, where the session is established with SIP end-to-end. This is called an in-band mechanism. The mechanism will use a canonical telephone number representation specified by the working group, including any mappings that might be needed between the SIP header fields and the canonical telephone number representation. The working group will consider choices for protecting identity information and credentials used. This protection will likely be based on a digital signature mechanism that covers a set of information in the SIP header fields, and verification will employ a credential that contains the public key that is associated with one or more telephone numbers. Credentials used with this mechanism will be derived from existing telephone number assignment and delegation models. That is, when a telephone number or range of telephone numbers is delegated to an entity, relevant credentials will be generated (or modified) to reflect such delegation. The mechanism must allow a telephone number holder to further delegate and revoke use of a telephone number without compromising the global delegation scheme.

Figure 14 describes in a simple way the proposed mechanism.

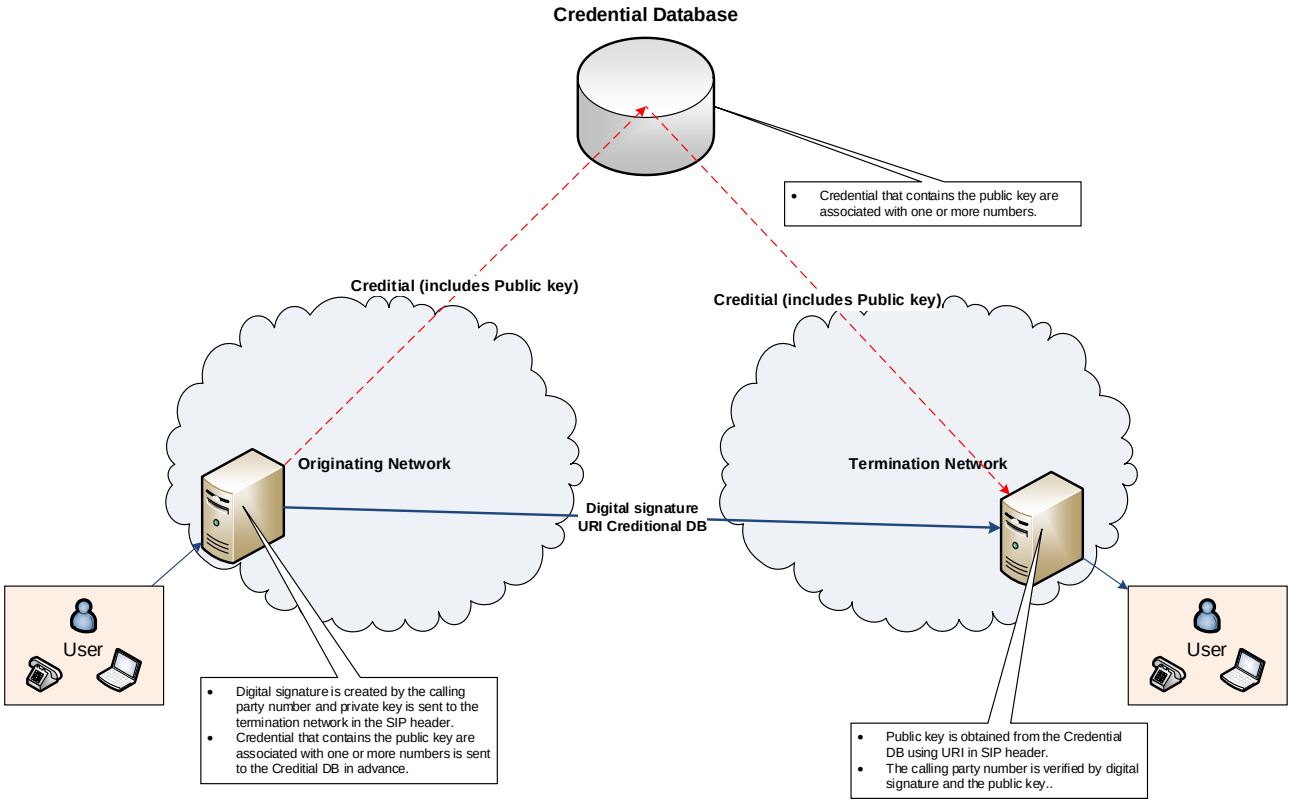

Figure 14: Proposed STIR in-band mechanism

This methodology will only be possible in the IP networks (e.g. Internet).

6 LEGAL ANALYSIS ON THE USE OF THE CLI

6.1 EUROPEAN REGULATORY FRAMEWORK

According to the Universal Service Directive[6] (USD) NRAs may require all providers of publicly available telephone services and/or providers of access to public communications networks to make available to end-users a CLI facility (art. 29 and Annex 1, part B in the USD) where the calling party's number is presented to the called party prior to the call being established. However, this obligation is subject to technical feasibility and economic viability. The provision does not give strong obligations, given that it is easy to argue technical or economic challenges. However, CLI facilities are normally available on modern telephone exchanges and can therefore increasingly be provided at little or no expense. If the facility is already available, the NRA is not required to impose obligations to provide this facility.

The use of a number as CLI should be seen as use of a number in relation to the European Framework. The CLI facility should be provided in accordance with relevant legislation on protection of personal data and privacy, in particular Directive 2002/58/EC[7] (the "e-Privacy Directive").

If it is technically feasible, operators should provide data and signals to facilitate the offering of CLI across Member State boundaries.

Most of the obligations stated in the USD and the e-Privacy Directive can be mapped into supplementary services. The following table shows the relevant articles mapped to the correspondent supplementary service.

Table 4: Mapping of the Directive obligation and service functionalities

Directive / Article	Functionality / Supplementary service
Directive 2002/22/CE Article 29 – 1 Annex I – part B – (b)	CLIP activation (*Calling Line Identification Presentation*)
Directive 2002/58/CE Article 8 – 1	CLIR activation (*Calling Line Identification Restriction*)
Directive 2002/58/CE Article 8 – 2	CLIP deactivation
Directive 2002/58/CE Article 8 – 3	ACR activation (*Anonymous Call Rejection*)
Directive 2002/58/CE Article 8 – 4	COLR activation (*Connected Line Identification Restriction*)
Directive 2002/58/CE Article 10 – (a)	MCID activation (*Malicious Call Identification* - in the called line*)*
Directive 2002/58/CE Article 10 – (b)	CLIR override activation *(Calling Line Identification Restriction override)*

[6] Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services as amended by Directive 2009/136/EC.

[7] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector as amended by Directive 2009/136/EC.

Directive / Article	Functionality / Supplementary service
Directive 2002/58/CE Article 11	ICB-CF activation (*Incoming Call Barring on Call Forwarding*)

End-users have the right to place anonymous calls. This is necessary to protect the anonymity of the calling party. Therefore the e-Privacy Directive states that the CLI facility should be possible to turn off on a per-call or per-line (subscription) basis. In particular help lines and similar organisations, have an interest in guaranteeing the anonymity of their callers. The possibility for the calling end-user to place anonymous calls should be offered using a simple means and free of charge.

However, in some cases the end-users' right to privacy with regard to CLI presentation may be restricted. In some cases operators may override the calling end-users restriction of the presentation of CLI. According to the e-Privacy Directive this may be justified on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls, and on a per-line basis for entities dealing with emergency calls, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls and allowing emergency services to carry out their tasks as effectively as possible.

According to the e-Privacy Directive the receiving end-user should also be able to prevent CLI presentation of incoming calls. This possibility should be offered using a simple means and free of charge for reasonable use of this function.

It is also necessary to protect the right of the called end-user to reject calls from unidentified or anonymous callers. Therefore the called end-user should have the opportunity to use an Anonymous Call Rejection (ACR) facility where the presentation of the CLI has been restricted by the calling end-user. ACR enables the called end-user to “automatically” reject incoming calls from end-users who have restricted the presentation of their CLI. However, this facility is in many countries considered not economically or technically feasible in mobile networks[8]. The possibility to place anonymous calls should also apply to calls to third countries originating in the EU as well as the possibility to reject anonymous calls originating in third countries.

The e-Privacy Directive also states that end-users should have the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the end-user’s terminal. The reason is to protect end-users from nuisance which may be caused by automatic call forwarding by others.

6.2 FRAMEWORK FOR NUMBER ALLOCATION/ASSIGNMENT

The international E.164 numbering plan is administrated by the ITU-T. It is segmented into a geographical component (characterised by country codes) and non-geographical components. The ITU operates under an International Treaty and the relations between the ITU and countries are covered by the ITU’s constitution and conventions.

In the E.164 numbering plan every country recognised by the United Nations is assigned a country code which is unique for that particular country[9]. Based on the subsidiarity principle, every country may, provided that the basic framework of the rules contained in E.164 is respected, define the national rules for administering the numbering plan under the assigned country code.

The way the ITU and its Member States have organised the E.164 numbering plan implies that the national E.164 numbering plan and associated numbering resources are considered to be national resources.

[8] The ECC Report 77 – Implementation of ACR supplementary service (March 2006) shows more information and details about the European implementation of this functionality. Link: http://www.erodocdb.dk/doks/filedownload.aspx?fileid=3216&fileurl=http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP077.PDF

[9] Shared Country Codes are the exception (e.g. Country Code “1”)

According to the Framework Directive[10] (FD) NRAs are responsible for establishing objective, transparent and non-discriminatory procedures for granting rights of use for national numbering resources and the management of the national numbering plans. The Authorisation Directive[11] (AD) states that Member States may implement an individual authorisation regime where the rights of use for national numbering resources are subject to individual granting. The granting of rights of use for national numbering resources shall be done through open, objective, transparent, non-discriminatory and proportionate procedures (as stated also in the FD). The conditions are listed in Annex 2 to this report. The NRAs may at a national level decide which of these conditions are most consistent with the administration of national numbering resources.

NRA's may at a national level decide to whom the rights of use for national numbering resources can be granted (end-users, providers of electronic communications networks and/or service or other parties). Access to numbering resources is essential for undertakings to compete in the electronic communications sector. It should be specified whether the rights of use can be transferred by the holder of the rights, and under which conditions.

The NRA's decision to grant rights of use for numbers shall be taken, communicated and made public as soon as possible after the receipt of the complete application by the NRA and within three weeks in the case of numbers that have been allocated for specific purposes within the national numbering plan.

6.3 LAWFUL INTERCEPTION

The e-Privacy Directive ensures the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services.

Except when legally authorised to do so, any kind of interception or surveillance of communications by persons or entities not being part of the communication, without the consent of the communicating parties, is prohibited.

Any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service is subject to confidentiality. This may include any naming, numbering or addressing information provided by the sender of information or the user of a connection to send the information. This indicates that the CLI which is used to identify a calling end-user would also be subject to confidentiality.

Member States may adopt legislative measures to carry out lawful interception and surveillance of electronic communications if necessary, appropriate and proportionate to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. The adoption of national legislative measures and the execution of these measures depend on the regulatory regime in each Member State.

6.4 USER RIGHTS VERSUS SERVICE PROVIDERS RIGHTS

6.4.1 Service providers perspective

With notable exceptions the NRA generally grants the right of use of numbers to an operator for a specific service provided by that operator. Operators use the numbers from the number block to offer services to their customers.

E.164 numbers can be used in different ways: to identify the caller in a call (the CLI is the only function) and/or to receive calls (routing function). In the past, origination and termination were offered as one bundled service, while nowadays these functions are increasingly separated and can even be offered by different operators.

[10] Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services as amended by Directive 2009/140/EC.

[11] Directive 2002/20/EC on the authorisation of electronic communications networks and services as amended by Directive 2009/140/EC.

In the traditional scheme a number is closely associated with a service. With the development of Over The Top (OTT) telephony this is no longer a requirement and both can be decoupled. Many of these OTT providers offer their users the choice of telephony services with and without numbers.

6.4.2 End-user perspective

When operators assign numbers to customers, the extent of the rights of use is not explicit. However, the rights of use are linked to the service.

Number portability gives the user the right to keep his number while switching to another operator for the same category of services. The existence of this absolute right is an indication that the “right of use” of an E.164 number by the operator to which the number is assigned is being eroded in favour of the user. But it is still unclear whether this right only applies when the user wants to change operator for the whole service or part of the service. Moreover, if the user of the ported number terminates the contract, the number will be transferred back to the operator which holds the original number block assignment. It can then be reassigned to a different end user.

6.5 CONSIDERATION OF IMPACTS

In the past it was not relevant to know who had the rights of use of a number as normally the number was de facto offered in combination with a specific service.

However, new business models have changed this practice. The debate on CLI flexibility illustrates the fact that clarity on the exact legal status of the different players in the supply chain of E.164 numbers is needed. If this is not clear, operators could start to build in limitations via their contracts with the customers. This could unjustly limit the flexibility asked by end-users.

In view of the technical evolution and the on-going change of service offers, strengthening the end-user rights in terms of use of E.164 numbers seems to be beneficial for end-users.

6.5.1 PROS of providing more flexible use of CLI

6.5.1.1 For end-users

For the called party, more flexible use will lead to less restriction by the caller of presentation of its CLI, so that calls/SMSs can be returned more often, even if it is not returned to the same platform or service that was used to initiate the communication. Nevertheless, this flexible use should only be used if a validation (of the number’s owner) is implemented, not allowing an anarchic use of the CLI. Furthermore, it is important that the use of alternative CLIs should not result in increased cost to callers who might want to call back to the caller.

For the calling party, flexible use of CLI offers convenience and empowerment. It provides that a single number for many services can be shown on multiple platforms.

Also, flexible use of CLI promotes competition, i.e. the calling party can choose an outgoing call service separate from the incoming call service where there is better value, using the same number, allowing the reduction in prices to international destinations for other operators.

6.5.1.2 For operators

CLI on outgoing calls, even if it is not on the original service to which it was allocated, will attract return calls on other access channels, growing the incoming operator’s benefits. For operators, generally VoIP or SMS service providers, the use of the user’s number will attract users to new applications and simplify the usage process associated to numbering.

Flexible use of CLI gives better statistics in call completion, since most of the time users do not want to complete anonymous calls.

The flexible use of numbers (CLI) may incentivise operators to develop new and innovative services using the same number as CLI allocated to the basic services (e.g. fixed or mobile), allowing to identify the user on multiple applications by a single number (e.g. VoIP or SMS applications).

6.5.1.3 For NRAs and other authorities

The flexible use of numbering resources will lead to an efficient resource management, avoiding the assignment of several numbers to the same end-user. At the same time, if this practice is allowed and regulated via a validation process, it may lead to a decrease of misuse or Calling/Caller ID spoofing, a problem that is appearing more frequently in networks. The consequence of this kind of regulated flexible use may lead to increased trust in CLI and promotion of the resources that NRAs control (E.164 numbers, IP addresses, domain names etc.).

6.5.2 CONS of providing more flexibility in use of CLI

6.5.2.1 For end users

The risk of consumer harm is higher with unregulated use of CLI, since another end-user could use the CLI (e.g. Calling/Caller ID spoofing). To avoid this situation CLI validation should be required. This validation mechanism could, depending on the arrangements involved, be an extra burden on the end-user.

On the other hand, if the validation measures discussed in this report are implemented then the risk of consumer harm (e.g. Calling/Caller ID Spoofing) is minimised. Spoofing can occur only when you have a party in the calling chain that has malicious intent and this is independent of the flexible use of CLI.

6.5.2.2 For operators

The existing service is linked to the assignment of the number. Additional services and/or service providers may then use that number as CLI. If the original service is cancelled after the number has been validated, the number could be assigned to another end-user. Then two different end-users could use the same CLI for different services. The validation should be made periodically in order to prevent the number being used by two different end-users at the same time when the number is re-assigned to a new end user by the original provider.

From the number block holder's point of view, this approach enables the end-user to make outgoing calls using another service provider's service, thereby losing traffic, and consequently revenue, for outgoing calls.

In some countries operators pay an administrative fee for the assignment of numbers and/or annual numbering fees to NRAs for rights to use number blocks. More flexible CLI use implies that some of the rights of use are transferred to the end-user.

6.5.2.3 For NRA and other authorities

Nowadays, numbers are used as a key to identify the operator and the end-user that are targets for lawful interception. It could be critical for law enforcement authorities to intercept the wrong access path or, in most of cases, intercept incompletely the originating communications. Thus, complexity could be added to fulfilment of the lawful interception obligation, since the mechanism could be extended to different accesses and networks (PSTN and Internet).

For emergency services, including Public Safety Answering Points (PSAP), flexible use of CLI may cause concern for certain applications. If the CLI is used, for example in an alternative third party VoIP-application emergency call, the call can appear as a normal emergency call, but in fact it may provide less information compared to a traditional call.

To reduce the risk of degraded emergency calls from smartphones, any such emergency call should at least be automatically diverted to the native client of the handset and the original provider's network. If there is no access to this network the alternative provider should at least process the call[12].

6.6 POLICY IMPLICATIONS / CONSIDERATIONS

In September 2009 ECC issued a report (ECC REP 133) related with the use of CLI – "*Increasing Trust in Calling Line Identification and Originating Identification*". This report reflects NRA's view of that time, but in substance it continues to be updated.

In relation with the recommendation (ECC REC (11)02) issued afterwards in May 2011 – "*Calling Line Identification and Originating Identification*", so far one identified item could be updated, if the flexibility of the CLI is supported, namely in point 11) of the recommended actions, where is stated:

"*that the originating operator/service provider and the subscriber should only use an identifier/a number in the OI/CLI which has been (a) associated to the calling subscriber at the time of subscription by the operator/service provider; (b) agreed between them and (c) the calling subscriber has right to use;*"

Point (b) could be deleted, since the procedure would diminish the user rights and add complexity to allow the use of the CLI.

[Other modifications may be introduced following the inputs from the public consultation of this document]

[12] One solution is that the alternative provider should send the caller location information. Such solutions may be dependent on international standards, namely those developed by ETSI under the standardisation mandate M/493, aimed to facilitate interaction between network access providers and service providers.

7 CONCLUSIONS

In this report several scenarios, which promote competition and innovation, are described where the CLI is used by different networks and the advantages and disadvantages for the end user and other stakeholders are analysed. If sufficient validation measures are implemented then the negative effects of CLI-flexibility are reduced, especially with regards to the risk of end user harm.

In order to facilitate increased flexibility in CLI use, while promoting greater customer empowerment and ensuring regulatory framework compliance:

- CLI validation techniques should be made mandatory. The alternative service provider should provide validation measures ensuring that the end user has the right to use the number. The validation should be made periodically in order to prevent the number being used by two different end-users at the same time when the number is re-assigned to a new end user by the original provider.

- When setting down the regulatory framework, the regulatory authorities should carefully consider which number types and under which criteria they consider can safely be used for flexible CLI purposes so that the risk of harm to consumers and other end-users is reduced.

- An end user, with rights of use to a number, should be permitted to use that number as CLI[13] in alternative services. Operators to whom numbers are assigned should not be able to restrict the use of those numbers as CLI for other services as long as the flexible use is in conformance with the national regulatory framework.

[13] ECC Recommendation (07)02 "Consumer Protection Against Abuse Of High Tariff Services" recommends "*that it is not allowed to use a premium rate number in CLIP*" and ECC Recommendation (11)02 "Calling Line Identification And Originating Identification" recommends *"that premium rate numbers should be excluded as valid OI/CLI. The NRA decides what national number ranges could or could not be used as OI/CLI*";

ANNEX 1: CLI RELEVANT ARTICLES FROM THE EU DIRECTIVES

A1.1 2002/20/EC – AUTHORISATION DIRECTIVE (AS AMENDED BY DIRECTIVE 2009/140/EC)

Article 5 – Rights of use for […] and numbers

1. […]
2. Where it is necessary to grant individual rights of use for radio frequencies and numbers, Member States shall grant such rights, upon request, to any undertaking for the provision of networks or services under the general authorisation referred to in Article 3, subject to the provisions of Articles 6, 7 and 11(1)(c) of this Directive and any other rules ensuring the efficient use of those resources in accordance with Directive 2002/21/EC (Framework Directive).

   Without prejudice to specific criteria and procedures adopted by Member States to grant rights of use of radio frequencies to providers of radio or television broadcast content services with a view to pursuing general interest objectives in conformity with Community law, the rights of use for radio frequencies and numbers shall be granted through open, objective, transparent, non-discriminatory and proportionate procedures, and, in the case of radio frequencies, in accordance with the provisions of Article 9 of Directive 2002/21/EC (Framework Directive). An exception to the requirement of open procedures may apply in cases where the granting of individual rights of use of radio frequencies to the providers of radio or television broadcast content services is necessary to achieve a general interest objective as defined by Member States in conformity with Community law.

   When granting rights of use, Member States shall specify whether those rights can be transferred by the holder of the rights, and under which conditions. In the case of radio frequencies, such provision shall be in accordance with Articles 9 and 9b of Directive 2002/21/EC (Framework Directive).

   […]

   […]

3. Decisions on the granting of rights of use shall be taken, communicated and made public as soon as possible after receipt of the complete application by the national regulatory authority, within three weeks in the case of numbers that have been allocated for specific purposes within the national numbering plan and within six weeks in the case of radio frequencies that have been allocated to be used by electronic communications services within the national frequency plan. The latter time limit shall be without prejudice to any applicable international agreements relating to the use of radio frequencies or of orbital positions.
4. Where it has been decided, after consultation with interested parties in accordance with Article 6 of Directive 2002/21/EC (Framework Directive), that rights for use of numbers of exceptional economic value are to be granted through competitive or comparative selection procedures, Member States may extend the maximum period of three weeks by up to a further three weeks.
   […]
5. […]

Article 6 – Conditions attached to the general authorisation and to the rights of use for […] numbers, and specific obligations

1. The general authorisation for the provision of electronic communications networks or services and the rights of use for radio frequencies and the rights of use for numbers may be subject only to the conditions listed in the Annex. Such conditions shall be non-discriminatory, proportionate and transparent and, in the case of rights of use for radio frequencies, shall be in accordance with Article 9 of Directive 2002/21/EC (Framework Directive).
2. Specific obligations which may be imposed on providers of electronic communications networks and services under Articles 5(1), 5(2), 6 and 8 of Directive 2002/19/EC (Access Directive) and Article 17 of Directive 2002/22/EC (Universal Service Directive) or on those designated to provide universal

service under the said Directive shall be legally separate from the rights and obligations under the general authorisation. In order to achieve transparency for undertakings, the criteria and procedures for imposing such specific obligations on individual undertakings shall be referred to in the general authorisation.

3. The general authorisation shall only contain conditions which are specific for that sector and are set out in Part A of the Annex and shall not duplicate conditions which are applicable to undertakings by virtue of other national legislation.
4. Member States shall not duplicate the conditions of the general authorisation where they grant the right of use for radio frequencies or numbers.

Annex – Part A – [Relevant] Conditions which may be attached to a general authorisation

1. […]
2. Accessibility by end users of numbers from the national numbering plan, numbers from the European Telephone Numbering Space, the Universal International Freephone Numbers, and, where technically and economically feasible, from numbering plans of other Member States, and conditions in conformity with Directive 2002/22/EC (Universal Service Directive).
3. […]
4. […]
5. […]
6. […]
7. Personal data and privacy protection specific to the electronic communications sector in conformity with Directive 2002/58/EC of the European Parliament and of the Council (Directive on privacy and electronic communications).
8. […]
9. […]
10. […]
11. Enabling of legal interception by competent national authorities in conformity with Directive 2002/58/EC and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
12. Terms of use during major disasters or national emergencies to ensure communications between emergency services and authorities.
13. […]
14. […]
15. […]
16. […]
17. […]
18. […]
19. […]

Annex – Part B – Conditions which may be attached to rights of use for numbers

1. Designation of service for which the number shall be used, including any requirements linked to the provision of that service and, for the avoidance of doubt, tariff principles and maximum prices that can apply in the specific number range for the purposes of ensuring consumer protection in accordance with Article 8(4)(b) of Directive 2002/21/EC (Framework Directive).
2. Effective and efficient use of numbers in conformity with Directive 2002/21/EC (Framework Directive).
3. Number portability requirements in conformity with Directive 2002/22/EC (Universal Service Directive).
4. Obligation to provide public directory subscriber information for the purposes of Articles 5 and 25 of Directive 2002/22/EC (Universal Service Directive).
5. Maximum duration in conformity with Article 5 of this Directive, subject to any changes in the national numbering plan.
6. Transfer of rights at the initiative of the right holder and conditions for such transfer in conformity with Directive 2002/21/EC (Framework Directive).
7. Usage fees in accordance with Article 13 of this Directive.

8. Any commitments which the undertaking obtaining the usage right has made in the course of a competitive or comparative selection procedure.
9. Obligations under relevant international agreements relating to the use of numbers.

A1.2 2002/21/EC – FRAMEWORK DIRECTIVE (AS AMENDED BY DIRECTIVE 2009/140/EC)

Article 10 – Numbering, naming and addressing

1. Member States shall ensure that national regulatory authorities control the granting of rights of use of all national numbering resources and the management of the national numbering plans. Member States shall ensure that adequate numbers and numbering ranges are provided for all publicly available electronic communications services. National regulatory authorities shall establish objective, transparent and non-discriminatory procedures for granting rights of use for national numbering resources.
2. National regulatory authorities shall ensure that national numbering plans and procedures are applied in a manner that gives equal treatment to all providers of publicly available electronic communications services. In particular, Member States shall ensure that an undertaking to which the right of use for a range of numbers has been granted does not discriminate against other providers of electronic communications services as regards the number sequences used to give access to their services.
3. Member States shall ensure that the national numbering plans, and all subsequent additions or amendments thereto, are published, subject only to limitations imposed on the grounds of national security.
4. Member States shall support the harmonisation of specific numbers or numbering ranges within the Community where it promotes both the functioning of the internal market and the development of pan-European services. The Commission may take appropriate technical implementing measures on this matter.
   These measures designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 22(3).
5. Where this is appropriate in order to ensure full global interoperability of services, Member States shall coordinate their positions in international organisations and forums in which decisions are taken on issues relating to the numbering, naming and addressing of electronic communications networks and services.

A1.3 2002/22/EC - UNIVERSAL SERVICE DIRECTIVE (AS AMENDED BY DIRECTIVE 2009/136/EC)

Article 28 – Access to numbers and services

1. Member States shall ensure that, where technically and economically feasible, and except where a called subscriber has chosen for commercial reasons to limit access by calling parties located in specific geographical areas, relevant national authorities take all necessary steps to ensure that end users are able to:

   a) access and use services using non-geographic numbers within the Community; and
   b) access all numbers provided in the Community, regardless of the technology and devices used by the operator, including those in the national numbering plans of Member States, those from the ETNS and Universal International Freephone Numbers (UIFN).

2. Member States shall ensure that the relevant authorities are able to require undertakings providing public communications networks and/or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reasons of fraud or misuse and to require that in such cases providers of electronic communications services withhold relevant interconnection or other service revenues.

Article 29 - Provision of additional facilities

1. Without prejudice to Article 10(2), Member States shall ensure that national regulatory authorities are able to require all undertakings that provide publicly available telephone services and/or access to public communications networks to make available all or parts of the additional facilities listed in Part B of Annex I, subject to technical feasibility and economic viability, as well as all or part of the additional facilities listed in Part A of Annex 1.

2. A Member State may decide to waive paragraph 1 in all or part of its territory if it considers, after taking into account the views of interested parties, that there is sufficient access to these facilities.

Annex I – Part B - List of [relevant] facilities referred to in Article 29

a) [...]
b) Calling-line identification
i.e. the calling party's number is presented to the called party prior to the call being established.

This facility should be provided in accordance with relevant legislation on protection of personal data and privacy, in particular Directive 2002/58/EC (Directive on privacy and electronic communications).

To the extent technically feasible, operators should provide data and signals to facilitate the offering of calling-line identity and tone dialling across Member State boundaries.

A1.4 2002/58/EC - DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATIONS

Article 5 – Confidentiality of the communications

1. […]
2. […]
3. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

Article 8 - Presentation and restriction of calling and connected line identification

1. Where presentation of calling line identification is offered, the service provider must offer the calling party the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.
2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.
3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling party or subscriber.
4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling party.
5. Paragraph 1 shall also apply with regard to calls to third countries originating in the Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.
6. Member States shall ensure that where presentation of calling and/or connected line identification is offered, the providers of publicly available electronic communications services inform the public thereof and of the possibilities set out in paragraphs 1, 2, 3 and 4.

Article 10 - Exceptions

Member States shall ensure that there are transparent procedures governing the way in which a provider of a public communications network and/or a publicly available electronic communications service may override:

a) the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, in accordance with national law, the data containing the identification of the calling subscriber will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service;
b) the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls.

Article 11 - Automatic call forwarding

Member States shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber's terminal.

Article 15 – Application of certain provisions of the Directive 95/46/EC

Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

ANNEX 2: LIST REFERENCES

[1] ECC Report 133 – “Increasing Trust in Calling Line Identification and Originating Identification”
[2] ECC/REC(11)02 – “Calling Line Identification and Originating Identification”