Electronic Communications Committee (ECC)
within the European Conference of Postal and Telecommunications Administrations (CEPT)

INCREASING TRUST IN

CALLING LINE IDENTIFICATION

AND

ORIGINATING IDENTIFICATION

Kristiansand, September 2009

Increasing Trust in Calling Line Identification and Originating Identification

0 EXECUTIVE SUMMARY

Calling Line Identification (CLI) can be understood as a set of parameters within telecommunications networks that provide users with capabilities of sending, receiving and displaying telephone numbers. The concept of Originating Identification (OI) provides users with similar kind of capabilities as the CLI, but the OI extends the traditional calling line identification to new networks, such as NGNs with identifiers other than E.164 numbers.

Communications today is more global than ever before and legislation within electronic communications vary hugely in different parts of the world. As calls pass country borders the transiting and terminating operators have very little or no means to verify correctness of electronic communications parameters received. Therefore, the correctness of various electronic communications parameters, such as CLI, depends mainly in the originating network.

The CLI was never meant to be used for authentication purposes for service applications that need a high level of trust, e.g. banking transactions, however, the CLI could be useful as one part of an authentication process. The CLI still has a certain level of trustworthiness, and it is thus useful for network services and many applications that are not considered as critical.

In some countries there are regulations/guidelines aiming to guarantee the trustworthiness of CLI. However, this report draws attention to the fact that no legal trustworthiness exists in all countries within the CLI and even for information purposes the CLI cannot necessarily be fully trusted, especially in cases where CLI is transferred between countries. This problem is not of technical nature.

Finally, the report lists guidelines regarding the OI/CLI. The guidelines are useful for the NRAs, operators and end-users. The most important conclusions are that the NRA should implement the relevant ECC Recommendation regarding the CLI as well as develop national OI/CLI related regulations/guidelines.

The annexes to this report provide more in-depth information on CLI and OI.

Increasing Trust in Calling Line Identification and Originating Identification

Table of contents

Increasing Trust in Calling Line Identification and Originating Identification

1 INTRODUCTION

Calling Line Identification (CLI) can be understood as a set of parameters within telecommunications networks that provide users with capabilities of sending, receiving and displaying telephone numbers. These parameters are used in services like Calling Line Identification Presentation (CLIP) and Calling Line Identification Restriction (CLIR), and their technical usage is standardized, for example, by ETSI [4] – [9]. Furthermore, this issue is dealt with the ECTRA/ECC Recommendations [1], [2], ETP Guidelines [3] and national regulations. Existing Recommendations and guidelines deal with CLI implementation in networks and this stage has generally been reached in Europe already for some time ago.

Today CLI information is widely passed worldwide between operators to provide end users with number information, which the telephones and terminal equipment may use to display the name of the calling party. Furthermore, the CLI information is used to call back, e.g. in a case of a missed call, to authenticate access to services such as a voice mail box, to trace the source of a malicious call, to access location databases to locate the caller to emergency services and route the call to its destination depending on the location or type of number (functionality e.g. in Intelligent Networks (IN) translation services). The list is not exhaustive.

There appears to be instances to suppress the transmission of CLI for commercial reasons. Such practices have an unfavourable effect on services based on CLI.

The concept of Originating Identification (OI) provides users with similar kind of capabilities as the CLI, but the OI extends the traditional CLI to future networks, such as NGNs with identifiers other than E.164 numbers [20]. In this report the term OI is understood to include also the CLI as an overall umbrella concept [10].

The usage of OI/CLI information is based on trust, that all operators involved in handling the call and in particular the originating operators only allow the correct contents of parameters to be transferred in the networks. With a growth in the electronic communication features offered and an increasing number of interconnected networks of different types (e.g. IP based networks) handling calls there are increasing challenges to guarantee the correctness of the received OI/CLI and some scope for abusing the OI/CLI facility.

Communications today is more global than ever before and legislation within electronic communications vary hugely in different parts of the world. As calls pass country borders the transiting and terminating operators have very little or no means to verify correctness of electronic communications parameters received. Therefore, the correctness of various electronic communications parameters, such as CLI, depends mainly in the originating network.

2 SCOPE

The CLI was never meant to be used for authentication purposes for service applications that need a high level of trust, e.g. banking transactions, however, the CLI could be useful as one part of an authentication process. The CLI still has a certain level of trustworthiness, and it is thus useful for network services and many applications that are not considered as critical.

In some countries there are regulations/guidelines aiming to guarantee the trustworthiness of CLI. However, this report draws attention to the fact that no legal trustworthiness exists in all countries within the CLI and even for information purposes the CLI cannot necessarily be fully trusted, especially in cases where CLI is transferred between countries. This problem is not of technical nature.

As originating network operators have the responsibility for the correctness of the information passed into the network, the user provided CLI information, which is not screened by the network, is out of scope of this. This means that the user provided CLI (not screened and passed) is not discussed in the report, although some of the guidelines deal with it.

This report aims to answer the following questions:

- How to ensure, to a certain level, that the correct OI/CLI information is generated and transferred in networks?
- Why is the trust worthiness of identifiers as important in the future networks as in current networks?
- What is the role for network operators and service providers in handling of the OI/CLI information?

This is not a technical report, but rather an informative one aimed for providing a general understanding regarding the CLI and OI. The report describes the possible problem areas and gives guidelines that can be useful to NRAs, operators

and end-users regarding the OI/CLI. In this report term OI or OI/CLI is used when originating information wider than just an E.164 number is considered. The term CLI is used to refer to E.164 number as a calling line identification.

3 REFERENCES

The following references are some of the most important ones regarding the scope of this report:

[1]	CEPT / ECTRA Recommendation of 22 June 2000 (ECTRA/REC(00)03) on the implementation and use of CLI (Calling Line Identification) within CEPT countries
[2]	ECC Recommendation (03)01 of 25 March 2003 (ECC/REC(03)01) implementation and use of CLI (Calling Line Identification) within CEPT countries
[3]	ETP – European Telecommunications Platform / CLI Working Group: ETP Guidelines for Calling Line Identification, Issue 4 September 2002
[4]	ETSI EN 300 089 (v3.1.1 2000-12) Calling Line Identification Presentation (CLIP) supplementary service; Service description
[5]	ETSI EN 300 092-1 (v2.1.1 2001-02) Calling Line Identification Presentation (CLIP) supplementary service; Digital Subscriber Signalling System No. One (DSS1) protocol; Part 1: Protocol specification
[6]	ETSI EN 300 356-3 (v4.2.1 2001-07) Signalling System No.7 (SS7);ISDN User Part (ISUP) version 4 for the international interface; Part 3: Calling Line Identification Presentation (CLIP) supplementary service
[7]	ETSI EN 300 090 (v1.2.1 2000-12) Calling Line Identification Restriction (CLIR) supplementary service; Service description
[8]	ETSI EN 300 093-1 (v1.2.4 1998-06) Calling Line Identification Restriction (CLIR) supplementary service; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification
[9]	ETSI EN 300 356-4 (v4.2.1 2001-07) Signalling System No.7 (SS7);ISDN User Part (ISUP) version 4 for the international interface; Part 3: Calling Line Identification Restriction (CLIR) supplementary service
[10]	ETSI TS 183 007 (v1.3.0 2008-01) Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Protocol specification
[11]	ETSI TS 129 163 V8.5.0 (2009-02) Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks (3GPP TS 29.163 version 8.5.0 Release 8)
[12]	ECC Recommendation (07)02 Consumer Protection against Abuse of High Tariff Services
[13]	Recommendation E.157[1] – International Calling Party Number Delivery
[14]	ETSI EN 301 798 (v1.1.1 2000-10) Anonymous Call Rejection (ACR) supplementary service; Service description
[15]	Directive 2002/22/EC of the European Parliament and of the Council, of 7 March 2002 - on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)
[16]	Directive 2002/58/EC of the European Parliament and of the Council, of 12 July 2002 - concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
[17]	Commission Recommendation 2003/558/EC, of 25 July 2003, on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services
[18]	Commission Decision 2007/176/EC, of 11 December of 2006, establishing a list of standards and/or specifications for electronic communications networks, services and associated facilities and services and replacing all previous versions
[19]	Directive 2006/24/EC of the European Parliament and of the Council, of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
[20]	ITU-T Rec. E.164 The international public telecommunication numbering plan

[1] ITU-T Rec. E.157 has been determined and has the status of a draft recommendation (status of April 2009)

4 ABBREVIATIONS

Abbreviation	Explanation
ACR	Anonymous Call Rejection
CEPT	European Conference of Postal and Telecommunications Administrations
CLI	Calling Line Identification
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
E.164	ITU-T Recommendation E.164: "The international public telecommunication numbering plan"
EC	European Community
ECC	Electronic Communications Committee (within the CEPT)
ECTRA	European Committee for Telecommunications Regulatory Affairs (earlier organization within the CEPT)
ETP	European Telecommunications Platform
ETSI	European Telecommunications Standards Institute
IN	Intelligent Networks
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU-T	International Telecommunication Union – Standardization Sector
MCID	Malicious Call Identification
MMS	Multimedia Messaging Service
NGN	Next Generation Networks
NRA	National Regulatory Authority
OI	Originating Identification
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
PLMN	Public Land Mobile Network
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
SCCP	Signalling Connection Control Part
SIP	Session Initiation Protocol
SMS	Short Message Service
SS7	Signalling System no. 7
USD	Universal Service Directive
VoIP	Voice over Internet Protocol (based networks)

5 CALLING LINE IDENTIFICATION

5.1 General Description of CLI

The Calling Line Identification Presentation service (CLIP) provides the called party with the possibility to identify the subscription of the calling party via the telephone number. Usually the called party associate (in case of a well known number) the received CLI with the name of the calling party. CLI has for many years been used within networks and forwarded between interconnected networks in order to support, for example, call processing, billing, operator assistance, customer care, emergency services and managing the network.

Where feasible, the originating public telephone switch shall transmit CLI information into the network and provide CLI restriction (CLIR) capabilities to calling users. Nevertheless, operators have full access to CLI information irrespective of CLI restriction requested by callers. However, network operators should only make use of such restricted CLI information where the information is essential to provide a telecommunications service or where legal requirements are concerned.

The network shall deliver the calling line identity to the called party during call establishment, regardless of the terminal's capability to handle the information unless the calling party has activated the Calling Line Identification Restriction.

Since the adoption of Recommendations "Implementation and use of CLI within CEPT countries" (ECTRA REC(00)03 [1] and ECC REC(03)01 [2] – both with the same name) the CLI is widely used and available in the CEPT countries,

and offers value for users. Furthermore, the European Telecommunications Platform (ETP) Guidelines for Calling Line Identifications [3] support these Recommendations by providing the operators best practice solutions within the CLI related issues. This implementation stage has now been reached in Europe.

5.2 Directives Associated to CLI

In the existing electronic communication framework Directives there are several requirements defined associated to the provisioning of CLI, such as access to emergency services (including the location based services) and directly related with a set of supplementary services used in modern telecommunications networks like CLIP, CLIR, ACR and MCID that should be taken in account [15] – [19].

The Universal Service Directive (USD) – Article 29, foreseen that Member States shall ensure that national regulatory authorities are able to require all undertakings that operate public telephone networks to make available to end-users the CLI. This facility is restricted to extent of technical feasible and economic viability and should be available across Member States boundaries.

The Directive on Privacy and Electronic Communications (2002/58/EC) (Article 8) defines a set of requirements associated to presentation and restriction of calling and connected line identification, namely that calling party's number should be presented to the called party prior to the call being established. Some exceptions are applicable to the restriction of CLI presentation (Article 10).

These legal requirements are included also in the draft proposals of Electronic Communications Reform that will replace the existing legal framework[2].

5.3 Problem Description

This report draws attention to the fact that no legal trustworthiness exists in all countries within the CLI and even for information purposes the CLI cannot necessarily be fully trusted, especially in cases where CLI is transferred between countries. This problem is mainly not of technical nature.

In addition, the following issues may exist (the list is not exhaustive):

- The use of VoIP and other non-traditional telecommunications systems without arrangements to send an OI/CLI that relates to the calling party;
- Incorrect implementations of software or configurations in the originating network elements and/or the end-user equipment.

Examples of fraudulent or misleading use of OI/CLI:

- Call return service: In case of receiving a premium rate number or a high tariff number (e.g. a satellite or international number), if the called party returns the call, the price charged is unexpectedly high. According to existing recommendation [12], this procedure is prohibited.
- Voice mail access: Voice mail services may be accessed with a CLI. With a fake CLI an unauthorised user may access voice mails and/or change voice mail configurations leaving the service inaccessible to the original user.
- Identity theft: With a fake CLI one can make calls pretending to be someone else. This results in e.g. billing/agreement problems with various services that are billed offline based on a CLI.
- Use of unassigned numbers as a CLI: A CLI received is not a number assigned in the national (or international) numbering plan. In this case a call return service is not possible and public authorities are not able to determine the source of the call.
- Use of numbers unassigned to a subscriber: A number assigned to an operator but not assigned to any subscriber. In this case the call return service is not possible. This practice is used by some operators, by modifying the original CLI, in order to benefit from cheaper interconnection prices.
- A service to provide a false CLI: There are service providers that give a possibility of using a false CLIs, e.g. by means of calling cards.
- Emergency services / lawful interception: Malicious calls to emergency centres. Misleading of law-enforcement authorities.

[2] The referenced Directives shall be reviewed after approval of the new regulatory framework.

6 ORIGINATING IDENTIFICATION

The Originating Identification Presentation (OIP) service provides the destination party with the possibility of receiving information about the source of the call. Usage of the OI is rather similar with usage of the CLI, but the OI concept is extended to cover also other networks than PSTN/ISDN/PLMN. SIP protocol is used to carry the OI information, meanwhile for the CLI Signalling System #7 (SS7) is used. Furthermore, the OI consists of different kinds of identifiers, not only E.164 numbers as is the case with the CLI.

The Originating Identification Restriction (OIR) service is a service offered to the originating party. It restricts the presentation of information regarding the source of the call to the destination party. When the OIR service is invoked, the originating network operator provides the destination network operator with the indication that the OI is not allowed to be presented to the destination party. In this case, no OI shall be included in the requests sent to the destination party. The presentation restriction function shall not influence the forwarding of the OI within the network as part of other services, such as communication diversion service.

7 THE USE OF OI/CLI IN FUTURE NETWORKS

As future networks, such as NGN, emulate PSTN as one of the function within them, no huge changes compared to PSTN are expected on the traditional voice services. That is why requirements are also very similar between NGN and PSTN. However, it should be noted that there are more roles for different players in future networks compared with legacy networks. These roles and especially the interfaces between subsequent operators/service providers may require additional security measures.

Terminals in future networks will have an increased linkage with the user and also with applications. This means that the role of users and applications may bring end-to-end security mechanisms that are not provided by the networks. Actually, end-to-end authentication will be increasingly used, and – theoretically – in addition to end-to-end authentication no other mechanisms are required.[3]

However, it is expected that OI information will be used in similar network and service applications as CLI and therefore it is essential that the aim is the OI (P-Asserted-Id in SIP) should have at least the same amount of trust. In addition to this, OI/CLI authentication in combination with end-to-end authentication may be used. It is always up to the application provider to decide what kinds of security mechanisms are applied.

It should be noticed that although a lot of standardization effort is going on to provide additional security measures in future networks, it is recommended that in critical applications proper security methods should be done by end-users themselves.

8 GUIDELINES

To increase trust in the usage of OI/CLI all parties in the electronic communication chain are required to follow the same principles. These principles are based on international standards and governmental regulations and guidelines[4]. The operators and service providers play a main role here. The overall responsibility lies, however, at the public authorities, typically within the NRAs.

The NRAs shall take the relevant EU Directives and the following guidelines into account when providing regulations/guidelines for OI/CLI. The order of the guidelines does not imply the order of importance.

These guidelines are subject to national legislation.

1. ECC Recommendation (03)01 of 25 March 2003 (ECC/REC(03)01) “Implementation and use of CLI (Calling Line Identification) within CEPT countries” shall be implemented.
2. National regulations/guidelines regarding the generating and handling of OI/CLI should be developed.
3. All electronic communications operators and service providers, national and international, involved in an electronic communication service that uses an E.164 number shall provide or transport and forward CLI information.

[3] Measures to ensure end-to-end secure communications at the application level are outside of the competences of the NRAs.

[4] By ”governmental regulations and guidelines” a national telecommunications law and/or orders by the NRA are meant.

4. The interconnecting operators shall include the transfer of the proper OI/CLI information in the interconnection agreements according to the rules of the NRAs of countries involved.

5. The access operator is responsible for the correctness of the CLI (network provided CLI or in case of user provided CLI and the coding is “verified and passed”).

6. An operator receiving electronic communications should not change the contents of the OI/CLI, if not specifically allowed in cases mentioned in regulations/standards (e.g. when sending the OI/CLI to the called party, appropriate prefixes can be added, for example in an international call, the prefix “00”, “+” or other nationally valid prefix). However, an operator receiving communications may have to change the content of an OI/CLI to convert a national significant number into the same number in an international E.164 format.

7. The access operator for an electronic communication service that uses an E.164 number, in case of involvement of transit operators should include in their contractual agreements that the CLI should not be unnecessarily modified in network-network interfaces till the destination network. Any such modification should be supported by international standards.

8. It should be possible to return a call by using CLI information presented to the called user. Therefore, CLI numbers used in an IP/PSTN interconnection with a VoIP provider without E.164 numbers should be marked as presentation restricted.

9. Depending on bilateral/multi-lateral agreement or restrictions in cases of national legal and regulatory frameworks, the originating network may restrict calling party number from being sent to the destination network when the CLIR supplementary service is applicable, in this case the calling party numbers sent across international boundaries shall contain always the restriction indicator and may also include the country code of the originating country, being marked in this case as a incomplete number in the international format [13].

10. Where a network operator accepts caller-provided numbers unscreened into the public network for transfer in the generic number parameter to be presented to the called user as the CLI, there should exist a written agreement (subject to national legislation) between the access network operator and the calling subscriber which numbers could be used.

11. The OI/CLI may be marked as restricted if the operator can assure that the information is not valid according to the national regulations. In this case the OI/CLI is not presented to the called party.

12. Originating operator should only use an identifier/a number in the OI/CLI which the user has right to use.

13. It is not allowed to use fictive/non-assigned identifiers/numbers as a OI/CLI.

14. Premium rate numbers should not be used as OI/CLI [12]. The NRA decides what national number ranges could or could not be used as OI/CLI.

15. If an originating party has ported his number, the original (ported) number shall be used as a CLI.

16. Calls to emergency services shall always carry the network validated CLI, only.

17. The CLI does not identify the calling party; it is rather an identifier of the subscription.

18. The CLI should not be used alone as an authorization tool for critical applications.

19. The principles of these guidelines should also be applied, where relevant, in all electronic communications networks and for all electronic communication services that make use of public numbering, naming and addressing resources.

20. These guidelines should also be applied, where technically feasible, in non-call-related services, such as SMS/MMS.

Increasing Trust in Calling Line Identification and Originating Identification

The Annexes for this document are meant for background and additional information and they are not integral part of the report. More detailed information on CLI and OI can be found in the reference documents.

ANNEX 1: Use of the CLI

The Calling Line Identification Presentation service (CLIP) provides the called party with the possibility to identify the subscription of the calling party via the telephone number. Usually the called party associate (in case of a well known number) the received CLI with the name of the calling party. In addition to the E.164 number, the calling line identity may include a sub-address generated by the calling user and transparently transported by the network. The network cannot be responsible for the content of this sub-address. The network shall deliver the calling line identity to the called party during call establishment, regardless of the terminal capability to handle the information unless the calling party has activated the Calling Line Identification Restriction (CLIR), in this situation no information about the source of the call is sent to the terminating user. There is another number identification option related to the Calling Party number identification. When the signalling network supports the Generic number and the terminating network supports the two number delivery option, it is possible to send to the user's terminal 2 CLIs in the SETUP message. The CLI is delivered to emergency services independently of the restriction value, for this it is necessary to configure the network interfaces to the PSAP with the feature "CLIR override".

Where more than one parameter is transferred, there is a choice about which parameter should be presented to the user and this choice may be determined by the design of the called party's terminal and also by user subscription. There are 3 options related to number delivery: CLI, generic number or both.

For more information please consult references [4] – [9].

A critical issue is where the information in the parameter was generated as this affects the degree of trust that should be put in the information. If the information was generated by a Communications Provider then it is much more likely to be correct than if it was input by the calling party. The called party is not aware who generated the information in case of 2 CLI delivery option. Information input by the caller is especially vulnerable to deliberate errors and misrepresentations as in fraud.

The CLI information is also used to populate other kind of parameters in the signalling and used in several supplementary services (e.g. Call Diversion services and Malicious Call Identification). The CLI is used both for voice calls and for services, such as SMS and MMS, to identify the calling line used by a calling party [11].

The CLI may also be used for services such as:
– call return service;
– malicious call identification;
– origin dependent routing;
– caller location determination.

The originating public telephone exchange shall transmit CLI information into the network and provide restriction capabilities to calling users. Network operators have full access to CLI information irrespective of CLI restriction requested by callers. However, network operators should only make use of such restricted CLI information where the information is essential to provide a telecommunications service. Where the caller has deliberately restricted the presentation of their CLI an appropriate indication shall be given to the called user. The CLI is delivered to emergency services independently of the restriction value.

A subscriber may generate a calling line identity for his network operator to be transferred to the called party using the generic number parameter. Where a network operator accepts caller-provided numbers unscreened into the public network for transfer in the generic number parameter and for presentation to the called user, there should exist a written agreement (subject to national legislation) between the network operator and the calling subscriber which numbers could be used. If the user provided number is screened and passed then it could be used in the CLI parameter.

The NRA may define which number ranges can be used as a CLI. Usage of special numbering ranges with high tariffs, such as premium rate numbers, should not be used as a CLI [12]. This is justified by possibility of caller return the call to these numbers where the cost applied is higher than the cost to normal telephone number.

Therefore the risk for misuse is high. However, if these numbers are allowed by national legislation to be used as a CLI, callers should be made aware of the charges prior to making any call to such a service.

The originating network operator shall ensure that where a fixed network non-geographic number (for example freephone or shared cost number) is used as a CLI, if allowed by the NRA, that the operation of emergency services, and billing by interconnected network operators is not affected.

ANNEX 2: Use of the OI

The Originating Identification Presentation (OIP) and the Calling Line Identification Presentation (CLIP) as a subset of the OIP present the originating/calling line identifier provided by the originating network, such as Public Switched Telephone Network (PSTN)/Integrated Services Digital Network (ISDN) or the Public Land Mobile Network (PLMN), to the called party. This identifier may be an E.164 telephone number.

Originating Identification (OI) within future networks, such as NGNs and IP-based PLMNs is basically the same as CLI within PSTN/ISDN/PLMN (e.g. GSM). Protocols, like SIP, are used to carry the OI information, meanwhile for the CLI Signalling System #7 (SS7) is used. Usage of the OI is rather similar with usage of the CLI, but the OI concept is extended to cover also other networks than PSTN/ISDN and circuit-switched PLMNs. Furthermore, the OI consists of different kinds of identifiers, not only E.164 numbers as is the case with the CLI.

The Originating Identification Presentation (OIP) service provides the destination party with the possibility of receiving information about the source of the call. In addition to this information, the OI from the originating party may include additional information generated by the originating user and in general transparently transported by the network. In the particular case where the “no screening” special arrangement does not apply; the originating network shall verify the content of this user generated information. The network operators cannot be responsible for the content of the user generated information unless the originating network operator has agreed with the user on correctness of the possible user generated information.

The Originating Identification Restriction (OIR) service is a service offered to the originating party. It restricts presentation of the originating party’s OI information to the destination party. When the OIR service is invoked, the originating network operator provides the destination network operator with the indication that the OIP is not allowed to be presented to the destination party. In this case, no OI shall be included in the requests sent to the destination party. The presentation restriction service shall not influence the forwarding of the OI within the network as part of other services, such as communication diversion service.

OI Implementation in SIP

The relevant headers in the SIP requests are [10]:

- The P-Preferred-Identity header field;
- The P-Asserted-Identity header field;
- The Privacy header field;
- The From header field.

The “P-Preferred-Identity” header field is meant to give to the user a possibility to input a user generated information. According to the specifications [10], 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 “P-Asserted-Identity” header field is meant to carry the network provided identifier (in ISUP the corresponding parameter is the Calling-Party-Number parameter)

The “Privacy” header field gives a user a possibility to restrict the presentation of his/her OI contained in the P-Asserted-Identity header.

The “From” header field contains the OI that the user wants to pass transparently through the network to the destination. This is comparable with the user provided (not screened, generic number) parameter in ISUP.