NICC ND 1439 v 4.2.1 (2020-11)

Guidance for Implementing ND1016 in SIP networks

NICC Standards Limited

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC. Pursuant to the [NICC IPR Policy](#), no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by NICC CLI TG.

1   Scope

General Condition of Entitlement C6 [1] sets the regulatory requirement that UK Communication Providers support Calling Line Identification facilities, and the Ofcom CLI Guidelines [2] elaborate the regulatory requirements that CPs must meet. ND1016 [3] provides the technical requirements of UK Communication Providers to fulfil the regulation.

This document takes ND1016 and provides guidance primarily for CPs that are implementing SIP networks. In order to provide clarity, the requirements of ND1016 are stated in terminology appropriate to SIP networks.

Although ND1016 also provides technical requirements associated with Connected Line Identity (COL), this is not within the scope of this guidance document, as the service predominately relates to legacy ISDN networks.

This document is a guidance document, whereas ND1016 is a normative one; thus if there is any discrepancy between the documents, ND1016 should be treated as authoritative.

2   Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] Ofcom General Conditions

[2] Ofcom CLI guidelines;   Guidelines for the provision of Calling Line Identification Facilities and other related services over Electronic Communications Networks. http://stakeholders.ofcom.org.uk/telecoms/policy/calling-line-id/caller-line-id/

[3] ND1016 - Requirements on Communications Providers in relation to Customer Line Identification display services and other related services

[4] ND1035 - SIP Network to Network Interface Signalling

[5] RFC3325 - Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

[6] ITU-T Recommendation Q.763 - Signalling System No. 7 - ISDN User Part formats and codes

[7] RFC3261 - SIP: Session Initiation Protocol

[8] RFC2543 - SIP: Session Initiation Protocol

[9] RFC3323 - A Privacy Mechanism for the Session Initiation Protocol (SIP)

[10] RFC3966 - The tel URI for Telephone Numbers

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document, the terms and definitions set out in ND1016 [3] apply.

3.2 Abbreviations

ACgPN Additional Calling Party Number
APRI   Address Presentation Restricted Indicator
CgPN   Calling Party Number
GN   Generic Number
NN   Network Number
NP   Network Provided
UPNV   User Provided Not Verified
UPVP   User Provided Verified and Passed

For the purposes of this document, the abbreviations set out in ND1016 [3] additionally apply.

4   Principles for the use of Customer Line Identities

Section 4 of ND1016 sets out that the intent of the document is to ensure that the cardinal principles of Privacy, Authenticity and Integrity be achieved. This guidance document is intended to provide explanatory text to the rules set out in ND1016 [3].

5   Customer Line Identities

5.1   Background

The term "CLI" can relate to either a Network Number or Presentation Number CLI. Section 5 of ND1016 [3] explains the difference between Network Number and Presentation Number CLIs, and how each can be classified.

5.2   Network Number

Section 5.2 of ND1016 [3] describes the function of the Network Number CLI. In UK networks, carriage of a Network Number CLI is mandatory, and as described in ND1016 [3] the Network Number CLI represents the point at which the call entered the public network. Where calls are received from networks not governed by ND1016 [3] i.e. international networks the rules of ND1016 [3] expect the first CP in the call path within scope of ND1016 [3] to insert a Network Number. The Network Number is used, for example, for validating interconnect bills, call tracing and reconciling call records generated by individual networks.

As set out in ND1035 [4], in SIP networks, the Network Number is carried in a P-Asserted-Id header field (RFC 3325 [5]).
In the case where a Presentation Number is not present the FROM header field may also contain the Network Number (subject to Network Number CLI classification).

5.3   Presentation Number

Section 5.3 of ND1016 [3] describes the function of the Presentation Number CLI. In general in UK networks, a Presentation Number CLI is optional from a regulatory perspective, and it is intended to represent a number to which the called party can make a return call.

In SIP networks, the Presentation Number, when available, is carried in the From header field.

Section 5.3 of ND1016 [3] sets out a series of criteria which must be fulfilled for Presentation Numbers.   It is the responsibility of the Originating Network to ensure that the Presentation Number is populated according to these criteria, which means that in the case of the originating customer on a SIP network providing invalid information, the Originating Network is expected to substitute other information into the field such as the Network Number.

5.4   Validity and reliability of Customer Line Information

No additional guidance at this time.

5.5   Classification of customer line information

Section 5.5 of ND1016 [3] sets out the classifications of CLIs, which are CLI Available, CLI Restricted and (in the case of Network Numbers) CLI Unavailable.

CLI Available means the contents of the CLI can be used for display purposes, whereas CLI Restricted means that the customer has asserted privacy over the CLI. It should be noted that even where a CLI is present and classified as CLI Restricted, it is still carried through the network, but the classification ensures that it is not presented in any form to the called customer.

The classification CLI Unavailable applies only to Network Number CLIs. It should not be utilised by UK SIP Originating Networks, but is instead intended to represent the case where a call has been received from networks not governed by ND1016, and the CLI was not present (so a Network Number CLI was injected). The intent of the classification CLI Unavailable is to ensure that such Network Numbers do not get inadvertently displayed (as would otherwise occur under certain signalling interworking cases), while ensuring that Anonymous Call Rejection is not invoked on Terminating Networks.

Note: the classification CLI Unavailable should not be confused with the use of a URI unavailable@unknown.invalid

In SIP, the classifications should be indicated within the public network as follows, using the example Presentation Number of 0800 1234567 and Network Number 01632 123456:

Note: although the following examples have different Presentation Number CLI and Network Number CLI, these could be the same (see 5.2). Also, it should be noted that in the SIP header fields both sip URI and tel URI formats may be used.

> **CLI Available**
> The following formats are permitted:
> From: <sip:+448001234567@domain;user=phone>
> P-Asserted-Identity: <sip:+441632123456@domain;user=phone>
>   Or
> From: <sip: +448001234567@domain;user=phone>
> P-Asserted-Identity: <sip:+441632123456@domain;user=phone>
> Privacy: none
>
> **CLI Restricted**
> The recommended format is:
> From: <sip:+448001234567@domain;user=phone>
> P-Asserted-Identity: <sip:+441632123456@domain;user=phone>
> Privacy: id;user
>
> Or alternatively the following format is permitted when either a Presentation Number is not available or is received from customer equipment or networks that do not support the recommended format (see note):
> From: <sip: anonymous@anonymous.invalid>
> P-Asserted-Identity: <sip:+441632123456@domain;user=phone>
> Privacy: id

Note: Whilst the standard for an anonymous URI is shown above any URI that contains a user field of 'anonymous' (case-insensitive) is acceptable.

CLI Unavailable

Classification CLI Unavailable is denoted by Privacy: id against the PAID when the From header field contains a CLI.

The following format details how the contents of the P-Asserted-Identity is considered to be classified CLI Unavailable:

From: <sip:+448001234567@domain;user=phone>
P-Asserted-Identity: <sip:+441632123456@domain;user=phone>
Privacy: id

5.6 Usage of Calling Line Identity by Customer Premises Equipment

No additional guidance at this time.

6   Rules relating to Calling Line Identification

This section provides guidance to fulfil the rules for handling CLIs as set out in ND1016 [3].

6.1   Responsibilities of the Originating Network with respect to CLI

Section 6.1 of ND1016 [3] sets out that it is the responsibility of the Originating Network to ensure that CLI Information is properly populated.

RULE CLI ORIG 1 – **Population of CLI information**
There is no SIP-specific guidance at this time – see advice on RULE ORIG CLI 4 for details of guidance on privacy.

RULE CLI ORIG 2 – **Network Number**
The SIP INVITE sent by the Originating Network must provide a P-Asserted-Identity header field (RFC3325) [5] containing the Network Number that uniquely identifies the originating access.

The format of P-Asserted-Identity header field should be:

sip: <+441632123456@domain;user=phone>
and/or
tel: +441632123456

For further details see ND1035 [4].

If the customer has an agreement to allow them to generate Network Numbers, and the SIP INVITE received by the Originating Network contains a P-Asserted-Identity header field (RFC 3325) [5], this must be screened to make sure the Originating Network is satisfied that it uniquely identifies the originating access. If screening fails or there is no agreement with the customer, any received P-Asserted-Identity header field is removed and replaced with a P-Asserted-Identity header field containing a Network Number that does identify the originating access.

RULE CLI ORIG 3 – **Presentation Number**
The SIP INVITE sent by the Originating Network must contain a From header field that will be populated with Presentation Number information.

The format of From header field should be:

sip: <+441632123456@domain;user=phone>
or
tel: +441632123456

For any more detail see ND1035 [4].

The Ofcom CLI Guidelines set out the distinction between Types 1, 2, 3, 4 and 5 Presentation Number services. Subject to rule CLI ORIG 4, the contents of the From header field should be populated as follows;

a) If the customer has not subscribed to a Presentation Number service

Any CLI received from the customer in the From header field in the INVITE will be removed by the Originating Network and the From header field populated with the Network Number.

b) If the customer has subscribed to Type 1 (network provided) Presentation Number service

Any CLI received from the customer in the From header field in the INVITE will be removed and the From header field populated with the network provided Presentation Number.

c) If the customer has subscribed to Type 2 (user provided) Presentation Number service

The CLI in the From header field in the INVITE must be screened to ensure it meets the criteria described in Section 5.3.

If the screening fails then dependent upon the service provided by the Originating Network this should be treated as either case a or b above.

d) If the customer has subscribed to Type 3/4/5 (user provided but cannot be screened – supported by contractual obligations between the Originating Network and the customer) Presentation Number services.

The CLI in the From header field in the INVITE is screened for validity by the Originating Network and passed untouched. If the From header field contains an anonymous URI (because the customer is forwarding a call and no Presentation Number CLI was received on the inbound leg) then it should be treated as case a) above in line with RULE CLI ORIG 4.

RULE CLI ORIG 4 – **Classification of CLIs**
The caller will have default settings for privacy, and also the Originating Network may receive privacy indications in the SIP INVITE as set out in Tables 6.1a and 6.1b below.

If the caller's CLI restriction service is…

a) CLI permanently restricted (Note 1), or
b) CLI presented by default (Note 2) and the caller expresses a wish that their CLI be restricted using <u>any</u> of the mechanisms set out in Table 6.1.a or
c) CLI restricted by default (Note 3) and the caller has not expressed a wish that their CLI be released using the mechanisms set out in Table 6.1.b,

…then both the P-Asserted-Identity and From header fields must be restricted as described in Section 5.5.

Note 1: also known as *permanent mode*
Note 2: also known as *per-call temporary mode – default 'restriction off.*
Note 3: This differs from *permanent mode* in that the caller is able to over-ride the restriction, and is also known as *per-call temporary mode – default 'restriction on.*

Table 6.1a - Mechanisms to express that CLI should be restricted where the caller's default is 'to be presented'

For default CLI presented, the following mechanisms may be used to express a wish that their CLI be restricted:

I.   The Privacy header field contains the priv-value 'id' (RFC 3325 [5]), **or**
   II.   The Privacy header field contains the priv-value 'user' (RFC 3325 [5]) **or**
  III.   The From header field URI contains an anonymous URI (Note 4), **or**
  IV.   The received digit string contains the prefix 141 or other agreed string to assert privacy (Note 5).

Note 4: For Type 3/4/5 CLIs the Originating Network should populate the From header field with an anonymous URI (see permissible formats in section 5.5). For Type 1 and 2 the From header field is populated by the network and should be restricted in line with the preferred format in Section 5.5. The P-Asserted-Identity header field should additionally be restricted Note 5: Any prefix used to assert privacy must be removed prior to the NNI.

Table 6.1b - Mechanisms to express that CLI should be presented where the caller's default is 'to be restricted'

For default CLI restricted, the following mechanisms may be used to express a wish that their CLI be released:
I.   The Privacy header field contains the priv-value 'none' (RFC 3325 [5]), **or**   II.   The received digit string contains the prefix 1470 or other agreed string to disable privacy. (Note 6)
Note 6: Any prefix used to disable privacy must be removed prior to the NNI.

RULE CLI ORIG 5 - **CLI format in signalling systems**
The preceding text about the application of RULES CLI ORIG 2 and CLI ORIG 3 provides guidance on the formatting of CLIs in SIP.

RULE CLI ORIG 6 – Per call invocation of CLI Restriction Service
The preceding text about the application of RULE CLI ORIG 4 provides guidance on the treatment of calls prefixed 141. If the Originating Network does not support invocation of CLI restriction service by dialled digits (prefix 141) then calls using prefix 141 must be routed to a non-chargeable announcement, telling the customer how to restrict their CLI, or to another call failure condition.

RULE CLI ORIG 7 – **Per call override of CLI Restriction Service**
This method applies where CLI is restricted by default.

If the Originating Network does not support invocation of CLI presentation service by dialled Digits (prefix 1470) then calls using prefix 1470 must be routed to a non-chargeable announcement, telling the customer how to release their CLI, or to another call failure condition.

RULE CLI ORIG 8 – Call Blocking
Blocking of calls should be carried out in line with RULE CLI ORIG 8 in ND1016 [3].

In the case where a call is to be blocked the INVITE request should be rejected with a 603 'Decline' response.

6.2 Responsibilities of the Terminating Network with respect to CLI

The Terminating Network is responsible for ensuring that CLI Display Services it provides are compliant with the Ofcom CLI Guidelines. ND1016 [3] defines CLI Display Service as *"The delivery of information to the called party that allows them to be informed of the calling party's line identity. This could be in the form of information that is displayed, recorded, interpreted by a database or provided via an audio message or by any other means".* Hence all methods by which a called party can be informed of the caller's identity are included in this definition, for example:

- Display of the CLI on the called equipment (telephone, computer etc.)

- Last number recall where the network "reads out" the number of the last call when a short code is dialled

- Informing the called party of the callers CLI by e-mail or SMS

- Making a list of incoming call details available on called equipment or via a Web browser

- Allowing a return call to be placed to a caller (without disclosing that number).

The guidance set out below on application of the Terminating Network Rules assumes that for SIP based services the Terminating Network will have received the CLI information in ND1035 [4]-compliant SIP or that signalling interworking to ND1035 [4] SIP has taken place prior to populating the signalling for the UNI.

RULE CLI TERM 1 - Presentation information
The contents of the URI in the From header field is to be used for all CLI Display Services. Note that it is possible for the same CLI to be present in the P-Asserted-Identity header field.

Delivery of diverting party information
Where the Terminating Network wishes to use the content of the History-Info header field for any application, such as providing a service to present diverting party information to the customer, it should be noted that under current specifications the content of a received History-Info header field may be either a Network Number or a Presentation Number (with no indication of which it is). Any such service shall respect any privacy marking associated with the History-Info header field.

RULE CLI TERM 2 - Display rules

The following guidance is given on how to populate the SIP header fields sent across the customer interface (see Note):

Header field population

P-Asserted-Identity header field

The Terminating Network shall not send a P-Asserted-Identity header field to a SIP endpoint.

From header field

The Terminating Network shall use the contents of the received From header field URI for all Caller Display Services.

Where a Privacy header field is received containing a priv-value of 'user' the Terminating Network shall ensure that the From header field sent to a SIP endpoint is anonymised:

<p align="center">sip:anonymous@anonymous.invalid</p>

Where the SIP URI received has a <u>user field</u> of 'anonymous' (case insensitive) then the From header field sent to the SIP endpoint should be:

<p align="center">sip:anonymous@anonymous.invalid</p>

Privacy header field

The Terminating Network shall not send a Privacy header field to the SIP endpoint.

Note: for the purposes of this document, customer interface means any interface to an entity which is not a Public Electronic Communications Network, i.e. "customer interface" includes connections to enterprise networks.

Where the received SIP From header field URI has a user fieldof 'anonymous' (case insensitive) or a Privacy header field contained priv-value of 'user' this should be used on non-SIP interfaces to inform the called party that the caller withheld their CLI.

RULE CLI TERM 3 - Anonymous Call Rejection

Anonymous calls are those where the caller has chosen to make the call anonymous, otherwise known as withholding their CLI. Calls where the CLI is classified as CLI Unavailable are not anonymous calls, as it is likely that the caller has no control of this CLI classification.

The Terminating Network can consider that the calling party has requested privacy when either:

1) The Privacy header field contains the priv-value 'user', or

2) The From header field URI contains a user field of "anonymous" (case insensitive)

RULE CLI TERM 4 - Deletion of stored information.

No additional guidance at this time.

RULE CLI TERM 5 - Diversion / Forwarding
This rule relates to where the Terminating Network provides a diversion service. (Diversion
applied by CPE is out of scope).The following guidance is given on how to populate the SIP header
fields sent to the 'diverted-to' network:

Header field population

P-Asserted-Identity header field
As received

From header field
As received

Privacy header field
As received

History-info header field

The history-info header field should be populated with the Network Number of the diverting
party by the (diverting) Terminating Network and the classification of that Network Number
must be honoured.

Note: ND1016 [3] provides for the optional conveyance of a Presentation Number
associated with the diverting line. The mechanism for accomplishing this in SIP is for
further study.

RULE CLI TERM 6 - End users without CLI Display Service
It is a called party's right to _not_ receive CLI. This is used for example when organisations such as
the Samaritans wish to assure callers that their call will be anonymous. Often this has been
achieved in PSTN networks by the organisation not subscribing to the CLI Display Service.
However where a CLI Display Service is part of the standard service, e.g. where the From: is sent
as standard as part of the SIP signalling to a device, then a mechanism for disabling this service
must be provided.

The following guidance is given on how to populate the SIP header fields sent on the customer
interface:

Header field population

P-Asserted-Identity header field
Not sent

From header field
URI set as follows:

    sip:unavailable@unknown.invalid

Privacy header field
Not sent

RULE CLI TERM 7 – Call Blocking
Blocking of calls should be carried out in line with RULE CLI TERM 7 in ND1016 [3].

The terminating network can take one of the following actions to block the call:

1) Reject the INVITE request with a 603 'Decline' response, or

2) Divert the call to a pre-answer announcement and then reject, or

3) Divert the call to a voicemail platform

Emergency calls are exempt from blocking and are identified either by the presence of a Resource-Priority header field populated as described in ND1035 [4] or by the called address.

6.3   Responsibilities of Transit Networks with respect to CLI

RULE CLI TRAN 1 - Signalling transparency
No additional guidance at this time

RULE CLI TRAN 2 – Call Blocking
Blocking of calls should be carried out in line with RULE CLI TRAN 2 in ND1016 [3].

The terminating network can take one of the following actions to block the call:

1) Reject the INVITE request with a 603 'Decline' response, or

2) Divert the call to a pre-answer announcement and then reject

Emergency calls are exempt from blocking and are identified either by the presence of a Resource-Priority header field populated as described in ND1035 [4] or by the called address.

6.4   Responsibilities of networks providing additional services with respect to CLI

Section 6.4 of ND1016 [3] sets out the requirements of networks providing additional services. There are a series of scenarios which are intended to be addressed by these requirements, but the over-riding characteristic is that the network providing the facility appears to the user to become the Originating Network. Example scenarios include Indirect Access (where a third party network is accessed by the calling party using an access code, and the call is routed according to that network's policy), and networks providing calling card facilities.

Section 6.4 of ND1016 [3] sets out that in this situation, the network providing the Additional Facility effectively becomes the Originating Network, and therefore the guidance to Originating Networks for populating SIP signalling fields set out in Section 6.1 of this document applies.

6.5   Responsibilities of networks interconnecting with networks not covered by this specification with respect to CLI

Section 6.5 of ND1016 [3] contains two rules. Sub-sections 6.5.1 and 6.5.2 of the present document cover RULES CLI NC1 and CLI NC2 respectively.

Non-UK networks may place a different emphasis on the contents of the From & P-Asserted-Identity header fields. UK operators should ensure that this is taken into account when interconnecting.

6.5.1   Guidance on RULE CLI NC1

This section provides guidance to fulfil the rules for handling CLIs received from networks not covered by ND1016 [3]. CLI Information can be received either from an IP or TDM interconnect. The received CLI Information has to be 'normalised' into CLI Information that is not signalling system specific and then used to populate the relevant UK signalling system.

There are three steps to this process:

1. Step One - map the received CLI Information into signalling agnostic CLI Information (see Section 6.5.1.1).
2. Step Two - take the signalling agnostic CLI Information from Step One and sanitise it for UK use (see Section 6.5.1.2).
3. Step Three - populate the UK signalling systems with the sanitised CLI Information from Step Two (see Section 6.5.1.3).

6.5.1.1   Step One - Interpret Ingress Signalling CLI Information to produce Signalling-agnostic CLI Information

6.5.1.1.1   ISUP ingress

In this subsection there are a number of cases where a call should be blocked. If a call is to be blocked then the UK network can either:

1) Reject the IAM request with REL Cause 21, Location 'user', or

2) Divert the call to a pre-answer announcement and then reject

Derivation of Network Number Information

Determination of the Network Number CLI is shown in Table 6.5.1.1.1A.

If any of the Calling Party Number parameter fields contain values other than those indicated in Table 6.5.1.1.1A the call is to be blocked.

Table 6.5.1.1.1A - Determination of the Network Number CLI

Input: ISUP CgPN parameter					Output: Network Number	
Numbering plan indicator	Nature of address indicator	Screening indicator	Number incomplete indicator	Are there any address signals?	E.164 number present?	Classification
E.164	National or International	NP or UPVP	Complete	Yes (Note 1)	Yes	Determined by ISUP CgPN APRI indicator - see Table 6.5.1.1.1B (Note 2)
Note 1: The level of validation of the address digits may vary as a network option.						
Note 2: If a valid Presentation Number CLI is present in the ISUP Generic Number parameter and the determination of the Presentation Number Classification shown in Table 6.5.1.1.1D results in CLI Restricted then the Network Number classification is CLI Restricted.						

Determination of the Network Number Classification is shown in Table 6.1.1.1B

Table 6.5.1.1.1B - Determination of the Network Number Classification

Input: ISUP CgPN parameter APRI indicator	Output: Network Number Classification (Note 3)
Presentation allowed	CLI Available
Presentation restricted	CLI Restricted
Presentation restricted by network	CLI Unavailable (Note 1)
Other (Note 2)	CLI Restricted
Note 1: If valid Presentation Number information is not present in the ISUP Generic Number parameter then the call is to be blocked.	
Note 2: Ref Table A.1/Q.763 [6] handling of unrecognized parameter values: default to "presentation restricted".	
Note 3: If Presentation Number classification is CLI Restricted then Network Number classification is set to CLI Restricted	

Derivation of Presentation Number Information

The Generic Number (GN) parameter is only valid if the Number Qualifier indicator is set to 'additional calling party number (ACgPN)', the Screening Indicator is 'UPNV', and a CLI was present in the ISUP Calling Party Number (CgPN) parameter.

If the above criteria are not met then the Generic Number parameter is discarded.

Determination of the Presentation Number CLI is shown in Table 6.5.1.1.1C

If any of the Generic Number parameter fields contain values other than those indicated in Table 6.5.1.1.1C the call is to be blocked.

Table 6.5.1.1.1C - Determination of the Presentation Number CLI

Input: ISUP GN(ACgPN) parameter					Output: Presentation Number	
APRI	Numbering plan indicator	Nature of address indicator	Number incomplete indicator	Are there any address signals?	E.164 number present?	Classification
Presentation allowed or Presentation restricted	E.164	National or International	Complete	Yes (Note)	Yes	Determined by ISUP GN APRI indicator - see Table 6.5.1.1.1D
Note: The level of validation of the address digits may vary as a network option.						

Determination of the Presentation Number Classification is shown in Table 6.5.1.1.1D

Table 6.5.1.1.1D - ISUP GN APRI handling

Input: ISUP GN parameter APRI	Output: Presentation Number Classification
Presentation allowed	CLI Available
Presentation restricted	CLI Restricted

6.5.1.1.2   SIP ingress

For the purposes of this section, it is assumed that the inbound signalling is RFC3261 [7] compliant. Where the signalling is RFC2543 [8] compliant, additional actions may be required, such as examining the display-name in the From header field to determine if anonymity has been asserted.

It is expected that CLIs received will be telephone numbers in E.164 format. The URIs should be either a tel-URI or a tel-uri expressed as a SIP-URI i.e. user=phone is present.

If the address signals are received in a sip URI then 'user=phone' must be present. If not present the call is to be blocked.

Address signals can be treated as containing an E.164 number when all of the following conditions apply:
1) The address signals are all numeric (The level of validation of the address signals may vary as a network option for example networks may carry out a number length check),
2) A country code is deemed to be present,
3) The address signals are prefixed with '+'; and
4) The phone-context parameter is not present.

In this subsection there are a number of cases where a call should be blocked. If a call is to be blocked then the UK network can either:

1) Reject the INVITE request with 603 'Decline', or

2) Divert the call to a pre-answer announcement and then reject

Derivation of Network Number and Presentation Number Information

Table 6.5.1.1.2A - Derivation of Network Number and Presentation Number Information

Is a P-Asserted-Identity header field URI present?	Does the P-Asserted-Identity header field URI contain an E.164 number? (Note 6)	From header field URI contains: (Note 1)	Privacy header field contains priv-value:	NN	NN Classification	PN	PN Classification (Note 2)
Yes	No (Note 9)	-	-	-	-	-	-
	Yes	an E.164 number	'id'	Yes	CLI Restricted	Yes	CLI Available
			'header'	Yes	CLI Restricted	Yes	CLI Available
			'user' (Note 3)	Yes	CLI Restricted	Yes	CLI Restricted
			'none' (or header field not present) (Note 4)	Yes	CLI Available	Yes	CLI Available
		an anonymous URI (Note 7)	- (Note 5)	Yes	CLI Restricted	No	no classification
No	N/A	an E.164 number	'id'	No	CLI Restricted	Yes	CLI Available
			'header'	No	CLI Restricted	Yes	CLI Available
			'user' (Note 3)	No	CLI Restricted	Yes	CLI Restricted
			'none' (or header field not present) (Note 4)	No	CLI Unavailable (Note 8)	Yes	CLI Available
		an anonymous URI (Note 7)	- (Note 5)	No	CLI Restricted	No	no classification
Note 1: Any From header field URI values not shown in this table shall result in the call being blocked.							
Note 2: A classification is only given when a Presentation Number CLI is present.							
Note 3: When priv-value 'user' is received the Network Number Classification is set to CLI Restricted							
Note 4: If priv-values 'id', 'header' or 'user' are present in the Privacy header field then priv-value 'none' is ignored and discarded							
Note 5: When the From header field contains an anonymous URI the Network Number Classification is set to CLI Restricted							
Note 6: P-Asserted-Identity header fields may contain either or both a SIP and tel URI. In the case where both are present the SIP-URI takes precedence							
Note 7: Case-insensitive string match to sip URI user field (i.e. to the left of '@').							
Note 8: The Network Number classification CLI Unavailable can exist when there is no CLI itself (See section 5.5 of the present document)							
Note 9: Any received P-Asserted-Identity that does not contain an E.164 number shall result in the call being blocked							

6.5.1.2   Step Two - Handling of CLI Information

Table 6.5.1.2A - Sanitising of received CLI Information

NN CLI information		PN CLI information		NN and classification	PN and classification	SIP header field population (See table 6.5.1.3.2A)	ISUP parameter population (see Table 6.5.1.3.1A)
E.164 Number present	Classification (Note 2)	E.164 Number present	Classification (Note 3)				
No	CLI Unavailable	Yes	CLI Available	Inject a NN classified CLI Unavailable	Pass on PN and classification	s1	i5
No	CLI Restricted	No	No classification	Inject an NN classified CLI Restricted	Not present	s5	i2
No	CLI Restricted	Yes	CLI Available	Inject an NN classified CLI Restricted	Pass on PN and classification	s1	i4
No	CLI Restricted	Yes	CLI Restricted	Inject an NN classified CLI Restricted	Pass on PN and classification	s4	i6
Yes	CLI Available	No	No classification	Pass on NN and classification	Not present	s3	i1
Yes	CLI Available	Yes	CLI Available	Pass on NN and classification	Pass on PN and classification	s2	i3
Yes	CLI Restricted	No	No classification	Pass on NN and classification	Not present	s5	i2
Yes	CLI Restricted	Yes	CLI Available	Pass on NN and classification	Pass on PN and classification	s1	i4
Yes	CLI Restricted	Yes	CLI Restricted	Pass on NN and classification	Pass on PN and classification	s4	i6
Yes	CLI Unavailable	Yes	CLI Available	Pass on NN classified CLI Unavailable	Pass on PN and classification	s1	i5
Note 1: For each output row the NN and PN are to be taken as a pair							
Note 2: The output of the Tables in 6.5.1.1 can result in NN CLI classifications of CLI Available or CLI Restricted or CLI Unavailable.							
Note 3: The output of the Tables in 6.5.1.1 can result in either no classification or PN CLI classifications of CLI Available or CLI Restricted.							

6.5.1.3   Step Three - Egress Signalling system population

6.5.1.3.1   ISUP Calling Party Number and Generic Number Parameter Population

Table 6.5.1.3.1A - ISUP Calling Party Number and Generic Number Parameter Population

ISUP parameter population value from Table 6.5.1.2A	ISUP Parameter	Field / Indicator	Value
i1	Calling Party Number	Address Signals field	NN
		Address Presentation Restriction Indicator	0
i2	Calling Party Number	Address Signals field	NN
		Address Presentation Restriction Indicator	1
i3	Calling Party Number	Address Signals field	NN
		Address Presentation Restriction Indicator	0
	Generic Number	Address Signals field	PN
		Address Presentation Restriction Indicator	0
i4	Calling Party Number	Address Signals field	NN
		Address Presentation Restriction Indicator	1
	Generic Number	Address Signals field	PN
		Address Presentation Restriction Indicator	0
i5	Calling Party Number	Address Signals field	NN
		Address Presentation Restriction Indicator	3 (Note)
	Generic Number	Address Signals field	PN
		Address Presentation Restriction Indicator	0
i6	Calling Party Number	Address Signals field	NN
		Address Presentation Restriction Indicator	1
	Generic Number	Address Signals field	PN
		Address Presentation Restriction Indicator	1
Note: The CLI Blocking Indicator in the National Forward Call Indicators shall be set to '0'			

6.5.1.3.2   SIP From and P-Asserted-Identity header field Population

Table 6.5.1.3.2A - SIP From and P-Asserted-Identity header field Population

SIP header field population value from Table 6.5.1.2A	INVITE header field (Note 1)
s1 (Note 2)	P-Asserted-Id: NN@domain;user=phone From: PN@domain;user=phone Privacy: id
s2	P-Asserted-Id: NN@domain;user=phone From: PN@domain;user=phone
s3	P-Asserted-Id: NN@domain;user=phone From: NN@domain;user=phone
s4	P-Asserted-Id: NN@domain;user=phone From: PN@domain;user=phone Privacy: id; user
s5	P-Asserted-Id: NN@domain;user=phone From: anonymous@anonymous.invalid Privacy: id
Note 1: The usage of tel URIs is also permitted, in accordance with RFC3966 [10] and RFC3325 [5].	
Note 2: Network Number classification CLI Unavailable cannot be explicitly signalled in SIP but is implied when NN classification is set to CLI Restricted and the accompanying PN CLI classification is set to CLI Available. As a result, in this case the distinction between NN CLI Unavailable and CLI Restricted in Table 6.5.1.2A is not maintained.	

6.5.2   Guidance on RULE CLI NC2

This section provides guidance to fulfil the rules for handling CLIs routed to networks not covered by ND1016 [3]. RULE CLI NC2 concerns the way that the obligations of RULE CLI TERM 2 (for a network to respect the CLI classification) are applied to calls handed over to networks not covered by this specification.

In order to ensure that CLI is not presented to the called customer unless it is marked as available for display, a network which interconnects to a network not covered by this specification must assess whether that network will act according to the classification (including when handing calls over to subsequent networks). Unless it is known (e.g. following assessment of data protection legislation applicable to the downstream network) that the classification will be respected, the sending network shall ensure that, where the CLI is classified as 'CLI Restricted' or 'CLI Unavailable', the CLIs (and, if appropriate to the signalling system, the classifications) is deleted before the calls are sent to such networks.

The following guidance is given on how to populate the SIP header fields sent to a network which is not trusted to respect the CLI classification:

Header field population

P-Asserted-Identity header field
A P-Asserted-Identity header field shall not be sent unless the received Network Number CLI classification is 'CLI Available'.

From header field
If the Presentation Number CLI is classified as 'CLI Restricted', then the From header field shall be anonymised i.e.
anonymous@anonymous.invalid

Privacy header field
If the P-Asserted-Identity header field is not sent then priv-value of 'id' shall not be included in any privacy header field.

Other header fields
Care should be taken to ensure that where CLI is classified as 'CLI Restricted' or 'CLI Unavailable', then other information which is potentially characterised as being restricted personal data does not appear in any form in other header fields such as the Contact header.

6.6   Responsibilities of networks performing interworking between signalling systems with respect to CLI

No additional guidance at this time.

7   Connected Line Identity

Section 7 of ND1016 [3] addresses network requirements associated with Connected Line Identity (COL). As the scope of this document is Calling Line Identity (CLI) only, there is no specific guidance with respect to COL.

8   Signalling format of customer line information

All CLIs are to be carried in SIP as international numbers, i.e. they shall include the appropriate country code preceded by +. For example +441234567890, +334321567890. See ND1035 [4] for further information.

9   Usage of customer line information for network operation

ND1016 sets out that its operation does not affect the ability of CPs to use received customer line identification data for purposes given in the Ofcom CLI Guidelines [2], to which CPs should refer.

History

Document history		
1.1.1	November 2015	Initial publication
2.1.1	October 2017	New publication with updates
3.1.1	October 2019	Published
4.1.1	February 2020	Published with updates
4.1.2	May 2020	Updated publication
4.2.1	November 2020	Modification to RULE CLI TERM 1 and TERM 2 to align with ND1016 regarding two number delivery