ATIS-1000073

Technical Report on Use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information

TECHNICAL REPORT

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

ATIS-1000073, *Technical Report on Use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information*

Is an ATIS Standard developed by the **Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000073

ATIS Technical Report on

Technical Report on Use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information

Alliance for Telecommunications Industry Solutions

Approved November 30, 2016

Abstract

This technical report documents the use of the Integrated Services Digital Network (ISDN) User Part (ISUP) Screening Indicator, as deployed in today's network, for conveying Caller ID Authentication information. The Technical Report (TR) assesses the reliability of the information conveyed in the ISUP Screening Indicator and identifies limitations based on current standards and regulations. In addition, the TR documents the changes required to standards, particularly ATIS-1000679, to increase the viability of using the ISUP Screening Indicator.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. International Telecommunication Union – Telecommunications Sector (ITU-T) and U.S. International Telecommunication Union – Radiocommunication Sector (ITU-R) Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PTSC, which was responsible for its development, had the following leadership:

M. Dolly, PTSC Chair (AT&T)

V. Shaikh, PTSC Vice-Chair (Applied Communications Sciences)

Table of Contents

Table of Figures

Table of Tables

ATIS Technical Report on –

Use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information

1 Introduction

The Federal Communications Commission (FCC), as part of its request to address robocalling and spoofing, requested an assessment of the feasibility of using the ISUP Screening Indicator for conveying Caller ID Authentication information interworked at a PSTN Gateway from/to either a digitally signed Session Initiation Protocol (SIP) P-Asserted-Identity (PAI) or FROM header.

This technical report documents the use of the ISUP Screening Indicator, as deployed in today's network, for conveying Caller ID Authentication information. The Technical Report (TR) assesses the reliability of the information conveyed in the ISUP Screening Indicator and identifies limitations based on current standards and regulations. In addition, the TR documents the changes required to standards, particularly ATIS-1000679, to increase the viability of using the ISUP Screening Indicator.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

ATIS-1000679.2015, *Interworking between Session Initiation Protocol (SIP) and ISDN User Part.*[1]

ATIS-1000625.1993(R2013), *Integrated Services Digital Network (ISDN) – Calling Line Identification Presentation and Restriction Supplementary Services*.[2]

ATIS-1000639.1995(S2016), *Calling Name Identification Restriction.*[3]

ATIS-1000639.a.2001(S2016), *Supplement to Calling Name Identification Restriction.*[4]

3GPP TS 29.163, *Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks.*[5]

RFC 3398, *Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping,* December 2002.[6]

GR-31-CORE, LSSGR CLASS[SM] Feature: Calling Number Delivery (FSD 01-02-1051) (a module of LSSGR, FR-64), Telcordia Technologies, June 2000.[7]

---

[1] Available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street NW, Suite 500, Washington, DC 20005, at: < https://www.atis.org/docstore/product.aspx?id=25371 >.

[2] Available from ATIS at: < https://www.atis.org/docstore/product.aspx?id=27977 >.

[3] Available from ATIS at: < https://www.atis.org/docstore/product.aspx?id=25490 >.

[4] Available from ATIS at: < https://www.atis.org/docstore/product.aspx?id=25491 >.

[5] Available from the Third Generation Partnership Project (3GPP) at: < www.3gpp.org >.

[6] Available from the Internet Engineering Task Force (IETF) at: < https://www.ietf.org/ >.

[7] Available from Telcordia at: < http://telecom-info.telcordia.com/site-cgi/ido/index.html >.

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

3.1 Definitions

Caller identity: The originating phone number included in call signalling used to identify the caller for call screening purposes. In some cases this may be the Calling Line Identification or Public User Identity. For the purposes of this study, the caller identity may be set to an identity other than the caller's Calling Line Identification or Public User Identity.

3.2 Acronyms & Abbreviations

APRI	Address Presentation Restricted Indicator
ASCII	American Standard Code for Information Interchange
AT	Access Tandem
ATIS	Alliance for Telecommunications Industry Solutions
CC	Country Code
CgPN	Calling Party Number
CLI	Calling Party Identification
CPE	Customer Premises Equipment
EO	End Office
IP	Internet Protocol
ITU-R	International Telecommunication Union – Radiocommunication Sector
ITU-T	International Telecommunication Union – Telecommunication Sector
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
NS/EP	National Security/Emergency Preparedness
TDM	Time-Division Multiplexing
TN	Telephone Number
PAI	P-Asserted-Identity
PSTN	Public Switched Telephone Network
SI	Screening Indicator
SIP	Session Initiation Protocol
SHAKEN	Signature-based Handling of Asserted information using toKENs
STIR	Secure Telephone Identity Revisited
URI	Uniform Resource Identifier

4 Architecture

Figure 4.1 illustrates the architectures where signaling interworking occurs, specifically at Public Switched Telephone Network (PSTN) gateways:

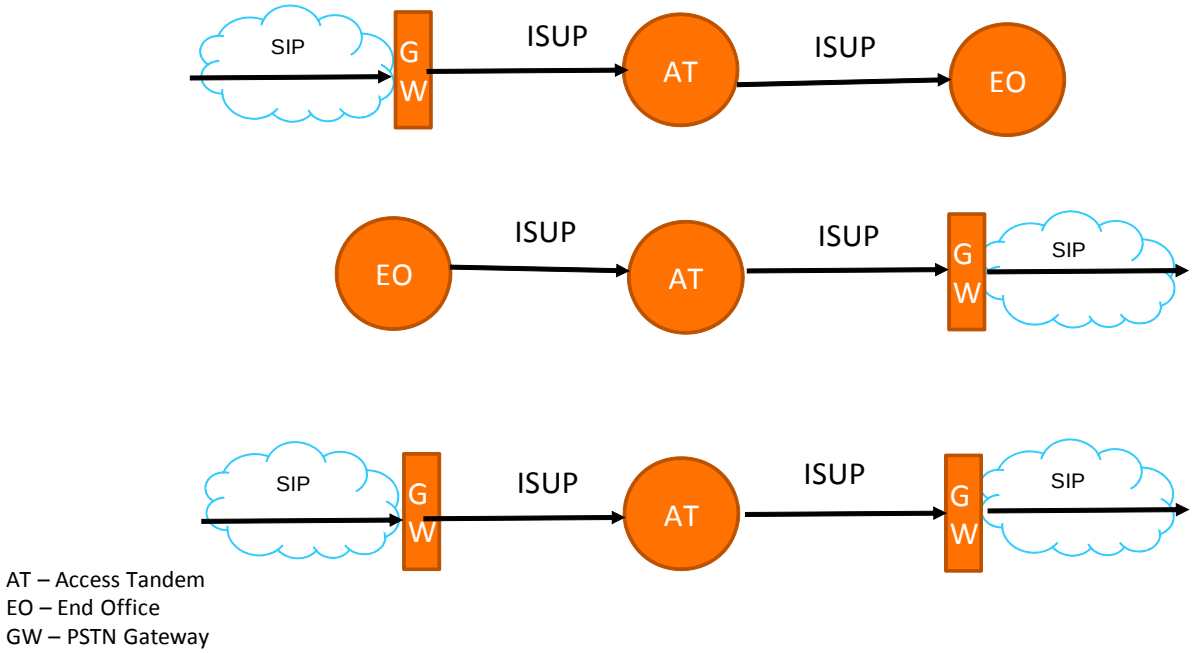

Figure 4.1 – ISUP/SIP Interworking Scenarios

5 PSTN Gateway Interworking

5.1 SIP to ISUP Interworking

The table below illustrates the existing SIP to ISUP interworking specified by ATIS-1000679.

Table 5.1 – SIP to ISUP

PAI Present	FROM Present	CgPN	Screening Indicator
No	No	Include a network provided E.164 number Or	Network provided
		omit the Address Signals	NA
No	Yes	FROM	User provided, not verified
Yes	No	PAI	Network provided
Yes	Yes	PAI	Network provided

5.2 ISUP to SIP Interworking

The table below illustrates the existing ISUP to SIP interworking specified by ATIS-1000679.

Table 5.2 – ISUP to SIP

CgPN (Complete E.164)	Screening Indicator	SIP
No	NA	FROM populated with "Unavailable@ Hostportion"
Yes	user provided, verified and passed or network provided	PAI and FROM
	user provided, not verified or user provided, verified and failed	FROM

5.3 Considerations

- Early implementations/deployments, particularly those supporting RFC 3398, where there is no Screening Indicator Mappings, do not support the parameter interworking defined in ATIS-1000679.
- P-Asserted-Identity (PAI) headers can be received from untrusted sources (e.g., Voice over Internet Protocol [VoIP] Wholesale or International Gateways).
- These currently get interworked into the Calling Party Number (CgPN) with a Screening Indicator (SI) of "network verified", which therefore will result in the CgPN being presented to the Called Party per ATIS-100625.

6 Proposed Solutions

6.1 Solution 1

Interwork successfully verified signed PAI or FROM headers, attesting that the device can use the Telephone Number (TN), into the CgPN with a SI value of "user provided, verified and passed".

Interwork unsigned PAI into a SI value of "user provided, verified and failed". This would result in switches compliant to ATIS-1000625 not passing CgPN to the end user. In the long term this will provide better integrity to the CgPN at those switches, but CgPN from VoIP or international gateways will not be passed to the end user due to the fact that gateways cannot attest to whether the TN can be used by the device.

Also, in the interim deployment period where authentication/verification of the CgPN is being deployed in VoIP networks, there will be service complaints due to the CgPN not being delivered when it actually should.

6.1.1 Standards Gap

Standards modifications are required to ATIS-1000679. Currently, there is no processing based on successfully verified signed SIP PAI or FROM headers. The table below illustrates changes to Table 5.1 in Section 5.1 if the PAI/FROM number is not signed. Changes are highlighted in bold.

Table 6.1 – SIP to ISUP if the PAI/FROM number is not signed

PAI Present	Number Present in FROM	CgPN	Screening Indicator
No	No	Include a network provided E.164 number	Network provided.
		omit the Address Signals	NA
No	Yes	FROM	**User provided, verified and failed.**
Yes	No	PAI	**User provided, verified and failed.**
Yes	Yes	PAI	**User provided, verified and failed.**

The table below illustrates changes to Table 5.1 in Section 5.1 if the PAI/FROM number is signed and successfully verified. Changes are highlighted in bold.

Table 6.2 – SIP to ISUP if the PAI/FROM number is signed and successfully verified

PAI Present	Number Present in FROM	CgPN	Screening Indicator
No	No	Include a network provided E.164 number	Network provided
		omit the Address Signals	NA
No	Yes	FROM	**User provided, verified and passed**
Yes	No	PAI	**User provided, verified and passed**
Yes	Yes	PAI	**User provided, verified and passed**

6.1.2 Considerations

It is unlikely there would be consensus to modify the global standards procedures in 3GPP TS 29.163.

There are potential service impacts unless PAI numbers from VoIP Enterprises are successfully signed and verified per Secure Telephone Identity Revisited (STIR)/ Signature-based Handling of Asserted information using toKENs (SHAKEN) (ATIS-1000074).

ATIS-10000625 is applicable for Integrated Services Digital Network (ISDN) and not analog line call processing. End office analog line call processing is compliant to GR-31-CORE, where there is no screening performed on the ISUP Calling Party Number Screening Indicator, thereby all CgPNs are sent to the user independent of the ISUP Calling Party Number Screening Indicator value. Thereby this potential solution provides no value to the majority of circuit switched users.

If it can be confirmed that switches with ISDN lines comply to ATIS-1000625, there would be greater integrity in the CgPN delivered to these customers, though CgPN from VoIP or International gateways will not be delivered, which will result in customer complaints.

6.2 Solution 2

Interwork successfully verified signed SIP PAI or FROM headers, attesting that the device can use the TN, into the CgPN with a SI value of “user provided, verified and passed”. If the PAI or FROM headers are not signed, no number is populated into the outgoing ISUP CgPN parameter.

6.2.1 Standards Gap

Standards modifications are required to ATIS-1000679. Currently, there is no processing based on successfully verified signed PAI or FROM headers. The table below illustrates changes to Table 5.1 in Section 5.1 if the PAI/FROM number is not signed. Changes are highlighted in bold.

Table 6.3 – SIP to ISUP if the PAI/FROM number is not signed

PAI Present	**Number Present in FROM**	**CgPN**	**Screening Indicator**
No	No	Include a network provided E.164 number or	Network provided
		omit the Address Signals	NA
No	Yes	**omit the Address Signals** (NOTE 1)	**NA**
Yes	No	**omit the Address Signals** (NOTE 1)	**NA**
Yes	Yes	**omit the Address Signals** (Note 1)	**NA**

NOTE 1: If the PAI/FROM number is a non-US E.164 number (as from an International Gateway), the PSTN Gateway may optionally include the International E.164 number.

The table below illustrates changes to Table 5.1 in Section 5.1 if the PAI/FROM number is signed and successfully verified. Changes are highlighted in bold.

Table 6.4 – SIP to ISUP if the PAI/FROM number is signed and successfully verified

PAI Present	**Number Present in FROM**	**CgPN**	**Screening Indicator**
No	No	Include a network provided E.164 number	Network provided
		omit the Address Signals	NA

PAI Present	Number Present in FROM	CgPN	Screening Indicator
No	Yes	FROM	**User provided, verified and passed**
Yes	No	PAI	**User provided, verified and passed**
Yes	Yes	PAI	**User provided, verified and passed**

6.2.2 Considerations

It is unlikely there would be consensus to modify the global standards procedures in 3GPP TS 29.163.

For the scenarios where the CgPN in either the PAI or FROM is dropped at the PSTN Gateway, there will be service complaints due to the change in customer perception and expectations. This includes calls from VoIP and International gateways, both in the interim deployment period, as well as in the long term.

This solution would require a waiver from the FCC to not relay the CgPN transparently (i.e., drop CgPN at the PSTN Gateway).

6.3 Solution 3

This solution is similar to Solution 2, where the successfully verified signed PAI or FROM headers, attesting that the device can use the TN, are interworked into the CgPN with a SI value of "user provided, verified and passed". It differs in that if the PAI or FROM headers are not signed, a "network provided" number (e.g., pseudo number that is unique to each carrier) is populated into the outgoing ISUP CgPN parameter with an indication of "network provided" in the SI field.

The pseudo number would be unique per carrier for the purpose of traceback and have an associated Calling Name with a value of "UNVERIFIED". This solution does not assume that all subscriptions have Calling Name service. Through consumer education, the pseudo number would be recognized as an unverified number. This is to ensure backward compatibility with earlier generations of caller ID devices that only support numeric American Standard Code for Information Interchange (ASCII) characters. However, for subscribers of the Calling Name service, a name string of "UNVERIFIED" or "UNVERIFIED NMBR" would be delivered in the name field (limit is still 15 characters for older Customer Premises Equipment [CPE]).

6.3.1 Standards Gap

Standards modifications are required to ATIS-1000679. Currently, there is no processing based on successfully verified signed PAI or FROM headers.

The table below illustrates changes to Table 5.1 in section 5.1 if the PAI/FROM number is not signed. Changes are highlighted in bold.

Table 6.5 – SIP to ISUP if the PAI/FROM number is not signed

PAI Present	Number Present in FROM	CgPN	Screening Indicator
No	No	Include a network provided E.164 number or	Network provided

PAI Present	Number Present in FROM	CgPN	Screening Indicator
		omit the Address Signals	NA
No	Yes	**Include a network provided pseudo E.164 number** (NOTE 1)	**Network provided**
Yes	No	**Include a network provided pseudo E.164 number** (NOTE 1)	**Network provided**
Yes	Yes	**Include a network provided pseudo E.164 number** (NOTE 1)	**Network provided**

NOTE 1: If the PAI/FROM number is a non-US E.164 number (as from an International Gateway), the PSTN Gateway may optionally include the received International E.164 number and set the Screening Indicator to "user provided, not verified".

The table below illustrates changes to Table 5.1 in Section 5.1 if the PAI/FROM number is signed and successfully verified. Changes are highlighted in bold.

Table 6.6 – SIP to ISUP if the PAI/FROM number is signed and successfully verified

PAI Present	Number Present in FROM	CgPN	Screening Indicator
No	No	Include a network provided E.164 number or	Network provided
		omit the Address Signals	NA
No	Yes	FROM	**User provided, verified and passed**
Yes	No	PAI	**User provided, verified and passed**
Yes	Yes	PAI	**User provided, verified and passed**

6.3.2 Considerations

It is unlikely there would be consensus to modify the global standards procedures in 3GPP TS 29.163.

For the scenarios where the Calling Party Number in either the PAI or FROM header is changed at the PSTN Gateway, there may be service complaints due to the change in customer perception and expectations with respect to what number is delivered in the CgPN. This includes calls from VoIP and International gateways, both

in the interim deployment period as well as in the long term. Though, this may be mitigated with consumer education when they receive the “UNVERIFIED” Calling Name value associated with the pseudo number.

7 Analysis

All potential solutions require development in the PSTN Gateways as per modifications to ATIS-1000679, and support of or interaction with the STIR/SHAKEN verification function. Currently, there is no processing based on successfully verified signed PAI or FROM headers. Some PSTN Gateways are older legacy equipment that may not be able to be modified to support the modifications to ATIS-1000679, and support of or interaction with the verification function.

It should be noted that all of the following solutions will result in the current CgPN the user expects to see no longer being delivered, and will impact services (e.g., National Security/Emergency Preparedness [NS/EP]).

NOTE: Investigation of potential implications on the NS/EP end user community will need specific consideration before adopting a candidate solution. It is possible that the candidate solutions may have unknown or unintended consequences to the NS/EP user community. For example, it is possible that a called party may decide to not answer a NS/EP Priority Services (e.g., GETS or WPS) call because it is displayed as a pseudo number, or the CgPN is not displayed when it was expected. Therefore, adoption of any proposed solution should consider identification of potential implications on NS/EP to ensure that appropriate mitigation measures are in place (e.g., NS/EP specific end user training and awareness).

- Solution 1 is the least desirable as it does not provide increased CgPN integrity to analog lines.
- Solution 2 provides increased CgPN integrity, but would require an FCC waiver in order to drop the CgPN when the PAI or FROM header is not signed and successfully verified, thereby attesting that the device can use the TN. In addition, it would be service impacting to customers who had expectations of receiving a CgPN from certain devices.
- Solution 3 is the most viable of the solutions as it provides the greatest integrity of the CgPN, while being the least impacting to existing customer expectations with respect to delivery of CgPN. However, for those networks with both Time-Division Multiplexing (TDM) and Internet Protocol (IP) architectural scenarios, this would be service-impacting and confusing to end user customers who had expectations of receiving a specific CgPN.

For all of the above, consideration needs to be given to when the STIR/SHAKEN verification framework would be widely deployed together with expectations for PSTN circuit switched retirement in order to understand the benefit of expending resources toward implementing one of these potential solutions.

8 Conclusion

This Technical Report assesses three potential industry solutions for using the ISUP Screening Indicator to convey Caller ID Authentication information. The pros and cons of each potential solution are provided for consideration in determining any future work.

Annex A
(informative)

A Excerpts from ATIS-1000679 on ISUP to SIP Interworking of Calling Party Identification Information

This annex will document supportive material from ATIS-1000679 on interworking Calling Party Identification (CLI) information between ISUP and SIP.

Table A.1 – Mapping of SIP From/P-Asserted-Identity/Privacy headers to ISUP CLI parameters

Has a "P-Asserted-Identity" header field containing a URI (Note 2) with an identity in the format "+CC"+"NDC"+"SN" been received?	**Has a "From" header field (Note 3) containing a URI with an identity in the format "+CC"+"NDC"+"SN" been received?**	**Calling Party Number parameter Address signals**	**Calling Party Number parameter APRI**
No	No	Network option to either include a network-provided E.164 number (see Table 6.5) or omit the Address Signals.	If a Privacy header field was received, set APRI as indicated in Table A.2. Otherwise, Network option to set APRI to "presentation restricted" or "presentation allowed".
No	Yes	Derived from the From header field (see Table 6.7).	If a Privacy header field was received, set APRI as indicated in Table A.2. Otherwise, Network option to set APRI to "presentation restricted" or "presentation allowed".
Yes	No	Derived from P-Asserted-Identity (see Table 6.6).	APRI = "presentation restricted" or "presentation allowed" depending on SIP Privacy header. (See Table A.2)
Yes	Yes	Derived from P-Asserted-Identity (see Table 6.6).	APRI = "presentation restricted" or "presentation allowed" depending on SIP Privacy header. (See Table A.2)

Table A.2 – Mapping of P-Asserted-Identity and Privacy Headers to the ISUP Calling Party Number Parameter

Source SIP header field and component	Source component value	Calling Party Number parameter field	Derived value of parameter field
-	-	Numbering Plan Indicator	"*ISDN (Telephony) numbering plan (Recommendation E.164)*"
P-Asserted-Identity, appropriate global number portion of the URI, assumed to be in form "+" CC+NDC+SN (Note 1)	CC	Nature of Address Indicator	If CC is equal to the country code of the country where I-IWU is located AND the next ISUP node is located in the same country then set to *"national (significant) number"* else set to "*international number*".
Privacy, priv-value component (Note 2)	Privacy header field absent	Address Presentation Restricted Indicator (APRI)	"*presentation allowed*"
	"*none*"		"*presentation allowed*"
	"*header*"		"*presentation restricted*"
	"*user*"		"*presentation restricted*"
	"*id*"		"*presentation restricted*"
-	-	Screening Indicator	"*network provided*"
P-Asserted-Identity, appropriate global number portion of the URI, assumed to be in form "+" CC+NDC+SN (Note 1)	CC, NDC, SN	Address Signals	If NOA is "*national (significant) number*" then set to NDC + SN. If NOA is "*international number*" then set to CC+NDC+SN

NOTE:

1 – It is possible that the P-Asserted-Identity header field includes both a tel: URI and a sip: URI. The handling of this case is for further study.

2 – It is possible to receive multiple priv-values, one of which is "*none*", the other "*id*", "header", or "user". In this case, APRI shall be set to "*presentation restricted*".

Table A.3 – Mapping of SIP From Header Field to ISUP Calling party number parameter

Source SIP header field and component	Source component value	Call party number parameter field	Derived value of parameter field
–	–	Type of Address	"supplemental user provided calling address – not screened"
From, userinfo component of URI assumed to be in form "+" CC+NDC+SN	CC	Nature of Address Indicator	If CC is equal to the country code of the country where I-IWU is located AND the next ISUP node is located in the same country then set to *"national (significant) number"* else set to "*international number*".
–	–	Numbering Plan Indicator	"*ISDN (Telephony) numbering plan (Recommendation E.164)*"
Privacy, priv-value component (Note 1)	Privacy header field absent	Address Presentation Restricted Indicator (APRI)	"presentation allowed"
	"none"		"presentation allowed"
	"header"		"presentation restricted"
	"user"		"presentation restricted"
	"id"		"presentation restricted"
	-	Screening Indicator	"user provided, not screened"
From, userinfo component assumed to be in form "+" CC+NDC+SN	CC, NDC, SN	Address Signals	If NOA is "*national (significant) number*" then set to NDC + SN. If NOA is "*international numbe*r" then set to CC+NDC+SN.

NOTE:

1 – It is possible to receive multiple priv-values, one of which is "none", the other "header", "user" or "id". In this case, APRI shall be set to "presentation restricted".

Table A.4 – ISUP CLI Parameters to SIP Header fields

<table>
<tr><th>Has a Calling Party Number parameter with complete E.164 number, with APRI = “presentation allowed” or “presentation restricted” been received?</th><th>P-Asserted-Identity header field</th><th>From header field: display-name (optional) and addr-spec</th><th>Privacy header field</th></tr>
<tr><td>N</td><td>Header field not included.</td><td>Unavailable@ Hostportion</td><td>Header field not included.</td></tr>
<tr><td rowspan="2">Y
(See Note 1)</td><td rowspan="2">If the Screening Indicator is “User provided, screening passed” or “Network provided”, then derived from Calling Party Number parameter address signals (see Table A.5). Otherwise, the P-Asserted-Identity header field is omitted.</td><td>display-name may be derived from Calling Party Number (CgPN) if possible.</td><td rowspan="2">If Calling Party Number parameter APRI = “restricted” then priv-value is set to “user”. “id” is also included when P-Asserted-Identity header field is provided. For other APRI settings Privacy header is not included or if included, “id” is not included. “user” also may not be included depending of privacy services applied. (See Table A.2)</td></tr>
<tr><td>addr-spec is derived from Calling Party Number parameter address signals (see Table A.6).</td></tr>
<tr><td colspan="4">NOTE:
1 – A Network Provided CLI in the CgPN parameter may occur on a call from an analogue access line. Therefore in order to allow the “display” of this Network Provided CLI at a SIP UAS it must be mapped into the SIP From header. It is also considered suitable to map into the P-Asserted-Identity header since in this context it is a fully authenticated CLI related exclusively to the calling line, and therefore valid as a User Provided – Passed Screening CLI for this purpose.</td></tr>
</table>

Table A.5 – Mapping of Calling Party Number parameter to SIP P-Asserted-Identity header fields

ISUP Parameter/field	Value	SIP Component	Value
Calling Party Number		P-Asserted-Identity header field	display-name (optional) and addr-spec
Nature of Address Indicator	"national (significant) number"	addr-spec	Add CC (of the country where the IWU is located) to CgPN address signals then map to URI.
	"international number"		Map complete CgPN address signals to URI.
Address signal	If NOA is "national (significant) number" then the format of the address signals is: NDC + SN If NOA is "international number" then the format of the address signals is: CC + NDC + SN	display-name	display-name may be mapped from Address Signal, if possible and network policy allows it.
		addr-spec	"+CC" "NDC" "SN" mapped to the appropriate global number portion of URI scheme used.

Table A.6 – Mapping of ISUP Calling Party Number parameter to SIP From header fields

ISUP Parameter / field	Value	SIP Component	Value
Calling Party Number		From header field	display-name (optional) and addr-spec.
Nature of Address Indicator	"national (significant) number"	addr-spec	Add CC (of the country where the IWU is located) to CgPN address signals then map to user portion of URI scheme used.
	"international number"		Map complete CgPN address signals to map to user portion of URI scheme used.
Address signal	If NOA is "national (significant) number" then the format of the address signals is: NDC + SN If NOA is "international number" then the format of the address signals is: CC + NDC + SN.	display-name	Display-name may be mapped from Address Signal, if possible and network policy allows it.