TTC STANDARD

JJ-90.22

Technical Specification on Network Asserted User Identity Information Transferring through Provider’s SIP Networks

（English Edition）

Version 1.1a

March 11, 2013

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

Introduction

This document provides the TTC original Standard formulated by the TTC Signaling working group.

The working group translated JJ-90.22 Japanese Version 1 (June 2, 2005) into English, and issued JJ-90.22 English Version on August 25, 2005.

In case of dispute, the original to be referred is the Japanese Edition of the text.

August 25, 2005
TTC Signaling Working Group

Contents

<Reference> 6
1. Overview 8
1.1. Scope 8
1.2. Objectives and Provisions of this Standard 8
1.3. Contents of this Standard 8
1.4. Terminology 8
2. Interworking Model for Network-asserted User Identity Information 9
2.1. Joint Trust Domain Model 9
2.2. Transfer Model for Network-asserted User Identity Information 10
3. Information Components 11
3.1. Notification/Restriction information 11
3.2. Network-asserted User Identity Information 11
3.2.1. SIP_URI 12
3.2.2. SIP_DISPLAYNAME 12
3.2.3. TEL_URI 12
3.2.4. TEL_DISPLAYNAME 12
3.3. Interpretation of Omitted Network-asserted User Identity Information Components 12
3.3.1. SIP_URI 12
3.3.2. SIP_DISPLAYNAME 12
3.3.3. TEL_URI 12
3.3.4. TEL_DISPLAYNAME 12
4. Transfer Process Model 13
4.1. Inbound Processing (Determine Content) 13
4.2. Transfer Process 13
4.3. Outbound Processing (Output) 13
5. Trust of a Connection Interface 14
5.1. Definition of Trust 14
5.1.1. Trustworthiness of Connection Interface Itself 14
5.1.2. Trustworthiness of Interconnected Domains 14
5.1.3. Trustworthiness of Network-asserted User Identity Information Processing in Interconnected Domains14
5.2. General Behaviors based on Trust 14
5.2.1. Inbound Boundary 14
5.2.2. Outbound Boundary 14
Annex a. Transferring Network-asserted User Identity Information in Interface A 15
a.1. Overview 15
a.2. Application Model 15
a.3. Interface Type 15
a.3.1. Technical References 15
a.3.2. Trustworthiness 15
a.3.3. SIP Messages to be Applied 15
a.3.4. Character Set Applied to SIP_DISPLAYNAME 16
a.4. Behaviors Particular to the Interface 16

a.4.1. Inbound Processing 16
a.4.2. Outbound Processing 16
Annex b. Transferring Network-asserted User Identity Information in Interface B 19
b.1. Overview 19
b.2. Application Model 19
b.3. Interface Type 19
b.3.1. Technical References 19
b.3.2. Trustworthiness 19
b.3.3. SIP Messages to be Applied 19
b.3.4. Character Set Applied to SIP_DISPLAYNAME 19
b.4. Behaviors Particular to the Interface 20
b.4.1. Inbound Processing 20
b.4.2. Outbound Processing 20
Annex c. Transferring Network-asserted User Identity Information in Interface C 22
c.1. Overview 22
c.2. Application Model 22
c.3. Interface Type 22
c.3.1. Technical References 22
c.3.2. Trustworthiness 22
c.3.3. SIP Messages to be Applied 22
c.3.4. Character Set Applied to SIP_DISPLAYNAME 22
c.4. Behaviors Particular to the Interface 23
c.4.1. Inbound Processing 23
c.4.2. Outbound Processing 28
Appendix i. : Notes on Specifications for Transferring Network-asserted User Identity Information 31
i.1. Transparent Transfer of Information 31
i.2. Interworking without translating into SIP Messages 31
i.3. Long-term Solution for Transfer of Network-asserted User Identity Information 31
Appendix ii. Guidelines in making rules for the new interface type 32
ii.1. Interface Type 32
ii.2. Interface-unique Behaviors 32
ii.2.1. Inbound Processing 32
ii.2.2. Outbound Processing 32
Appendix iii. : Trustworthiness of network-asserted user identity information at Interface B 33
iii.1. Overview 33
iii.2. Necessary Requirements in Interface B 33
iii.3. Security Risk When Not Satisfying Necessary Requirements 33
iii.4. Solution Examples 33
iii.4.1. Use of TLS 33
iii.4.2. Making use of SIP REGISTER/INVITE 33
iii.4.3. Authentication by a Shared Key 34
iii.4.4. Limiting the Source IP Address 34
Limiting Used Ports 34

<Reference>

1. Relationship with International Recommendations

There is no particular relation to international recommendations.

2. History of Revised Version

Revision.	Date	Description
Version 1.0	June 2, 2005	Initial publication (revision of TS-1004, Version 1.0; clarification of parameter interworking conditions in Interface C)
Version 1.1	March 6, 2009	Correction in c.4.1.1. “presentation restricted” to “notification”
Version 1.1a	March 11, 2013	Correction to mistranslations in Table c-6/JJ-90.22 and the footnote in page 25.

3. References

3.1. Normative References

[1] Andreasen, F., “Media Gateway Control Protocol (MGCP),” RFC 3435, Internet Engineering Task Force (IETF), January 2003.

[2] International Telecommunications Union, “The International Public Telecommunications Numbering Plan,” ITU-T Recommendation E.164, 1997.

[3] “SIP: Session Initiation Protocol,” TTC Standard JF-IETF-RFC3261, Ver. 1, The Telecommunication Technology Committee (TTC), June 2005.

[4] “A Privacy Mechanism for the Session Initiation Protocol (SIP),” TTC Standard JF-IETF-RFC3323, Ver. 1, The Telecommunication Technology Committee (TTC), June 2005.

[5] “Short Term Requirements for Network Asserted Identity,” TTC Standard JF-IETF-RFC3324, Ver. 1, The Telecommunication Technology Committee (TTC), June 2005.

[6] “Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks,” TTC Standard JF-IETF-RFC3325, Ver. 1, The Telecommunication Technology Committee (TTC), June 2005.

[7] “Technical Specification on SIP to TTC ISUP Interworking,” TTC Standard JF-IETF-RFC3398, Ver. 1, The Telecommunication Technology Committee (TTC), June 2005.

[8] “The tel URI for Telephone Numbers,” TTC Standard JF-IETF-RFC3966, Ver. 1, The Telecommunication Technology Committee (TTC), June 2005.

[9] “ISUP formats and codes,” TTC Standard JT-Q763, Ver. 20, The Telecommunication Technology Committee (TTC), May 2002.

[10] “ISUP signaling procedures,” TTC Standard JT-Q764, Ver. 12, The Telecommunication Technology Committee (TTC), May 2002.

[11] “Inter-Carrier Interface based on ISUP,” TTC Standard JJ-90.10, Ver. 6, The Telecommunication Technology Committee (TTC), April 2003.

[12] “Technical Specification of the Framework on Provider’s SIP Networks,” TTC Standard JJ-90.21, The Telecommunication Technology Committee (TTC), June 2005.

3.2. Informative References

[13] Peterson, J. and Jennings, C., “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP),” draft-ietf-sip-identity-04, Internet Engineering Task Force (IETF), Work in Progress, February

2005.

[14] "Technology Report on Session Initiation Protocol (SIP)," TR-1007, The Telecommunication Technology Committee (TTC), March 2003.

4. Industrial Property Rights

Information regarding submission of the TTC "The Policy for the Handling of Industrial Property Rights" is available on TTC's home page.

5. Contact

Signaling Working Group

1. Overview

1.1. Scope

This standard applies to a provider’s SIP network (SIP trust domain) as specified in JJ-90.21 [12] that wishes to send and receive network-asserted user identity information specified in this standard via a connection interface.

1.2. Objectives and Provisions of this Standard

- This standard specifies a general interworking model for the appropriate sending and receiving of network-asserted user identity information via a connection interface (not necessarily SIP) between a provider’s SIP network (SIP trust domain) and other provider’s network or user (including cases of indirect connection).
- This standard specifies specific behaviors at a provider’s SIP network boundary so that network-asserted user identity information related to the calling (originating) user can be used between that provider’s SIP network (SIP trust domain) and other provider’s network.
- For users managed by a provider’s SIP network (SIP trust domain), this standard specifies specific Behaviors at a provider’s SIP network boundary to enable the provision of CLIP/CLIR services or equivalent as provided by an ISUP network via an interconnect interface of the type specified in JJ-90.10 [11].

1.3. Contents of this Standard

This standard specifies the requirements and connection-interface conditions that a provider’s SIP network must satisfy in order to appropriately send and receive network-asserted user identity information within the scope prescribed in Section 1.1. This document is configured as follows.

- Main body: Specifies the transfer model for the network-asserted user identity information targeted by this standard.
- Attached materials: Describes boundary processing at the connection interface of a provider’s SIP network by interface type.
  Transfer of network-asserted user identity information in Interface A (Annex A)
  Transfer of network-asserted user identity information in Interface B (Annex B)
  Transfer of network-asserted user identity information in Interface C (Annex C)
- Appendices: Provides reference information for the main body of the document and attached materials.

Appendix 1: Cautionary notes on specifications for transferring network-asserted user identity information
Appendix 2: Guidelines on establishing new interface types
Appendix 3: Trustworthiness of network-asserted user identity information in Interface B

1.4. Terminology

The terminology in this standard related to JF-IETF-RFC3261 [3] basically conforms to Annex 1 of TR-1007 [14] and to JJ-90.21 [12].

The following defines major terms used in the main body, Annexes, and appendices of this standard.

Inbound (direction)

The direction corresponding to the transfer of a signaling message from other provider’s network to one’s own provider’s SIP network; it is independent of call-related (outgoing call, incoming call) direction.

Outbound (direction)

The direction corresponding to the transfer of a signaling message from one’s own provider’s SIP network to other provider’s network; it is independent of call-related (outgoing call, incoming call) direction.

Boundary

Signal node or node group positioned on the local network side at the boundary between one’s own provider’s SIP network (local network) and other provider’s network (including terminals).

Anonymous URI

URI used when one wants to make URI information anonymous. The specific format is as follows as recommended by JF-IETF-RFC3323 [4].

sip:`anonymous@anonymous.invalid`

Notification/Restriction information

Information specifying whether a user is allowing or prohibiting the notification of its network-asserted user identity information to another user receiving a signaling message.

Network-asserted user identity information

In a trusted network, information describing the identity of a user that is asserted by the network through authentication or other means (or verified by the network if provided by the user). An example of network-asserted user identity information is an E.164 [2] number that is reachable to the user.

SIP trust domain

A network consisting of trusted SIP nodes as defined in JF-IETF-RFC3324 [5]. A provider’s SIP network is not necessarily a SIP trust domain as specified in this document.

Joint trust domain

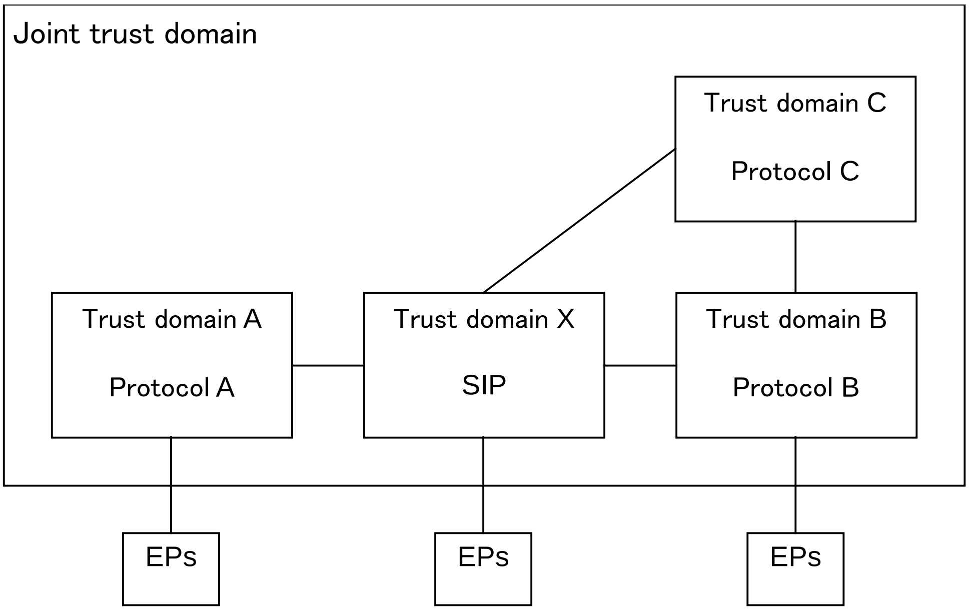
An extension of a trust domain as specified in Section 2.1 in a protocol other than SIP.

2. Interworking Model for Network-asserted User Identity Information

2.1. Joint Trust Domain Model

As defined in JF-IETF-RFC3324 [5], an SIP trust domain prescribes domain-intrinsic rules called Spec(T) and exchanges network-asserted user identity information. This structure can be extended and applied to connections with ISUP and other non-SIP networks. Prescribing fixed rules in this way enables an extended trust domain to be viewed as a joint trust domain (including SIP trust domains) that integrates networks interconnected by trusted interfaces.

Figure 1 shows a conceptual diagram of a joint trust domain. Here, protocols A, B, and C may each be a SIP protocol or a non-SIP protocol such as ISDN User Part (ISUP) [9][10] or Media Gateway Control Protocol (MGCP) [1].



EPs (endpoints) are terminals not belonging to a trust domain.

Figure 1/JJ-90.22: Joint trust domain model

2.2. Transfer Model for Network-asserted User Identity Information

Figures 2 and 3 shows logical transfer models for network-asserted user identity information passing through a SIP trust domain.

Determine Content (inbound boundary)

When a signaling message arrives at a SIP trust domain from the outside, its content MUST be examined in accordance with current conditions at the boundary in question. The SIP node at this boundary must determine by a certain rules the message sender’s network-asserted user identity information and notification/restriction information that needs to be provided, and MUST include them with the message to be transferred within the SIP trust domain.

Transfer (within trust domain)

Within the SIP trust domain, network-asserted user identity information and notification/restriction information shall be transferred transparently via SIP nodes as long as no special objectives exist. At this time, the SIP-message headers containing this information shall conform to JF-IETF-RFC3325 [6]: network-asserted user identity information shall be contained in the P-Asserted-Identity header and the notification/Restriction information shall be included in the Privacy header.

Output (outbound boundary)

At the outbound boundary, network-asserted user identity information shall be mapped to the signaling message to be transferred to the outside (or shall be deleted) according to a certain rules.

The operations in the inbound direction and those in the outbound direction should be specified by the connection interfaces at the respective boundaries. General guidelines for formulating such specifications are given in Appendix 2. In addition, specific processes based on these guidelines are given in each of the Annexes. Note also that a boundary SIP node (as opposed to a SIP node within the SIP trust domain) may be a SIP UA (including Back-To-Back User Agent (B2BUA)) or a SIP proxy server.

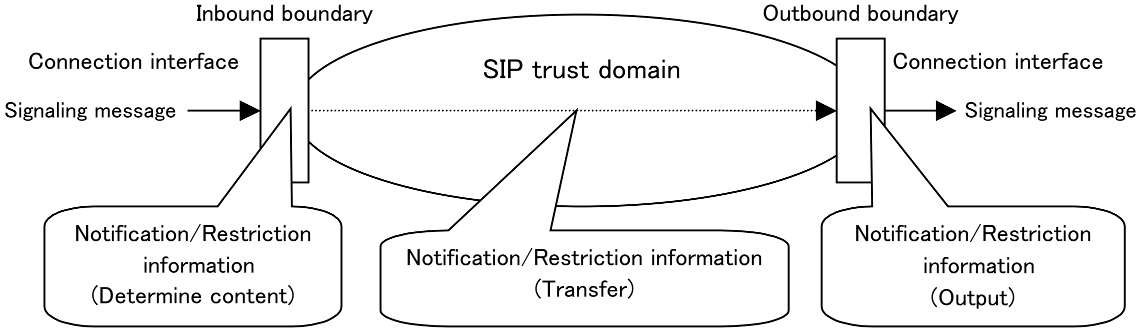

Inbound boundary
Outbound boundary
Connection interface
SIP trust domain
Connection interface
Signaling message
Signaling message
Notification/Restriction information (Determine content)
Notification/Restriction information (Transfer)
Notification/Restriction information (Output)

Figure 2/JJ-90.22: Transfer model for notification/Restriction information

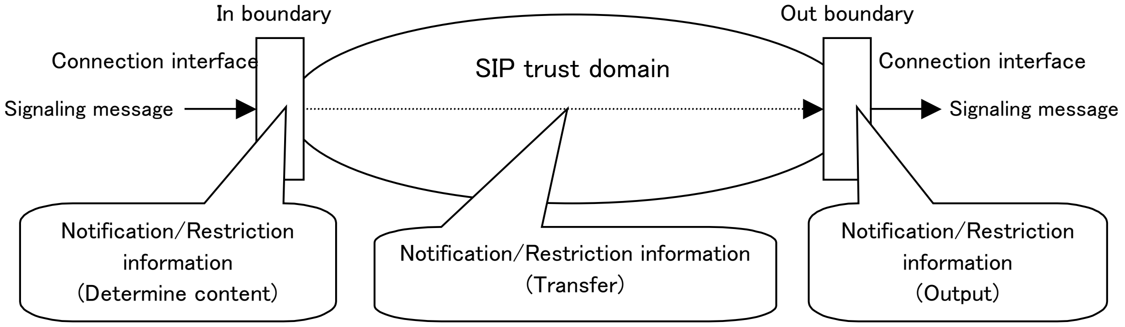

In boundary
Out boundary
Connection interface
SIP trust domain
Connection interface
Signaling message
Signaling message
Notification/Restriction information (Determine content)
Notification/Restriction information (Transfer)
Notification/Restriction information (Output)

Figure 3/JJ-90.22: Transfer model for network-asserted user identity information

3. Information Components

Notification/Restriction information and network-asserted user identity information are prescribed as follows[1].

3.1. Notification/Restriction information

Notification/Restriction information takes on a “notification” or “restriction” value.

3.2. Network-asserted User Identity Information

Network-asserted user identity information in a SIP trust domain consists of the following four components. Each of these components is carried in a corresponding field of the P-Asserted-Identity header.

(1) SIP_URI : Network-asserted user identity information component reachable in the SIP network

(2) SIP_DISPLAYNAME : Network-asserted user identity information component linked with the SIP_URI and consisting of information other than a number to be displayed to the called user

(3) TEL_URI : Network-asserted user identity information component consisting of a E.164 [2]

[1] Provider’s SIP networks to which this document applies use the P-Asserted-Identity header to carry network-asserted user identity information. They do not use the From header, Reply-To header, or the like that may be used in an End-To-End manner.

number reachable from the Global Switched Telephone Network (GSTN)

(4) TEL_DISPLAYNAME : Network-asserted user identity information component consisting of a dial number by which the calling user can be reached based on a numbering plan

3.2.1. SIP_URI

The SIP_URI information component enables the calling user to be reached in a SIP network. It MUST be a globally unique SIP URI [2] (Address-of-Record (AoR)).

3.2.2. SIP_DISPLAYNAME

The SIP_DISPLAYNAME information component should be displayed to the called user in a SIP network. It MUST be in text format. This information MAY be an individual’s name or nickname, a company’s name, a title, etc., as used in existing e-mail.

3.2.3. TEL_URI

The TEL_URI information component is a telecommunications number reachable from the GSTN beyond the SIP network. It uses either the tel URI global-number format (that begins with +) specified in JF-IETF-RFC 3966 [8] or the local-phone-number format. In the case of the latter format, phone-context=+81 shall be set. Also, the use of visual-separator is NOT RECOMMENDED. This information component MAY include tel URI parameters.

3.2.4. TEL_DISPLAYNAME

The TEL_DISPLAYNAME information component is a string of digits used by the called user to call the calling user.

3.3. Interpretation of Omitted Network-asserted User Identity Information Components

This section presents the (default) interpretation for omission of each of the network-asserted user identity information components.

3.3.1. SIP_URI

Omission of the SIP_URI information component [3] indicates that the caller does not have an appropriate sip URI. This case shall be handled as if the SIP_URI was an anonymous URI as long as no special restrictions exist.

3.3.2. SIP_DISPLAYNAME

Omission of the SIP_DISPLAYNAME information component indicates that a display format different from the SIP_URI is not particularly desired. This case must be interpreted as an indication that the SIP_URI character string SHOULD be used for display in the SIP network as long as no special restrictions exist.

3.3.3. TEL_URI

Omission of the TEL_URI information component indicates that the calling user has no E.164 [2] number for receiving incoming calls.

3.3.4. TEL_DISPLAYNAME

Omission of the TEL_DISPLAYNAME information component indicates that a dial number different from the number

[2] The sips URI is left for future study.

[3] The case of no SIP_URI and TEL_URI only often corresponds to a user accommodated by the GSTN.

indicated by the TEL_URI information component is not particularly desired, or that accurate information pertaining to the dialing numbering plan that can be used by the callee is not held. In this case, the TEL_URI character string SHOULD be interpreted as the TEL_DISPLAYNAME information component as long as no special restrictions exist.

4. Transfer Process Model

4.1. Inbound Processing (Determine Content)

At the inbound boundary, the value of notification/Restriction information MUST first be determined. Specifically, at each connection interface where rules for determining that value are applied, the rules MUST be applied according to the corresponding Annex for that interface or another document.

Similarly, the contents of network-asserted user identity information MUST be determined according to the contents and call state of the received message, network-applied policies, etc. At each connection interface where rules for determining the four components given in Section 3.2 (SIP_URI, SIP_DISPLAYNAME, TEL_URI, TEL_DISPLAYNAME) are applied, the rules MUST be applied according to the corresponding Annex for that interface or another document so that the rules are used uniformly at various inter-network connections and so that they conform to the usage described in Section 3.2.

4.2. Transfer Process

If the value of notification/restriction information is “restriction,” a Privacy header containing the value of id MUST be included in the message within the SIP trust domain. If the value of notification/restriction information is “notification,” a Privacy header containing the value of id MUST NOT be included in the message.

The network-asserted user identity information is transferred within the SIP trust domain by the P-Asserted-Identity header. As specified in JF-IETF-RFC3325 [6], the P-Asserted-Identity header can contain two types of URIs: sip [4] and tel. The four network-asserted user identity information components described in Section 3.2 MUST be included in the P-Asserted-Identity header in the following way.

(1)The SIP_URI component is contained in the addr-spec part of sip URI.
(2)The SIP_DISPLAYNAME component is contained in the displayname part of sip URI.
(3)The TEL_URI component is contained in the addr-spec part of tel URI.
(4)The TEL_DISPLAYNAME component is contained in the displayname part of tel URI.

4.3. Outbound Processing (Output)

At the outbound boundary, the components related to caller information of the signaling message to be output must be determined according to the values of notification/restriction information and network-asserted user identity information and other conditions.

Here, the rules for constructing caller-related information shall be specified according to an appropriate document for each of the connection-interface types where the signaling message is output. In addition, the rules must be applied according to the corresponding Annex for each interface or another document so that the rules are used uniformly at various inter-network connections and so that they conform to the usage described in Section 3.2.

[4] Although JF-IETF-RFC3325 [6] states that a sips URI may be used instead of the sip type, only the sip URI is considered within the scope of this standard; the sips URI is left for future study.

5. Trust of a Connection Interface

5.1. Definition of Trust

A connection interface can be trusted if the following conditions are satisfied[5].

5.1.1. Trustworthiness of Connection Interface Itself

The connection between the nodes that send and receive signaling messages is secure; messages cannot be read or tampered by a third party other than the interconnected networks, and messages cannot be received by a third party through spoofing.

5.1.2. Trustworthiness of Interconnected Domains

Signaling messages cannot be read or tampered by a third party within the interconnected domains.

5.1.3. Trustworthiness of Network-asserted User Identity Information Processing in Interconnected Domains

Processing of network-asserted user identity information in a connection interface with other provider's network in the interconnected domains shall conform to the processes specified in Section 5.2.

5.2. General Behaviors based on Trust

5.2.1. Inbound Boundary

If the connection interface receiving the signaling message can be trusted, notification/restriction information and network-asserted user identity information SHOULD be retained as received provided that network policies and signal capability allows for that.

If the connection interface receiving the signaling message cannot be trusted, the network MUST determine notification/restriction information and network-asserted user identity information (even if received null) by some message authentication process and attach that information.

5.2.2. Outbound Boundary

If the connection interface sending the signaling message can be trusted, notification/restriction information and network-asserted user identity information SHOULD be retained as received provided that network policies and signal capability allows for that.

If the connection interface sending the signaling message cannot be trusted and if the value of notification/Restriction information is "restriction", any network-asserted user identity information MUST NOT pass through that connection interface. If the value of notification/restriction information is "notification", the network-asserted user identity information to be output shall be determined by a certain rules in accordance with network polices or other guidelines.

[5] It must be kept in mind that the trustworthiness of a connection interface is not symmetric. It may be seen as trustworthy by the network on one side but as untrustworthy by the network on the opposite side.

Annex a. Transferring Network-asserted User Identity Information in Interface A

a.1. Overview

This Annex specifies the rules for exchanging notification/restriction information and network-asserted user identity information between SIP trust domains. The specifications described in this Annex conform to the interface-specification guidelines given in Appendix ii.

a.2. Application Model

This Annex concerns the configuration shown in Figure a-1 Specifications for processes other than those described in this Annex conform to the specifications given in JJ-90.21 [12] for Interface A

Here, SIP is applied to the connection interface and a interworking SIP node (e.g., SIP proxy server, B2BUA) to a boundary.

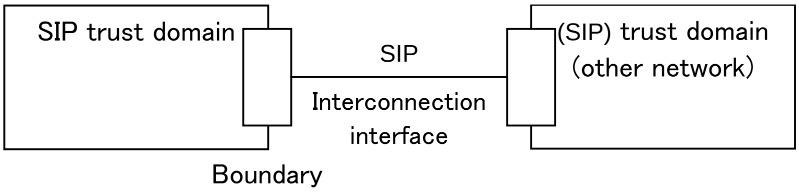


Figure a-1/JJ-90.22: SIP trust domain interconnection model

Note that the specifications given in this Annex do not apply to all instances of Interface A. Rather, they are limited to SIP networks that can be trusted as specified in Section 5.1 of this document [6].

a.3. Interface Type

a.3.1. Technical References

JF-IETF-RFC3261[3] , JF-IETF-RFC3323[4], JF-IETF-RFC3324 [5], JF-IETF-RFC3325 [6]

a.3.2. Trustworthiness

This is a mutually trustful type of interface when SIP trust domains and the connection interface must satisfy the conditions for trustworthiness which is specified in this framework. In addition, the trust domains themselves trust each other and the behaviors at the respective boundaries conform to those specified in this document.

a.3.3. SIP Messages to be Applied

a.3.3.1. Inbound Boundary

Initial INVITE request (referred to below as simply “INVITE request”)

SIP messages other than the above must not include a P-Asserted-Identity header.

a.3.3.2. Outbound Boundary

Initial INVITE request (referred to below as simply “INVITE request”)

SIP messages other than the above must not include a P-Asserted-Identity header.

[6] If a connected SIP network cannot be trusted as specified in Section 5.1 of this document, operations at the boundary in question must conform to the case of no trust as specified in Section 5.2 and not to the specifications given in this attachment.

a.3.4. Character Set Applied to SIP_DISPLAYNAME

Only character strings composed of UTF-8 code shall be applied[7].

a.4. Behaviors Particular to the Interface

a.4.1. Inbound Processing

a.4.1.1. Determining Notification/Restriction Information

If the received INVITE request includes a Privacy header set to id, the value of notification/restriction information shall be "restriction;" for all other conditions, it shall be "notification."

a.4.1.2. Determining Network-asserted User Identity Information

Network-asserted user identity information is determined from the content of the P-Asserted-Identity header in the INVITE request.

SIP_URI:

The addr-spec part of sip URI in the P-Asserted-Identity header of the INVITE request contains the SIP_URI component.

SIP_DISPLAYNAME:

The displayname part of sip URI in the P-Asserted-Identity header of the INVITE request contains the SIP_DISPLAYNAME component.

If enclosed in quotes, the string excluding those quotes is taken to be SIP_DISPLAYNAME.

TEL_URI:

The addr-spec part of tel URI in the P-Asserted-Identity header of the INVITE request contains the TEL_URI component.

TEL_DISPLAYNAME:

The displayname part of tel URI in the P-Asserted-Identity header of the INVITE request contains the TEL_DISPLAYNAME component.

If enclosed in quotes, the string excluding those quotes is taken to be TEL_DISPLAYNAME.

a.4.2. Outbound Processing

a.4.2.1. Outputting Notification/Restriction Information

If the value of notification/Restriction information is "Restriction," a Privacy header set to id is included in the INVITE request.

If the value of notification/Restriction information is "notification," no Privacy header set to id is included in the INVITE request.

a.4.2.2. Outputting Network-asserted User Identity Information

Network-asserted user identity information is included in the P-Asserted-Identity header of the INVITE request.

[7] Use of character strings other than UTF-8 code is left for further study.

SIP_URI:

The addr-spec part of sip URI in the P-Asserted-Identity header of the INVITE request to be sent contains the SIP_URI component. This content shall be in proper sip URI format having an effective and global scope.

SIP_DISPLAYNAME:

The displayname part of sip URI in the P-Asserted-Identity header of the INVITE request to be sent contains the SIP_DISPLAYNAME component.

This content shall be a character string composed only of UTF-8 code [8]. If the value of notification/Restriction information is “Restriction,” the character strings listed in Attached Table A-1 shall be used for displaying the reason for that Restriction. Also, if the call originates in the GSTN, the conditions listed in Attached Table A-1 can be applied, but if the call originates in a SIP network, the application of character strings other than those listed in Attached Table A-1 can be supposed.

Table a-1/JJ-90.22: Character strings indicating reason for Restriction

SIP_DISPLAYNAME	Meaning
Unavailable	No caller ID: service unavailable
Anonymous	No caller ID: rejected by user
Interaction with other service	No caller ID: service conflict
Coin line/payphone	No caller ID: call from public telephone

TEL_URI:

The addr-spec part of tel URI in the P-Asserted-Identity header of the INVITE request to be sent contains the TEL_URI component.

As shown in Attached Table A-2, a visual-separator is not included. It is possible to include URI parameters for tel URI.

Table a-2/JJ-90.22: TEL_URI format

TEL_URI	No. of Digits	Use	Remarks
+country-code National-Number	Max. 15 digits	Originating call on international network (overseas)	Begins with a number other than 81 or 0
+81A0CDEFGHJK	12 digits	Originating call on mobile/PHS network	A is 7, 8, or 9
+8150CDEFGHJK	12 digits	Originating call on IP phone (category B)	
+81ABCDEFGHJ	10 or 11 digits	Originating call on local fixed telephone network Originating call on IP phone (category A)	A and B are both non-zero
<Free Format>: phone-context=+81	Max. 16 digits (See Note)	Operator-originating call, etc.	

Note: When performing full-digit mapping with GSTN, some restrictions apply on the ISUP side (JJ-90.10 [11]). For SIP-SIP transfer, no restrictions apply provided that the carriers in question have so agreed.

[8] Use of character strings other than UTF-8 code is left for further study. If code other than UTF-8 should be received, it is recommended that an error not be generated and that processing be allowed to continue.

TEL_DISPLAYNAME:

The displayname part of tel URI in the P-Asserted-Identity header of the INVITE request to be sent contains the TEL_DISPLAYNAME component.

This content shall be a string of digits each from 0 to 9 and shall follow the format given in Attached Table a-3 based on the dialing plan of (domestic) local fixed telephone networks.

Table a-3/JJ-90.22: TEL_DISPLAYNAME format

TEL_DISPLAYNAME	No. of Digits	Use	Remarks
010 country-code National-Number	Max. 18 digits	Originating call on international network (overseas)	Country code begins with a number other than 81 or 0
0A0CDEFGHJK	11 digits	Originating call on mobile/PHS network	A is 7, 8, or 9
050CDEFGHJK	11 digits	Originating call on IP phone (category B)	
0ABCDEFGHJ	9 or 10 digits	Originating call on local fixed telephone network Originating call on IP phone (category A)	A, B, and C are each non-zero
0AB0-		Logical number	A and B are both non-zero
Free Format		Operator-originating call, etc.	

Annex b. Transferring Network-asserted User Identity Information in Interface B

b.1. Overview

This Annex specifies the rules for exchanging notification/restriction information and network-asserted user identity information between a SIP trust domain and SIP user. The specifications described in this Annex conform to the interface-specification guidelines given in Appendix ii.

b.2. Application Model

This Annex concerns the configuration shown in Figure b-1.

Here, SIP is applied to the connection interface and an outbound proxy as seen from a SIP UA (at time of calling) corresponds to the boundary.

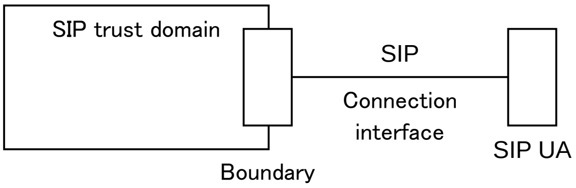


Figure b-1/JJ-90.22: SIP trust domain and SIP user interconnection model

b.3. Interface Type

b.3.1. Technical References

JF-IETF-RFC3261[3], JF-IETF-RFC3323[4], JF-IETF-RFC3324 [5], JF-IETF-RFC3325 [6]

b.3.2. Trustworthiness

The SIP UA can trust the SIP trust domain (but the SIP trust domain cannot trust the SIP UA). As seen from the SIP UA, the SIP trust domain must satisfy the conditions for framework trustworthiness. Appendix 3 shall be referenced with regard to the trustworthiness of network-asserted user identity information as seen from the SIP UA.

b.3.3. SIP Messages to be Applied

b.3.3.1. Inbound Boundary

Initial INVITE request (referred to below as simply “INVITE request”)

b.3.3.2. Outbound Boundary

Initial INVITE request (referred to below as simply “INVITE request”)

b.3.4. Character Set Applied to SIP_DISPLAYNAME

Only character strings composed of UTF-8 code shall be applied [9].

[9] Use of character strings other than UTF-8 code is left for further study. If code other than UTF-8 should be received, it is recommended that an error not be generated and that processing be allowed to continue.

b.4. Behaviors Particular to the Interface

b.4.1. Inbound Processing

b.4.1.1. Determining Notification/Restriction Information

If the received INVITE request includes a Privacy header set to id, the value of notification/restriction information shall be “Restriction;

If the received INVITE request includes a Privacy header set to none, the value of notification/restriction information shall be “notification.”

For all other conditions, value of notification/restriction information shall be determined by separate settings made by the calling user or by policies of the SIP trust domain.

b.4.1.2. Determining Network-asserted User Identity Information

Network-asserted user identity information is determined from data set in the SIP trust domain after authenticating the calling user sending the INVITE request.

However, if the INVITE request includes a P-Preferred-Identity header and if the validity of its content can be verified, that value may be used.

b.4.2. Outbound Processing

b.4.2.1. Concealment of Network-asserted User Identity Information

If the value of notification/Restriction information is “Restriction,” no P-Asserted-Identity header is included in the INVITE request.

If the called user requests it, the value of SIP_DISPLAYNAME may be included in the displayname part of the From header at the boundary.

Consequently, if notification/Restriction information is set to “restriction,” the character strings listed in Table b-1 as reasons for Restriction may be used for that purpose.

Table b-1/JJ-90.22: Character strings indicating reason for Restriction

SIP_DISPLAYNAME	Meaning
Unavailable	No caller ID: service unavailable
Anonymous	No caller ID: rejected by user
Interaction with other service	No caller ID: service conflict
Coin line/payphone	No caller ID: call from public telephone

b.4.2.2. Outputting Network-asserted User Identity Information

If notification/restriction information is set to “notification,” the P-Asserted-Identity header may be included in the INVITE request. The content of this header is the same as that of the P-Asserted-Identity header exchanged between SIP trust domains as specified in Annex A. However, if TEL_URI is not equivalent to TEL_DISPLAYNAME, the content of TEL_URI must be changed to its TEL_DISPLAYNAME equivalent.

This equivalency may follow rules particular to the SIP trust domain in question, but the equivalents listed in Table B-2 are the same as those based on standard dialing plans in existing local fixed telephone networks, mobile and PHS networks, and international networks.

Table b-2/JJ-90.22: TEL_URI and TEL_DISPLAYNAME Equivalents

TEL_URI	TEL_DISPLAYNAME
tel:+81A0BCDEFGHJK	0A0CDEFGHJK
tel:+81ABCDEFGHJ	0ABCDEFGHJ
tel:+81ABCDEFGH	0ABCDEFGH
tel:+ country-code National-Number	010 country-code National-Number

Note also that the value of TEL_DISPLAYNAME or that of SIP_DISPLAYNAME may be set in the displayname part of the From header at the boundary.

Annex c. Transferring Network-asserted User Identity Information in Interface C

c.1. Overview

This Annex specifies the rules for exchanging notification/restriction information and network-asserted user identity information between a SIP trust domain and TTC ISUP network. The specifications described in this Annex conform to the interface-specification guidelines given in Appendix 2.

c.2. Application Model

This Annex concerns the configuration shown in Figure c-1.

Here, the Media Gateway Controller (MGC) corresponds to a boundary in a framework related to network-asserted user identity information, and the processing that it performs conforms to the specifications of JF-IETF-RFC3398 [7].

The connection interface is assumed to apply TTC-based ISUP protocol as in interface C of JJ-90.21 [12], and conforms in particular to JJ-90.10 [11] in the case of different carriers.

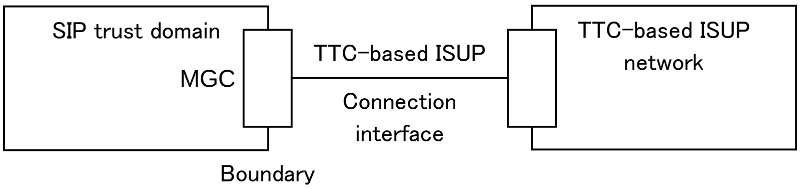


Figure c-1/JJ-90.22: SIP trust domain and TTC ISUP interconnection model

c.3. Interface Type

c.3.1. Technical References

JT-Q763 [9], JT-Q764 [10], JJ-90.10 [11], JF-IETF-RFC3398 [7]

c.3.2. Trustworthiness

This is a mutually trustful type of interface. However, the TTC-based ISUP network and the connection interface must satisfy the conditions for trustworthiness specified in Section 5 of this document.

c.3.3. SIP Messages to be Applied

c.3.3.1. Inbound Boundary

INVITE request mapped from an ISUP address message (IAM)

c.3.3.2. Outbound Boundary

INVITE request mapped to an ISUP address message (IAM)

c.3.4. Character Set Applied to SIP_DISPLAYNAME

Only character strings composed of UTF-8 code shall be applied[10].

[10] Use of character strings other than UTF-8 code is left for further study. If code other than UTF-8 should be received, it is recommended that an error not be generated and that processing be allowed to continue.

c.4. Behaviors Particular to the Interface

c.4.1. Inbound Processing

c.4.1.1. Determining Notification/Restriction Information

If a valid generic number[11] parameter (see Section c.4.1.2) exists in the IAM, the address presentation restricted indicator must be examined in this parameter. If its value is “presentation allowed,” the value of notification/restriction information is “notification.” All other values of the display indicator including “presentation restricted” means that the value of notification/restriction information is “restriction.”

If a valid generic number parameter does not exist in the IAM but a calling party number parameter does exist in a valid IAM, the address presentation restricted indicator of this calling party number parameter must be examined. If its value is “presentation allowed,” the value of notification/Restriction information is “notification.” All other values including “presentation restricted.” mean that the value of notification/restriction information is “restriction.”

If a calling party number parameter does not exist in the IAM, the value of notification/restriction information is “restriction.”

c.4.1.2. Determining Network-asserted User Identity Information

Valid generic number parameter:

The values listed in Table c-1 constitute conditions for a valid generic number parameter, which provides the elements for generating network-asserted user identity information.

Table c-1/JJ-90.22: Conditions for a valid generic number parameter

Field	Value	Meaning
Number Qualifier Indicator	00000110	Additional calling party number
Nature of Address indicator	0000011	National-Number
Number incomplete indicator	0	Complete
Numbering plan indicator	001	ISDN (telephone) numbering plan (Recommendation E.164 [2])
Address Presentation Restriction indicator	00 or 01	presentation allowed or presentation restricted
Screening Indicator	01 or 11	User provided and network verification is passed, or network provided
Address signal	Max. 16 digits	

Valid calling party number parameter:

The values listed in Table c-2 constitute conditions for a valid calling party number parameter, which provides the elements for generating network-asserted user identity information.

[11] TTC specific ISUP parameter

Table c-2/JJ-90.22: Conditions for a valid calling party number parameter

Field	Value	Meaning
Nature of Address indicator	0000011 0000100 1111110	National-Number International number Network specific number
Number incomplete indicator	0	Complete
Numbering plan indicator	001	ISDN (telephone) numbering plan (Recommendation E.164 [2])
Address Presentation Restriction indicator	00 or 01	presentation allowed or presentation restricted
Screening Indicator	01 or 11	User provided, network verification is passed, or network provided
Address Signal	Max. 16 digits	

Main number:

This is a number determined in the following way.

If a valid generic number parameter exists, the main number is obtained from this parameter (Nature of Address indicator and address information). If it does not exist but a valid calling party number parameter does, the main number is obtained from that parameter (Nature of Address indicator and address signal). If neither a valid generic number parameter nor valid calling party number parameter exists, the main number is considered to be null[12].

Mapping to various information components:

SIP_URI:

If the value of notification/restriction information is "notification," SIP_URI may be omitted. If the value is "restriction," the use of SIP_URI is essential.

When generating SIP_URI, the user part takes on a tel URI format by applying the conversion rules of Table c-4 Table c-4 from the main number. The host part takes on a value unique to the SIP trust domain. The user=phone parameter may also be set at this time. A sip URI that can be achieved by application of the above rules is applied to SIP_URI, and if none can be achieved, either an anonymous URI should be applied or SIP_URI omitted.

If, however, the main is null, a SIP_URI that requires no number information (such as an anonymous URI) must be set.

SIP_DISPLAYNAME:

If the value of notification/restriction information is "restriction," the value of SIP_DISPLAYNAME is determined from the value of cause of no ID[13] parameter as shown in Table c-3[14]. The value of SIP_DISPLAYNAME is case sensitive but is unaffected by the use of quotes.

[12] The case in which a valid generic number exists but a valid calling party number does not is not normally considered. The processing to perform if such a case occurs depends on carrier policy.

[13] The parameter, cause of no ID, is TTC specific

[14] Same as the mapping method given in Section 12.1 of JF-IETF-RFC3398 [7] from the cause of no ID parameter to the displayname part of the From header.

Table c-3/JJ-90.22: Conversion rules from cause of no-ID parameter to SIP_DISPLAYNAME

Parameter Value	Meaning	SIP_DISPLAYNAME
No parameter	-	Unavailable
0000001	No caller ID: rejected by user	Anonymous
0000010	No caller ID: service conflict	Interaction with other service
0000011	No caller ID: call from public telephone	Coin line/payphone

If the value of notification/restriction information is "notification," SIP_DISPLAYNAME may be omitted or the value of TEL_DISPLAYNAME may be applied.

TEL_URI:

If a calling party number parameter exists, TEL_URI takes on the character string obtained by applying the conversion rules of Table c-4. If a calling party number parameter does not exist, TEL_URI is left to be null.

Table c-4 lists the conversion rules to tel URI from the set format of address information in the calling party number parameter specified in JJ-90.10 [11] (Table 4-4) [15].

Table c-4/JJ-90.22: Conversion rules from ISUP number type and address information to tel URI

Use	Nature of Address	Address Signal	tel URI
Originating call on international network (overseas)	International number	country-code + National-Number	tel:+country-code National-Number
Originating call on mobile/PHS network	National-Number	A0CDEFGHJK	tel:+81A0CDEFGHJK
Originating call on local fixed telephone network	National-Number	ABCDEFGHJ	tel:+81ABCDEFGHJ
Operator-originating call, etc.	Network specific number	Free Format	tel:<Free Format>;phone-context=+81

TEL_DISPLAYNAME:

If the value of notification/Restriction information is "restriction," TEL_DISPLAYNAME may be omitted or a value derived from the main number may be applied.

If the value of notification/restriction information is "notification," TEL_DISPLAYNAME is derived from the main number. Here, if the SIP trust domain has enough information with regard to the dialing plan of the callee, that information is used to set a value. If it does not have enough information, TEL_DISPLAYNAME takes on the character string obtained by applying the conversion rules of Table c-5.

Table c-5 lists conversion rules based on standard dialing plans in GSTN.

[15] Equivalent to the rules given in Section 12.1 of JF-IETF-RFC3398 [7] with JJ-90.10 noted.

Table c-5/JJ-90.22: Conversion rules from ISUP number type and address information to TEL_DISPLAYNAME

Use	Nature of Address	Address Signal	TEL_DISPLAYNAME
Originating call on international network (overseas)	International number	country-code + National-Number	010 country-code National-Number
Originating call on mobile/PHS network	National-Number	A0CDEFGHJK	0A0CDEFGHJK
Originating call on local fixed telephone network	National-Number	ABCDEFGHJ	0ABCDEFGHJ
Logical number	National-Number	AB0-	0AB0-
Operator-originating call, etc.	Network specific number	Optional	Optional

Table c-6 summarizes ISUP→SIP interworking conditions in inbound processing.

Table c-6/JJ-90.22: ISUP→SIP interworking conditions in input processing

ISUP

Generic number		Calling party number		Cause of no ID
Yes/No	Address Presentation Restriction indicator	Yes/No	Address Presentation Restriction indicator	Yes/No
Yes	Presentation Allowed	Yes	Presentation Allowed	Yes/No
			Other	
		No	—	
	Other	Yes	Presentation Allowed	Yes
				No
			Other	Yes
				No
		No	—	Yes/No
No	—	Yes	Presentation Allowed	Yes/No
			Other	Yes
				No
		No	—	Yes
				No

SIP

Notification / Restriction	SIP		TEL	
	URI	DISPLAYNAME	URI	DISPLAYNAME
Notification	Generic number or omitted	Generic number or omitted	Calling Party number	Generic number
Not generally considered; configuration depends on provider’s policy.				
Restriction	Generic number	Cause of no ID	Calling Party number	Generic number or omitted
		"unavailable"		
		Cause of no ID		
		"unavailable"		
Not generally considered; configuration depends on provider’s policy.				
Notification	Calling Party number	Calling Party number	Calling Party number	Calling Party number
Restriction		Cause of no ID		Calling Party number or omitted
		"unavailable"		
	Anonymous URI, etc.	Cause of no ID	Not set	Not set
		"unavailable"		

c.4.2. Outbound Processing

c.4.2.1. Outputting Notification/Restriction Information

If the value of notification/restriction information is “restriction” and if a calling party number parameter is to be output as a result of the processing described in Section c.4.2.2, the display indicator of the calling party number parameter must be set to “presentation restricted.” If the value of notification/restriction information is “notification,” the address presentation restriction indicator of the calling party number parameter must be set to “presentation allowed.”

Also, if a generic number parameter is to be output as a result of the processing described in Section c.4.2.2, the address presentation restriction indicator of the generic number parameter must be set to “presentation allowed” if the value of notification/restriction information is “notification” and to “presentation restricted” if that value is “restriction.” Furthermore, for the case that the display indicator of the generic number parameter is equal to “presentation allowed,” the display indicator of the calling party number parameter must be set to “presentation restricted” regardless of the content of notification/restriction information.

c.4.2.2. Outputting Network-asserted User Identity Information

If TEL_URI is not null, the calling party number parameter must be derived from the value of TEL_URI.

The conversion rules from the value of TEL_URI to the calling party number parameter follow Table c-7. If TEL_URI begins with “+81”, number type is set to “domestic” and address information to that number with “+81” removed. If it begins with “+” other than “+81”, nature of address indicator is set to “international number” and address information to that number with “+” removed. If it begins with a character other than “+”, number type is set to “network unique” and address information is unchanged. In addition, the Screening Indicator is set to “network provided.” Setting of calling party number parameter fields other than nature of address indicator, address signal, and Screening Indicator shall conform to the settings specified in JJ-90.10 [11].

Table c-7/JJ-90.22: Conversion rules from tel URI to nature of address and address signal of ISUP number

tel URI	Use	Nature of Address	Address Signal
tel:+country-code National-Number	Originating call on international network (overseas)	International number	country-code + National-Number
tel:+81A0CDEFGHJK	Originating call on mobile/PHS network	National-Number	A0CDEFGHJK
tel:+81ABCDEFGHJ	Originating call on local fixed telephone network	National-Number	ABCDEFGHJ
tel:optional;phone-context=+81	Operator-originating call, etc.	Network specific number	Optional

If TEL_DISPLAYNAME exists but differs from TEL_URI, a generic number parameter shall be output. The conversion rules from TEL_DISPLAYNAME to a generic number parameter state that, for a value beginning with “0” other than “010” or “00”, nature of address indicator is set to national number and address signal to that number with “0” removed. For patterns other than the above, no mapping to a generic number is performed. In addition, the Screening Indicator is set to “network provided.” Setting of generic number parameter fields other than nature of address indicator, address signal, and Screening Indicator shall conform to the settings specified in JJ-90.10 [11].

This equivalency may follow rules particular to the SIP trust domain in question, but the equivalents listed in Table c-8 are the same as those based on standard dialing plans in existing local fixed telephone networks and mobile and PHS networks.

Table c-8/JJ-90.22: TEL_URI and TEL_DISPLAYNAME Equivalents

TEL_URI	TEL_DISPLAYNAME
tel:+81A0BCDEFGHJK	0A0CDEFGHJK
tel:+81ABCDEFGHJ	0ABCDEFGHJ
tel:+81ABCDEFGH	0ABCDEFGH

If the value of notification/restriction information is “restriction” and if a calling party number parameter or a generic number parameter has been derived, a cause of no ID parameter shall be output in accordance with the value of SIP_DISPLAYNAME. The values that can be set for the cause of no ID parameter follow the inverse of Table c-3. However, if a value for SIP_DISPLAYNAME is not shown in the Table c-3 column, the cause of no ID parameter shall be set to “rejected by user.”

Table c-9 summarizes SIP→ISUP interworking conditions in output processing.

Table c-9/JJ-90.22: SIP→ISUP interworking conditions in output processing

SIP					ISUP				
Notification /Restriction	TEL			SIP	Calling party number		Generic number		Cause of no ID
	URI	DISPLAYNAME		DISPLAYNAME					
	Yes/No	Yes/No	Equivalency with URI	Yes/No	Address signal, etc.	Address presentation restriction indicator	Address signal, etc.	Address presentation restriction indicator	
Notification	Yes	Yes	Equivalent	Yes/No	TEL_URI	Presentation allowed	Not set	—	Not set
			Not equivalent			Presentation restricted	TEL_DISPLAYNAME	Presentation allowed	
		No	—			Presentation allowed	Not set	—	
	No	—	—		Not set	—	Not set	—	
Restriction	Yes	Yes	Equivalent	Yes	TEL_URI	Presentation restricted	Not set	—	SIP_DISPLAYNAME
				No					“Rejected by User” or omitted
			Not equivalent	Yes			TEL_DISPLAYNAME	Presentation restricted	SIP_DISPLAYNAME
				No					“Rejected by User” or omitted
		No	—	Yes			Not set	—	SIP_DISPLAYNAME
				No					“Rejected by User” or omitted
	No	—	—	Yes	Not set	—	Not set	—	Not set
				No					

Appendix i. : Notes on Specifications for Transferring Network-asserted User Identity Information

i.1. Transparent Transfer of Information

It is assumed that the mapping of network-asserted user identity information from SIP to protocol A and the mapping of network-asserted user identity information from protocol A to SIP shall be specified by Annexes to this document or by separate technical documents.

In these cases, for mapping performed from protocol A to a SIP trust domain and then back again to protocol A, the transfer of network-asserted user identity information may not be completely transparent. This type of mismatch should be allowed within the framework of this document.

If completely transparent transfer of information via a SIP trust domain is needed, additional means such as message encapsulation should be investigated.

i.2. Interworking without translating into SIP Messages

The SIP message may not be generated because the node at the inbound boundary and the node at outbound boundary are the same due to the configuration of the SIP trust domain, message-routing rules, etc.

In this case as well, the results of processing at the outbound boundary including the message to be sent should be designed so that they are the same as if they had passed virtually through the SIP signaling network.

i.3. Long-term Solution for Transfer of Network-asserted User Identity Information

The JF-IETF-RFC3323 [4], JF-IETF-RFC3324 [5], and JF-IETF-RFC3325 [6] RFCs referenced by this document are considered by the Internet Engineering Task Force (IETF) to be a short-term solution to the transfer of caller information. As for a long-term solution, Ref. [13] is currently being discussed. The idea behind that work is to transfer network-asserted user identity information on an end-to-end basis within a SIP message. It can be considered, however, that the short-term solution given within the networks specified in this document can coexist with such a long-term solution. We will therefore include only a short-term solution within the framework prescribed by this document, and will study the reflection of a long-term solution once related documents in IETF have been completed as RFCs.

Appendix ii. Guidelines in making rules for the new interface type

This appendix describes guidelines for drawing up connection interface rules in accordance with a transfer model that calls for the passage of network-asserted user identity information through a joint trust domain as prescribed in this document. To add a new interface in the future for the model described in this document, it should be specified as an Annex to this document or by a document created by an appropriate organization or a provider that provides services in accordance with the guidelines described in Section 2.1 (Interface Type) and Section 2.2 (Interface-unique Behaviors) of this appendix. The Annexes provided with this document (Annex a, Annex b, and Annex c) satisfy the guidelines presented in this appendix.

ii.1. Interface Type

- Technical References
- Trustworthiness
  - Trusted or not trusted
- SIP messages to be applied
- Character set applied to SIP_DISPLAYNAME

ii.2. Interface-unique Behaviors

Interworking behaviors on target SIP messages must be specified.

ii.2.1. Inbound Processing

For a trusted connection interface:

- Determine content of notification/restriction information: Rules for determining notification or restriction.
- Determine content of network-asserted user identity information: Rules for configuring network-asserted user identity information from a received signaling message.

For a non-trusted connection interface:

- Determine content of notification/restriction information: Rules for determining notification or restriction.
- Determine content of network-asserted user identity information: Rules for determining network-asserted user identity information

ii.2.2. Outbound Processing

For a trusted connection interface:

- Output notification/restriction information: Interworking rules to determine a value, “notification” or “restriction”.
- Output network-asserted user identity information: Rules for placing content derived from each network-asserted user identity information component onto the sending message.

For a non-trusted connection interface:

- If the value of notification/Restriction information is “notification restricted”, rules are needed to make network-asserted user identity information anonymous in the output message.
- Output network-asserted user identity information: If the value of notification/Restriction information is “notification allowed”, rules are needed to place the content derived from each network-asserted user identity information component onto the output message.

Appendix iii.: Trustworthiness of network-asserted user identity information at Interface B

iii.1. Overview

This appendix describes requirements for a SIP UA to use network-asserted user identity information transferred from a SIP network to the SIP UA via interface B (SIP UNI) in an architecture model specified in JJ-90.21 [12]. It also describes security risk when necessary requirements are not satisfied and gives several solution examples that can be effective for satisfy those necessary requirements.

iii.2. Necessary Requirements in Interface B

Prevention of tampering:

Messages received by the SIP UA via the connection interface shall not be tampered with by a third party.

Prevention of spoofing:

Messages received by the SIP UA shall be forwarded accurately from the SIP trust domain without the occurrence of any spoofing.

iii.3. Security Risk When Not Satisfying Necessary Requirements

If the conditions described in Section 3.2 above are not satisfied, signals that have been tampered with or subjected to spoofing by a third party may be received and processed by the SIP UA. As a result, the value presented to the called user as network-asserted user identity information cannot be trusted. The following security risk of a malicious attack therefore exists. Note here that it is very difficult to isolate such a malicious attack in an IP network and that special care should therefore be taken.

Security risk:

A message may be sent under the disguise of a particular person and received as such inflicting actual harm to concerned parties.

In addition, an indefinite number of users may receive network-asserted user identity information under the disguise of a party which is being targeted for an attack. If those users are unable to detect the disguise, a number of them may return calls to that party obstructing his communications.

Within the scope of this document, all users on GSTN that can receive calls by existing E.164 [2] numbers are vulnerable to attack. This security risk needs to be eliminated.

iii.4. Solution Examples

The following presents several schemes that can be used to satisfy the requirements described above. Please note that these are only examples and are not guaranteed to be all-inclusive. Other schemes exist that can also satisfy these requirements.

iii.4.1. Use of TLS

The following processing can be effective for satisfying requirements.

- Transport Layer Security (TLS) when used between the SIP UA and the SIP network' boundary at interface B.

iii.4.2. Making use of SIP REGISTER/INVITE

The following processing can be effective for satisfying requirements.

- The possibility of eavesdropping and tampering by a third party at interface B can be eliminated.

- The SIP UA performs register processing with the provider's SIP network using the REGISTER message.
- Here, the value of the Contact header in the REGISTER request sent from the SIP UA can be set to a value that is practically impossible to infer (by setting the userinfo part to a sufficiently random value).
- Only if the Request-URI of a received INVITE request has the same value as the Contact header previously set by the SIP UA, this INVITE request is determined to have been sent from a valid SIP trust domain and the network-asserted user identity information in this request can be used for a certain purposes.

Also, to prevent the value used in a REGISTER message from leaking to the outside, the value used in the Contact header during call establishment dialogs (i.e., the Contact header in the sending INVITE request and 1xx and 2xx responses to the received INVITE request) and the value used in the Contact header of the REGISTER request should be made different.

iii.4.3. Authentication by a Shared Key

The following processing can be effective for satisfying requirements.

- A shared key can be used between the SIP UA and the boundary at interface B so that a hash value based on that key and the nonce value can be included in a predetermined header or in the body of a message sent from the boundary.

iii.4.4. Limiting the Source IP Address

The following processing can be effective for satisfying requirements.

- Packet filtering can be performed by some means at interface B to ensure that a received packet having a source IP address corresponding to a SIP network boundary (group) is indeed a packet from a provider's SIP network boundary (group). This prevents spoofing with respect to the source IP address.
- A received INVITE request packet is determined to have been sent from a valid SIP trust domain only if the source IP address of that packet agrees with a previously set address of a SIP-network-boundary (group). The network-asserted user identity information in the packet can then be used without worry.

Limiting Used Ports

The following processing can be effective for satisfying requirements.

- The port number used by a SIP message sent from the boundary of the SIP network at interface B to the SIP UA can be limited to specific ports.
- Packet filtering can then be performed by some means at interface B to ensure that a received packet having a port number the same as a specified port is indeed a packet from a SIP network boundary (group). This prevents specified ports from being used by other parties.

Note that the above also means that a specified port can no longer be used for other purposes.