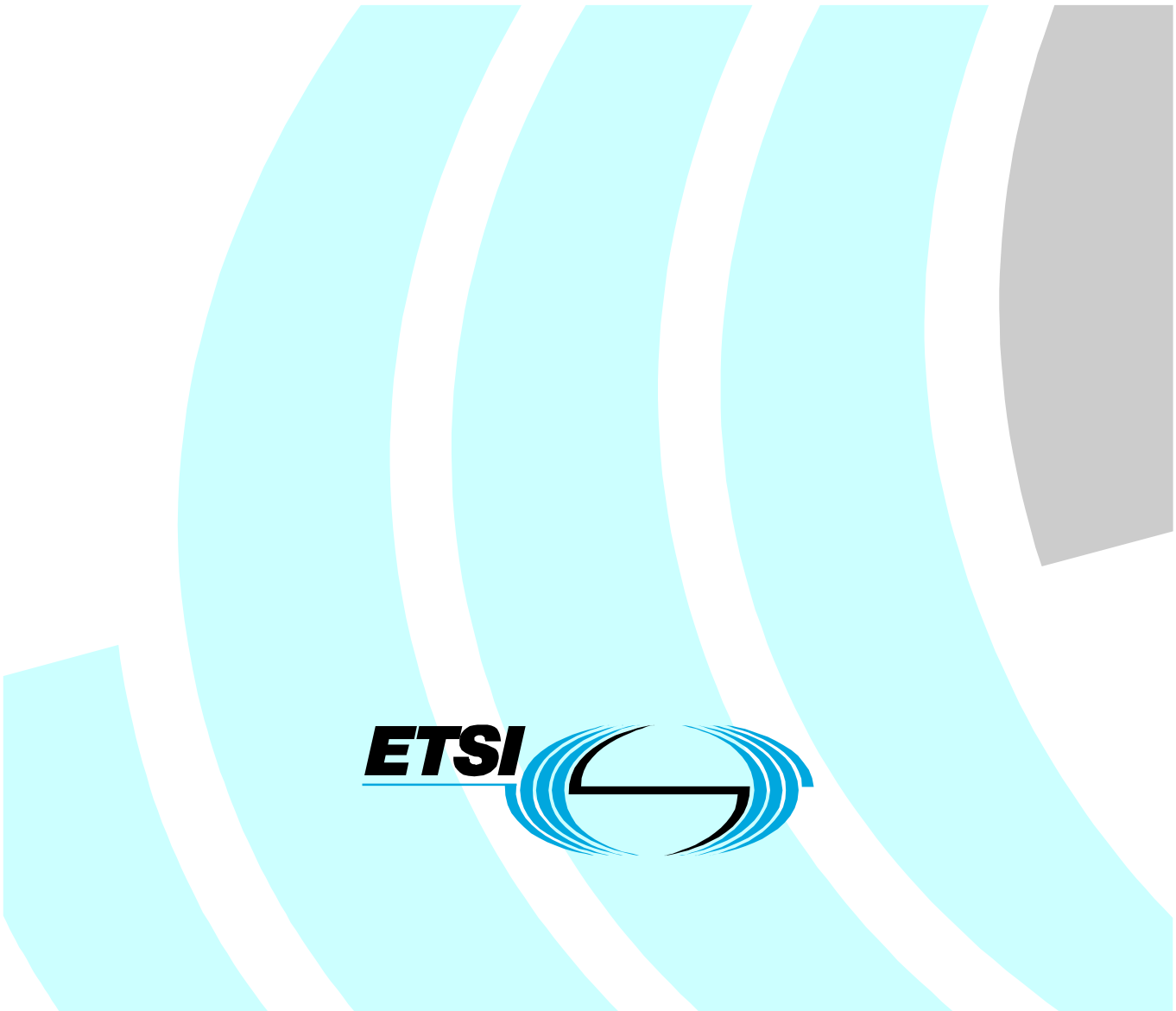
ETSI EG 202 303 V1.1.1 (2004-04)

ETSI Guide

Corporate telecommunication Networks (CN); User identification in a SIP/QSIG environment



Reference
DEG/ECMA-00278

Keywords
endorsement, H.323, PISN, QSIG, signalling

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Guide (EG) has been produced by ECMA on behalf of its members and those of the European Telecommunications Standards Institute (ETSI).

Brief history

The present document investigates user identification within Corporate telecommunication Networks (CNs) (also known as enterprise networks) comprising a mixture of Private Integrated Services Network (PISNs) and Internet Protocol (IP) networks. It focuses on similarities and differences between numbers used in PISNs and Universal Resource Identifiers (URIs) used in IP networks, in particular where the Session Initiation Protocol (SIP) is used.

The present document is based upon the practical experience of ECMA member companies and the results of their active and continuous participation in the work of ISO/IEC JTC1, ITU-T, ETSI, IETF and other international and national standardization bodies. It represents a pragmatic and widely based consensus.

1 Scope

The present document examines means of identifying or naming users of telephony services within a Corporate telecommunication Network (CN) (also known as an enterprise network). Numeric names (numbers) are used in traditional Private Integrated Services Networks (PISNs) using QSIG as the network signalling protocol. They are also used for external communication, e.g. with a public Integrated Services Digital Network (ISDN). Names need not be numeric in Internet Protocol (IP) networks employing signalling protocols such as the Session Initiation Protocol (SIP). The present document therefore looks at naming schemes that are appropriate within corporate IP networks, in particular corporate IP networks employing SIP as the signalling protocol. It also investigates naming schemes that are appropriate in a mixed QSIG/SIP CN and the treatment of names at an interworking point. It details the use of names not only for selecting a user to participate in a call, but also as a means of identifying a user in a call to other users in that call. ENUM and private ENUM-like services are also examined.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ECMA-143 (2001): "Private Integrated Services Network (PISN) - Circuit Mode Bearer Services - Inter-Exchange Signalling Procedures and Protocol (QSIG-BC)".

[2] ECMA-155 (1997): "Private Integrated Services Networks - Addressing".

[3] ECMA-164 (2001): "Private Integrated Services Network (PISN) - Inter-Exchange Signalling Protocol - Name Identification Supplementary Services (QSIG-NA)".

[4] ECMA-165 (2001): "Private Integrated Services Network (PISN) - Generic Functional Protocol for the Support of Supplementary Services - Inter-Exchange Signalling Procedures and Protocol (QSIG-GF)".

[5] ETSI EG 201 940 (2001): "Human Factors (HF); User identification solutions in converging networks".

[6] ETSI TR 101 326 (2002): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); The procedure for determining IP addresses for routeing packets on interconnected IP networks that support public telephony".

[7] IETF RFC 2396 (1998): "Uniform Resource Identifiers (URI): Generic Syntax".

[8] IETF RFC 2806 (2000): "URLs for Telephone Calls".

[9] IETF RFC 2916 (2000): "E.164 number and DNS".

[10] IETF RFC 3261 (2002): "SIP: Session Initiation Protocol".

[11] IETF RFC 3323 (2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[12] IETF RFC 3324 (2002): "Short Term Requirements for Network Asserted Identity".

[13] IETF RFC 3325 (2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

[14] ITU-T Recommendation E.164 (1997): "The international public telecommunication numbering plan".

[15] ITU-T Recommendation H.323 (2003): "Packet-based multimedia communications systems".

3 Definitions

For the purposes of the present document, the terms and definitions given in RFC 2396 [7], ECMA-143 [1] and RFC 3261 [10] and the following apply:

Corporate telecommunication Network (CN) (also known as enterprise network): sets of privately-owned or carrier-provided equipment that are located at geographically dispersed locations and are interconnected to provide telecommunication services to a defined group of users

NOTE: A CN can comprise a PISN, a private IP network (intranet) or a combination of the two.

gateway: point of interworking between a PISN employing QSIG and a SIP network

identifier: name by which the user of a network is known

identification domain: set of identifiers controlled by a single administration

identification number: number used to identify an existing party in a call (e.g. the calling party)

IP network: network, unless otherwise stated a CN, offering connectionless packet-mode services based on the Internet Protocol (IP) as the network layer protocol

number: identifier comprising a numeric string

numbering domain: identification domain in which identifiers are numbers

PISN number: number identifying an entity in a PISN

privacy: withholding of a user's identity from other users in a call in compliance with the wishes of that user

Private Integrated Service Network (PISN): private switched circuit network

selection number: number used as the basis for routing a call to a destination (i.e. identifying the intended party in a call)

SIP network: IP network using SIP for the establishment of communication sessions (calls)

sub-domain: part of a numbering domain in which all numbers share the same leading digits

trust domain: collection of network nodes between which there is either direct or transitive trust in the authenticity of identifiers and the respecting of privacy requirements

4 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CN	Corporate telecommunication Network
DNS	Domain Name System
IP	Internet Protocol
ISDN	Integrated Services Digital Network
NPI	Numbering Plan Identification
PISN	Private Integrated Services Network
PNP	Private Numbering Plan
PUA	Personal User Agent
SIP	Session Initiation Protocol
TON	Type Of Number
UCI	Universal Communications Identifier

URI Universal Resource Identifier

5 Background

Since the 1980s, the traditional way of providing voice services (including fax and modem services) in an enterprise has been through the use of a Private Integrated Services Network (PISN) employing circuit-switched technology. Users of a PISN are identified by numbers (telephone numbers). If a user has been assigned a number, a second user can submit that number to the network in order to establish a call to the first user. Management of assigned numbers for a given network is conducted within a framework known as a numbering plan. This identification technique is similar to that employed in (public) Integrated Services Digital Networks (ISDNs), where the numbering plan is ITU-T Recommendation E.164 [14].

ECMA-155 [2] describes numbering and addressing in a PISN. It describes the use of E.164 and private numbering plans in a PISN and defines a method of structuring private numbering plans. It also specifies various forms of number that can be used for identifying parties.

In the late 1990s, a trend of convergence between voice networks and data networks began, whereby the Internet Protocol (IP) started to be used to carry voice traffic (including associated signalling) alongside traditional data traffic. Identification in IP networks is based upon the Domain Name System (DNS), "Internet names" (see clause 6.2) and Universal Resource Identifiers (URIs), and this principle is therefore applicable also to voice traffic in IP networks.

Because of the large investment by many enterprises in traditional telecommunication networks (PISNs), evolution towards the use of IP networks for voice is often planned to take place over a number of years. This means that PISNs and IP networks carrying voice traffic frequently need to co-exist within the same CN, and smooth interworking between the two environments is necessary. This therefore means that the different methods of identification in the two types of network need to be understood and overcome. The present document investigates this issue, with particular focus on the identification schemes supported by the QSIG protocol in PISNs and SIP in IP networks.

Work has been done in ETSI on naming (TR 101 326 [6]). The focus of that work was public telephony rather than CNs.

6 Naming schemes

6.1 The meaning of a name

The term "name" is commonly applied to the identity of an entity in a telecommunication network, and the term "naming" is applied to the technique of identifying entities by name. This is in contrast to the terms "address" and "addressing", which are commonly applied to the location at which an entity is to be found and the technique of identifying such locations. The general distinction between a name and an address is that a name can remain with an entity even when that entity is mobile and moves between different addresses.

6.2 Names and users

A name is often used to identify a human user, but it can also be used to identify other resources, e.g. a group of users or an automaton. For the purposes of the present document a name is considered to be associated with a user. A user can have more than one name, either to reflect different roles of that user (e.g. business and private) or to reflect different networks in which the user has a presence.

Even within a single network a user can have more than one name for the same role, different names being used for different services. For example a name used for email might also be used for certain other services within the IP network, e.g. for voice or multimedia communications with other users in that or other IP networks. However, an alternative name (in the form of a telephone number) is likely to be required for voice communication outside the IP environment, e.g. involving a public ISDN or PSTN.

In order for a user to establish a communication session with a second user, the first user submits to his local network the name of the second user. It is the task of that network, in conjunction with other networks if necessary, to locate the user associated with that name and establish communication with that user.

6.3 Numeric and non-numeric names

A name can comprise a string of digits (0 to 9), in which case it is a numeric name, otherwise known as a number. Numbers are used in legacy circuit-switched networks, and therefore there are compatibility advantages in using numbers in IP networks. Also numbers are suitable for submission by a human user to a network by means of a device with a limited set of keys, e.g. a conventional telephone. However, a non-numeric name can have a close correspondence with the everyday name of a user, and can therefore be easier to remember or guess.

6.4 Context of a name

Ideally a name should be globally unique so that it has meaning anywhere in the world on a network that supports that type of name. Such a name is said to be fully qualified. Sometimes, particularly on legacy systems, names are used that are meaningful only within a local context, e.g. within a given network or a given geographic region. A local name generally needs to be combined with additional information to produce a fully qualified name.

6.5 Allocation of names

Within a given context, names might be allocated to users on an arbitrary basis. However, this is not always the case. In some contexts names are allocated in accordance with some structure, e.g. organizational, geographic or based on network topology. This makes routing easier but at the expense of lack of flexibility to accommodate long term or short term mobility.

6.6 Naming schemes in circuit-switched networks

Naming schemes in circuit-switched networks (including PISNs, public ISDNs, PSTNs, cellular wireless networks, etc.) are invariably based on numbers. Historically a number represented an address rather than a name, but with the advent of features such as number portability, terminal mobility and user mobility, there has been a gradual evolution over the last two decades towards a number representing a name rather than an address. This is completely true in cellular wireless networks and is generally the case in modern PISNs. For the purposes of the present document a number is assumed to be used as a name rather than an address.

The numbering plan defined in ITU-T Recommendation E.164 [14] ("E.164") is the basis for numbering in all carrier networks and is also applicable to all entities in CNs that need to be directly reachable from carrier networks. An international (fully qualified) E.164 number begins with a country code and is meaningful world-wide (globally unique). By contrast a partial E.164 number lacks some of the leading digits and is meaningful only within a particular region or network. For example, an E.164 number that lacks the country code (a national number) is meaningful only within the country concerned.

Because they begin with a country code, E.164 numbers reflect network topology at the international level. Depending on country they may also reflect network topology at the national level or below.

Within a PISN a private numbering plan can be used to provide a more convenient method of naming (e.g. shorter and/or more easily remembered numbers). An entity in a PISN in which a private numbering plan is used will often have two names: an E.164 number and a private number. However, entities that do not need to be directly reachable by name from outside the PISN can manage with only a private number and no E.164 number. A complete private number is meaningful throughout the domain of the private network (e.g. throughout the PISN) but is not globally unique. A private numbering plan can but need not reflect network topology. The imposition of a topology has implications for user mobility. A partial private number lacks one or more leading digits and is meaningful only within a region of the PISN.

PISNs and other circuit-switched networks often also support an alpha-numeric name for display purposes. Such a display name complements the number and is not a replacement for the number, since it is not necessarily unique within the context in which the number is unique. The display name cannot be used directly as the means of identifying a user with whom communication is to be established, i.e. it cannot be used as the basis for routing. However, directory services might provide a means of translating a display name to a number. Display names are not discussed further in the present document.

6.7 Naming schemes in IP networks

The DNS system provides a method of naming hosts in an IP network and a method of translating a domain name into the IP address of the host concerned. Public DNS servers are deployed in the public Internet and are open to queries from any source. In contrast, private DNS servers are deployed in a closed network (e.g. a CN) for the purpose of resolving domain names within that network and are open to queries only from within that network.

However, the DNS system alone is not sufficient for identifying users, and therefore a name of the form:

user@domain

is generally adopted for applications requiring the identification of users (e.g. email, telephony). The term "internet name" is used in TR 101 326 [6] for this form of name, and this term is also used in the present document. The domain field is the domain name identifying a host where the user field can be interpreted. The domain field should be fully qualified so that it is globally unique, and this therefore makes the internet name globally unique.

6.8 Universal Communications Identifier (UCI)

EG 201 940 [5] proposes a Universal Communications Identifier (UCI) that would provide a single unique identifier (name) for a user of communication services. The UCI comprises three parts: a non-unique alpha-numeric part representing the user's real name or alias, a unique numeric part based on E.164, and a set of flags indicating, for example, a business user. The alpha-numeric part has some similarities to the display name that often accompanies internet addresses (e.g. in front of email addresses or SIP URIs). The numeric part would identify the user's Personal User Agent (PUA), as defined in EG 201 940 [5]. The PUA would perform actions on the user's behalf to facilitate the sending, management and reception of communications. In this respect the numeric part is similar to the address-of-record URI in SIP (see clause 9.2) and the PUA performs a similar role to a SIP proxy. A UCI namespace needs to be established within the E.164 scheme, and this must be done in such a way that UCI numbers can be dialled from countries that do not participate in UCI.

To establish a call, as a minimum the unique numeric part needs to be submitted. Compared with internet names this has the advantage that it can be entered even at the simplest of terminals, but has the disadvantage that it is less memorable than an alpha-numeric name.

At present UCI is of interest as a possible future development but does not at present have an impact on QSIG/SIP environments. It is not considered further in the present document.

7 Signalling protocols

The internationally-standardized network signalling protocol for PISNs is QSIG, as specified in ECMA-143 [1], ECMA-165 [4] and other ECMA Standards. QSIG uses numbers for naming and provides support for the forms of number specified in ECMA-155 [2].

The use of IP networks to carry voice and multimedia traffic has led to the development of new signalling protocols to support voice and multimedia communications in this environment. One such protocol, known as "H.323", is specified in ITU-T Recommendation H.323 [15] and other recommendations. Another such protocol, is the Session Initiation Protocol (SIP), specified by IETF in RFC 3261 [10] and other RFCs. Both H.323 and SIP are being deployed in CNs. The process of evolution means that QSIG-based PISNs and H.323/SIP-based IP networks frequently need to co-exist within the same CN, and smooth interworking between the protocols concerned is necessary.

Various protocols employed in IP networks use URIs (RFC 2396 [7]) for identifying specific resources. A URI always begins with a scheme identifier (e.g. *http:*). The framework specified in RFC 2396 [7] is quite flexible and the fields that follow the scheme identifier depend on the particular scheme. Some schemes accommodate internet names, e.g. the *mailto:* scheme for email. In addition to the scheme identifier and internet name, such URIs can contain other information (e.g. parameters).

SIP uses URIs for identifying users. The SIP URI (RFC 3261 [10]) accommodates an internet name. However, other URI schemes can be used in SIP, including the telephone URI (RFC 2806 [8]), which accommodates a number. H.323 can use numbers as the means of identifying users, but it can also use alpha-numeric names and URIs.

The capability of using non-numeric names, in particular internet names, in SIP and H.323 can lead to difficulties interworking with PISNs, where numbers are used to identify users. The remainder of the present document examines the implications of this in more detail, focusing on the use of QSIG as the signalling protocol in PISNs and SIP in IP networks. However, much of what is said concerning SIP is also applicable to H.323, which is not considered further in the present document.

8 Overview of naming, numbering and addressing in QSIG

8.1 Numbers as a means of identifying entities

The main method of identifying entities in QSIG is by means of PISN numbers. A PISN number can identify any entity that can be the target destination of a call, e.g.:

- an individual user (who may be mobile or may be tied to a particular access);
- a particular network access;
- a particular service;
- a predefined group of users or group of network accesses.

When used to identify an individual user, service, etc., a number can be regarded as a name, but when used to identify a particular network access it can be regarded as an address. However, ECMA-155 [2] does not make this distinction.

NOTE 1: In fact ECMA-155 [2] uses the term address for the combination of number and subaddress. Subaddresses are not considered further in the present document.

Typically a number is used to identify a user. Because of Wireless Terminal Mobility (WTM) or Personal User Mobility (PUM), a number identifying a user is not necessarily associated with a particular access, although in the case of non-mobile users this association will exist.

NOTE 2: For non-mobile users this association can change on an infrequent basis, e.g. when the user moves permanently to a different office.

A number is referred to as a selection number when used as the basis for routing a call to a destination (i.e. identifying the intended party in a call). A number is referred to as an identification number when identifying an existing party in a call (e.g. the calling party).

8.2 Numbering plans

Management of assigned numbers for a given network is conducted within a framework known as a numbering plan. A PISN employs one or more numbering plans and each PISN number belongs to a numbering plan. ECMA-155 [2] allows PISNs to use the E.164 numbering plan. It also defines structured Private Numbering Plans (PNPs) for use in PISNs.

NOTE: ECMA-155 [2] also permits the use of DCC (data country code) and ICD (international code designator) numbering plans within a PISN. These are mainly for use with Asynchronous Transfer Mode (ATM) and are not discussed further in the present document.

For both E.164 and PNPs, numbers can be complete or partial. A partial number lacks some of the leading digits and is therefore significant only within a particular sub-domain. In the case of E.164, for example, an international number has global significance (i.e. it is fully qualified) whereas a national number lacks a country code and has significance only within the country concerned. In the case of a PNP, a complete number has significance within the numbering domain of the PNP (e.g. the CN) and a regional number has significance only within a certain part of that numbering domain.

Therefore a number must be qualified by a separate Numbering Plan Identification (NPI, identifying the numbering plan to which it belongs) and a separate Type Of Number (TON, indicating the completeness of the number).

Alternatively, the numbering plan and completeness of the number can be implicit in the number itself, e.g. by the use of prefix digits. An implicit number is indicated by a special value in the NPI.

8.3 Use of numbers in QSIG

QSIG uses numbers for the following purposes:

- in the Called party number information element for identifying the intended destination of a call (i.e. a selection number);
- in the Calling party number and Connected number information elements for identifying the calling and connected (answering) party respectively;
- in various remote operations for identifying parties involved in supplementary services or additional network features, e.g. transferred-to party, diverted-to party, diverted-from party.

QSIG also has a name supplementary service (ECMA-164 [3]) that provides additional identification information (typically a name) for a party in the form of a character string. The name is conveyed in dedicated remote operations during call establishment and also in certain operations of other supplementary services.

9 Overview of identification in SIP

9.1 URIs as a means of identifying entities

SIP uses URIs to identify entities participating in communication sessions. Although RFC 3261 [10] defines the SIP scheme (and the secure equivalent SIPS) specifically for use within SIP, any form of URI can in principle be used, including the telephone URI scheme defined in RFC 2806 [8]. All SIP implementations must support SIP URIs.

In contrast to identifiers in QSIG, URIs are virtually never used to identify physical addresses. The SIP routing process provides translation from URI (as it appears in the SIP Request-URI field) to IP address.

9.1.1 Telephone URI

The telephone URI is currently defined in RFC 2806 [8]. However, a revised version of RFC 2806 [8] is in preparation (*draft-ietf-iptel-rfc2806bis-02*), and the information below relates to this draft revised edition.

A telephone URI is of the form:

tel:telephone-subscriber

where telephone-subscriber is a number followed by optional parameters. A number can be a global number (i.e. an E.164 number, beginning with "+") or a local number. An example of a telephone URI with a global number is as follows:

tel: +4321098765

The significance of a local number depends on the numbering domain. However, the *phone-context* parameter, which must be included in the case of a local number, provides additional information that makes the number globally unique.

EXAMPLE:

tel:1234;phone-context=+411234

tel:1234;phone-context=ecma.ch

The first example indicates that telephone number 1234 is to be interpreted within context +411234, i.e. within the context of all E.164 numbers beginning with +411234 The second example indicates that telephone number 1234 is to be interpreted within the context of domain name *ecma.ch* The draft revised edition of RFC 2806 [8] requires the use of global E.164 numbers except for numbers that cannot be represented that way (e.g. numbers from private numbering plans, emergency numbers, directory assistance numbers, etc.).

9.1.2 SIP URI

A SIP URI is of the form:

sip:userinfo:password@host:port;uri-parameters?headers

The use of password is deprecated (for security reasons) and port, uri-parameters and most headers are not of relevance to the present discussion. Therefore for the purposes of the present document a SIP URI is of the form:

sip:userinfo@host or

sip:userinfo@host;uri-parameters

where *host* is a domain name or IP address and *userinfo* is a particular resource at the host being addressed.

NOTE 1: userinfo@host is effectively an internet name (user@domain).

EXAMPLE 1:

sip:john@ecma.ch

sip:1234@ecma.ch

The *userInfo* field can contain a telephone-subscriber string, as defined in RFC 2806 [8] for a telephone URI (see clause 9.1.1). In this case the SIP URI parameter *user* = should be present with value *phone*. This is the only SIP URI parameter of relevance to the present document.

EXAMPLE 2:

sip: +4321098765@ecma.ch;user=phone

sip:1234;phone-context=+411234@ecma.ch;user=phone

NOTE 2: The second example is not necessarily equivalent to the second of the previous set of examples, where the absence of "user=phone" means that the userinfo field should not be interpreted as a telephone-subscriber string.

NOTE 3: There is a distinction between parameters to the SIP URI (e.g. user=) and parameters to the telephone-subscriber string (e.g. phone-context=).

Clause 19.1.6 of RFC 3261 [10] gives rules for converting a telephone URI to a SIP URI. The telephone-subscriber string in the telephone URI becomes the *userinfo* field of the SIP URI and a suitable *host* field is added.

NOTE 4: Recent discussions in the IETF have identified the need for an additional parameter to the SIP URI: user=dialString. This indicates that the userInfo field contains a dial string, which may require translation in order to yield a true identifier (e.g. removal of prefix digits).

9.1.3 Display name

In addition, a URI can be accompanied by a display name in some cases.

EXAMPLE:

"John"<sip:1234@ecma.ch>

9.2 Use of URIs in SIP

SIP uses URIs for the following purposes:

- in the Request-URI for routing a request;
- in the To header, for indicating the logical recipient of a request (unlike the Request-URI, the URI in the To header is not changed by proxies) (see note 1);
- in the From header, for indicating the initiator or a request (see note 1);

- in the Contact header, for indicating the contact point for further requests in a dialog or for indicating a new target in a 3xx response (see note 1);
- in the Reply-To header, for indicating the address for replies using a new request outside the scope of the current dialog (e.g. a new INVITE request);
- in the Route header, for identifying a proxy for routing a request through;
- in the Record-Route header, for identifying a proxy involved in a request so that further requests in the same dialog can be forced through that proxy;
- in the P-Asserted-Identity header for conveying party identification information between trusted SIP entities (see note 2);
- in the P-Preferred-Identity header for a UA to convey to its proxy the particular identity (out of several valid identities) by which the user is to be known for the purposes of the present call (see note 2);
- in the Refer-to header in the REFER method.

NOTE 1: URIs in these headers can include a display name.

NOTE 2: The P-Asserted-Identity and P-Preferred-Identity headers are defined in RFC 3325 [13].

In addition, new headers to be defined in new RFCs might include URIs.

A distinction should be made between address-of-record URIs (e.g. in Request-URI, To header and From header) and contact URIs (e.g. the first use above of Contact header). An address-of-record URI identifies a user whereas contact URIs identify a device. The process of registering using the SIP REGISTER method temporarily binds an address-of-record URI to a contact URI for a device. Therefore a contact header is somewhere between a name and an address and is not considered further in the present document.

10 Comparison of numbers and non-numeric names for use in SIP

Through various forms of URI, SIP can use both numbers and non-numeric names for identification. This is in contrast to QSIG, where only numbers are used.

10.1 Numbers in SIP

The use of numbers for identification in SIP has the advantage of compatibility with legacy systems, including PISNs, PSTNs and public ISDNs. Normally, the only means available to a user on a legacy network for making a call to another user is by submitting (dialling) the number of the called user. If the calling user is not aware of the number of the called user, he can look it up in a directory (electronic or otherwise) and then submit it (or cause it to be submitted automatically). Routing by name or URI is not possible on legacy networks. Therefore a user in a SIP network must have a number in order to be reachable from a legacy network. Likewise, a number must be used in order to reach a user in a legacy network from a SIP network.

A disadvantage of using numbers in SIP is the use of different numbering plans and types of number, leading to the need to insert leading digits to produce a fully qualified number and the need to deal with prefix digits or other characters (e.g. "+" in front of an international E.164 number).

Numbers can be placed in the *userinfo* field of a SIP URI or in a telephone URI. The use of number-based URIs in SIP networks facilitates interworking with legacy networks and also permits the use of SIP phones with just a traditional telephone keypad. There are also likely to be performance advantages based on being able to route on leading digits without the need to interrogate large databases. However, the *host* field of a SIP URI is generally non-numeric, which makes interworking with a SIP URI somewhat less simple. On the other hand, even the telephone URI requires a *context* parameter if the number is not fully qualified, and this too can make interworking less simple.

Whichever URI scheme is used, there are still issues to be considered concerning whether the number is fully qualified or partial. In general a fully qualified number is to be preferred, although there may be situations in which partial numbers can be of benefit (e.g. a URI submitted from a phone to its local proxy). Care has to be taken not to send a partial number outside its domain. The *phone-context* parameter in the telephone URI can be a way of defining the context of a number, but still care must be taken not to send a URI outside the domain where the value in *phone-context* is meaningful.

10.2 Non-numeric names in SIP

As stated in clause 6.3, a non-numeric name can have a close correspondence with the everyday name of a user, and can therefore be easier to remember or guess. Since non-numeric names are routinely used for certain services (e.g. email), the use of the same name for telephony can be advantageous.

SIP URIs (without *user=phone*) contain internet names in which the *userinfo* part is not limited to numeric digits and in general will contain alphabetic characters. For this reason a SIP URI can convey meaningful names of users, services, etc.. Email addresses are often remembered if the user part is in a conventional form (e.g. firstName.lastName) and the host part is a recognizable company domain name (e.g. MyOwnCompany.com). Similarly, well-chosen SIP URIs can be more easily remembered, particularly if they are similar to email addresses.

EXAMPLE:

sip:john@ecma.ch

mailto:john@ecma.ch

For these reasons, some enterprises will be keen to move away from numbering and fully exploit the advantages of internet names in URIs, but there are difficulties to be overcome, particular when interworking with circuit-switched networks. Also there might be performance penalties.

10.3 Summary

Although the use of numbers as the basis for identification in SIP in URIs is likely to be quite common in the short to medium term, URIs not based on numbers (e.g. based on the user's everyday name) are likely to be introduced in parallel, with users having more than one identifier (aliases), e.g. a number and an alpha-based SIP URI. Different identifiers might be used for different services, e.g. internet names for services other than telephony and perhaps for telephony within the IP network and numbers for interworking with circuit-switched networks.

11 Interworking scenarios

Each network has one or more identification domains. A PISN typically forms part of the global numbering domain for E.164 numbers and also has its own numbering domain for private numbering.

Where a PISN has more than one numbering domain, some users may have a number in more than one numbering domain, e.g. an E.164 number and a private number. There may or may not be an algorithmic means of mapping between a user's number in one numbering domain and a user's number in another numbering domain.

In a SIP network using SIP URIs for identification, the identification domain is the set of identifiers served by a particular host.

In a QSIG-SIP interworking environment, two basic scenarios are identifiable:

1) A common numbering/identification domain spans the QSIG and SIP networks. In other words, a common numbering plan exists and numbers can be passed between the two networks. The boundary between the two networks may correspond to a sub-domain boundary, and therefore it may be necessary to convert numbers to a higher level before crossing the boundary. Also it may be necessary to add/remove prefix digits if one network uses implicit numbering or if both networks use implicit numbering with different prefixes.

2) The networks belong to different numbering/identification domains. In this case, identifiers received from one network need to be mapped or translated to identifiers suitable for sending to the other network. Mapping may be algorithmic (e.g. insertion and/or removal of digits) or on an individual identifier basis by table look-up. If an identifier has no corresponding identifier in the other network it cannot be passed.

In a given situation, both scenarios can co-exist, e.g. one for private numbers and the other for E.164 numbers.

12 Interworking functions

12.1 Converting PISN numbers to URIs

12.1.1 Selection and identification numbers

Considerations differ slightly according to whether the PISN number is a selection number (Called party number information element) or an identification number.

12.1.2 Choice of URI scheme

A PISN number could be converted to a SIP URI, a telephone URI or some other URI. It is important that the scheme chosen is understood by at least the first proxy. A SIP URI will always be understood, but other schemes such as telephone URIs will not necessarily be supported. Use of a SIP URI is assumed below.

12.1.3 Choice of host

If a SIP URI is chosen, it is necessary to provide a value for the host portion of the URI. For a selection number (QSIG Called party number information element) the host needs to be a domain that can interpret the *userinfo*, which will be derived from the PISN number. There may be a single domain for accessing all numbers, or it may be necessary to select the domain according to the number. The former is easier for the gateway but places more burden on proxies. There may be different domains for E.164 and PNP numbers. For an identification number it must be the domain to which the gateway belongs.

12.1.4 Mapping the number to a URI *userinfo* field

An E.164 international number could be placed directly as a global number in the *userinfo* field of a SIP URI. An E.164 national or subscriber number would first need to be converted to an international number.

For preference, a PNP number should be converted to an E.164 international number and treated as above. Where this is not feasible, a PNP number could be placed directly in the *userinfo* field as a local number, provided the domain concerned recognizes such numbers. It may require converting the PNP number to a higher level (e.g. a complete number) and/or the addition of prefix digits. Alternatively the *phone-context* parameter can be used to indicate the context of a PNP number, as illustrated by the following examples. In these examples, the domain name of the SIP proxy is mysip.net, but it could be the same as the domain name used for the phone context (myco.com).

PNP TON	Example number	Example phone context	Example SIP URI
Level 2 regional number	456789	+44123	sip:456789:phone-context=+44123@mysip.net;user=phone
		level2.myco.com	sip:456789:phone-context=level2.myco.com@mysip.net;user=phone
Level 1 regional number	56789	+441234	sip:56789:phone-context=+441234@mysip.net;user=phone
		level1.myco.com	sip:56789:phone-context=level1.myco.com@mysip.net;user=phone
Local number	6789	+4412345	sip:6789:phone-context=+4412345@mysip.net;user=phone
		level0.myco.com	sip:6789:phone-context=level0.myco.com@mysip.net;user=phone

An implicit number might need to be analysed. For example, if prefix digits indicate a public network number, it could be converted to an international E.164 number and treated as above.

If crossing an identification domain boundary, each PNP number will require mapping to a *userinfo* value either algorithmically or by table look-up. In the latter case *userinfo* values need not be limited to telephone numbers - they could be non-numeric names.

In each of the above cases where a telephone number is placed in the *userinfo* field, parameter *user=phone* should be included in the SIP URI.

12.2 Converting URIs to PISN numbers

12.2.1 Selection and identification numbers

Considerations differ slightly according to whether the PISN number to be generated is a selection number (derived from the To header or the Request-URI) or an identification number.

12.2.2 Support of different URI schemes

The gateway may support only a single URI scheme, in which case this would probably need to be SIP URIs, or may support more than one, including, for example, telephone URIs. Support of SIP URIs is assumed below.

12.2.3 Use of the host field

For a selection number, the host field should identify the gateway's domain - otherwise the call should not have been routed to this gateway.

For an identification number, other domains might be indicated. The ability to convert URIs from other domains cannot be assumed, unless the *userinfo* field contains a global E.164 number.

12.2.4 Mapping the URI *userinfo* field to a PISN number

If the *userinfo* field contains a telephone number, it may be possible to use this directly as a PISN number or it may be necessary to carry out some conversion, e.g. addition of prefix digits.

If crossing an identification domain boundary, it may be possible to map *userinfo* values to PISN numbers algorithmically or by table look-up. In the latter case *userinfo* values need not be limited to telephone numbers - they could be non-numeric names.

If present, the *phone-context* parameter of the *telephone-subscriber* string should be taken into account. This may provide information that can be mapped directly to PNP and NPI fields in the QSIG number information element (see PNP examples in clause 12.1.4).

13 Use of ENUM

RFC 2916 [9] ("ENUM") specifies a method of mapping E.164 numbers to URIs. Basically a domain name is created by reversing the full international E.164 number, placing a dot between each digit, and appending ".e164.arpa". This gives a domain name that can be used to perform a DNS look-up. The result is a limited set of URIs that can be used as potential contacts for the number concerned. This can include, of course, SIP URIs and telephone URIs.

RFC 2916 [9] is applicable only to E.164 numbers. It is a centralized service based on the "e164.arpa" root, and therefore for a given E.164 number there is only one logical place in the Internet where authoritative records can be obtained.

ENUM therefore is a useful means of converting fully qualified E.164 numbers to SIP URIs and could be used by gateways when handling calls from QSIG to SIP where the QSIG Called party number information element contains an E.164 number. Although simple conversion to a SIP or telephony URI can be done without the aid of ENUM, the use of ENUM can add value, e.g. by selectively choosing the *host* part of the URI.

A replacement for RFC 2916 [9] is currently in a fairly advanced state of drafting (*draft-ietf-enum-rfc2916bis-06*). The replacement allows the use of an ENUM-like private service where the suffix is something other than ".e164.arpa" (e.g. ".e164.MyOwnCompany.com"). This could be a useful means of resolving private numbers to SIP URIs. Normally it would require fully qualified private numbers. It could also handle DDI numbers, e.g. by first converting them to fully qualified private numbers. Although simple conversion to a SIP or telephony URI can be done without the aid of a private ENUM-like service, the use such a service can add value, e.g. by selectively choosing the *host* part of the URI or by providing a non-numeric *userinfo* part.

Useful information on the relationship between ENUM and SIP is contained in draft-ietf-sipping-e164-02.

Depending on country, a CN can operate a public ENUM service at level 2 (level 0 being international and level 1 being national) for resolving certain numbers from the national numbering plan, e.g. numbers for a city or numbers relating to the CN itself. Such a service is available to the general public and insecure, and therefore it might be inappropriate as a means of making available detailed information on routing within the CN. However, internally, a CN could operate a closed ENUM service for resolving internal numbers (private or E.164). A split DNS could offer both, effectively with a firewall between the two.

There has been some discussion in ENUM circles of providing a reverse ENUM service that translates an internet name to a number. This would potentially be of use to a QSIG-SIP gateway but nothing is yet standardized.

14 Asserted identity and privacy in SIP

The IETF has published two RFCs on identity and privacy that have the potential to provide better solutions to the problem of mapping to and from the QSIG Calling party number and Connected number information elements. This clause contains an overview of the two RFCs and describes how they can be used to enhance QSIG-SIP interworking. Detailed mapping scenarios are described in annex A.

14.1 Overview of asserted identity RFC

Asserted identity is specified in informational RFC 3325 [13] and provides headers for conveying identity information between trusted entities. It is based on requirements in informational RFC 3324 [12].

The document introduces two new "P-headers" (preliminary, private or proprietary headers), P-Asserted-Identity and P-Preferred-Identity. The reason for making them P-headers is that they are intended only as a preliminary solution or a solution aimed at specific applications, and are regarded as not fitting into the main SIP-Internet architecture. Because it defines only P-headers, the RFC is informational, not standards track. There is work in progress in the IETF to produce a new standards track RFC that relies on cryptography rather than trust, and the use of this in CNs should be investigated when the work matures. Although RFC 3325 [13] is sometimes viewed as a short term solution, there is also a body of opinion that says that solutions based on RFC 3325 [13] may be appropriate even in the long term in appropriate trusted environments (e.g. CNs).

The P-Asserted-Identity header contains (name-addr/addr-spec) for the party whose identity is asserted. This is implicitly the party from whom the message is sent, e.g. the calling party in the case of an INVITE request. The header is generated by a proxy that is able to authenticate the user (by some means outside the scope of the RFC, e.g. SIP Digest Authentication) and forwarded between trusted entities. It may be forwarded to untrusted entities (normally only to UAs), but must not be forwarded to untrusted entities if the user has requested privacy by means of the Privacy header (see clause 14.2). However, an additional value "id" is introduced to the Privacy header to indicate that the asserted-id is private.

The P-Preferred-Identity header is for an untrusted UA to provide a "hint" to its (trusted) proxy as to which of several identities it wishes to be known by for the purposes of the current call. The proxy may take account of this and forward this identity (assuming it is able to authenticate it) in a P-Asserted-Identity header or replace it.

14.2 Overview of general privacy RFC

RFC 3323 [11] defines a Privacy header that can be inserted by a UA (or a proxy acting in accordance with user instructions) and can specify one or more of the following types of privacy:

- "header" - removal of identifying information from all headers that the UA cannot deal with (e.g. Contact, Via);
- "session" - removal of identifying information in SDP bodies (i.e. session IP addresses);
- "user" - application of privacy measures that would normally be performed at the UA (e.g. making the From header anonymous);
- "none" - no privacy, overriding any pre-existing agreement for a proxy to provide privacy;
- "critical" - the privacy services requested are critical and if they cannot be provided the request should be rejected.

In addition, the asserted identity RFC adds "id" (asserted-id privacy).

The Privacy header is acted upon by a "privacy service", typically collocated with a proxy.

14.3 Applicability to QSIG-SIP interworking

14.3.1 Trust within a CN

CNs are often suitable environments for treatment as trusted domains from the point of view of identity and privacy. This is indeed the case in a conventional QSIG network, since each node trusts any identity provided by another node. Also a node sending an identity that requires privacy can trust a node to which it is sent not to disclose that identity to untrusted entities, in particular to users who are not entitled to receive that information. Trust is transitive, in that it operates through transit nodes.

If the CN is SIP-based, it is often quite reasonable for all SIP entities to be regarded as part of a trust domain where:

- all proxies trust each other;
- all UAs trust their proxies; and
- trust is transitive.

In general a proxy will not trust its UAs, although it might trust certain UAs, e.g. gateways.

Within a trust domain, all entities must conform to a certain set of specifications, which the asserted identity RFC calls "Spec(T)". For a given trust domain, Spec(T) will specify, among other things, the security mechanisms used for communication between SIP entities and the means of authenticating users.

Very large CNs might comprise more than one trust domain.

If the CN contains both SIP and QSIG, with interworking between the two by means of gateways, it would be quite reasonable for a single trust domain to embrace both parts of the network. This would allow:

- identities from the QSIG network to be passed to the SIP network and trusted by entities in the SIP network;
- identities from the SIP network to be passed to the QSIG network;
- privacy indications associated with identities from the QSIG network to be honoured by the SIP network; and
- privacy indications associated with identities from the SIP network to be honoured by the QSIG network.

In this case, the QSIG-SIP gateway will trust the nearest proxy and vice versa.

Conversely, the lack of a single trust domain covering the SIP and QSIG networks means the following:

- identities from the QSIG network can be passed to the SIP network (if privacy is not required) but SIP entities will not be able to trust these identities (unless a separate means of authentication is available);
- identities from the SIP network should not be passed to the QSIG network unless the gateway has separate means of authenticating them;
- identities marked as private from the QSIG network should not be passed to the SIP network;
- identities marked as private from the SIP network will not be passed to the gateway.

To achieve this, the QSIG-SIP gateway should not trust the nearest proxy and the nearest proxy should not trust the QSIG-SIP gateway. This scenario is perhaps less likely within a CN than the single trust domain described earlier, although it could apply in very large CNs.

14.3.2 Trust outside a CN

When a CN interworks with a carrier ISDN network, it is normally the case that the CN trusts the carrier network but not vice versa. A CN will normally trust an identity provided by a carrier network (this is true for a QSIG network). Also a CN may or may not trust a carrier network to honour any privacy associated with identities provided to the carrier network. On the other hand, a carrier network will not normally trust an identity provided by a CN, and although in the case of ISDN it may deliver such an identity to the destination user, it will mark it as user-provided. In this case it might also deliver the identity of the access, which it can guarantee. A carrier network will not normally deliver an identity for which privacy is required to a CN.

These considerations apply more or less independently of whether the CN is circuit-switched (QSIG) or SIP.

When a CN interworks with a carrier SIP network, considerations might be different. It the carrier network is the public Internet, it is unlikely that the CN will trust identities received from that carrier network and it is unlikely that the CN will be prepared to submit identities subject to privacy to that carrier network. On the other hand, if the carrier SIP network is administered to a standard comparable with that of carrier ISDN networks, then the CN might be prepared to trust it to the same degree as a carrier ISDN network.

It is a matter for the entity that interworks directly with a carrier SIP network to determine the degree of trust.

If the QSIG network interworks directly with a trusted or untrusted carrier SIP network (i.e. the gateway communicates with a proxy in the carrier network), then it should behave as it would when interworking with a corporate SIP network within or outside gateway's trust domain respectively.

If the QSIG network interworks via a corporate SIP network with a carrier SIP network, it is a matter for a proxy in the corporate SIP network to take necessary steps to protect the CN from the carrier network. This includes preventing untrusted identities from the carrier network penetrating into the CN and preventing disclosure of private identities to the carrier network. If there is a single trust domain within the CN, the QSIG-SIP gateway can behave as normal for this situation and rely on the SIP network to provide the necessary protection from the carrier network. In other words the principle of transitive trust applies.

15 Conclusions

Numbers can be used in SIP for identifying users, by encapsulation within SIP or telephone URIs. This is likely to be common practice in the short to medium term, because of the need to interwork with legacy networks, including QSIG. However, non-numeric names (internet names) are likely to be introduced in parallel, with users having more than one name. Different names might be used for different services, e.g. internet names for services other than telephony and perhaps for telephony within the IP network and numbers for interworking with circuit-switched networks.

The use of numbers simplifies interworking with QSIG, particularly if the two networks are part of the same identification domain. The use of non-numeric names in the SIP network necessarily means that there will be a domain boundary between the SIP network and the QSIG network and therefore mapping will be required. e.g. by table look-up.

A private ENUM-like service might be a convenient way of providing mapping from numbers to SIP URIs at an interworking point.

Annex A (informative): Mapping between QSIG information elements and SIP P-Asserted-Identity and Privacy headers

A.1 Mapping QSIG Calling party number information element to SIP elements

Without the asserted identity RFC, SIP provides only the From header as a suitable vehicle for conveying information from the QSIG Calling party number information element. The From header is normally provided by a UAC and passed unchanged through proxies to the UAS. Mapping the Calling party number to the From header has two problems:

1) Even if a downstream proxy is aware that the identity is subject to privacy, it cannot remove it before passing on to an untrusted entity, except by behaving as a back-to-back UA.

2) A downstream proxy (beyond the first proxy) is not aware of whether the UAC is a trusted entity and therefore cannot rely on the accuracy of the information in From.

Within a trusted domain, the P-Asserted-Identity header gets around these problems. If the gateway trusts the nearest proxy, the identity should be placed in a P-Asserted-Identity header and if presentation is restricted a Privacy header should be included with priv-value = "id".

If the gateway does not trust the nearest proxy it may still include a P-Asserted-Identity header, but only if the presentation is not restricted. If presentation is restricted the gateway should include a Privacy header with priv-value = "id".

NOTE: In this case the proxy will probably not trust the gateway and will ignore (and not pass on) the P-Asserted-Identity header. An alternative would be to use the P-Preferred-Identity header instead, but it is unlikely that the proxy will have a means of validating the identity, so likewise this is likely to be ignored (and not passed on). There does not seem to be a case for using the P-Preferred-Identity header.

Regardless of trust, the gateway should incorporate the identity in the From header if presentation is not restricted and include an anonymous value in the From header if presentation is restricted.

If presentation is restricted, the gateway may use the Privacy header to request other types of privacy, e.g. "header" or "session". For example, "header" privacy would hide the gateway's identity in the Contact header, and "session" privacy would hide the gateway's IP address in SDP. The need for this is lessened by the fact that gateway identities do not reveal the identity of the user in the QSIG network, although they might reveal the identity of the QSIG network. However, to honour such privacy requests requires the presence of special equipment (e.g. back-to-back UAs) in the local SIP network.

A.2 Mapping QSIG Connected number information element to SIP elements

The asserted identity RFC provides the only means at present for conveying information derived from the QSIG Connected number information element. Note that the Contact header should identify the gateway rather than the connected party.

If the gateway trusts the nearest proxy, the identity should be placed in a P-Asserted-Identity header and if presentation is restricted a Privacy header should be included with priv-value = "id".

If the gateway does not trust the nearest proxy it may still include a P-Asserted-Identity header, but only if the presentation is not restricted. If presentation is restricted the gateway should include a Privacy header with priv-value = "id".

NOTE: In this case the proxy will probably not trust the gateway and will ignore (and not pass on) the P-Asserted-Identity header. An alternative would be to use the P-Preferred-Identity header instead, but it is unlikely that the proxy will have a means of validating the identity, so likewise this is likely to be ignored (and not passed on). There does not seem to be a case for using the P-Preferred-Identity header.

A.3 Mapping SIP elements to QSIG Calling party number information element

Without the asserted identity RFC, SIP provides only the From header as a suitable source of information for populating the QSIG Calling party number information element. Use of the From header has two problems:

1) It cannot be trusted, since it comes from the UAC, which normally is untrusted.

2) It can contain an anonymous value if privacy is required.

Within a trusted domain, the P-Asserted-Identity header, in conjunction with the Privacy header, gets around these problems. If the gateway trusts the nearest proxy and a P-Asserted-Identity header is present, the gateway should use information from that header to derive the QSIG Calling party number information element. If a Privacy header is also present with priv-value = "id", the presentation indicator should be set to presentation restricted.

Within a CN, it will normally be the case that the gateway trusts the nearest proxy. However, if the gateway does not trust the nearest proxy, it should not make use of the P-Asserted-Identity header, if present. Depending on the presence of a Privacy header with priv-value = "id", the presentation indication should be set to either "not available due to interworking" or "presentation restricted", in either case with no number.

This leaves the difficult question of whether to make use of the From header at all for cases where no P-Asserted-Identity header is received. Logic dictates that it should not be used, because it comes from an untrusted source and a QSIG network assumes that information in the Calling party number information element can be trusted.

NOTE: The ability to set the screening indicator to "user provided, not screened" would appear to indicate that it is generally acceptable to put untrusted numbers in the information element, provided this value of the screening indicator is used. However, this value of the screening indicator normally means that the number has been supplied by a PBX or CN to a public ISDN and the public ISDN has been unable to screen the number. Such numbers tend to be trusted in CNs for caller display purposes, since they do not normally come from end user equipment. Identities in the SIP From header, however, come from end user equipment and are much more likely to be falsified. Therefore deriving a number from the From header and marking it "user provided, not screened" may cause an undue level of trust to be given to the number in the QSIG network.

However, until implementation of the P-Asserted-Identity header (or the long term alternative) becomes common, the From header will often be the only means of populating the Calling party number information element. Some administrations may be prepared to accept this risk in order to obtain the benefits of caller display. Therefore gateways should be allowed to use the From header in the absence of more reliable information. This should be a configurable option. Where this option applies, the presence of display name "Anonymous" should be used to set the presentation indicator to "presentation restricted". Otherwise, if no number can be derived from the contents of the From header, the presentation indicator should be set to "not available due to interworking". The screening indicator should be set to "user provided, not screened".

A.4 Mapping SIP elements to QSIG Connected number information element

The asserted identity RFC provides the only suitable source of information at present for populating the QSIG Connected number information element.

If the gateway trusts the nearest proxy and a P-Asserted-Identity header is present, the gateway should use information from that header to derive the QSIG Connected number information element. If a Privacy header is also present with priv-value = "id", the presentation indicator should be set to presentation restricted.

Within a CN, it will normally be the case that the gateway trusts the nearest proxy. However, if the gateway does not trust the nearest proxy, it should not make use of the P-Asserted-Identity header, if present. Depending on the presence of a Privacy header with priv-value = "id", the presentation indication should be set to either "not available due to interworking" or "presentation restricted", in either case with no number.

Annex B (informative): Bibliography

IETF RFC 1034 (1987): "Domain names - concepts and facilities".

History

Document history			
V1.1.1	February 2004	Membership Approval Procedure	MV 20040423: 2004-02-24 to 2004-04-23
V1.1.1	April 2004	Publication	