TECHNICAL REPORT

ISO/IEC TR 12861

First edition
2009-04-15

Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Identification and routing

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseaux d'entreprise de prochaine génération (NGCN) — Identification et routage

Reference number
ISO/IEC TR 12861:2009(E)

© ISO/IEC 2009

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2009 – All rights reserved

Not for Resale

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 2
3.1 External definitions 2
3.2 Other definitions 3
4 Abbreviated terms 3
5 Background 4
6 Identified entities 4
7 Types of identifier 5
7.1 SIP, SIPS and TEL URIs as user identifiers (AoRs) 5
7.1.1 Use of E.164 numbers 8
7.1.2 Private numbers formatted as telephone-subscriber strings 10
7.1.3 Email-style SIP URIs 11
7.2 Dial strings 12
7.3 Service identifiers 13
7.4 Device identifiers 13
8 Routing 14
8.1 General routing principles 14
8.2 Routing to the enterprise domain 15
8.3 Routing to the home server within the enterprise domain 15
8.4 Roaming considerations 16
9 Identification delivery and restriction 17
9.1 Identification delivery 17
9.2 Authenticity 17
9.3 Restriction 18
10 Summary of requirements and standardisation gaps 19
10.1 Requirements on NGNs 19
10.2 Requirements on enterprise networks 20
10.3 Standardisation gaps 20

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 12861 was prepared by Ecma International (as ECMA TR/96) and was adopted, under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

--`,,```,,,,````-`-,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

This Technical Report is one of a series of Ecma publications that explore IP-based enterprise communication involving Corporate telecommunication Networks (CNs) (also known as enterprise networks) and in particular Next Generation Corporate Networks (NGCN). The series particularly focuses on inter-domain communication, including communication between parts of the same enterprise, between enterprises and between enterprises and carriers. This particular Technical Report discusses issues related to user identities and routing and builds upon concepts introduced in ISO/IEC TR 12860.

This Technical Report 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 JTC 1, ITU-T, ETSI, IETF and other international and national standardization bodies. It represents a pragmatic and widely based consensus. In particular, Ecma acknowledges valuable input from experts in ETSI TISPAN.

© ISO/IEC 2009 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — Identification and routing

1 Scope

This Technical Report is one of a series of publications that provides an overview of IP-based enterprise communication involving Corporate telecommunication Networks (CNs) (also known as enterprise networks) and in particular Next Generation Corporate Networks (NGCN). The series particularly focuses on session level communication based on the Session Initiation Protocol (SIP) [4], with an emphasis on inter-domain communication. This includes communication between parts of the same enterprise (on dedicated infrastructures and/or hosted), between enterprises and between enterprises and public networks. Particular consideration is given to Next Generation Networks (NGN) as public networks and as providers of hosted enterprise capabilities. Key technical issues are investigated, current standardisation work and gaps in this area are identified, and a number of requirements are stated. Among other uses, this series of publications can act as a reference for other standardisation bodies working in this field, including ETSI TISPAN, 3GPP, IETF and ITU-T.

This particular Technical Report discusses session level user identification and routing. It uses terminology and concepts developed in ISO/IEC TR 12860. It identifies a number of requirements impacting NGN standardisation and concerning deployment of enterprise networks.

The scope of this Technical Report is limited to communications with a real-time element, including but not limited to voice, video, real-time text and instant messaging.

2 Normative references

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

[1] ISO/IEC 11571:1998, *Information technology — Telecommunications and information exchange between systems — Private Integrated Services Networks — Addressing*

[2] ECMA TR/86, *Corporate Telecommunication Networks — User Identification in a SIP/QSIG Environment*

[3] ISO/IEC TR 12860:2009, *Information technology — Telecommunications and information exchange between systems — Next Generation Corporate Networks (NGCN) — General*

[4] IETF RFC 3261, *SIP: Session Initiation Protocol*

[5] IETF RFC 3263, *Session Initiation Protocol (SIP): Locating SIP Servers*

[6] IETF RFC 3323, *A Privacy Mechanism for the Session Initiation Protocol (SIP)*

[7] IETF RFC 3325, *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

[8] IETF RFC 3327, *Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts*

[9] IETF RFC 3608, *Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration*

[10] IETF RFC 3761, *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*

[11] IETF RFC 3966, *The tel URI for Telephone Numbers*

[12] IETF RFC 4474, *Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)*

[13] IETF RFC 4916, *Connected Identity in the Session Initiation Protocol (SIP)*

[14] IETF RFC 4967, *Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier*

[15] IETF RFC 5031, *A Uniform Resource Name (URN) for Emergency and Other Well-Known Services*

[16] IETF draft-ietf-sip-gruu-15, *Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)*

NOTE At the time of publication of this Technical Report, the IETF had approved draft-ietf-sip-gruu-15 as a standards track RFC but had not published the RFC and had not allocated an RFC number. If the draft is no longer available, readers should look for the RFC with the same title.

[17] ITU-T Rec. E.164, *The international public telecommunication numbering plan*

[18] ITU-T Rec. H.350, *Directory services architecture for multimedia conferencing*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 External definitions

This Technical Report uses the following terms defined in ISO/IEC TR 12860:

- Domain
- Enterprise network
- Home server
- Next Generation Corporate Network (NGCN)
- Next Generation Network (NGN)
- Private network traffic
- Public network traffic
- Roaming
- Roaming hub

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

- SIP intermediary

This Technical Report uses the following terms defined in ISO/IEC 11571 [1]:

- Numbering plan
- Private numbering plan

3.2 Other definitions

3.2.1
Number-based SIP URI
A SIP or SIPS URI that contains a user=phone parameter, denoting the presence of a telephone number in telephone-subscriber format in the user part.

NOTE The telephone number can be an E.164 number or a private number.

3.2.2
Home number-based SIP URI
A number-based SIP URI for a user in which the domain part identifies the domain that provides home server (registrar and proxy) functionality for that user.

3.2.3
Transient number-based SIP URI
A number-based SIP URI for a user in which the domain part does not identify the domain that provides home server (registrar and proxy) functionality for that user.

NOTE Transient number-based SIP URIs are aliases for the home number-based SIP URI for the telephone number concerned. Typically they are used during the routing of a SIP request. The domain part might, for example, contain the domain of an NGN that supports the enterprise concerned, rather than the enterprise itself.

3.2.4
Telephone number
A numeric identifier that conforms to the numbering plan of a circuit-switched network.

4 Abbreviated terms

AoR	Address of Record
B2BUA	Back-to-Back UA
DNS	Domain Name System
GRUU	Globally Routable UA URI
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISDN	Integrated Services Digital Network
NGCN	Next Generation Corporate Network
NGN	Next Generation Network
PSTN	Public Switched Telephone Network
SIP	Session Initiation Protocol

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

UA	User Agent
URI	Universal Resource Identifier
URN	Universal Resource Name

5 Background

General concepts of NGCNs are discussed in [3]. In particular, that document describes use of the Session Initiation Protocol (SIP) [4] for session level communications within enterprise networks and with other domains. It focuses on enterprise networks based on enterprise infrastructure (NGCN), but also covers hosting on other networks, in particular NGNs, using the same infrastructure that supports public networks.

A major consideration for SIP-based communications is identification of the users involved and routing based on such identifiers. When one user initiates a communications session, that user needs to identify the user with which the session is to be established, and the network needs to establish the session to that user or to a nominated alternative. The second user often needs to receive the identity of the first user (the calling user) for various purposes. Likewise the first user often needs to receive the identity of the user to which the communication session is eventually established, which might not be the user to which establishment was originally requested.

SIP provides various forms of identifiers for users. These have already been discussed in ECMA TR/86 [2], primarily for the purpose of interworking with circuit-switched enterprise networks based on the QSIG signalling protocol. However, the topic needs to be examined from the broader perspective of NGCNs and their SIP-based operation with other domains.

6 Identified entities

Identifiers are needed for entities involved in communication within an enterprise network. For the purposes of this Technical Report, the most important identified entity is a user. A user's identifier is used for several purposes, including;

- indicating the user with which a communication is to be established;
- identifying a user already participating in a communication (e.g., the identity of the calling user or the identity of the user who has responded to a communication request);
- charging.

Although in many cases a user identifier, or an Address of Record (AoR), can identify a single human user, often it can indicate something else, e.g.:

- a role or function performed by a single human user (e.g., director of finance), this identifier remaining the same even though the occupant of the role might change;
- a group of human users (e.g., a department or function);
- a service or function performed by an automaton (e.g., voicemail or conferencing service).

A user identifier does not explicitly identify a particular device (e.g., terminal, server). In particular cases there may be a one-to-one relationship between device and user, but in many cases this will not be so:

- a user can have more than one device (e.g., a user with a PC, a fixed phone and a mobile phone or PDA; a service replicated on a number of servers);
- a device can support more than one user (e.g., two or more users sharing a telephone; a server supporting two or more services).

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Unless otherwise stated, the term identifier is used in this Technical Report is to mean a user identifier.

Identifiers are also required to identify entities other than users.

One example is for device identification. Device identifiers are generally used for purposes different from those for which user identifiers are used, e.g.:

- to ensure that a follow on communication reaches the same device as a previous communication;
- to identify a device for diagnostic purposes.

Another example is service identification, e.g., emergency services.

Yet another example is session or call identification, e.g., the IP Multimedia Subsystem (IMS) Charging Identifier (ICID).

Some uses of identifiers require the receiver of an identifier to obtain evidence of authenticity, i.e., to authenticate the identifier. Methods of authenticating identifiers are outside the scope of this Technical Report.

7 Types of identifier

7.1 SIP, SIPS and TEL URIs as user identifiers (AoRs)

For session level communications based on SIP, identifiers are in the form of Universal Resource Identifiers (URIs). For most purposes this means SIP (or SIPS) URIs of the form sip:user@example.com, where “example.com” is the domain part and identifies a domain in accordance with the domain name system (DNS) and “user” is the user part and identifies a particular user within that domain. Also parameters can be present. SIP and SIPS URI formats are defined in RFC 3261 [4]. For the purposes of this document, considerations for SIPS URIs (which denote certain security requirements for accessing the resource) are identical to those for SIP URIs, and therefore SIPS URIs are not explicitly mentioned in the remainder of this document.

When a SIP URI is used as an AoR, in present day deployments the user part is usually in the form of a telephone number, either an E.164 number (in accordance with the E.164 number plan [17]) or a private number (in accordance with a private numbering plan [1]), e.g.:

sip: +4321098765@example.com;user=phone

sip:1234;phone-context=+411234@example.com;user=phone

sip:1234;phone-context=switzerland.example.com@example.com;user=phone

The first example is a fully qualified E.164 number. The remaining examples represent private numbers.

In these examples the user part is formatted as what is defined as a telephone-subscriber string in RFC 3966 [11] for use in a TEL URI, and is in fact fully qualified (globally unique). This is denoted by the presence of the user=phone parameter. RFC 3261 recommends the inclusion of the user=phone parameter when the user part contains a telephone number in telephone-subscriber format. This Technical Report strongly endorses that recommendation.

REQUIREMENT E1: Enterprises shall include the user=phone parameter in SIP URIs in which the user part is a telephone-subscriber string.

This Technical Report refers to SIP URIs containing the user=phone parameter and a telephone-subscriber string as number-based SIP URIs.

© ISO/IEC 2009 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Another example found in practice is:

sip:1234@example.com;user=phone

In this example the user part is not formatted as a telephone-subscriber string and is not globally unique, but is unique within the context of the domain part. Although perhaps not intended by the authors of RFC 3261, it is found in practice and therefore should be handled if received. This format should not be used, particularly as it may cause problems interworking with NGN (for both private network traffic and public network traffic). This is because within NGN the presence of user=phone is often used as an indication that the user part can be treated as a telephone-subscriber string, which in this case it cannot because of the lack of a phone-context parameter.

REQUIREMENT E2: Enterprises shall avoid using URIs in which the user=phone parameter is present but the user part does not contain a telephone-subscriber string.

Yet another example found in practice is:

sip:1234@example.com

The user part in this example, whilst it is not marked as being a telephone number, very often is a telephone number. URIs formatted in this way should be treated as email style identifiers, since they rely on the domain part to make them globally unique.

The advantage of a number-based SIP URI is that the number can be used in legacy networks to reach the enterprise user or to identify the enterprise user as a caller. ECMA TR/86 [2] discusses this matter extensively for interworking between SIP and QSIG. The same advantage applies when an enterprise network interworks with other networks using SIP (public networks or other enterprise networks) if those networks might in turn interwork with legacy networks. Other forms of user part (referred to here as email style) have limitations when it comes to interworking. However, forms that reflect the name of the user have obvious attractions from a usability perspective, e.g.:

sip:john@example.com

Internally an enterprise network can use email-style SIP URIs (i.e., URIs that do not contain a telephone number), but may need to map to telephone number forms for inter-domain use or when interworking with legacy networks.

To be reachable directly from the public telephone network (PSTN/ISDN) a user must be identifiable by an E.164 number. Users not identifiable by an E.164 number are still reachable internally by means of a private number or other form of SIP URI, and can be reached indirectly from the public telephone network (e.g., via an attendant). Such users may also be directly reachable from other SIP networks where the caller is able to enter a SIP URI. In some countries the availability of E.164 numbers is such that it is impracticable or too costly to assign one per user.

Often within an enterprise all SIP URIs identifying users will have the same value in the domain part (i.e., example.com in the examples above). This allows identifiers to be portable within the enterprise (e.g., between different departments or between different geographic locations). Some enterprises will use sub-domains of their top level domain (e.g., domain1.example.com and domain2.example.com) in SIP URIs, or even different top level domains, particularly as a result of a merger or the desire to promote different brand names.

Where a user is identified by a telephone number, this can also be expressed by means of a TEL URI, RFC 3966 [11] containing the telephone number formatted as a telephone-subscriber string, e.g.:

tel: +4321098765

tel:1234;phone-context=+411234

tel:1234;phone-context=switzerland.example.com

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

However, for some purposes within a SIP environment SIP (or SIPS) URIs must be used, so a TEL URI can only be an alias for a SIP URI.

Although a TEL URI can be derived from a SIP URI that has the user=phone parameter, certain information is lost in the process, in particular the domain part and any parameters of the SIP URI other than user=phone (e.g., the gr parameter - see 7.4). Any attempt then to convert the resulting TEL URI back to a SIP URI will not necessarily result in the same domain part and may lack important parameters.

All SIP and TEL URIs are globally unique. This is achieved through the domain part of the SIP URI and/or (except where a fully qualified E.164 number is given) the context parameter of a telephone-subscriber string in a number-based SIP URI or a TEL URI.

Since SIP (or SIPS) and TEL URIs are fully qualified and hence globally unique, in principle any form can be applied to inter-domain working. However, there are some additional considerations.

There may be a desire not to disclose private numbering plans or other email-style identification schemes outside the enterprise network. Furthermore, other domains might be restricted in the forms they can handle, and in particular might only support E.164 numbers when they provide interworking with legacy networks. Therefore, even where non-E.164 forms of identifier are used within an enterprise, there might be a need to publish E.164 aliases for use outside the enterprise. Where a particular user is not assigned an E.164 number (because of shortage or cost), an alternative E.164 number (e.g., that of an attendant) might need to be published for reaching that user from outside the enterprise.

Figure 1 illustrates the relationships between different forms of SIP and TEL URIs.

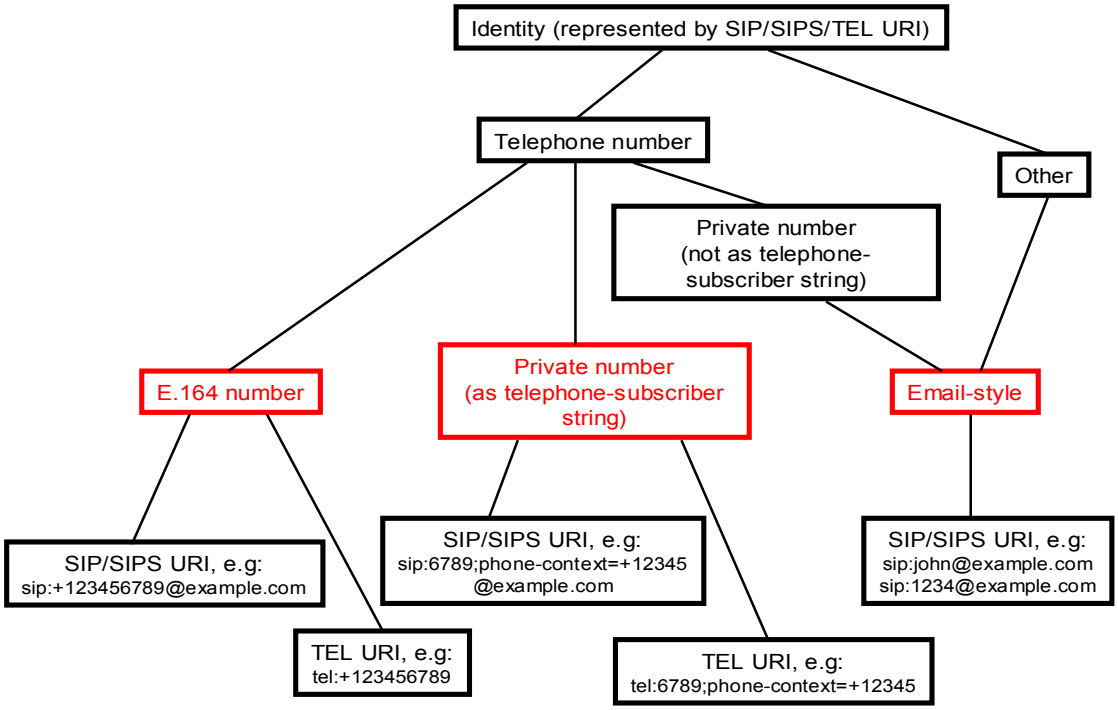

Figure 1 — Relationships between different forms of SIP and TEL URIs

Additional considerations apply to each of the three basic forms of identifier (shown in red in the Figure): E.164 numbers, private numbers formatted as telephone-subscriber strings and email-style identifiers. A given user may have multiple identifiers as aliases.

When part or all of an enterprise network is hosted, the hosting infrastructure will need to support all types of SIP and TEL URI discussed above. In particular, an NGN that hosts enterprise functions will need to support these different types, at least for private network traffic.

© ISO/IEC 2009 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

REQUIREMENT N1: An NGN or other public network hosting enterprise functions shall support the different types of user identifier described above, at least for private network traffic.

7.1.1 Use of E.164 numbers

When a user has a fully qualified E.164 number (international number) as identifier, it can be used universally, including within the PSTN. The E.164 number can always be used for establishing a communication to the user concerned and (subject to authentication) is always meaningful if delivered as the identification of a user involved in a communication. It can be stored in directories or in call detail records. However, as discussed earlier in 7.1, there may be some users who are not assigned E.164 numbers.

NOTE National and subscriber E.164 numbers are not fully qualified and can be represented in SIP and TEL URIs by inclusion of a phone-context parameter. Such numbers are not seen as meaningful for use within enterprise networks.

When an E.164 number is represented as a SIP URI, a domain part is included. In common with any other SIP URI, normally this will be the domain that provides home server (registrar and proxy) functionality for that identifier, in other words the home domain. That home domain's name must be used in the To URI of a SIP REGISTER request when registering a User Agent (UA) as a contact for an E.164 number, and inbound requests to an E.164 number must be routed to the home server within that home domain. Thus for a given E.164 number there must be a SIP URI that uses the home domain's name. We can call this the home number-based SIP URI for that E.164 number. For an E.164 number assigned by an appropriate authority to an enterprise (and assigned by that enterprise to a user of the enterprise network), normally the domain part of the home number-based SIP URI will be that of the enterprise, or a sub-domain thereof.

There is no clear definition of what the domain part of a SIP URI representing an E.164 number should contain. One possibility might be to use the domain that “owns” the E.164 number, but the concept of ownership is unclear. Does an enterprise domain “own” the E.164 numbers assigned to it? Does a public network “own” the E.164 numbers assigned to an enterprise? What if the enterprise obtains services associated with these numbers from multiple public networks or moves from one public network to another?

In practice, since a fully qualified E.164 number is globally unique anyway, in many circumstances values other than the home domain are placed in the domain part, e.g., the domain of a public network through which a communication needs to be routed to reach the domain to which the number is assigned, or a domain through which a communication has been routed. The domain denoted by the domain part should at least be able to route the request onwards towards the destination. Therefore if a SIP URI containing an E.164 number is the target of a SIP request, the request can be routed to the domain given in the domain part and that domain will be able to route the request onwards, in this case to the enterprise domain concerned. Compared with the home number-based SIP URI for a given telephone number, SIP URI's for the same E.164 number but with different domain parts are merely aliases for that home number-based SIP URI. In practice, such aliases are often used, although perhaps not the original intent of RFC 3261. In this Technical Report these aliases are called transient number-based SIP URIs, because often their use is of a transient nature during routing.

The choice of domain part for a home number-based SIP URI for an E.164 number merits consideration. For a home server in a dedicated NGCN (supported by the enterprise's own infrastructure) it is fairly clear that the home number-based SIP URI should use the enterprise's own domain name (or a sub-domain thereof). If the NGCN uses services of an NGN for external communications, a potential alternative might be to use the NGN's domain name, but this would lead to a number of problems, e.g.:

- Placing the NGN's domain name in the Request-URI of a SIP REGISTER request (e.g., REGISTER sip:ngn.com) would, according to normal SIP routing rules, cause the request to be routed to the NGN, rather than to the home server in the NGCN. Special measures would need to be used in the NGCN to prevent that.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2009 – All rights reserved
Not for Resale

- A request originated in the NGCN to another NGCN user identified by a SIP URI using the NGN's domain name would, according to normal SIP routing rules, cause the request to be routed to the NGN, which presumably would then route it back to the home server in the NGCN. To prevent this undesirable behaviour, special measures would need to be taken within the NGCN.

- The NGCN operator might require the user to be reachable from more than one NGN, in which case any benefits of basing the home number-based SIP URI on the domain name of one of the NGNs would not apply to the other NGNs.

- Identifiers would need to change if the NGCN operator were to change the NGN operator from which services are obtained, i.e., identifiers would not be portable.

- This would be inconsistent with other identifiers (see 7.1.3), which are forced to use the domain name of the enterprise.

REQUIREMENT N2: An NGN or other public network providing services based on SIP to an NGCN shall allow use of the enterprise domain name in the domain part of SIP URIs containing E.164 numbers.

When hosting is used, it might be possible to use the hosting organisation's domain name (e.g., that of a hosting NGN or NGCN) as the domain part of home number-based SIP URIs. This too has some significant drawbacks, e.g.:

- If an enterprise network is a mixture of dedicated NGCN and hosted domains, users in hosted domains would have identifiers based on the hosting organisation's domain name and users in NGCN domains would have identifiers based on the enterprise's domain name. This would prevent identifier portability in support of users who change location or for other reasons need to change domain within the enterprise network.

- If different domains of an enterprise network are supported by different hosting networks, again identifier portability would be lost.

- Identifiers would need to change if the enterprise changes the organisation from which it obtains hosting services.

- This would be inconsistent with other identifiers (see 7.1.3), which are forced to use the domain name of the enterprise.

REQUIREMENT N3: An NGN or other network that hosts enterprise users shall allow use of the enterprise domain name in the domain part of SIP URIs containing E.164 numbers.

Notwithstanding the need to have a home number-based SIP URI, normally based on the enterprise's domain name, practices within public networks tend to modify the domain part during routing and during the delivery of calling or connected user identification. In other words, aliases in the form of transient number-based SIP URIs are used. This is discussed further in the context of routing (see Clause 8) and identification delivery (see Clause 9). The use of transient number-based SIP URIs has a number of consequences:

1) There is not a single unique SIP URI that represents a given E.164 number.

2) The rules in RFC 3261 for comparing SIP URIs do not consider SIP URIs with different domain parts as being equivalent, although in practice these URIs are equivalent.

3) An endpoint that has stored in its address book an E.164 number represented as a SIP URI will be unable to match received SIP URIs against that stored SIP URI according to normal RFC 3261 comparison rules unless the two URIs happen to have the same domain part. This might interfere with functionality at the endpoint, e.g., the ability to display a name and other details based on address book look-up, or the ability to check a caller's identity against a black list or white list.

© ISO/IEC 2009 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4) The domain part of a SIP URI containing an E.164 number, when received as the source of a SIP request, does not necessarily represent the domain in which that SIP request originated and thus the domain of the remote user in the communication.

Therefore when an E.164 number is represented as a SIP URI, it is only the user part that is meaningful to other users as a means of identifying the user (although the domain part of a SIP URI will help in routing a request back to the identified user and may be of use in determining where a request has come from). The number could equally well be represented as a TEL URI, but TEL URIs are not suitable for all purposes:

1) They are unsuitable for including in a Request-URI and for routing in accordance with RFC 263 [5].

2) They are unsuitable for signing in accordance with RFC 4474 [12] (see also 9.2).

3) They are unsuitable for use as contact URIs to identify particular endpoints.

Because of potential modification of the domain part of a SIP URI by SIP intermediaries, the domain part must be considered unreliable as a means of determining the enterprise to which the user of an E.164 number belongs. This is unfortunate, because a user receiving a SIP URI as the identity of a communication partner might not recognise the E.164 number but might recognise the domain.

With these considerations in mind, it is impossible to avoid the use of SIP URIs representing E.164 numbers, but because a given E.164 number does not have a unique domain part such URIs have to be treated with care. For some purposes they can be treated as TEL URIs and the domain part ignored, but there are occasions when the domain part can be useful. For example, when displaying the identity of a communication partner to a user, the domain part may on occasions be of value.

It is recommended that transient number-based SIP URIs should be avoided or at least used with care in enterprise networks.

REQUIREMENT E3: An enterprise shall avoid the use of transient number-based SIP URIs as aliases for home number-based SIP URIs identifying enterprise users.

REQUIREMENT N4: An NGN that hosts enterprise network capabilities shall avoid the use of transient number-based SIP URIs as aliases for home number-based SIP URIs identifying enterprise users.

When publishing identifiers for users, e.g., in directories, on business cards, on web pages, care needs to be taken. By publishing only the telephone number or the home number-based SIP URI based on the enterprise's domain name, problems can be avoided.

REQUIREMENT E4: When publishing user identifiers based on E.164 numbers, enterprises should publish only the E.164 number (alone or as a TEL URI) and/or the home number-based SIP URI.

7.1.2 Private numbers formatted as telephone-subscriber strings

Even though such private numbers are fully qualified, in general they cannot be used outside the enterprise concerned. Public NGNs may support them within the context of private network traffic (e.g., between hosted enterprise users and/or between NGCN sites), but are not expected to support them for public network traffic. They are not supported in PSTN. Generally they are supported within non-SIP domains of the enterprise network concerned (e.g., circuit-switched). Compared with E.164 numbers, they have the benefit of brevity (insofar as users need remember only the number if the phone-context is automatically appended) and any user in an enterprise network can be assigned a private number, even though there may be a shortage of E.164 numbers.

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Examples of private numbers formatted as telephone-subscriber strings are:

sip:1234;phone-context=+411234@example.com;user=phone

sip:1234;phone-context=switzerland.example.com@example.com;user=phone

The first of these examples says that the number 1234 is to be interpreted within the context of the entity to which E.164 numbers beginning with 411234 are assigned. The second of these examples says that the number 1234 is to be interpreted within the context of the domain switzerland.example.com. The combination of the number and the contents of the phone-context parameter is globally unique.

NOTE Where a numeric phone-context is used, appending the phone number to the phone-context does not necessarily result in a valid international E.164 number. For example:

sip:5555;phone-context=+441123456789@example.com;user=phone

is not necessarily the same as:

sip:+4411234567895555@example.com;user=phone

Private numbers here are considered the equivalent of Private Numbering Plan (PNP) Numbers as defined in ISO/IEC 11571 [1] and therefore belong to a PNP, also defined in ISO/IEC 11571.

The considerations for the domain part of SIP URIs carrying E.164 numbers apply also to the domain part of SIP URIs carrying private numbers formatted as telephone-subscriber strings. This includes the concepts of home and transient number-based SIP URI. Essentially the domain part is used only for routing purposes, given the existence of the phone-context parameter in the user part. Therefore it is possible to put any value in there (e.g., the domain of an NGN providing services to an NGCN or hosting the enterprise network), provided the identified domain can route a request onwards to the correct destination. However, the concept of a home number-based SIP URI and the advantages of basing this on the domain name of the enterprise apply.

Sometimes a public network such as an NGN will support private numbers for an enterprise (e.g., when hosting enterprise users or when providing transit connectivity between domains of an enterprise). It is important that enterprise domain name be supported in SIP URIs containing private numbers.

REQUIREMENT N5: An NGN or other public network providing services based on SIP to an NGCN and supporting private numbers shall allow use of the enterprise domain name in the domain part of SIP URIs containing private numbers.

REQUIREMENT N6: An NGN or other network that hosts enterprise users shall allow use of the enterprise domain name in the domain part of SIP URIs containing private numbers.

As for E.164 numbers, only telephone numbers (together with phone-context) or home number-based SIP URIs should be published for users, e.g., in directories, on business cards. However, because private numbers may not be usable outside the enterprise, particularly when legacy public networks are involved, identifiers based on E.164 numbers will generally be more appropriate for publication outside the enterprise.

REQUIREMENT E5: When publishing user identifiers based on private numbers, enterprises should publish only the private number (alone or as a TEL URI) or the home number-based SIP URI.

7.1.3 Email-style SIP URIs

Email-style SIP URIs are usable only within the SIP environment. Therefore even if a user has an email-style SIP URI, the user will also require an alias E.164 number and/or private number to be able to be reached directly from PSTN or from private circuit-switched networks.

© ISO/IEC 2009 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

For the purposes of this document, any SIP URI that does not contain a telephone number formatted as a telephone-subscriber string and is not a dial string (see 7.2) is considered an email-style identifier, even though it might comprise only digits in the user part and might even contain a user=phone parameter. Examples include:

sip:john@example.com

sip:1234@example.com

The latter example may in practice contain a telephone number, but it is not formatted as a telephone-subscriber string and therefore is considered an email style identifier.

In email-style SIP URIs there is no context within the user part, so the domain part is essential to provide the context. In contrast to number-based SIP URIs, aliases for the domain part are not possible.

If email-style identifiers are to be used, generally an enterprise will wish to use its own domain name in the domain part. Using the domain name of a hosting organisation or a public network that provides trunking services can lead to conflicts.

Obviously when publishing an email-style identifier, it needs to be published complete with domain part. Identifier portability is possible throughout the domain concerned.

7.2 Dial strings

To establish communication to a user, the caller typically “dials” a string of digits or other characters (or invokes such a string en bloc from an address book or similar). Although a dial string can simply be an identifier for the called user, often it has a different form, e.g.:

- an identifier together with prefix digits to indicate the numbering plan (e.g., “0” for E.164) or the type of number (e.g., “00” for international, “0” for national, no prefix for local number) or both;
- an identifier together with additional information (e.g., for public network selection or accounting purposes);
- a code specific to a particular network context (e.g., to denote an emergency call or a call to an attendant);
- a code to invoke a supplementary service;
- an abbreviated dialling code.

Interpretation of a dial string will depend on local context.

A dial string typically has to undergo translation to obtain the identifier of the target destination. This translation can be carried out in the caller's UA (in which case it does not appear in signalling) or by a SIP intermediary in the caller's domain. In the latter case the dial string needs to be conveyed within a SIP URI using the user=dialstring parameter as defined in RFC 4967 [14], together with a context parameter in the user part, e.g.:

sip:00123456789;phone-context=switzerland.example.com@example.com;user=dialstring

There is no defined way to convey a dial string in a TEL URI.

Dial strings as targets of SIP requests will normally be absorbed at or before the home server of the user making the request and should not appear downstream of that point. In particular, they should not occur at a trunking interface between an NGCN and an NGN.

REQUIREMENT N7: An NGCN or NGN shall not pass dial strings across the NGCN-NGN interface.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.3 Service identifiers

A service in an enterprise network or outside can be considered as a user and can be identified by any of the identifiers discussed above for users.

However, sometimes a service has a broader scope geographically and/or administratively and may be provided by a number of separate entities, choice being dependent on context. These entities may be geographically dispersed and/or accessible from multiple domains. Therefore a SIP URI, which requires a domain part, is not ideally suited. Also a TEL URI is not ideally suited, because mechanisms for routing based on a TEL URI are geared towards resolving the TEL URI to a particular SIP URI without necessarily taking context into account (e.g., geographic location of the caller). In principle SIP URIs and TEL URIs can be used, but they are not ideal.

An alternative is to use a service Uniform Resource Name (URN), as defined in RFC 5031 [15]. This establishes a registry for service URNs and includes initial registrations for emergency services. Other values can be registered for other services. A caller can establish a communication using a service URN as a target, and during routing this is resolved to an address of an appropriate service entity.

7.4 Device identifiers

A SIP URI that identifies a user is known as an Address of Record (AoR). SIP URIs can also identify particular devices or UAs. One important case in SIP where it is necessary to identify a device, rather than a user, is for communication within the context of a dialog. A dialog is established between two UAs as a result of a successful INVITE request, for example, and any further messages within the context of that dialog need to be sent to the peer UA by means of that UA's URI, known as its contact URI. Targeting a mid-dialog request at the user's AoR would not necessarily reach the correct UA.

Contact URIs are SIP (or SIPS) URIs, and it is not necessarily possible to distinguish a contact URI from an AoR by inspection. However, often the domain part of a contact URI will identify a particular sub-domain of the enterprise where the device is to be found or even the device itself.

A UA can assign its own contact URI, provided it is globally unique. One way is to use the device's host name in the domain part and something of local significance (e.g., to identify the particular user if the device serves multiple users) in the user part. This works well for some types of UA (e.g., gateways, media servers, etc.), but does not work for devices like fixed or mobile phones that have dynamically assigned IP addresses and do not register their host name to IP address mapping in the DNS. Placing the IP address in the domain part, whilst allowed, does not work when the device is behind a Network Address Translation (NAT) device, since the IP address is unlikely to be globally unique and is not globally reachable. In such circumstances it works only for communications within the same IP addressing domain.

It is still common practice to use locally-significant contact URIs (e.g., using an IP address in the domain part), with B2BUAs performing mapping as domain boundaries are crossed. This works when the necessary B2BUAs are on the path (as is the case with requests and responses within the context of an existing dialog). However, it can lead to problems when a contact URI is used as the target of a request outside the context of an existing dialog, because the path taken may not be able to provide the appropriate translation.

The solution to this is to use a Globally Routable UA URI (GRUU) [16], which is a URI assigned by the home server to the UA (at registration time). It has the home server's domain name in the domain part, and the user part contains sufficient information to route requests to the correct UA. A GRUU can be formed just by adding a gr= parameter to the user's AoR, which is fine when anonymity is not required. When anonymity is required the user part will contain an unrecognisable value, which means it must be treated like an email-style URI. Examples of GRUUs are as follows:

sip:john@example.com;gr=kjh29x97us97d

sip:+123456789@example.com;user=phone;gr=kjh29x97us97d

sip:asd887f9dfkk76690@example.com;gr

© ISO/IEC 2009 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

When part or all of an enterprise network is hosted, the hosting infrastructure will need to support all types of SIP URI discussed above as device identifiers, including the different forms of GRUU. In particular, an NGN that hosts enterprise functions will need to support these different types of device identifier, at least for private network traffic.

REQUIREMENT N8: An NGN or other public network hosting enterprise functions shall support the different types of device identifier described above, including GRUUs, at least for private network traffic.

8 Routing

8.1 General routing principles

The principle of routing in SIP is that a SIP request targeted at a user identified by a SIP (or SIPS) URI is first routed (directly or indirectly) on the basis of the domain part to a SIP intermediary responsible for the DNS domain in that SIP URI. This intermediary then uses its location service to look up one or more registered contacts (SIP UAs) representing that user. The request is then forwarded to one or more of those UAs.

The calling UA can be pre-configured with an “outbound proxy” address to which all requests are sent, and that SIP intermediary will route onwards towards the home server of the target user. This is a very common situation, and therefore the discussion below assumes the presence of an outbound proxy. Where there is no outbound proxy, the calling UA takes on the routing role normally carried out by the outbound proxy.

Sometimes further SIP intermediaries will be involved en route to the home server. Routing from the outbound proxy to the home server of the target user can be considered in two stages:

1) routing to the target user's domain;

2) routing to the home server within the target user's domain.

Within the enterprise network (including hosted domains) it should be possible to base routing of a SIP request on any of the SIP URIs identifying the target, e.g., based on E.164 number, based on private number, email style, and also including device identifiers such as GRUUs.. The same applies within public networks when the target is within an enterprise network, except that private number formats need not apply.

REQUIREMENT E6: Within an enterprise network (including any hosted domains) it must be possible to route SIP requests in which the target is a SIP URI based on an E.164 number (home and transient forms), a SIP URI based on a private number (home and transient forms) or an email style SIP URI, including device identifiers such as GRUUs.

REQUIREMENT N9: An NGN that hosts enterprise network capabilities shall be able to route SIP requests in which the target is a SIP URI based on an E.164 number (home and transient forms), a SIP URI based on a private number (home and transient forms) or an email style SIP URI, including device identifiers such as GRUUs.

REQUIREMENT N10: Within a public network it must be possible to route SIP requests in which the target is a SIP URI identifying an enterprise user, the SIP URI being either based on an E.164 number (home and transient forms) or email style, including device identifiers such as GRUUs.

If a request is targeted at a TEL URI, the TEL URI must first be converted to a SIP or SIPS URI. This can also be achieved by DNS look-up in accordance with ENUM [10]. If a request is targeted at a service URN, that must first be converted to a SIP or SIPS URI. Means to achieve this are outside the scope of this Technical Report. Special considerations for calls to emergency services will be discussed in a further document in this series. If the target of a request is a dial string, this must first be converted to a SIP or SIPS URI (directly or via a TEL URI or service URN) in accordance with the local dial plan.

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

NGNs that host enterprise functionality will have delegated domain proxy functionality for the enterprise domain, so that they are able to look at the user part of a request to the enterprise domain and commence the second stage of routing, either to an appropriate NGCN domain or to a hosted domain. In the case of request from the public network, this will be after the break-in point, i.e., it applies only to private network traffic.

8.2 Routing to the enterprise domain

This is achieved by routing based only on the domain part of the target SIP URI. RFC 3263 [5] specifies a series of DNS look-ups to identify the transport protocol to be used, an appropriate SIP server and a port on that server.

In simple cases this procedure will result in direct routing from the outbound proxy to the enterprise domain. However, there are situations where routing is indirect.

One example is where the target URI submitted by the calling UA is a transient number-based SIP URI, having a domain part that is not that of the enterprise. In this case routing will be via that other domain, which will then repeat RFC 3263 procedures for routing onwards towards the enterprise domain. This situation might arise where the calling user has stored such a URI in his/her address book, having received a previous communication via the domain concerned that provided that alias as the caller's identifier.

A second example is where the target URI submitted by the calling UA is the home number-based SIP URI for the target user (i.e., the domain part indicates the enterprise domain) but DNS look-up reveals that the enterprise domain can be reached only via an intermediate domain. This might be the domain of an NGN serving the enterprise domain, or some other domain through which the enterprise domain wishes to be reached.

A third example is where the target URI submitted by the calling UA is a TEL URI containing an E.164 number. Initial look-up of the E.164 number (e.g., using ENUM) reveals a domain by which that number can be reached, rather than the enterprise domain. This might be the domain of an NGN serving the enterprise domain, or some other domain through which the enterprise domain wishes to be reached.

Within an NGN environment, routing on a SIP URI representing an E.164 number is often achieved by ignoring the domain part and performing a look-up on the E.164 number alone (e.g., using ENUM) to derive a SIP URI. The domain part of that replacement SIP URI can be that of the NGN serving the enterprise, e.g., an NGN via which an NGCN can be reached. Thus even if a request starts off with the home number-based SIP URI as target, this can be changed en route to a transient number-based SIP URI, which would eventually need to be translated back to the home number-based SIP URI.

Such behaviour is problematic, in that important information from parameters of the original SIP URI can be lost, e.g., a gr= parameter in a GRUU. This is one of the reasons for recommending that the use of transient number-based SIP URIs be avoided (see 7.1.1). Also it clearly will not work for email-style SIP URIs. Further standardisation work is required to find a satisfactory way of routing email-style URIs, GRUUs, etc. within an NGN environment. This is a particular issue when it is necessary to route via the NGN serving an NGCN in order to reach an NGCN, as is the case with the subscription-based business trunking.

NGNs that host enterprise functionality and therefore handle private network traffic as well as public network traffic will often devote separate resources to the two types of traffic. Therefore routing can be different depending on traffic type.

8.3 Routing to the home server within the enterprise domain

In the simple case the domain part of the target SIP URI is sufficient to identify the home server (or cluster of servers for load-sharing or resilience). In other words, all users having that domain part in their SIP URI are supported by the same home server or cluster. In this case any requests arriving in the domain (or submitted by users within the domain) should arrive directly at the correct home server.

Where different identifiers with the same domain part are served by different home servers, perhaps administratively and/or geographically distributed, each home server (or cluster) can be considered to be in a

© ISO/IEC 2009 All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

separate sub-domain of the enterprise domain. These can be different sub-domains of an NGCN, sub-domains hosted on different hosting infrastructures (e.g., different NGNs) or a mixture.

A request arriving at SIP intermediary in the domain (arriving directly from an enterprise user or arriving from outside the domain) may need to be routed onwards towards the appropriate home server. This involves performing a look-up based on the user part of the SIP URI. Particularly in the case of identifiers based on telephone numbers, there may be some structure that allows a look-up to be based on just a portion of the user part (e.g., the leading digits), but with email-style SIP URIs a look-up based on the full user part will be necessary. One vehicle for this could be a directory look-up, e.g., based on H.350 [18]. The result could either be a different domain name (e.g., site1.example.com) that can be further resolved to get to an appropriate home server, or it could give the required IP address directly.

The result of the initial look-up can be placed in a SIP Route header field, so that the initial look-up does not need to be repeated at downstream SIP intermediaries prior to reaching the target home server. This has the advantage that it does not overwrite the existing target (e.g., the AoR of the called user). If onwards routing is achieved by redirection, the Route header field can be placed in the headers part of the SIP URI in the Contact header field of the 3xx response, thereby causing the resulting recursed request to contain the Route header field.

NOTE There are issues with the use of the Route header field in NGN, because its use is not properly defined for IMS. It is not clear how this will be resolved.

8.4 Roaming considerations

When an enterprise user roams into another domain, its UA still needs to register with its home server, and inbound and outbound SIP requests will still need to be routed via the home server.

The REGISTER request will be targeted at the domain name of the home server, e.g.:

REGISTER sip:server.enterprise.com

The request is submitted to a proxy in the visited domain. In principle, that proxy can employ normal DNS look-up of the domain to find the address of the home server. In practice, account has to be taken of roaming agreements, and one possibility is that a REGISTER request will need to be routed via a domain acting as a routing hub.

This has particular impact on NGN, since a common roaming situation that needs to be supported as soon as possible is an NGCN user roaming into an NGN. If the NGCN has a roaming agreement with certain NGNs (including possibly the same NGN that is used for trunking), then roaming to any other NGN or mobile network will depend on roaming agreements between the NGNs with which the NGCN has a roaming agreement and those other networks. An NGN with which the NGCN has a roaming agreement may need to act as a roaming hub. Therefore visited NGNs may need to find a way for routing a REGISTER request to a suitable NGN acting as roaming hub, and that latter NGN will need to route the request onward into the NGCN. Further standardisation work is required to find a satisfactory way of routing REGISTER requests through NGNs towards an NGCN in support of roaming NGCN users.

Having successfully registered, inbound and outbound requests can be handled by existing SIP mechanisms. The Path header field [8] in a REGISTER request will tell the home server how to route inbound requests to the roaming UA. The Service-Route header field [9] in a REGISTER response will tell the roaming UA how to route outbound requests to the home server.

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

9 Identification delivery and restriction

9.1 Identification delivery

The source of a SIP request is generally of importance to the recipient of that request. In particular, the source of an INVITE or MESSAGE request generally needs to be delivered to the called user or his/her terminal for a variety of reasons, e.g.:

- to allow the user or an application to determine whether to accept the communication;
- to allow the user to greet the caller appropriately;
- to allow the user to initiate a return communication back to the caller; and/or
- to allow an application to present related information (e.g., account details) to the user.

Similarly, the originator of a call also needs to receive the identity of the party that has answered the call (connected identity), and owing to call forwarding this can be different from the user that was originally targeted (the user "dialled").

Other instances of identification delivery include the original and intermediate target identities (for requests that have been retargeted).

A SIP, SIPS or TEL URI can be used for this purpose.

When delivering an E.164 number as a SIP URI in a request, the meaning of the domain part is merely that a request routed back to that domain should be able to reach the entity that originated the first request. It says nothing about "ownership" of the E.164 number. It probably means that the request originated at or traversed the indicated domain, but it is certainly not a definite indication that the request originated at the domain. If the recipient has knowledge of that domain, the user may be able to draw conclusions. For example, if the domain is known to be a public network operator, then the true originator of the request may well be in some other domain beyond the public network. On the other hand, if the domain is a known and trusted enterprise, it might be reasonable to assume that the request originated in that domain and that the E.164 number represents a user in that enterprise. This can be helpful if the E.164 number is not recognised, but basically the domain part should be used with care. If an E.164 number is delivered as a TEL URI there is no domain part.

Obviously for email style SIP URIs, the indicated domain will be meaningful. For private numbers in telephone-subscriber format, the phone-context parameter will be meaningful.

As stated in 7.1, there may be a desire not to disclose private numbering plans or other internal identification schemes outside the enterprise network. Furthermore, it may not be known whether other domains provide interworking with legacy networks, which might only be able to accept an E.164 number as caller or connected user identification. Therefore, even where non-E.164 forms of identity are used for private network traffic, these might need to be converted to E.164 numbers for public network traffic. This needs to be done at or before the point of break-out.

9.2 Authenticity

For some purposes it is important to the recipient of a delivered identity that the identity is asserted to be correct by a reliable authority. The URI in the From header field can easily be forged, and therefore that alone should not be taken as reliable. Within a closed environment the P-Asserted-Identity header field defined in RFC 3325 [7] can fulfill this requirement by asserting an identity that has been authenticated by a reliable authority. The SIP intermediary responsible for the domain of the caller inserts this header field, having authenticated the caller by other means (digest authentication, TLS mutual authentication). The P-Asserted-Identity header field can also be forged, so it should be relied upon only when received by secure means from an entity within the same trust domain. If received from outside the trust domain (or over an unsecured transport) the header field should be discarded and not passed on.

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

For calls or requests passing through several SIP intermediaries, particular between domains, there has to be reliance on transitive trust in order to use the P-Asserted-Identity URI. If a trust domain boundary is crossed, P-Asserted-Identity cannot be used. For these reasons RFC 4474 [12] defines the Identity header field (and associated Identity-Info header field), whereby the SIP intermediary at the originating domain can sign an assertion that the URI in the From header field is correct, having authenticated the UA by other means. This cryptographically signed assertion can be passed to the destination, where it can be verified, subject to the signer's certificate chain being acceptable. This avoids the transitive trust and trust domain boundary problems.

NOTE This still depends on trust, however. The verifier can trust the assertion only if it trusts the signer's certificate. Also there is still an issue of transitive trust if the signer's own certificate is not directly trusted by the verifier but the certification authority is trusted. This is particular so if there are intermediaries in the certification chain.

Although the use of P-Asserted-Identity will often be sufficient within a single domain enterprise network or perhaps even within a multi-domain enterprise network, for inter-domain communication the Identity header field might be required.

RFC 4916 [13] specifies the use of the Identity header field for connected identity.

The Identity header field can only be used to sign a SIP URI, because a TEL URI does not contain a domain. A signed SIP URI containing an E.164 number means that the request either originated at or transited the domain concerned, and does not denote “ownership” of the E.164 number. Although signed, the URI still has to be used with care.

In particular, there are issues with an E.164 number received from a PSTN gateway, since the PSTN gateway has no means to authenticate what it receives from the PSTN. Even if the PSTN itself can be relied on, there could be another network beyond the PSTN that delivers false information to the PSTN. For this reason there have been suggestions in the IETF that SIP URIs based on PSTN numbers obtained from PSTN should be marked accordingly when asserted in SIP.

9.3 Restriction

Sometimes delivery of the caller's identity needs to be suppressed, e.g., for privacy reasons. This can be achieved by placing an anonymous or alternative value (e.g., that of an attendant) in the From header field and omitting the P-Asserted-Identity header field. However, sometimes the P-Asserted-Identity header field is used within a domain (between SIP intermediaries) for other purposes (e.g., accounting) and should not be suppressed across such interfaces. The Privacy header field defined in RFC 3323 [6] and augmented in RFC 3325 [7] indicates that the P-Asserted-Identity header field is not to be passed to an untrusted entity (e.g., an untrusted UA or an entity in another domain that is not trusted) or across an insecure transport. Restriction is likely to be more important for inter-domain working, where disclosure of an identity might be acceptable within an enterprise network but not outside the enterprise network.

Within an enterprise network comprising multiple (sub-)domains, the passing of restricted identities will depend on the trust relationship between domains. For example, between an NGCN and an NGN-hosted domain, it depends on the trust relationship between the NGCN operator and the NGN operator. Often it will be desirable to have trust between such domains.

Outside the enterprise, the passing of restricted identities will depend on the trust relationship between the enterprise and any other domain, e.g., a public network operator such as an NGN.

Restriction requires an anonymous value in the From header field, even inside a domain where the identity is carried within the P-Asserted-Identity header field. This can be a completely anonymous value or one that discloses the domain but not the user, e.g.:

sip:anonymous@anonymous.invalid

sip:anonymous@example.com

In the latter case, there can still be an Identity header field signing the value. This would then denote that the request has originated at an authenticated user within the domain example.com, without disclosing the identity of the user.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

10 Summary of requirements and standardisation gaps

This Technical Report analyses the types of identifier used in SIP within enterprise networks. Examples of number-based SIP URIs are as follows:

sip: +4321098765@example.com;user=phone

sip:1234;phone-context=+411234@example.com;user=phone

sip:1234;phone-context=switzerland.example.com@example.com;user=phone

Corresponding examples of TEL URIs are as follows:

tel: +4321098765

tel:1234;phone-context=+411234

tel:1234;phone-context=switzerland.example.com

Examples of email-style SIP URIs are as follows:

sip:john@example.com

sip:1234@example.com

This Technical Report also analyses how routing can be based on these identifiers and how the identifier of a party involved in a communication can be delivered to other parties.

10.1 Requirements on NGNs

This document places the following requirements on NGNs that need to be taken into account during ongoing standardisation work related to NGN.

REQUIREMENT N1: An NGN or other public network hosting enterprise functions shall support the different types of user identifier described above, at least for private network traffic.

REQUIREMENT N2: An NGN or other public network providing services based on SIP to an NGCN shall allow use of the enterprise domain name in the domain part of SIP URIs containing E.164 numbers.

REQUIREMENT N3: An NGN or other network that hosts enterprise users shall allow use of the enterprise domain name in the domain part of SIP URIs containing E.164 numbers.

REQUIREMENT N4: An NGN that hosts enterprise network capabilities shall avoid the use of transient number-based SIP URIs as aliases for home number-based SIP URIs identifying enterprise users.

REQUIREMENT N5: An NGN or other public network providing services based on SIP to an NGCN and supporting private numbers shall allow use of the enterprise domain name in the domain part of SIP URIs containing private numbers.

REQUIREMENT N6: An NGN or other network that hosts enterprise users shall allow use of the enterprise domain name in the domain part of SIP URIs containing private numbers.

REQUIREMENT N7: An NGCN or NGN shall not pass dial strings across the NGCN-NGN interface.

© ISO/IEC 2009 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

REQUIREMENT N8: An NGN or other public network hosting enterprise functions shall support the different types of device identifier described above, including GRUUs, at least for private network traffic.

REQUIREMENT N9: An NGN that hosts enterprise network capabilities shall be able to route SIP requests in which the target is a SIP URI based on an E.164 number (home and transient forms), a SIP URI based on a private number (home and transient forms) or an email style SIP URI, including device identifiers such as GRUUs.

REQUIREMENT N10: Within a public network it must be possible to route SIP requests in which the target is a SIP URI identifying an enterprise user, the SIP URI being either based on an E.164 number (home and transient forms) or email style, including device identifiers such as GRUUs.

10.2 Requirements on enterprise networks

This document places the following requirements on the use of identifiers within enterprise networks in general.

REQUIREMENT E1: Enterprises shall include the user=phone parameter in SIP URIs in which the user part is a telephone-subscriber string.

REQUIREMENT E2: Enterprises shall avoid using URIs in which the user=phone parameter is present but the user part does not contain a telephone-subscriber string.

REQUIREMENT E3: An enterprise shall avoid the use of transient number-based SIP URIs as aliases for home number-based SIP URIs identifying enterprise users.

REQUIREMENT E4: When publishing user identifiers based on E.164 numbers, enterprises should publish only the E.164 number (alone or as a TEL URI) and/or the home number-based SIP URI.

REQUIREMENT E5: When publishing user identifiers based on private numbers, enterprises should publish only the private number (alone or as a TEL URI) or the home number-based SIP URI.

REQUIREMENT E6: Within an enterprise network it must be possible to route SIP requests in which the target is a SIP URI based on an E.164 number (home and transient forms), a SIP URI based on a private number (home and transient forms) or an email style SIP URI, including device identifiers such as GRUUs.

10.3 Standardisation gaps

The following standardisation gaps have been identified during the analysis:

- Further standardisation work is required to find a satisfactory way of routing email-style URIs, GRUUs, etc. within an NGN environment. This is a particular issue when it is necessary to route via the NGN serving an NGCN in order to reach an NGCN, as is the case with the subscription-based business trunking.

- Further standardisation work is required to find a satisfactory way of routing REGISTER requests through NGNs towards an NGCN in support of roaming NGCN users.

--`,,```,,,,````-`-,,`,,`,`,,`---

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.110

Prix basé sur 20 pages

© ISO/IEC 2009 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale