SIPPING Working Group	J. van Elburg	
Internet-Draft	Ericsson Telecommunicatie B.V.	
Intended status: Informational	K. Drage	
Expires: August 23, 2009	Alcatel-Lucent	
	February 19, 2009	

TOC

The Session Initiation Protocol (SIP) P-Private-Network-Indication Private-Header (P-Header)
draft-vanelburg-sipping-private-network-indication-03.txt

Status of this Memo

Copyright Notice

Abstract

This document describes why a private network indication is needed. A private network indication allows other nodes in a network to treat private network traffic to a different set of rules then public network

traffic. The indication also distinguishes one private network from another private network.

Table of Contents

1. Introduction

TOC

1.1. General

TOC

ETSI TISPAN defines Next Generation Networks (NGN) which uses the 3rd-Generation Partnership Project (3GPP) IMS (IP Multimedia Subsystem) which in turn uses SIP (RFC3261 [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” June 2002.)) as its main signalling protocol. (For more information on the IMS, a detailed description can be found in 3GPP TS 23.228 [3GPP.23.228] (3GPP, “IP Multimedia Subsystem (IMS); Stage 2,” .) and 3GPP TS 24.229 [3GPP.24.229] (3GPP, “Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3,” .).)

1.2. Business communication

TOC

In the context of its work on business communiction support in public next generation networks (NGN), ETSI TISPAN has identified a framework [ETSI.181.019] (ETSI, “Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business Communication Requirements,” July 2007.) for the support of business communication capabilities by the NGN. As well as the direct attachment of Next Generation Corporate Network (NGCN) equipment, this includes the capability to "host" functionality relating to the enterprise network within the NGN itself.
These hosting arrangements are:

a) virtual leased line, where NGCN sites are interconnected through the NGN;

b) business trunking application, where the NGN hosts transit capabilities between NGCN's, break-in capabilities from NGN to NGCN and break-out capabilities from NGCN to NGN; and

c)

> hosted enterprise services, where an NGN hosts originating and/or terminating business communication capabilities for business communication users that are directly attached to an NGN.

ETSI TISPAN has requirements that can be met by the introduction of an explicit indication for private network traffic.
The traffic generated or received by an NGN on behalf of a private network can be either:

*public network traffic: traffic sent to the NGN for processing according to normal rules of the NGN. This type of traffic is known as public network traffic;

*private network traffic: traffic sent to the NGN for processing according to an agreed set of rules specific to an enterprise. This type of traffic is known as private network traffic. Private network traffic is normally within a single enterprise, but private network traffic can also exist between two different enterprises if not precluded for regulatory reasons.

1.3. Indication types

TOC

A private network indication as proposed by this document should not be confused with an indication to the local user that the remote user is in the same private network. This has traditionally resulted in PBXs providing distinctive ringing on incoming calls, but has also been used as input to services provided to the end user, e.g. different forwarding conditions and so on. Traditionally, this has only been applied where the call does not enter the public network at all, but we regard that limitation as a technical limitation rather than as one precluded by the desires of the service (i.e. traditionally there has been no special indication of this from the public network). Without such an indication one would have to rely on calling line identity, which would need to be reliable and trusted, to avoid a false indication that this is a private network internal call when it is in fact someone wishing to use that indication for fraudulent purposes. There may be a need for such a explicit indication, but that is not covered by this document.
Rather private network indication as proposed by this document is an indication to each and every network element traversed that this is private network traffic as opposed to public network traffic. This indication is not for the end user on the private network. It is an indication that special service arrangements apply for an enterprise, and therefore it is an indication of service on behalf of an

enterprise, not an indication of service to an end private network (NGCN) user.
In order to allow NGN IMS nodes to perform different processing ETSI TISPAN formulated the following requirements on NGN:

1. The NGN shall distinguish public network traffic from private network traffic.

2. The NGN shall distinguish private network traffic belonging to one enterprise from that belonging to another enterprise.

To summarize a few example reasons for a public telecommunication network to make the distinction between the two types of traffic:

*Different regulations apply to the two types of traffic, most notably lawful intercept requirements. Another example is emergency calls may be handled differently depending on the type of traffic.

*Different charging regimes may apply.

*Call recording for business reasons (e.g. quality control, training, non-repudiation) might apply only to a specific type of traffic.

*Different levels of signalling and/or media transparency may apply to the different types of traffic.

The indication is not regarded as appropriate as an indication from the end UA attached to an NGCN or hosted enterprise service equipment in the NGN. In this case any mixture of traffic from the same device relates to two or more distinct users, one belonging to the enterprise network and receiving service from that enterprise network, and one belonging to the NGN and receiving service from that network. Any distinction between the traffic types from such a device should be based on the authentication performed.
There are several reasons why there is a need for an explicit indication in the signalling:

1. As calling and target addresses can not in all cases be used to determine whether a certain call is to be treated as private or public network traffic.

2. Separate nodes in the network need to be able to act on the type of traffic being handled, when implicit schemes would be used it would require distribution of such enterprise specific logic over multiple nodes of multiple operators. That is clearly not a manageable architecture.

3. There may be cases where treating the call as a public network call although both participants are from the same enterprise is advantageous to the enterprise.

Given the above background this document will formulate requirements on SIP for support of an explicit private network indication.

---

2. Conventions

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

---

3. Definitions

TOC

3.1. Public network traffic

TOC

Traffic sent to or received from a public telecommunication network for processing according to the normal rules.

3.2. Private network traffic

TOC

Traffic sent to or received from a public telecommunication network for processing according to an agreed set of rules specific to an enterprise or a community of closely related enterprises.

3.3. Trust domain

TOC

The term Trust Domain in this document is taken from RFC3324 [RFC3324] (Watson, M., “Short Term Requirements for Network Asserted Identity,” November 2002.). A trust domain applies to the private network indication. The rules for specifying such a trust domain are specified in RFC3324 [RFC3324] (Watson, M., “Short Term Requirements for Network

Asserted Identity," November 2002.) which require the filling out a Spec (T).
The Spec (T) need not specify the same contents and trust domain boundaries that are used for other headers like the P-Asserted-Identity.

---

4. Application of terminology

TOC

Figure 1 shows the interconnection of sites belonging to two enterprise networks using the public network. Traffic in the public network relating to the interconnection of the two sites of enterprise 1 are tagged as private network traffic relating to enterprise 1. In certain cases an enterprise can also choose to send traffic from one enterprise site to another enterprise site as public network traffic when this is beneficial to the enterprise. Traffic in the public network relating to the interconnection of the two sites of enterprise 2 are tagged as private network traffic relating to enterprise 2. Enterprise 1 also generates traffic to public phones and this is public network traffic (untagged in the public network).

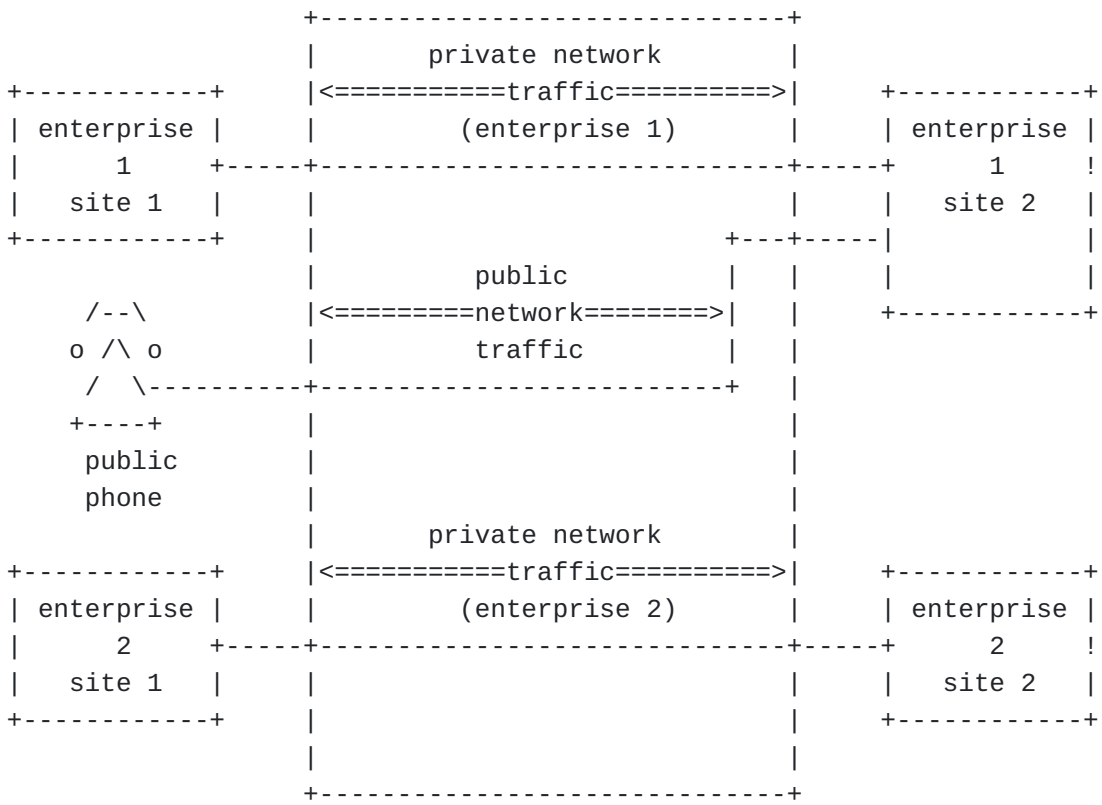

Figure 1

Figure 2 shows the interconnection of sites belonging to an enterprise networks using the public network, and supported in the public network by a server providing a business trunking application. The business trunking application providing routeing capabilities for the enterprise traffic, and supports the identification of calls to and from public network users, break-in and break out of that traffic. (Note that the business trunking application may consist of a concatenation of application logic provided to the originating enterprise site and application logic that is provided to the terminatig enterprise site.) Traffic in the public network relating to the interconnection of the two sites of enterprise 1 are tagged as private network traffic relating to enterprise 1. The business trunking application also routes traffic to public phones and this is public network traffic (untagged in the public network).

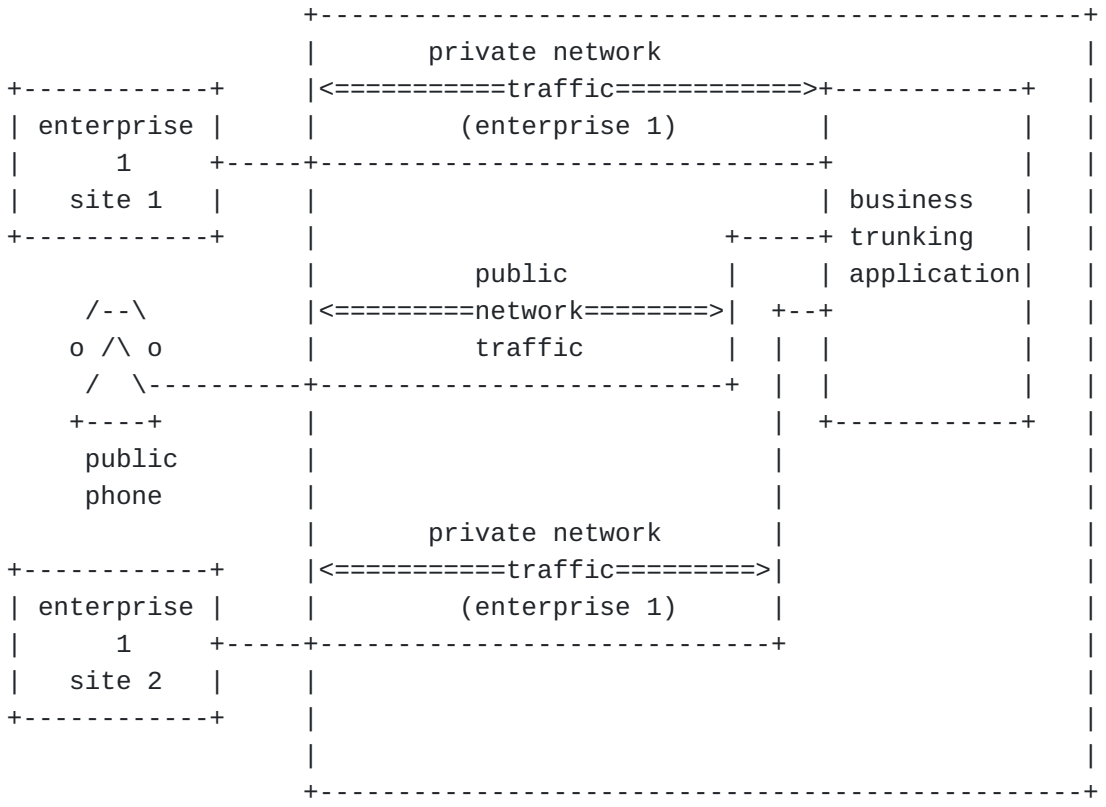

Figure 2

Figure 3 shows the interconnection of a site belonging to an enterprise network to a server providing a hosted enterprise service application (also known as Centrex). The hosted enterprise service application supports phones belonging to the enterprise and is also able to route traffic to or from public network phones using break-in or break-out functionality. Traffic in the public network relating to the interconnection of the site of enterprise 1 and the hosted enterprise service belonging to enterprise 1 are tagged as private network traffic

relating to enterprise 1. The hosted enterprise service application also routes traffic to public phones and this is public network traffic (untagged in the public network). Traffic from the enterprise phones would not normally be tagged (such a tag is added at the server providing the hosted enterprise services application. (Note that the hosted enterprise service logic may be preceded or subseded by a business trunking application that offers services on behalf of an enterprise site.)

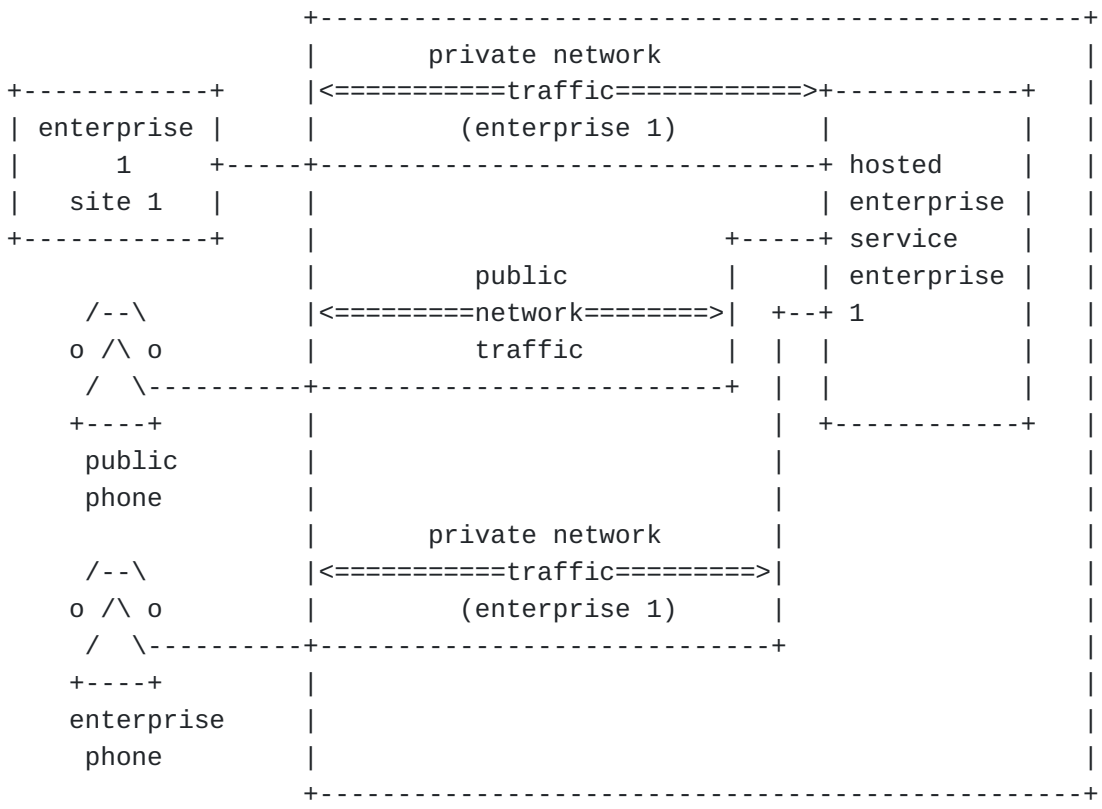

Figure 3

---

5. Requirements

TOC

This section lists the requirements on SIP derived from consideration in Section 1 (Introduction):

> **R1:** It is REQUIRED that an indication can be send in SIP initial requests for a dialog or SIP standalone requests that indicates

that the request or associated session is to be treated according to the rules of private network traffic.

R2: The indication from R1 can be inserted by a SIP proxy belonging to an administrative entity where for onward routeing, the traffic within that administrative entity needs to be so distinguished. The indication is not needed where the traffic is assumed to be all public, or where the traffic is assumed to be all private.

R3: The indication from R1 can be removed by a SIP proxy belonging to an administrative entity where for onward routeing, the traffic no longer needs to be so distinguished. An example exists where the traffic reaches an NGCN site where the traffic is now assumed to all private network traffic. Another example is on the final hop to the UA.

R4: It is REQUIRED that the indication from R1 allows entities to determine the set of rules that are applicable, these rules may be enterprise specific.

R5: It is REQUIRED that the indication from R1 allows entities receiving it to distinguish private network traffic from different enterprises.

R6: The identifier to distinguish private network traffic belonging to one enterprise from that belonging to another enterprise must be globally unique. Business communication arrangements for any particular enterprise can be expected to span multiple NGN operators potentially in multiple countries.

R7: The indication from R1 relates primarily to the SIP signaling. Applying the same concept to media may be possible, but is not necessarily meaningful where media is routed differently from signalling.

---

6. Overview of solution

TOC

The mechanism proposed in this document relies on a new header field called 'Private-Network-Indication' that contains an private network identifier expressed as a domain name, for example:

```
P-Private-Network-Indication: ericsson.com
```

A proxy server which handles a message can, based on authentication of the source of a message and configuration or local policy, insert such

a Private-Network-Indication header field into the message and forward it to other trusted proxies to be handled as private network traffic. A proxy that is about to forward a message to a proxy server or UA that it does not trust MUST remove the Private-Network-Indication header. The private network identifier expressed as a domain name allows it to be globally unique identifier associated with the enterprise. Domain name is used as it allows reuse of a company owned internet domain name, without requiring an additional private network identifier registry. When the enterprise needs more then one identifier it can freely add subdomains that it has under its own control.
The formal syntax for the Private-Network-Indication header is presented in Section 8 (P-Private-Network-Indication header field definition).

7. Behaviour

TOC

7.1. UA behaviour

TOC

Use of this extension by UA's is not foreseen. Therefore there is no particular UA behaviour specified in connection to the Private-Network-Indication header field.

7.2. Proxy behaviour

TOC

7.2.1. Private-Network-Indication generation

TOC

Proxies that are responsible for determining certain traffic is to be treated as private network traffic or contain a breakin function that converts incoming public network traffic to private network traffic MUST insert a Private-Network-Indication header field in to requests for a dialog or requests for a standalone transaction where the value MUST be set to the private network identifier corresponding to the enterprise to which the traffic belongs.

TOC

7.2.2. Private-Network-Indication consumption

Proxies that are responsible for applying different processing behaviours to specific private network traffic as to public network traffic MUST support this extension. The Private-Network-Indication header MUST NOT be used by a proxy in case it is received on a request it received from an entity that it does not trust, in such case it MUST be removed before the request is forwarded.

7.2.3. Private-Network-Indication removal

TOC

Proxies that are at the edge of the trustdomain or contain a breakout function that converts incoming private network traffic to public network traffic MUST remove the Private-Network-Indication header field before forwarding a request that contains such a header with a value.

---

8. P-Private-Network-Indication header field definition

TOC

This document defines the SIP P-Private-Network-Indication header. This header field can be added by a proxy to initial requests for a dialog or standalone requests. The presence of the P-Private-Network-Indication header field signifies to proxies that understand this header field that the request is to be treated as private network traffic. The P-Private-Network-Indication header field contains a domain name value that allows the private network traffic to be associated with an enterprise to which it belongs and that allow proxies that understand this header to process the request according to the request processing behaviours configured for a specific enterprise. The augmented Backus-Naur Form (BNF) (RFC5234 [RFC5234] (Crocker, D. and P. Overell, “Augmented BNF for Syntax Specifications: ABNF,” January 2008.)) syntax of the P-Private-Network-Indication header field is the following:

```
P-Private-Network-Indication =
                        "P-Private-Network-Indication" HCOLON PNI-value
                                                    *(SEMI PNI-param)
PNI-param                 = generic-param
PNI-value                 = hostname
```

EQUAL, HCOLON, SEMI, hostname and generic-param are defined in RFC3261 [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” June 2002.).

The following is an example of a P-Private-Network-Indication header field:

```
P-Private-Network-Indication: ericsson.com
```

---

9. Security considerations

TOC

The private network indication being defined in this document is to be used in an environment where elements are trusted and where attackers are not supposed to have access to the protocol messages between those elements. Traffic protection between network elements is sometimes achieved by using IPsec and sometimes by physically protecting the network. In any case, the environment where the private network indication will be used ensures the integrity and the confidentiality of the contents of this header field.
A private network indication received from an untrusted node MUST NOT be used and the information MUST be removed from a request or response before it is forwarded to entities in the trust domain.
There is a security risk if a private network indication is allowed to propagate out of the trust domain where it was generated. In that case sensitive information would be revealed by such a breach. To prevent such a breach from happening: Proxies MUST NOT insert the information when forwarding requests to a next hop located outside the trust domain. When forwarding the request to a trusted node, proxies MUST NOT insert the header unless they have sufficient knowledge that the route set includes another proxy in the trust domain that understands the header, such as the own proxy. There is no automatic mechanism to learn the support for this specification. Proxies MUST remove the information when forwarding requests to untrusted nodes or when the proxy does not have knowledge of any other proxy in the route set that is able to understand the header.

---

10. Applicability

TOC

According to RFC 3427 [RFC3427] (Mankin, A., Bradner, S., Mahy, R., Willis, D., Ott, J., and B. Rosen, “Change Process for the Session Initiation Protocol (SIP),” December 2002.), P-headers have a limited applicability. Specifications of P-headers such as this RFC need to clearly document the useful scope of the proposal, and explain its limitations and why it is not suitable for the general use of SIP on the Internet.
The P-Private-Network-Indication header field is intended to be used in controlled closed networks like 3GPP IMS and ETSI TISPAN NGN networks.

The P-Private-Network-Indication header field does not seem useful in a general internet environment.

11. IANA considerations

TOC

This document defines a new SIP header field: P-Private-Network-Indication. This header field needs to be registered by the IANA in the SIP Parameters registry under the Header Fields subregistry.

12. Acknowledgments

TOC

The authors thank Bruno Chatras, John Elwell and Salvatore Loreto for providing comments on an early version of this draft.

13. References

TOC

13.1. Normative references

TOC

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3261]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, June 2002 (TXT).
[RFC3324]	Watson, M., "Short Term Requirements for Network Asserted Identity," RFC 3324, November 2002 (TXT).
[RFC3427]	Mankin, A., Bradner, S., Mahy, R., Willis, D., Ott, J., and B. Rosen, "Change Process for the Session Initiation Protocol (SIP)," RFC 3427, December 2002 (TXT).
[RFC5234]	Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF," STD 68, RFC 5234, January 2008 (TXT).

13.2. Informative references

TOC

[ETSI.181.019]	ETSI, "Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business Communication Requirements," ETSI TS 181 019 V2, July 2007.
[3GPP.23.228]	3GPP, "IP Multimedia Subsystem (IMS); Stage 2," 3GPP TS 23.228 V8.
[3GPP.24.229]	3GPP, "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3," 3GPP TS 24.229 V8.
[RFC3455]	Garcia-Martin, M., Henrikson, E., and D. Mills, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)," RFC 3455, January 2003 (TXT).
[RFC3841]	Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Caller Preferences for the Session Initiation Protocol (SIP)," RFC 3841, August 2004 (TXT).
[I-D.drage-sipping-service-identification]	Drage, K., "A Session Initiation Protocol (SIP) Extension for the Identification of Services," draft-drage-sipping-service-identification-02 (work in progress), October 2008 (TXT).

Appendix A. Alternative solutions discussed

TOC

A.1. General

TOC

It would be technical possible, but extremely complex to perform this function without an explicit indication. For example, a logical distinction of proxies to handle private network traffic relating to enterprise 1, enterprise 2 and the public network traffic could be made by assigning different SIP URIs to these logical entities. This is not regarded as a viable solution.
Several solutions have been raised and whether or not they are suitable and fulfill the requirements need to be discussed:

- *Attribute on existing header?

- *Token on some existing header?

*Resource-Priority header?

*P-Asserted-Service header?

*Request-Disposition header?

*P-Access-Network-Information header?

*URI parameter?

*New P-header?

*New header?

A.2. Attribute on existing header

TOC

A.3. Token value on existing header

TOC

A.4. Resource-Priority header

TOC

Some of the distinctive functions are already provided for in this header. A potential mechanism would be to define a namespace for private network traffic. It would however be impossible to define a namespace for each enterprise, and therefore some additional parameter would need to be defined to carry the unique identifier of the particular enterprise to which the private network traffic relates. Successful usage may also require a tightening of the procedures for use of the Resource-Priority header (much at the moment is left to the particular application of this header).
Private network traffic may, but is not necessarily handled with a different priority then public network traffic. Use of the Resource-Priority header however seems to imply that the main focus of the indication is on prioritizing private network traffic. This may render use of the Resource-Priority header as less appropriate for our particular purpose.

TOC

A.5. P-Asserted-Service header

The services envisaged by the P-Asserted-Service header field (draft-drage-sipping-service-identification [I-D.drage-sipping-service-identification] (Drage, K., "A Session Initiation Protocol (SIP) Extension for the Identification of Services," October 2008.)) are those applied to the end user. The end user in these cases is the end user of the enterprise or NGCN, not the enterprise itself. Therefore this header is not considered suitable for this problem.

A.6. Request-Disposition header

TOC

The Request-Disposition header field (RFC3841 [RFC3841] (Rosenberg, J., Schulzrinne, H., and P. Kyzivat, "Caller Preferences for the Session Initiation Protocol (SIP)," August 2004.)) specifies caller preferences for how a server should process a request. The caller in these cases is the end user of the enterprise or NGCN, not the enterprise itself. Therefore this header is not considered suitable for this problem. Further RFC3841 explicitly states that the set of request disposition directives is not extensible.

A.7. P-Access-Network-Information

TOC

The P-Access-Network-Info header field (RFC3455 [RFC3455] (Garcia-Martin, M., Henrikson, E., and D. Mills, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)," January 2003.)) contains information about the access network that a UA uses to get IP connectivity. However the access that one uses does not define the private network that a call that one sets up is to be part of. Particular examples that illustrate this:

*A Hosted Enterprise Services user (i.e. Centrex) uses the access of the operator while still being able to setup calls that will turn out to be private network traffic.

*A corporate network UE that attaches to an operator network, but receives services from its home corporate network.

TOC

A.8. URI parameter

A marking on the entities within the Via header that are treating this as private network traffic. Potential marking on the route header of entities that are expected to treat it as private network traffic.

A.9. New header

TOC

A.9.1. General

TOC

If none of the existing headers is appropriate a logical step is to define a new header for the private network indication.

A.9.2. Full SIP header field

TOC

A full SIP header is appropriate when the usage of this information element is more general then closed networks like ETSI TISPAN NGN or 3GPP IMS.

A.9.3. New P-header

TOC

In case no general usage is foreseen other then usage in closed networks like those specified by ETSI TISPAN NGN or 3GPP IMS a P-header seems the appropriate choice.

Appendix B. Revision Information

TOC

B.1. version 00

TOC

1. 2008-02-18, Initial version

B.2. version 01

TOC

1. 2008-02-23, Added a solution based on a new header. Added Overview, Behaviour and Header Definition sections. Updated the trust domain definition. Improved some of the existing text based on comments from John Elwell.

B.3. version 02

TOC

1. 2008-07-11, Changed to a P-header. Changed title. Added Terminology application and Applicability sections. Moved the Potential solutions section to appendix Alternative solutions discussed.

B.4. version 03

TOC

1. 2009-02-19, Updated boilerplate.

Authors' Addresses

TOC

	Hans Erik van Elburg
	Ericsson Telecommunicatie B.V.
	Ericssonstraat 2
	Rijen 5121 ML
	The Netherlands
Email:	HansErik.van.Elburg@ericsson.com
	Keith Drage
	Alcatel-Lucent
	The Quadrant, Stonehill Green, Westlea
	Swindon SN5 7DJ
	UK
Email:	drage@alcatel-lucent.com