            The Session Initiation Protocol (SIP) P-Private-Network-Indication
                          Private Header (P-Header)

Abstract

   This document specifies the SIP P-Private-Network-Indication P-header
   used by the 3GPP. The P-Private-Network-Indication indicates that
   the message is part of the message traffic of a private network and
   identifies that private network. A private network indication allows
   nodes to treat private network traffic according to a different set
   of rules than the set applicable to public network traffic.

Table of Contents

1. Introduction

1.1. Overview

   ETSI TISPAN (Telecommunications and Internet converged Services and
   Protocols for Advanced Networking) defined Next Generation Networks
   (NGNs), which use the 3GPP IP Multimedia Subsystem (IMS), which, in
   turn, uses SIP [RFC3261] as its main signaling protocol. For more
   information on the IMS, a detailed description can be found in 3GPP
   TS 23.228 [3GPP.23.228] and 3GPP TS 24.229 [3GPP.24.229]. 3GPP and
   ETSI TISPAN have identified a set of requirements that can be met by
   defining a new optional SIP header, according to the procedures in
   RFC 5727 [RFC5727].

1.2. Applicability

   The P-Private-Network-Indication header field is intended to be used
   in controlled closed networks like 3GPP IMS and ETSI TISPAN NGNs.
   The P-Private-Network-Indication header is not intended for the
   general Internet environment and is probably not suitable for such an
   environment.

   For example, there are no mechanisms defined to prevent spoofing of
   this header. So, if a network were to accept calls carrying this
   header from the general Internet, an attacker would be able to inject
   information into private networks.

1.3. Background

   The P-Private-Network-Indication header field has been referred to in
   3GPP IMS specifications and has already been used in some networks as
   an indicator for a specific capability. The header field has already
   been implemented in some vendors' equipment in some countries. RFC
   5727 [RFC5727] prohibits the new proposal of P-header "unless
   existing deployments or standards use the prefix already". The
   P-Private-Network-Indication header field is already used by existing
   deployments and 3GPP standards; therefore, this is exactly the case
   where the P-header is allowed as an exception.

1.4. Business Communication

   ETSI TISPAN has identified a framework, which was adopted by 3GPP as
   [3GPP.22.519], for the support of business communication capabilities
   by the NGN. In addition to the direct attachment of Next Generation
   Corporate Network (NGCN) equipment, this includes the capability to
   "host" functionality relating to an enterprise 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, where the NGN
    converts public network traffic to private network traffic for
    delivery at a served NGCN; and break-out capabilities, where the
    NGN converts private network traffic from a served NGCN to public
    network traffic; 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 a public NGN on behalf of a
private network can be either:

1) public network traffic: traffic sent to or received from an NGN
    for processing according to the rules for ordinary subscribers of
    a public telecommunication network. This type of traffic is
    known as public network traffic.

2) 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 exchanged within a single
    enterprise, but private network traffic can also be exchanged
    between two or more different enterprises, based on some prior
    arrangements, if not precluded for regulatory reasons.

1.5. Indication Types

A private network indication as proposed by this document indicates
to the receiving network element (supporting this specification) that
this request is related to private network traffic as opposed to
public network traffic. This indication does not identify an end
user on a private network and is not for delivery to an end user on
the private network. It is an indication that special service
arrangements apply (if such service is configured based on private
network traffic) for an enterprise; therefore, it is an indication of
service on behalf of an enterprise, not an indication of service to a
private network's end user.

In order to allow NGN IMS nodes to perform different processing, ETSI TISPAN formulated the following requirements for NGN. The NGN shall:

a) distinguish public network traffic from private network traffic; and

b) distinguish private network traffic belonging to one enterprise from that belonging to another enterprise.

To summarize, a few example reasons for a public NGN to make the distinction between the two types of traffic include:

1) Different regulations apply to two types of traffic, for example, emergency calls may be handled differently depending on the type of traffic.

2) Different charging regimes may apply.

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

4) Different levels of signaling and/or media transparency may apply to the different types of traffic.

There are several reasons why there is a need for an explicit indication in the signaling:

a) Caller and callee addresses cannot always be used to determine whether a certain call is to be treated as private or public network traffic.

b) Nodes spanning multiple networks often need to have different behavior depending upon the type of traffic. When this is done using implicit schemes, enterprise-specific logic must be distributed across multiple nodes in multiple operators' networks. That is clearly not a manageable architecture and solution.

c) 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.

Based on the background provided, this document formulates requirements for SIP to support an explicit private network indication and defines a P-header, P-Private-Network-Indication, to support those requirements.

2. Conventions

   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].

3. Definitions

3.1. Traffic

   In the context of this document, the term "traffic" is understood as
   all communication pertaining to and/or controlled by a SIP
   transaction or dialog.

3.2. Public Network Traffic

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

3.3. Private Network Traffic

   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.

3.4. Break-In

   Act of converting public network traffic to private network traffic.
   The header defined in this specification will be added to indicate
   the traffic is a private network traffic after conversion.

3.5. Break-Out

   Act of converting private network traffic to public network traffic.
   The header defined in this specification will be removed to indicate
   the traffic is a public network traffic after conversion.

3.6. Trust Domain

   The term "trust domain" in this document is taken from P-Asserted-
   Identity [RFC3324]. A trust domain applies to the private network
   indication. The rules for specifying such a trust domain are
   specified in P-Asserted-Identity [RFC3324] and require the
   specification of a Spec(T) as covered in Section 2.4 of [RFC3324].

   The same information is required to specify a Spec(T) for purposes of
   P-Private-Network-Indication as for P-Asserted-Identity [RFC3324].
   However, if a network is using P-Private-Network-Indication as well
   as other header fields subject to Spec(T) (such as P-Asserted-
   Identity), the Spec(T) for each header field will probably be
   different from the others.

4. Application of Terminology

   Figure 1 shows the interconnection of sites belonging to two private
   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).
   There may be circumstances where traffic in the public network
   between two different private networks is tagged as private network
   traffic using a pre-arranged domain name agreed by the two involved
   enterprises. This is illustrated by the interconnection of the site
   from enterprise 3 and the site from enterprise 4.

```
                    +------------------------------+
                    |       private network        |
    +-----------+   |<========traffic=========>|   +-----------+
    | enterprise|   |        (enterprise 1)        |   | enterprise|
    |     1     +-----+--------------------------+-----+    1      !
    |   site 1  |   |                              |   |  site 2   |
    +-----------+   |                        +---+-----|          |
                    |          public        |   |     |          |
      /--\          |<========network======>|   |     +-----------+
     o /\ o         |         traffic        |   |
      /  \----------+--------------------------+   |
     +----+         |                              |
      public        |                              |
      phone         |                              |
                    |       private network        |
    +-----------+   |<========traffic=========>|   +-----------+
    | enterprise|   |        (enterprise 2)        |   | enterprise|
    |     2     +-----+--------------------------+-----+    2      !
    |   site 1  |   |                              |   |  site 2   |
    +-----------+   |                              |   +-----------+
                    |                              |
                    |       private network        |
    +-----------+   |<========traffic=========>|   +-----------+
    | enterprise|   |  (pre-arranged domain name)  |   | enterprise|
    |     3     +-----+--------------------------+-----+    4      !
    |   site 1  |   |                              |   |  site 1   |
    +-----------+   |                              |   +-----------+
                    |                              |
                    +------------------------------+
```
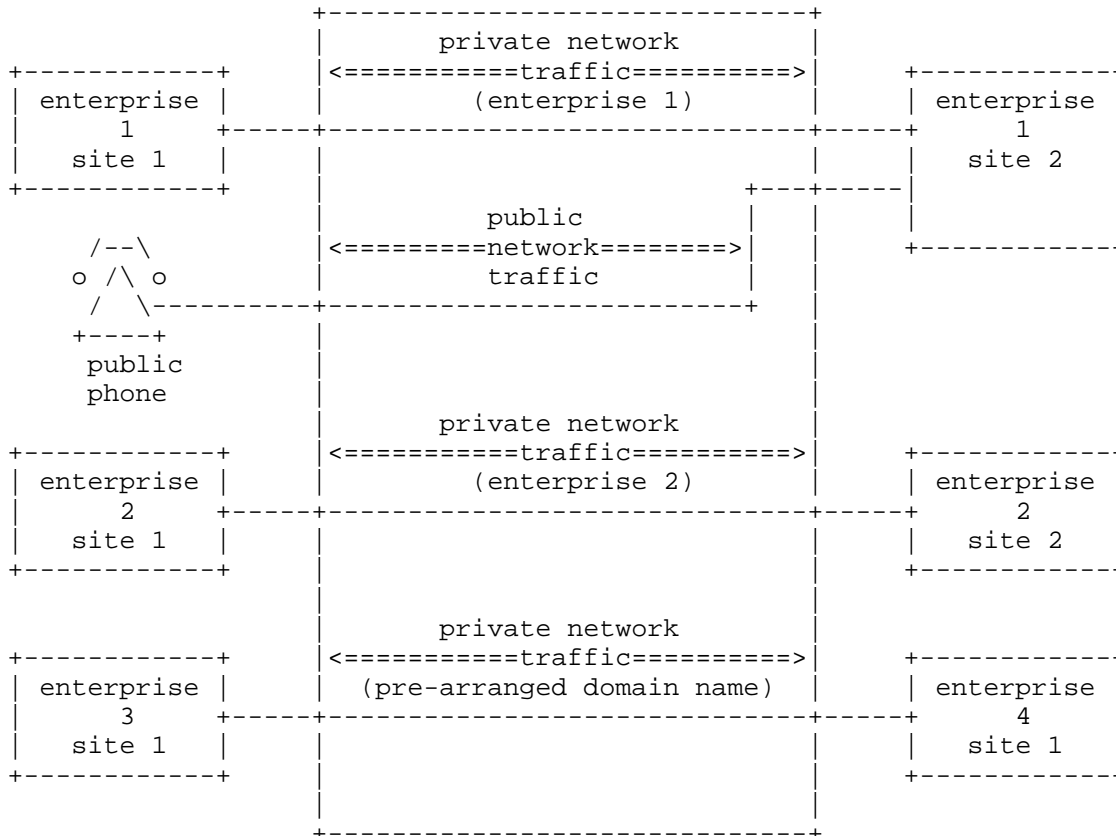
                        Figure 1: Two Private Networks

   Figure 2 shows the interconnection of sites belonging to a private
   network using the public network and supported in the public network
   by a server providing a business trunking application. The business
   trunking application provides routing capabilities for the enterprise
   traffic and supports the identification of calls to and from public
   network users and routing of 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
   terminating enterprise site.) Traffic in the public network relating
   to the interconnection of the two sites of enterprise 1 is 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).

```
                 +-------------------------------------------------+
                 |                 private network                 |
   +-----------+ |<==========traffic===========>+-----------+     |
   | enterprise| |             (enterprise 1)   |           |     |
   |     1     +-----+--------------------------+           |     |
   |  site 1   | |   |                          | business  |     |
   +-----------+ |   |                  +-----+ | trunking  |     |
                 |   |       public     |     | | application|    |
    /--\         |<========network======>|   +--+           |     |
   o /\ o        |       traffic     |   | | |           |     |
    /  \---------+-------------------------+ | |           |     |
    +----+       |                          | | +-----------+     |
    public       |                          | |                   |
    phone        |                          | |                   |
                 |            private network|  |                   |
   +-----------+ |<==========traffic========>|                   |
   | enterprise| |           (enterprise 1) |                     |
   |     1     +-----+--------------------------+                   |
   |  site 2   | |                              |                   |
   +-----------+ |                              |                   |
                 |                              |                   |
                 +-------------------------------------------------+
```

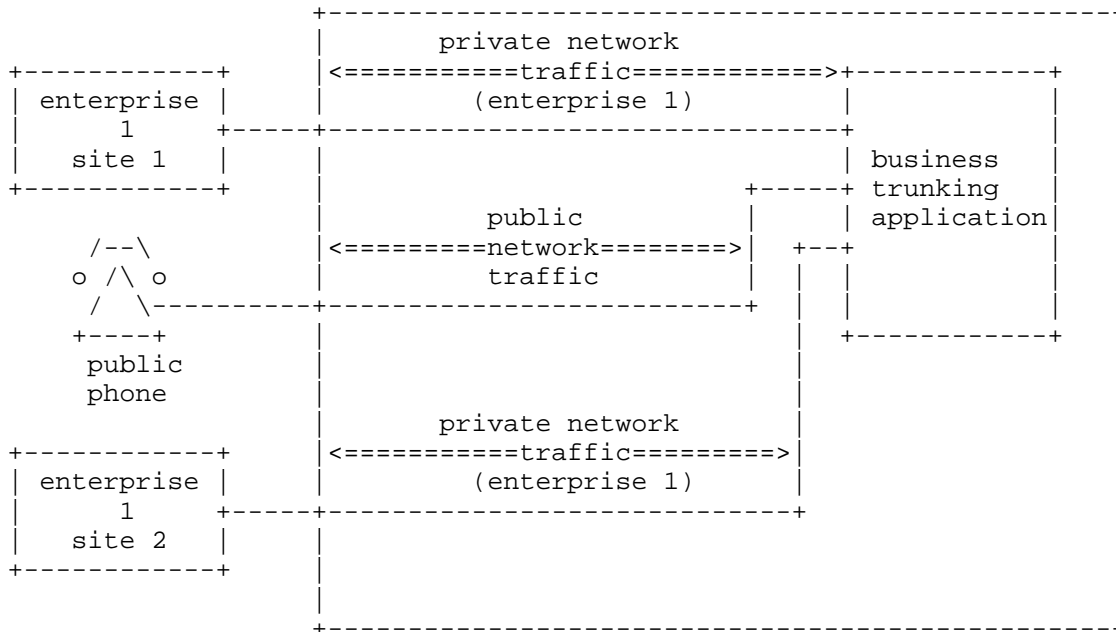   Figure 2: Private Network and Business Trunking

   Figure 3 shows the interconnection of sites belonging to a private
   network on 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 and 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 is 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, but it can be tagged
   as private network traffic. (Note that the hosted enterprise service
   logic may precede or succeed a business trunking application that
   offers services on behalf of an enterprise site.)

```
                +----------------------------------------------------+
                |                private network                     |
  +-----------+ |<==========traffic============>+-----------+       |
  | enterprise| |            (enterprise 1)      |           |       |
  |     1     +-----+--------------------------+ hosted      |       |
  |   site 1  | |   |                          | enterprise  |       |
  +-----------+ |   |                 +-----+ service        |       |
                |   |        public   |     | | enterprise   |       |
     /--\       |<========network=======>|   +--+ 1          |       |
    o /\ o      |            traffic    |   | |    |          |       |
   /  \---------+------------------------+   | |    |          |       |
   +----+       |                          |  +-----------+   |
    public      |                          |                   |
    phone       |                          |                   |
                |          private network  |                   |
     /--\       |<==========traffic========>|                   |
    o /\ o      |            (enterprise 1)  |                   |
   /  \---------+------------------------+   |                   |
   +----+       |                          |                   |
   enterprise   |                          |                   |
     phone      |                          |                   |
                +----------------------------------------------------+
```
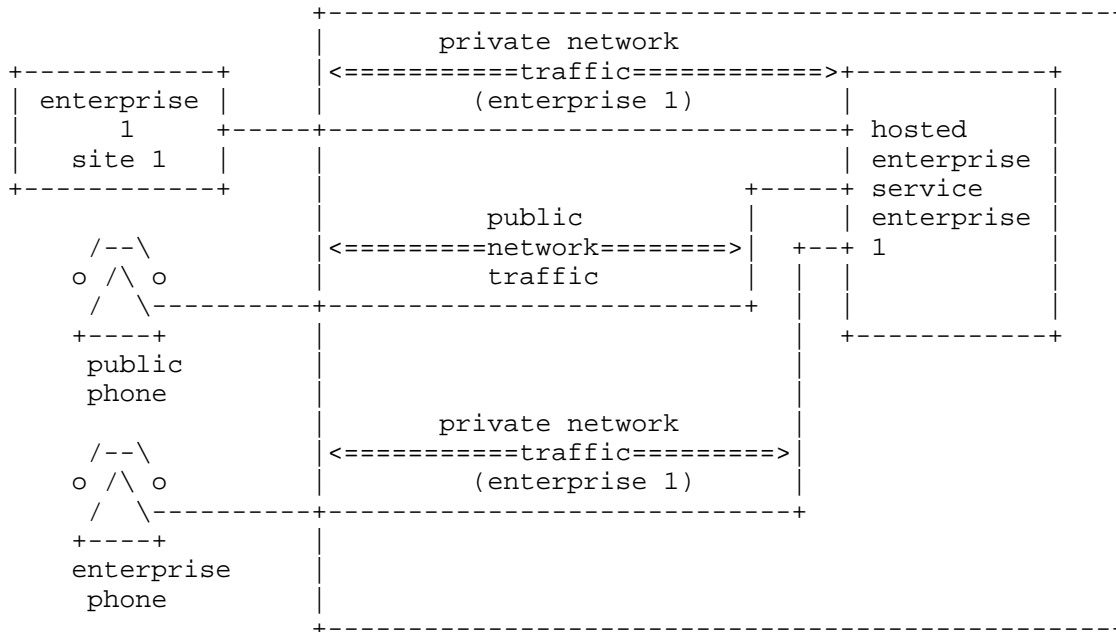
               Figure 3: Hosted Service and Private Network

5. Overview of Solution

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

   P-Private-Network-Indication: example.com

   A proxy server that handles a message MAY insert such a P-Private-
   Network-Indication header field into the message based on
   authentication of the source of a message, configuration, or local
   policy. A proxy server MAY forward the message to other proxies in
   the same administrative domain or proxies in a trusted domain to be
   handled as private network traffic. A proxy that forwards a message
   to a proxy server or user agent (UA) that it does not trust MUST
   remove the P-Private-Network-Indication header field before
   forwarding the message.

   The private network identifier expressed as a domain name allows it
   to be a globally unique identifier, associated with the originating
   and/or terminating enterprise(s). 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 than one identifier, it can freely add subdomains under
its own control.

The formal syntax for the P-Private-Network-Indication header is
presented in Section 7.

6. Proxy Behavior

6.1. P-Private-Network-Indication Generation

Proxies that are responsible for determining certain traffic to be
treated as private network traffic or contain a break-in function
that converts incoming public network traffic to private network
traffic MUST insert a P-Private-Network-Indication header field into
incoming or outgoing requests for a dialog or for a standalone
transaction. The value MUST be set to the private network identifier
corresponding to the enterprise(s) to which the traffic belongs.

6.2. P-Private-Network-Indication Consumption

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

6.3. P-Private-Network-Indication Removal

Proxies that are at the edge of the trust domain or contain a break-
out function that converts incoming private network traffic to public
network traffic MUST remove the P-Private-Network-Indication header
field before forwarding a request that contains such a header field.

6.4. P-Private-Network-Indication Verification

When proxies supporting this specification receive a P-Private-
Network-Indication header field in a SIP request from a trusted node,
proxies MUST check whether the received domain name in the request is
the same as the domain name associated with the provisioned domain
name. If the received domain name does not match, proxies MUST
remove the P-Private-Network-Indication header field.

7. P-Private-Network-Indication Header Field Definition

   This document defines the SIP P-Private-Network-Indication header
   field. 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
   the 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 allows proxies
   that understand this header field to process the request according to
   the local policy configured for a specific enterprise(s).

   The Augmented Backus-Naur Form (ABNF) [RFC5234] syntax of the
   P-Private-Network-Indication header field is described below:

   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 RFC
   3261 [RFC3261].

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

   P-Private-Network-Indication: example.com

8. Security Considerations

   The private network indication defined in this document MUST only be
   used in the traffic transported between network elements that are
   mutually trusted. Traffic protection between network elements can be
   achieved by using security protocols such as IP Encapsulating
   Security Payload (ESP) [RFC4303] or SIP / Transport Layer Security
   (SIP/TLS) or sometimes by physical protection of the network. In any
   case, the environment where the private network indication will be
   used needs to ensure 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.
   Additionally, local policies may be in place that ensure that all
   requests entering the trust domain for private network indication
   from untrusted nodes with a private network indication will be
   discarded.

There is a security risk if a private network indication is allowed
to propagate out of the trust domain where it was generated. The
indication may reveal information about the identity of the caller,
i.e., the organization that he belongs to. That is sensitive
information. It also reveals to the outside world that there is a
set of rules that this call is subject to that is different then the
rules that apply to public traffic. That is sensitive information
too. 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 field unless they have
sufficient knowledge that the route set includes another proxy in the
trust domain that understands this header field. However, how to
learn such knowledge is out of the scope of this document. 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 this header field.

9. IANA Considerations

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

      RFC Number: [RFC7316]

      Header Field Name: P-Private-Network-Indication

      Compact Form: none

10. Acknowledgments

   The authors would like to thank Richard Barnes, Mary Barnes, Atle
   Monrad, Bruno Chatras, John Elwell, and Salvatore Loreto for
   providing comments on an early version of this document. Further, we
   thank John Elwell for performing the expert review.

11. References

11.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [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.

   [RFC3324] Watson, M., "Short Term Requirements for Network Asserted
              Identity", RFC 3324, November 2002.

   [RFC5234] Crocker, D., Ed., and P. Overell, "Augmented BNF for
              Syntax Specifications: ABNF", STD 68, RFC 5234, January
              2008.

11.2. Informative References

   [3GPP.22.519]
              3GPP, "Business Communication Requirements", TS 22.519.

   [3GPP.23.228]
              3GPP, "IP Multimedia Subsystem (IMS); Stage 2", 3GPP TS
              23.228 V8, July 2007.

   [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, July 2007.

   [RFC5727] Peterson, J., Jennings, C., and R. Sparks, "Change Process
              for the Session Initiation Protocol (SIP) and the Real-
              time Applications and Infrastructure Area", BCP 67, RFC
              5727, March 2010.

   [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC
              4303, December 2005.

Authors' Addresses

   Hans Erik van Elburg
   Detecon International Gmbh
   Oberkasselerstrasse 2
   Bonn   53227
   Germany

   EMail: ietf.hanserik@gmail.com

   Keith Drage
   Alcatel-Lucent
   The Quadrant, Stonehill Green, Westlea
   Swindon SN5 7DJ
   UK

   EMail: drage@alcatel-lucent.com

   Mayumi Ohsugi
   NTT Corporation

   Phone: +81 422 36 7502
   EMail: mayumi.ohsugi@ntt-at.co.jp

   Shida Schubert
   NTT Corporation

   Phone: +1 415 323 9942
   EMail: shida@ntt-at.com

   Kenjiro Arai
   NTT Corporation
   9-11, Midori-cho 3-Chome
   Musashino-shi, Tokyo   180-8585
   Japan

   Phone: +81 422 59 3518
   EMail: arai.kenjiro@lab.ntt.co.jp
   URI: http://www.ntt.co.jp