INTERNET-DRAFT
Internet Engineering Task Force
PINT Working Group
Issued: 18 February 2000
Expires: 18 August 2000

Scott Petrack,
MetaTel
Lawrence Conroy,
Siemens Roke Manor Research

The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services

<draft-ietf-pint-protocol-03.txt>

Status of this Memo

Copyright Notice

Abstract

This document contains the specification of the PINT Service Protocol 1.0, which defines a protocol for invoking certain telephone services from an IP network. These services include placing basic calls, sending and receiving faxes, and receiving content over the telephone. The protocol is specified as a set of enhancements and additions to the SIP 2.0 and SDP protocols.

This document is intended for the PSTN-Internet Interworking (PINT) working group of the Internet Engineering Task Force. Comments are

solicited and should be addressed to the working group's mailing list at
pint@lists.research.bell-labs.com and/or the authors.

Contents

1. Introduction

The desire to invoke certain telephone call services from the Internet has been identified by many different groups (users, public and private network operators, call center service providers, equipment vendors, see [7]). The generic scenario is as follows (when the invocation is successful):

1. an IP host sends a request to a server on an IP network;
2. the server relays the request into a telephone network;
3. the telephone network performs the requested call service.

As examples, consider a user who wishes to have a callback placed to his/her telephone. It may be that a customer wants someone in the support department of some business to call them back. Similarly, a user may want to hear some announcement of a weather warning sent from a remote automatic weather service in the event of a storm.

We use the term "PSTN/Internet Interworking (PINT) Service" to denote such a complete transaction, starting with the sending of a request from an IP client and including the telephone call itself. PINT services are distinguished by the fact that they always involve two separate networks:
an IP network to request the placement of a call, and the Global Switched Telephone Network (GSTN) to execute the actual call. It is understood that Intelligent Network systems, private PBXs, cellular phone networks, and the ISDN can all be used to deliver PINT services. Also, the request for service might come from within a private IP network that is disconnected from the whole Internet.

The requirements for the PINT protocol were deliberately restricted to providing the ability to invoke a small number of fixed telephone call services. These "Milestone PINT services" are specified in section 2. Great care has been taken, however, to develop a protocol that is aligned with other Internet protocols where possible, so that future extensions to PINT could develop along with Internet conferencing.

Within the Internet conference architecture, establishing media calls is done via a combination of protocols. SIP [1] is used to establish the association between the participants within the call (this association between participants within the call is called a "session"), and SDP [2] is used to describe the media to be exchanged within the session. The PINT protocol uses these two protocols together, providing some extensions and enhancements to enable SIP clients and servers to become PINT clients and servers.

A PINT user who wishes to invoke a service within the telephone network uses SIP to invite a remote PINT server into a session. The invitation contains an SDP description of the media session that the user would like to take place. This might be a "sending a fax session" or a "telephone call session", for example. In a PINT service execution session the media is transported over the phone system, while in a SIP session the media is normally transported over an internet.

When used to invoke a PINT service, SIP establishes an association between a requesting PINT client and the PINT server that is responsible for invoking the service within the telephone network. These two entities are not the same entities as the telephone network entities involved in the telephone network service. The SIP messages carry within their SDP payloads a description of the telephone network media session.

Note that the fact that a PINT server accepts an invitation and a session is established is no guarantee that the media will be successfully transported. (This is analogous to the fact that if a SIP invitation is accepted successfully, this is no guarantee against a subsequent failure of audio hardware).

The particular requirements of PINT users lead to some new messages. When a PINT server agrees to send a fax to telephone B, it may be that the fax transmission fails after part of the fax is sent. Therefore, the PINT client may wish to receive information about the status of the actual telephone call session that was invoked as a result of the established PINT session. Three new requests, SUBSCRIBE, UNSIUBSCRIBE, and NOTIFY, are added here to vanilla SIP to allow this.

The enhancements and additions specified here are not intended to alter the behaviour of baseline SIP or SDP in any way. The purpose of PINT

extensions is to extend the usual SIP/SDP services to the telephone world. Apart from integrating well into existing protocols and architectures, and the advantages of reuse, this means that the protocol specified here can handle a rather wider class of call services than just the Milestone services.

The rest of this document is organised as follows: Section 2 describes the PINT Milestone services; section 3 specifies the PINT functional and protocol architecture; section 4 gives examples of the PINT 1.0 extensions of SIP and SDP; section 5 contains some security considerations for PINT. The final section contains descriptions of how the PINT protocol may be used to provide service over the GSTN.

For a summary of the extensions to SIP and SDP specified in this document, Section 3.2 gives an combined list, plus one each describing the extensions to SIP and SDP respectively.

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 RFC 2119. In addition, the construct "MUST .... OR ...." implies that it is an absolute requirement of this specification to implement one of the two possibilities stated (represented by dots in the above phrase). An implementation MUST be able to interoperate with another implementation that chooses either of the two possibilities.

1.1 Glossary
Requestor - An Internet host from which a request for service originates

PINT Service - A service invoked within a phone system in response to a request received from an PINT client.

PINT Client - An Internet host that sends requests for invocation of a PINT Service, in accordance with this document.

PINT Gateway - An Internet host that accepts requests for PINT Service and dispatches them onwards towards a telephone network.

Executive System - A system that interfaces to PINT Server and to a telephone network that executes a PINT service. It need not be directly associated with the Internet, and is represented by the PINT Server in transactions with Internet entities.

Requesting User - The initiator of a request for service. This role may be distinct from that of the "party" to any telephone network call that results from the request.

(Service Call) Party - A person who is involved in a telephone network call that results from the execution of a PINT service request, or a telephone network-based resource that is involved (such as an automatic Fax Sender or a Text-to-Speech Unit).

2. PINT Milestone Services

The original motivation for defining this protocol was the desire to invoke the following three telephone network services from within an IP network:

2.1 Request to Call

A request is sent from an IP host that causes a phone call to be made, connecting party A to some remote party B.

2.2 Request to Fax

A request is sent from an IP host that causes a fax to be sent to fax machine B. The request MUST contain a pointer to the fax data (that could reside in the IP network or in the Telephone Network), OR the fax data itself. The content of the fax MAY be text OR some other more general image data. The details of the fax transmission are not accessible to the IP network, but remain entirely within the telephone network.

The PINT Request to Fax service does not involve "Fax over IP": the IP network is only used to send the request that a certain fax be sent. Of course, it is possible that the resulting telephone network fax call happens to use a real-time IP fax solution, but this is completely transparent to the PINT transaction.

2.3 Request to Hear Content

A request is sent from an IP host that causes a phone call to be made to user A, and for some sort of content to be spoken out. The request MUST EITHER contain a URL pointing to the content, OR include the content itself. The content MAY be text OR some other more general application data. The details of the content transmission are not accessible to the IP network, but remain entirely within the telephone network. This service could equally be called "Request to have Content Spoken"; the user's goal is to hear the content spoken to them. The mechanism by which the request is formulated is outside the scope of this document; however, an example might be that a Web page has a button that when pressed causes a PINT request to be passed to the PSTN, resulting in the content of the page (or other details) being spoken to the person.

2.4 Relation between PINT milestone services and traditional telephone services

There are many different versions and variations of each telephone call service invoked by a PINT request. Consider as an example what happens when a user requests to call 1-800-2255-287 via the PINT Request-to-Call service.

There may be thousands of agents in the call center, and there may be any number of sophisticated algorithms and pieces of equipment that are used to decide exactly which agent will return the call. And once this choice is made, there may be many different ways to set up the call: the agent's phone might ring first, and only then the original user will be called; or perhaps the user might be called first, and hear some horrible music or pre-recorded message while the agent is located.

Similarly, when a PINT request causes a fax to be sent, there are hundreds of fax protocol details to be negotiated, as well as transmission details within the telephone networks used.

PINT requests do not specify too precisely the exact telephone-side service. Operational details of individual events within the telephone network that executes the request are outside the scope of PINT. This does not preclude certain high-level details of the telephone network session from being expressed within a PINT request. For example, it is possible to use the SDP "lang" attribute to express a language preference for the Request-to-Hear-Content Service. If a particular PINT system wishes to allow requests to contain details of the telephone-network-side service, it uses the SDP attribute mechanism (see section 3.4.2).

3. PINT Functional and Protocol Architecture

3.1. PINT Functional Architecture

Familiarity is assumed with SIP 2.0 [1] and with SDP [2].

PINT clients and servers are SIP clients and servers. SIP is used to carry the request over the IP network to the correct PINT server in a secure and reliable manner, and SDP is used to describe the telephone network session that is to be invoked or whose status is to be returned.

A PINT system uses SIP proxy servers and redirect servers for their usual purpose, but at some point there must be a PINT server with the means to relay received requests into a telephone system and to receive acknowledgement of these relayed requests. A PINT server with this

capability is called a "PINT gateway". A PINT gateway appears to a SIP system as a User Agent Server. Notice that a PINT gateway appears to the PINT infrastructure as if it represents a "user", while in fact it really represents an entire telephone network infrastructure that can provide a set of telephone network services.

So the PINT system might appear to an individual PINT client as follows:

```
                           /\/\/\/\/\/\/\            /\/\/\/\/\/\/\/\
___________                \          __/___      ___\_             \
|  PINT   |      PINT      \   PINT  | PINT |     |Exec| Telephone  /
| client  |<-------------->|  server |gatewy|=====|Syst| Network    \
|_________|    protocol    /  cloud  |______|     |____|  Cloud     /
                           \            \            /              \
                           /\/\/\/\/\/\/\            \/\/\/\/\/\/\/\/
```

Figure 1: PINT Functional Architecture

The system of PINT servers is represented as a cloud to emphasise that a single PINT request might pass through a series of location servers, proxy servers, and redirect servers, before finally reaching the correct PINT gateway that can actually process the request by passing it to the Telephone Network Cloud.

The PINT gateway might have a true telephone network interface, or it might be connected via some other protocol or API to an "Executive System" that is capable of invoking services within the telephone cloud.

As an example, within an I.N. (Intelligent Network) system, the PINT gateway might appear to realise the Service Control Gateway Function. In an office environment, it might be a server adjunct to the office PBX, connected to both the office LAN and the office PBX.

The Executive System that lies beyond the PINT gateway is outside the scope of PINT.

3.2. PINT Protocol Architecture

This section explains how SIP and SDP work in combination to convey the information necessary to invoke telephone network sessions.

The following list summarises the extension features used in PINT 1.0. Following on from this the features are considered separately for SDP and then for SIP:

1) Telephony URLs in SDP Contact Fields
2) Refinement of SIP/SDP Telephony URLs
    * Inclusion of private dialling plans

3) Specification of Telephone Service Provider (TSP) and/or
   phone-context URL-parameters
4) Data Objects as session media
4a) Protocol Transport formats to indicate the treatment of the media
   within the GSTN
5) Implicit (Indirect) media streams and opaque arguments
6) In-line data objects using multipart/mime
7) Refinement/Clarification of Opaque arguments passed onwards to
   Executive Systems
   * Framework for Presentation Restriction Indication
   * Framework for Q.763 arguments
8) An extension mechanism for SDP to specify strictures and force
   failure when a recipient does NOT support the specified extensions,
   using "require" headers.
9) Mandatory support for "Warning" headers to give more detailed
   information on request disposition.
10) Mechanism to register interest in the disposition of a requested
   service, and to receive indications on that disposition.

Both PINT and SIP rely on features of MIME[4]. The use of SIP 2.0 is implied by PINT 1.0, and this also implies compliance with version 1.0 of MIME.

3.2.1. SDP operation in PINT

The SDP payload contains a description of the particular telephone network session that the requestor wishes to occur in the GSTN. This information includes such things as the telephone network address (i.e. the "telephone number") of the terminal(s) involved in the call, an indication of the media type to be transported (e.g. audio, text, image or application data), and an indication if the information is to be transported over the telephone network via voice, fax, or pager transport. An indication of the content to be sent to the remote telephone terminal (if there is any) is also included.

SDP is flexible enough to convey these parameters independently. For example, a request to send some text via voice transport will be fulfilled by invoking some text-to-speech-over-the-phone service, and a request to send text via fax will be fulfilled by invoking some text-to-fax service.

The following is a list of PINT 1.0 enhancements and additions to SDP.

a. A new network type "TN" and address types "RFC2543" and "X-..."
   (section 3.4.1)
b. New media types "text", "image", and "application",

new protocol transport keywords "voice", "fax" and "pager" and the associated format types and attribute tags (section 3.4.2)

c. New format specific attributes for included content data (section 3.4.2.4)
d. New attribute tags, used to pass information to the telephone network (section 3.4.3)
e. A new attribute tag "require", used by a client to indicate that some attribute is required to be supported in the server (section 3.4.4)

3.2.2. SIP Operation in PINT

SIP is used to carry the request for telephone service from the PINT client to the PINT gateway, and may include a telephone number if needed for the particular service. The following is a complete list of PINT enhancements and additions to SIP:

f. The multipart MIME payloads (section 3.5.1)
g. Mandatory support for "Warning:" headers (section 3.5.2)
h. The SUBSCRIBE and NOTIFY, and UNSUBSCRIBE requests (section 3.5.3)
i. Require: headers (section 3.5.4)
j. A format for PINT URLS within a PINT request (section 3.5.5)
k. Telephone Network Parameters within PINT URLs (section 3.5.6)

Section 3.5.8 contains remarks about how BYE requests are used within PINT. This is not an extension to baseline SIP; it is included here only for clarification of the semantics when used with telephone network sessions.

3.3. REQUIRED and OPTIONAL elements for PINT compliance

Of these, only the TN network type (with its associated RFC2543 address type) and the "require" attribute MUST be supported by PINT 1.0 clients and servers. In practice, most PINT service requests will use other changes, of which references to Data Objects in requests are most likely to appear in PINT requests.

Each of the other new PINT constructs enables a different function, and a client or server that wishes to enable that particular function MUST do so by the construct specified in this document. For example, building a PINT client and server that provide only the Request-to-Call telephone call service, without support for the other Milestone services, is allowed.

The "Require:" SIP header and the "require" attribute provide a mechanism that can be used by clients and servers to signal their need and/or ability to support specific "new" PINT protocol elements.

It should be noted that many optional features of SIP and SDP make sense as specified in the PINT context. One example is the SDP a=lang: attribute, which can be used to describe the preferred language of the callee. Another example is the use of the "t=" parameter to indicate that the time at which the PINT service is to be invoked. This is the normal use of the "t=" field. A third example is the quality attributes. Any SIP or SDP option or facility is available to PINT clients and servers without change.

Conversely, support for Data Objects within Internet Conference sessions may be useful, even if the aim is not to provide a GSTN service request. In this case, the extensions covering these items may be incorporated into an otherwise "plain" SIP/SDP invitation. Likewise, support for SDP "require" may be useful, as a framework for addition of features to a "traditional" SIP/SDP infrastructure. Again, these may be convenient to incorporate into SIP/SDP implementations that would not be used for PINT service requests. Such additions are beyond the scope of this document, however.

3.4. PINT Extensions to SDP

PINT 1.0 adds to SDP the possibility to describe audio, fax, and pager telephone sessions. It is deliberately designed to hide the underlying technical details and complexity of the telephone network. The only network type defined for PINT is the generic "TN" (Telephone Network). More precise tags such as "ISDN", "GSM", are not defined. Similarly, the transport protocols are designated simply as "fax", "voice", and "pager"; there are no more specific identifiers for the various telephone network voice, fax, or pager protocols. Similarly, the data to be transported are identified only by a MIME content type, such as "text" data, "image" data, or some more general "application" data. An important example of transporting "application" data is the milestone service "Voice Access to Web Content". In this case the data to be transported are pointed to by a URI, the data content type is application/URI, and the transport protocol would be "voice". Some sort of speech-synthesis facility, speaking out to a Phone, will have to be invoked to perform this service.

This section gives details of the new SDP keywords.

3.4.1. Network Type "TN" and Address Type "RFC2543"

The TN ("Telephone Network") network type is used to indicate that the

terminal is connected to a telephone network.

The address types allowed for network type TN are "RFC2543" and private address types, which MUST begin with an "X-".

Address type RFC2543 is followed by a string conforming to a subset of the "telephone-subscriber" BNF specified in figure 4 of SIP [1]). Note that this BNF is NOT identical to the BNF that defines the "phone-number" within the "p=" field of SDP.

Examples:

```
    c= TN  RFC2543  +1-201-406-4090

    c= TN  RFC2543  12014064090
```

A telephone-subscriber string is of one of two types:
global-phone-number or
local-phone-number.
These are distinguished by preceeding a global-phone-number with a "plus" sign ("+"). A global-phone-number is by default to be interpreted as an internationally significant E.164 Number Plan Address, as defined by [6], whilst a local-phone-number is a number specified in the default dialling plan within the context of the recipient PINT Gateway.

An implementation MAY use private addressing types, which can be useful within a local domain. These address types MUST begin with an "X-", and SHOULD contain a domain name after the X-, e.g. "X-mytype.mydomain.com". An example of such a connection line is as follows:

```
      c= TN X-mytype.mydomain.com  A*8-HELEN
```

where "X-mytype.mydomain.com" identifies this private address type, and "A*8-HELEN" is the number in this format. Such a format is defined as an "OtherAddr" in the ABNF of Appendix A. Note that most dialable telephone numbers are expressable as local-phone-numbers within address RFC2543; new address types SHOULD only be used for formats which cannot be so written.

3.4.2. Support for Data Objects within PINT

One significant change over traditional SIP/SDP Internet Conference sessions with PINT is that a PINT service request may refer to a Data Object to be used as source information in that request. For example, a PINT service request may specify a document to be processed as part of a

GSTN service by which a Fax is sent. Similarly, a GSTN service may be take a Web page and result in a vocoder processing that page and speaking the contents over a telephone.

The SDP specification does not have explicit support for reference to or carriage of Data Objects within requests. In order to use SDP for PINT, there is a need to describe such media sessions as "a telephone call to a certain number during which such-and-such an image is sent as a fax".

To support this, two extensions to the session description format are specified. These are some new allowed values for the Media Field, and a description of the "fmtp" parameter when used with the Media Field values (within the context of the Contact Field Network type "TN").

An addition is also made to the SIP message format to allow the inclusion of data objects as sub-parts within the request message itself. The original SDP syntax (from [2]) for media-field is given as:

```
   media-field =         "m=" media space port ["/" integer]
                         space proto 1*(space fmt) CRLF
```

When used within PINT requests, the definition of the sub-fields is expanded slightly. The Media sub-field definition is relaxed to accept all of the discrete "top-level" media types defined in [4]. In the milestone services the discrete type "video" is not used, and the extra types "data" and "control" are likewise not needed. The use of these types is not precluded, but the behaviour expected of a PINT Gateway receiving a request including such a type is not defined here.

The Port sub-field has no meaning in PINT requests as the destination terminals are specified using "TN" addressing, so the value of the port sub-field in PINT requests is normally set to "1". A value of "0" may be used as in SDP to indicate that the terminal is not receiving media. This is useful to indicate that a telephone terminal has gone "on hold" temporarily. Likewise, the optional integer sub-field is not used in PINT.

As mentioned in [2], the Transport Protocol sub-field is specific to the associated Address Type. In the case that the Address Type in the preceeding Contact field is one of those defined for use with the Network Type "TN", the following values are defined for the Transport Protocol sub-field:
"voice", "fax", and "pager".

The interpretation of this sub-field within PINT requests is the treatment or disposition of the resulting GSTN service. Thus, for transport protocol "voice", the intent is that the service will result

in a GSTN voice call, whilst for protocol "fax" the result will be a GSTN fax transmission, and protocol "pager" will result in a pager message being sent.

Note that this sub-field does not necessarily dictate the media type and subtype of any source data; for example, one of the milestone services calls for a textual source to be vocoded and spoken in a resulting telephone service call. The transport protocol value in this case would be "voice", whilst the media type would be "text".

The Fmt sub-field is described in [2] as being transport protocol-specific. When used within PINT requests having one of the above protocol values, this sub-field consists of a list of one or more values, each of which is a defined MIME sub-type of the associated Media sub-field value. The special value "-" is allowed, meaning that there is no MIME sub-type. This sub-field retains (from [2]) its meaning that the list will contain a set of alternative sub-types, with the first being the preferred value.

For experimental purposes and by mutual consent of the sender and recipient, a sub-type value may be specified as an <X-token>, i.e. a character string starting with "X-". The use of such values is discouraged, and if such a value is expected to find common use then it SHOULD be registered with IANA using the standard content type registration process (see Appendix C).

When the Fmt parameter is the single character "-" (a dash), this is interpreted as meaning that a unspecified or default sub-type can be used for this service. Thus, the media field value "m=audio 1 voice -<CRLF>" is taken to mean that a voice call is requested, using whatever audio sub type is deemed appropriate by the Executive System. PINT service is a special case, in that the request comes from the IP network but the service call is provided within the GSTN. Thus the service request will not normally be able to define the particular codec used for the resulting GSTN service call. If such an intent IS required, then the quality attribute may be used (see "Suggested Attributes" section of [2]).

3.4.2.1. Use of fmtp attributes in PINT requests

For each element of the Fmt sub-field, there MUST be a following fmtp attribute. When used within PINT requests, the fmtp attribute has a general structure as defined here:

```
    "a=fmtp:" <subtype> <space> resolution
                             *(<space> resolution)
```

```
                       (<space> ";" 1(<attribute>)
                                    *(<space> <attribute>))
where:
    <resolution> := (<uri-ref> | <opaque-ref> | <sub-part-ref>)
```

A fmtp attribute describes the sources used with a given Fmt entry in the Media field. The entries in a Fmt sub-field are alternatives (with the preferred one first in the list). Each entry will have a matching fmtp attribute. The list of resolutions in a fmtp attribute describes the set of sources that resolve the matching Fmt choice; all elements of this set will be used.

It should be noted that, for use in PINT services, the elements in such a set will be sent as a sequence; it is unlikely that trying to send them in parallel would be successful.

A fmtp attribute can contain a mixture of different kinds of element. Thus an attribute might contain a sub-part-ref indicating included data held in a sub-part of the current message, followed by an opaque-ref referring to some content on the GSTN, followed by a uri-ref pointing to some data held externally on the IP network.

To indicate which form each resolution element takes, each of them starts with its own literal tag. The detailed syntax of each form is described in the following sub-sections.

3.4.2.2. Support for Remote Data Object References in PINT Where data objects stored elsewhere on the IP Network are to be used as sources for processing within a PINT service, they may be referred to using the uri-ref form. This is simply a Uniform Resource Identifier (URI), as described in [9].

Note that the reference SHOULD be an absolute URI, as there may not be enough contextual information for the recipient server to resolve a relative reference; any use of relative references requires some private agreement between the sender and recipient of the message, and SHOULD be avoided unless the sender can be sure that the recipient is the one intended and the reference is unambiguous in context.

This also holds for partial URIs (such as"uri:http://aNode/index.htm") as these will need to be resolved in the context of the eventual recipient of the message.

The general syntax of a reference to an Internet-based external data object in a fmtp line within a PINT session description is:

```
    <uri-ref> := ("uri:" URI-reference)
```

where URI-reference is as defined in Appendix A of [9]

For example:

```
      c= TN RFC2543 +1-201-406-4090
      m= text 1  fax plain
      a=fmtp:plain  uri:ftp://ftp.isi.edu/in-notes/rfc2468.txt
```

or:

```
      c= TN RFC2543 +1-201-406-4090
      m= text 1  fax plain
      a=fmtp:plain
uri:http://www.ietf.org/meetings/glance_minneapolis.txt
```

means get this data object from the Internet and use it as a source for the requested GSTN Fax service.

3.4.2.3. Support for GSTN-based Data Objects in PINT

PINT services may refer to data that are held not on the IP Network but instead within the GSTN. The way in which these items are indicated need have no meaning within the context of the Requestor or the PINT Gateway; the reference is merely some data that may be used by the Executive System to indicate the content intended as part of the request. These data form an opaque reference, in that they are sent "untouched" through the PINT infrastructure.

A reference to some data object held on the GSTN has the general definition:

```
    <opaque-ref> := ("opr:" *uric)
```

where uric is as defined in Appendix A of [9].

For example:

```
      c= TN RFC2543 +1-201-406-4090
      m= text 1  fax plain
      a=fmtp:plain  opr:APPL.123.456
```

means send the data that is indexed ON THE GSTN by the reference value "APPL.123.456" to the fax machine on +1-201-406-4090. The Executive System may also take the Telephone URL held in the To: field of the enclosing SIP message into account when deciding the context to be used for the data object dereference.

Of course, an opaque reference may also be used for other purposes; it

could, for example, be needed to authorise access to a document held on the GSTN rather than being required merely to disambiguate the data object. The purpose to which an opaque reference is put, however, is out of scope for this document. It is merely an indicator carried within a PINT Request.

An opaque reference may have no value in the case where the value to be used is implicit in the rest of the request. For example, suppose some company wishes to use PINT to implement a "fax-back service". In their current implementation, the image(s) to be faxed are entirely defined by the telephone number dialled. Within the PINT request, this telephone number would appear within the "To:" field of the PINT request, and so there is no need for an opaque reference value.

If there are several resolutions for a PINT Service Request, and one of these is an opaque reference with no value, then that opaque reference MUST be included in the attribute line, but with an empty value field.

For example:

```
      c= TN RFC2543 +1-201-406-4090
      m= text 1  fax plain
      a=fmtp:plain  uri:http://www.sun.com/index.html opr:
```

might be used to precede some data to be faxed with a covering note.

In the special case where an opaque reference is the sole resolution of a PINT Service Request, AND that reference needs no value, there is no need for a Fmt list at all; the intent of the service is unambiguous without any further resolution.

For example:

```
      c= TN RFC2543 +1-201-406-4090
      m= text 1  fax -
```

means that there is an implied content stored on the GSTN, and that this is uniquely identified by the combination of SIP To-URI and the Contact field of the session description.

3.4.2.4. Session Description support for included Data Objects

As an alternative to pointing to the data via a URI or an opaque reference to a data item held on the GSTN, it is possible to include the content data within the SIP request itself. This is done by using multipart MIME for the SIP payload. The first MIME part contains the SDP description of the telephone network session to be executed. The other

MIME parts contain the content data to be transported.

Format specific attribute lines within the session description are used to indicate which other MIME part within the request contains the content data. Instead of a URI or opaque reference, the format-specific attribute indicates the Content-ID of the MIME part of the request that contains the actual data, and is defined as:

```
    <sub-part-ref> := ("spr:" Content-ID)
```

where Content-ID is as defined in Appendix A of [3] and in [10]).

For example:

```
      c= TN RFC2543 +1-201-406-4090
      m= text 1  fax plain
      a=fmtp:plain  spr:<Content-ID>
```

The <Content-ID> parameter is the Content-ID of one of the MIME parts inside the message, and this fragment means that the requesting user would like the data object held in the sub-part of this message labelled <Content-ID> to be faxed to the machine at phone number +1-201-406-4090.

See also section 3.5.1 for a discussion on the support needed in the enclosing SIP request for included data objects.

3.4.3. Attribute Tags to pass information into the Telephone Network

It may be desired to include within the PINT request service parameters that can be understood only by some entity in the "Telephone Network Cloud". SDP attribute parameters are used for this purpose. They MAY appear within a particular media description or outside of a media description.

These attributes may also appear as parameters within PINT URLS (see section 3.5.6) as part of a SIP request.

This is necessary so that telephone terminals that require the attributes to be defined can appear within the To: line of a PINT request as well as within PINT session descriptions.

The purpose of these attributes is to allow the client to specify extra context within which a particular telephone number is to be interpreted. There are many reasons why extra context might be necessary to interpret a given telephone number:

a. The telephone number might be reachable in many different ways (such as via competing telephone service providers), and the PINT client wishes to indicate its selection of service provider.
b. The telephone number might be reachable only from a limited number of networks (such as an '800' freephone number).

c. The telephone number might be reachable only within a single telephone network (such as the '152' customer service number of BT). Similarly, the number might be an internal corporate extension reachable only within the PBX.

However, as noted above, it is not usually necessary to use SDP attributes to specify the phone context. URLs such as 152@pint.bt.co.il within the To: and From: headers and/or Request-URI, normally offer sufficient context to resolve telephone numbers.

If the client wishes the request to fail if the attributes are not supported, these attributes SHOULD be used in conjunction with the "require" attribute (section 3.4.4) and the "Require:org.ietf.sdp.require" header (section 3.5.4).

It is not possible to standardise every possible internal telephone network parameter. PINT 1.0 attributes have been chosen for specification because they are common enough that many different PINT systems will want to use them, and therefore interoperability will be increased by having a single specification.

Proprietary attribute "a=" lines, that by definition are not interoperable, may be nonetheless useful when it is necessary to transport some proprietary internal telephone network variables over the IP network, for example to identify the order in which service call legs are to be be made. These private attributes SHOULD BE, however, subject to the same IANA registration procedures mentioned in the SDP specification[2] (see also this Appendix C).

3.4.3.1. The phone-context attribute

An attribute is specified to enable "remote local dialling". This is the service that allows a PINT client to reach a number from far outside the area or network that can usually reach the number. It is useful when the sending or receiving address is only dialable within some local context, which may be remote to the origin of the PINT client.

For example, if Alice wanted to report a problem with her telephone, she might then dial a "network wide" customer care number; within the British Telecom network in the U.K., this is "152". Note that in this case she doesn't dial any trunk prefix - this is the whole dialable number. If dialled from another operator's network, it will not connect to British Telecom's Engineering Enquiries service; and dialling "+44 152" will not normally succeed. Such numbers are called Network-Specific Service Numbers.

Within the telephone network, the "local context" is provided by the physical connection between the subscriber's terminal and the central

office. An analogous association between the PINT client and the PINT server that first receives the request may not exist, which is why it may be necessary to supply this missing "telephone network context". This attribute is defined as follows:

```
a=phone-context: <phone-context-ident>
phone-context-ident     =  network-prefix / private-prefix
```



```
network-prefix          =  intl-network-prefix / local-network-prefix
intl-network-prefix     =  "+" 1*DIGIT
local-network-prefix    =  1*DIGIT
excldigandplus          =  (0x21-0x2d,0x2f,0x40-0x7d))
private-prefix          =  1*excldigandplus 0*uric
```

An intl-network-prefix and local-network-prefix MUST be a bona fide network prefix, and a network-prefix that is an intl-network-prefix MUST begin with an E.164 service code ("country code").

It is possible to register new private-prefixes with IANA so as to avoid collisions. Prefixes that are not so registered MUST begin with an "X-" to indicate their private, non-standard nature (see Appendix C).

Example 1:

```
c= TN    RFC2543  1-800-765-4321
a=phone-context:+972
```

This describes an terminal whose address in Israel (E.164 country code 972) is 1-800-765-4321.

Example 2:

```
c= TN    RFC2543  1-800-765-4321
a=phone-context:+1
```

This describes an terminal whose address in North America (E.164 country code 1) is 1-800-765-4321.

The two telephone terminals described by examples 1 and 2 are different; in fact they are located in different countries.

Example 3:

```
c=TN RFC2543  123
a=phone-context:+97252
```

This describes a terminal whose address when dialled from within the network identified by +97252 is the string "123". It so happens that +97252 defines one of the Israeli cell phone providers, and 123 reaches customer service when dialled within that network.

It may well be useful or necessary to use the SDP "require" parameter in conjunction with the phone-context attribute.

Example 4:

```
c= TN  RFC2543  321
a=phone-context:X-acme.com-23
```


This might describe the telephone terminal that is at extension 321 of PBX number 23 within the acme.com private PBX network. It is expected that such a description would be understandable by the acme.com PINT server that receives the request.

Note that if the PINT server receiving the request is inside the acme.com network, the same terminal might be addressable as follows:

```
c= TN  RFC2543 7-23-321
```

(assuming that "7" is dialled in order to reach the private PBX network from within acme.com)

3.4.3.2. Presentation Restriction attribute

Although it has no affect on the transport of the service request through the IP Network, there may be a requirement to allow originators of a PINT service request to indicate whether or not they wish the "B party" in the resulting service call to be presented with the "A party's" calling telephone number. It is a legal requirement in some jurisdictions that a caller be able to select whether or not their correspondent can find out the calling telephone number (using Automatic Number Indication or Caller Display or Calling Line Identity Presentation equipment). Thus an attribute may be needed to indicate the originator's preference.

Whether or not the default behaviour of the Executive System is to present or not present a party's telephone number to the correspondent GSTN terminal is not specified, and it is not mandatory in all territories for a PINT Gateway or Executive System to act on this attribute. It is, however, defined here for use where there are

regulatory restrictions on GSTN operation, and in that case the Executive System can use it to honour the originator's request.

The attribute is specified as follows:

```
    a=clir:<"true" | "false">
```

This boolean value is needed within the attribute as it may be that the GSTN address is, by default, set to NOT present its identity to correspondents, and the originator wants to do so for this particular call. It is in keeping with the aim of this attribute to allow the originator to specify what treatment they want for the requested service call.

The expected interpretation of this attribute is that, if it is present and the value is "false" then the Calling Line Identity CAN be presented to the correspondent terminal, whilst if it is "true" then it if possible the Executive System is requested to NOT present the Calling Line Identity.

3.4.3.3. ITU-T CalledPartyAddress attributes parameters

These attributes correspond to fields that appear within the ITU-T Q.763 "CalledPartyAddress" field (see [8] ,section 3.9). PINT clients use these attributes in order to specify further parameters relating to Terminal Addresses, in the case when the address indicates a "local-phone-number". In the case that the PINT request contains a reference to a GSTN terminal, the parameters may be required to correctly identify that remote terminal.

The general form of this attribute is:
"a=Q763-<token>((":" <value>) |"")".
Three of the possible elements and their use in SDP attributes are described here. Where other Q763 elements are to be used, then these should be the subject of further specification to define the syntax of the attribute mapping. It is recommended that any such specification maintains the value sets shown in Q.763.

The defined attributes are:

```
a=Q763-nature:  - indicates the "nature of address indicator".
                    The value MAY be any number between 0 and 127.
                    The following values are specified:

                "1" a subscriber number
                "2" unknown
```

"3" a nationally significant number
"4" an internationally significant number

The values have been chosen to coincide with the values in Q.763. Note that other values are possible, according to national rules or future expansion of Q.763.

a=Q763-plan: - indicates the numbering plan to which the address belongs. The value MAY be any number between 0 and 7. The following values are specified:

"1" Telephone numbering plan (ITU-T E.164)
"3" Data numbering plan (ITU-T X.121)
"4" Telex numbering plan (ITU-T F.69)

The values have been chosen to coincide with the values in Q.763. Other values are allowed, according to national rules or future expansion of Q.763.

a=Q763-INN - indicates if routing to the Internal Network Number is allowed. The value MUST be ONE of:

"0" routing to internal network number allowed
"1" routing to internal network number not allowed

The values have been chosen to coincide with the values in Q.763.

Note that it is possible to use a local-phone-number and indicate via attributes that the number is in fact an internationally significant E.164 number. Normally this SHOULD NOT be done; an internationally significant E.164 number is indicated by using a "global-phone-number" for the address string.

3.4.4. The "require" attribute

According to the SDP specification, a PINT server is allowed simply to ignore attribute parameters that it does not understand. In order to force a server to decline a request if it does not understand one of the PINT attributes, a client SHOULD use the "require" attribute, specified as follows:

    a=require:<attribute-list>

where the attribute-list is a comma-separated list of attributes that

appear elsewhere in the session description.

In order to process the request successfully the PINT server must BOTH understand the attribute AND ALSO fulfil the request implied by the presence of the attribute, for each attribute appearing within the attribute-list of the require attribute.

If the server does not recognise the attribute listed, the PINT server MUST return an error status code (such as 420 (Bad Extension) or 400 (Bad Request)), and SHOULD return suitable Warning: lines explaining the problem or an Unsupported: header containing the attribute it does not understand. If the server recognizes the attribute listed, but cannot fulfil the request implied by the presence of the attribute, the request MUST be rejected with a status code of (606 Not Acceptable), along with a suitable Unsupported: header or Warning: line.

The "require" attribute may appear anywhere in the session description, and any number of times, but it MUST appear before the use of the attribute marked as required.

Since the "require" attribute is itself an attribute, the SIP specification allows a server that does not understand the require attribute to ignore it. In order to ensure that the PINT server will comply with the "require" attribute, a PINT client SHOULD include a Require: header with the tag "ietf.org.sdp.require" (section 3.5.4)

Note that the majority of the PINT extensions are "tagged" and these tags can be included in Require strictures. The exception is the use of phone numbers in SDP parts. However, these are defined as a new network and address type, so that a receiving SIP/SDP server should be able to detect whether or not it supports these forms. The default behaviour for any SDP recipient is that it will fail a PINT request if it does not recognise or support the TN and RFC2543 or X-token network and address types, as without the contents being recognised no media session could be created. Thus a separate stricture is not required in this case.

3.5. PINT Extensions to SIP 2.0

PINT requests are SIP requests; Many of the specifications within this document merely explain how to use existing SIP facilities for the purposes of PINT.

3.5.1. Multi-part MIME (sending data along with SIP request)

A PINT request can contain a payload which is multipart MIME. In this

case the first part MUST contain an SDP session description that includes at least one of the format specific attribute tags for "included content data" specified above in section 3.4.3. Subsequent parts contain content data that may be transferred to the requested Telephone Call Service. As discussed earlier, within a single PINT request, some of the data MAY be pointed to by a URI within the request, and some of the data MAY be included within the request.

Where included data is carried within a PINT service request, the Content Type entity header of the enclosing SIP message MUST indicate this. To do so, the media type value within this entity header MUST be set to a value of "multipart". There is a content sub-type that is intended for situations like this in which sub-parts are to be handled together. This is the multipart/related type (defined in [19]), and it's use is recommended.

The enclosed body parts SHOULD include the part-specific Content Type headers as appropriate ("application/sdp" for the first body part holding the session description, with an appropriate content type for each of the subsequent, "included data object" parts). This matches the standard syntax of MIME multipart messages as defined in [4].

For example, in a multipart message where the string "------next-------" is the boundary, the first two parts might be as follows:

```
------next-------
Content-Type: application/sdp
....
c= TN RFC2543 +1-201-406-4090
m= text 1 pager plain
a=fmtp:plain spr:17@mymessage.acme.com

----------next-------
Content-Type: text/plain
Content-ID:  17@mymessage.acme.com

This is the text that is to be paged to +1-201-406-4090

----------next-----------
```


The ability to indicate different alternatives for the content to be transported is useful, even when the alternatives are included within the request. For example, a request to send a short message to a pager might include the message in Unicode [5] and an alternative version of

the same content in text/plain, should the PINT server or telephone network not be able to process the unicode.

PINT clients should be extremely careful when sending included data within a PINT request. Such requests SHOULD be sent via TCP, to avoid fragmentation and to transmit the data reliably. It is possible that the PINT server is a proxy server that will replicate and fork the request, which could be disastrous if the request contains a large amount of application data. PINT proxy servers should be careful not to create many copies of a request with large amounts of data in it. If the client does not know the actual location of the PINT gateway, and is using the SIP location services to find it, and the included data makes the PINT request likely to be transported in several IP datagrams, it is RECOMMENDED that the initial PINT request not include the data object but instead hold a reference to it.

3.5.2. Warning header

A PINT server MUST support the SIP "Warning:" header so that it can signal lack of support for individual PINT features. As an example, suppose the PINT request is to send a jpeg picture to a fax machine, but the server cannot retrieve and/or translate jpeg pictures from the Internet into fax transmissions.

In such a case the server fails the request and includes a Warning such as the following:

```
Warning:  305  pint.acme.com  Incompatible media format:  jpeg
```

SIP servers that do not understand the PINT extensions at all are strongly encouraged to implement Warning: headers to indicate that PINT extensions are not understood.

Also, Warning: headers may be included within NOTIFY requests if it is necessary to notify the client about some condition concerning the invocation of the PINT service (see next).

3.5.3. Mechanism to register interest in the disposition of a PINT service, and to receive indications on that disposition

It can be very useful to find out whether or not a requested service has completed, and if so whether or not it was successful. This is especially true for PINT service, where the person requesting the service is not (necessarily) a party to it, and so may not have an easy way of finding out the disposition of that service. Equally, it may be useful to indicate when the service has changed state, for example when the service call has started.

Arranging a flexible system to provide extensive monitoring and control during a service is non-trivial (see section 6.4 for some issues); PINT 1.0 uses a simple scheme that should nevertheless provide useful information. It is possible to expand the scheme in a "backwards compatible" manner, so if required it can be enhanced at a later date. Such enhancement would be expected to be the subject of a separate document.

The PINT 1.0 status registration and indication scheme uses three new methods; SUBSCRIBE, UNSUBSCRIBE, and NOTIFY. These are used to allow a PINT Requesting entity to register an interest in (or "subscribe" to) the status of a service request, to indicate that a prior interest has lapsed (i.e "unsubscribe" from the status), and for the gateway to return service indications. All of these messages follow the same procedure as used for all the SIP requests other than INVITE; the recipient MUST acknowledge the request with a final response message, otherwise the request will be repeated.

3.5.3.1. Opening a monitoring session with a SUBSCRIBE request

When a SUBSCRIBE request is sent to a PINT Server, it indicates that a user wishes to receive information about the status of a service session. The request identifies the session of interest by including the original session description along with the request, using the SDP global-session-id that forms part of the origin-field to identify the service session uniquely.

The SUBSCRIBE request (like any other SIP request about an ongoing session) is sent to the same server as was sent the original INVITE, or to a server which was specified in the Contact: field within a subsequent response (this might well be the PINT gateway for the session).

Whilst there are situations in which re-use of the Call-ID used in the original INVITE that initiated the session of interest is possible, there are other situations in which it is not. In detail, where the subscription is being made by the user who initiated the original service request, the Call-ID may be used as it will be known to the receiver to refer to a previously established session. However, when the request comes from a user other than the original requesting user, the SUBSCRIBE request constitutes a new SIP call leg, so the Call-ID SHOULD NOT be used; the only common identifier is the origin-field of the session description enclosed within the original service request, and so this MUST be used.

Rather than have two different methods of identifying the "session of interest" the choice is to use the origin-field of the SDP sub-part included both in the original INVITE and in this SUBSCRIBE request.

Note that the request MUST NOT include any sub-parts other than the session description, even if these others were present in the original INVITE request. A server MUST ignore whatever sub-parts are included within a SUBSCRIBE request with the sole exception of the enclosed session description.

The request MAY contain a "Contact:" header, specifying the PINT User Agent Server to which such information should be sent.

In addition, it SHOULD contain an Expires: header, which indicates for how long the PINT Requestor wishes to receive notification of the session status. We refer to the period of time before the expiration of the SUBSCRIBE request as the "subscription period". See section 5.1.4. for security considerations, particularly privacy implications.

A value of 0 within the Expires: header indicates a desire to receive one single immediate response (i.e. the request expires immediately). It is possible for a sequence of monitoring sessions to be opened, exist, and complete, all relating to the same service session.

A successful response to the SUBSCRIBE request includes the session description, according to the Gateway. Normally this will be identical to the last cached response that the Gateway returned to any request concerning the same SDP global session id (see [2], section 6, o= field). The t= line may be altered to indicate the actual start or stop time, however. The Gateway might add an i= line to the session description to indicate such information as how many fax pages were sent. The Gateway SHOULD include an Expires: header indicating how long it is willing to maintain the monitoring session. If this is unacceptable to the PINT Requestor, then it can close the session by sending an immediate UNSUBSCRIBE message (see 3.5.3.3).

In principle, a user might send a SUBSCRIBE request after the telephone network service has completed. This allows, for example, checking up "the morning after" to see if the fax was successfully transmitted. However, a PINT gateway is only required to keep state about a call for as long as it indicated previously in an Expires: header sent within the response to the original INVITE message that triggered the service session, within the response to the SUBSCRIBE message, within the response to any UNSUBSCRIBE message, or within its own UNSUBSCRIBE message (but see section 3.5.8, point 3).

If the Server no longer has a record of the session to which a Requestor has SUBSCRIBEd, it returns "606 Not Acceptable", along with the

appropriate Warning: 307 header indicating that the SDP session ID is no longer valid. This means that a requesting Client that knows that it will want information about the status of a session after the session terminates SHOULD send a SUBSCRIBE request before the session terminates.

3.5.3.2. Sending Status Indications with a NOTIFY request

During the subscription period, the Gateway may, from time to time, send a spontaneous NOTIFY request to the entity indicated in the Contact: header of the "opening" SUBSCRIBE request. Normally this will happen as a result of any change in the status of the service session for which the Requestor has subscribed.

The receiving user agent server MUST acknowledge this by returning a final response (normally a "200 OK"). In this version of the PINT extensions, the Gateway is not required to support redirects (3xx codes), and so may treat them as a failure.

Thus, if the response code class is above 2xx then this may be treated by the Gateway as a failure of the monitoring session, and in that situation it will immediately attempt to close the session (see next).

The NOTIFY request contains the modified session description. For example, the Gateway may be able to indicate a more accurate start or stop time.

The Gateway may include a Warning: header to describe some problem with the invocation of the service, and may indicate within an i= line some information about the telephone network session itself.

Example:

```
NOTIFY  sip:petrack@pager.com SIP/2.0
To: sip:petrack@pager.com
From: sip:R2F.pint.com@service.com
Call-ID: 19971205T234505.56.78@pager.com
CSeq: 4711 SUBSCRIBE
Warning: xxx  fax aborted, will try for the next hour.
Content-Type:application/sdp

c=...
i=3 pages of 5 sent
t=...
```

3.5.3.3. Closing a monitoring session with an UNSUBSCRIBE request

At some point, either the Client's representative User Agent Server or the Gateway may decide to terminate the monitoring session. This is achieved by sending an UNSUBSCRIBE request to the correspondent server. Such a request indicates that the sender intends to close the monitoring session immediately, and, on receipt of the final response from the receiving server, the session is deemed over.

Note that unlike the SUBSCRIBE request, which is never sent by a PINT gateway, an UNSUBSCRIBE request can be sent by a PINT gateway to the User Agent Server to indicate that the monitoring session is closed. (This is analogous to the fact that a gateway never sends an INVITE, although it can send a BYE to indicate that a telephone call has ended.)

If the Gateway initiates closure of the monitoring session by sending an UNSUBSCRIBE message, it SHOULD include an "Expires:" header showing for how much longer after this monitoring session is closed it is willing to store information on the service session. This acts as a minimum time within which the Client can send a new SUBSCRIBE message to open another monitoring session; after the time indicated in the Expires: header the Gateway is free to dispose of any record of the service session, so that subsequent SUBSCRIBE requests can be rejected with a "606" response.

If the subscription period specified by the Client has expired, then the Gateway may send an immediate UNSUBSCRIBE request to the Client's representative User Agent Server. This ensures that the monitoring session always completes with a UNSUBSCRIBE/response exchange, and that the representative User Agent Server can avoid maintaining state in certain circumstances.

3.5.3.4. Timing of SUBSCRIBE requests

As it relies on the Gateway having a copy of the INVITEd session description, the SUBSCRIBE message is limited in when it can be issued. The Gateway must have received the service request to which this monitoring session is to be associated, which from the Client's perspective happens as soon as the Gateway has sent a 1xx response back to it.

However, once this has been done, there is no reason why the Client should not send a monitoring request. It does not have to wait for the final response from the Gateway, and it can certainly send the SUBSCRIBE request before sending the ACK for the Service request final response. Beyond this point, the Client is free to send a SUBSCRIBE request when it decides, unless the Gateway's final response to the initial service

request indicated a short Expires: time.

However, there are good reasons (see 6.4) why it may be appropriate to start a monitoring session immediately before the service is confirmed by the PINT Client sending an ACK. At this point the Gateway will have decided whether or not it can handle the service request, but will not have passed the request on to the Executive System. It is therefore in a good position to ask the Executive System to enable monitoring when it sends the service request onwards. In practical implementations, it is likely that more information on transient service status will be available if this is indicated as being important BEFORE or AS the service execution phase starts; once execution has begun the level of information that can be returned may be difficult to change.

Thus, whilst it is free to send a SUBSCRIBE request at any point after receiving an Interim response from the Gateway to its service request, it is recommended that the Client should send such a monitoring request immediately prior to sending an ACK message confirming the service if it is interested in transient service status messages.

3.5.4. The "Require:" header for PINT

PINT clients use the Require: header to signal to the PINT server that a certain PINT extension of SIP is required. PINT 1.0 defines two strings that can go into the Require header:

```
org.ietf.sip.subscribe  -- the server can fulfill SUBSCRIBE requests
                           and associated methods (see section 3.5.3)

org.ietf.sdp.require    -- the PINT server (or the SDP parser associated
                           to it) understands the "require" attribute
                           defined in (section 3.4.4)
```

Example:

```
      Require:org.ietf.sip.subscribe,org.ietf.sdp.require
```

A client SHOULD only include a Require: header where it truly requires the server to reject the request if the option is not supported.

3.5.5. PINT URLs within PINT requests

Normally the hostnames and domain names that appear in the PINT URLs are the internal affair of each individual PINT system. A client uses the appropriate SDP payload to indicate the particular service it wishes to invoke; it is not necessary to use a particular URL to identify the

service.

A PINT URL is used in two different ways within PINT requests: within the Request-URI, and within the To: and From: headers. Use within the Request-URI requires clarification in order to ensure smooth interworking with the Telephone Network serviced by the PINT infrastructure, and this is covered next.

3.5.5.1. PINT URLS within Request-URIs

There are some occasions when it may be useful to indicate service information within the URL in a standardized way:

a. it may not be possible to use SDP information to route the request if it is encrypted;
b. it allows implementation that make use of I.N. "service indicators";
c. It enables multiple competing PINT gateways to REGISTER with a single "broker" server (proxy or redirect) (see section 6.3)

For these reasons, the following conventions for URLs are offered for use in PINT requests:

1. The user portion of a sip URL indicates the service to be requested. At present the following services are defined:

```
R2C   (for Request-to-Call)
R2F   (for Request-to-Fax)
R2HC  (for Request-to-Hear-Content)
```

The user portions "R2C", "R2F", and "R2HC" are reserved for the PINT milestone services. Other user portions MUST be used in case the requested service is not one of the Milestone services. See section 6.2 for some related considerations concerning registrations by competing PINT systems to a single PINT proxy server acting as a service broker.

2. The host portion of a sip URL contains the domain name of the PINT service provider.

3. A new url-parameter is defined to be "tsp" (for "telephone service provider"). This can be used to indicate the actual telephone network provider to be used to fulfil the PINT request.

Thus, for example:-

```
INVITE sip:R2C@pint.pintservice.com SIP/2.0
INVITE sip:R2F@pint.pintservice.com;tsp=telco.com SIP/2.0
INVITE sip:R2HC@pint.mycom.com;tsp=pbx23.mycom.com SIP/2.0
INVITE sip:13@pint.telco.com SIP/2.0
```

3.5.6. Telephony Network Parameters within PINT URLs

Any legal SIP URL can appear as a PINT URL within the Request-URI or To: header of a PINT request. But if the address is a telephone address, we indicated in section 3.4.3 that it may be necessary to include more information in order correctly to identify the remote telephone terminal or service. PINT clients MAY include these attribute tags within PINT URLs if they are necessary or a useful complement to the telephone number within the SIP URL. These attribute tags MUST be included as URL parameters as defined in [1] (i.e. in the semi-colon separated manner).

The following is an example of a PINT URL containing extra attribute tags:

sip:+9725228808@pint.br.com;user=phone;require=Q763-plan;a=Q763-plan:4

As we noted in section 3.4.3, these extra attribute parameters will not normally be needed within a URL, because there is a great deal of context available to the help the server interpret the phone number correctly. In particular, there is the SIP URL within the To: header, and there is also the Request-URI. In most cases this provides sufficient information for the telephone network.

The SDP attributes defined in section 3 above will normally only be used when they are needed to supply necessary context to identify a telephone terminal.

3.5.7. REGISTER requests within PINT

A PINT gateway is a SIP user agent server. A User Agent Server uses the REGISTER request to tell a proxy or redirect server that it is available to "receive calls" (i.e. to service requests). Thus a PINT Gateway registers with a proxy or redirect server the service that is accessible via itself, whilst in SIP, a user is registering his/her presence at a particular SIP Server.

There may be competing PINT servers that can offer the same PINT service trying to register at a single PINT server. The PINT server might act as a "broker" among the various PINT gateways that can fulfil a request. A format for PINT URLs was specified in section 3.5.5 that enables independent PINT systems to REGISTER an offer to provide the same service. The registrar can apply its own mechanisms and policies to decide how to respond to INVITEs from clients seeking service (See section 6.3 for some possible deployment options). There is no change between SIP and PINT REGISTER semantics or syntax.

Of course, the information in the PINT URLs within the REGISTER request may not be sufficient to completely define the service that a gateway

can offer. The use of SIP and SDP within PINT REGISTER requests to enable a gateway to specify in more detail the services it can offer is the subject of future study.

3.5.8. BYE Requests in PINT

The semantics of BYE requests within PINT requires some extra precision. One issue concerns conferences that "cannot be left", and the other concerns keeping call state after the BYE.

The BYE request [1] is normally used to indicate that the originating entity no longer wishes to be involved in the specified call. The request terminates the call and the media session. Applying this model to PINT, if a PINT client makes a request that results in invocation of a telephone call from A to B, a BYE request from the client, if accepted, should result in a termination of the phone call.

One might expect this to be the case if the telephone call has not started when the BYE request is received. For example, if a request to fax is sent with a t= line indicating that the fax is to be sent tomorrow at 4 AM, the requestor might wish to cancel the request before the specified time.

However, even if the call has yet to start, it may not be possible to terminate the media session on the telephone system side. For example, the fax call may be in progress when the BYE arrives, and perhaps it is just not possible to cancel the fax in session. Another possibility is that the entire telephone-side service might be completed before the BYE is received. In the above Request-to-Fax example, the BYE might be sent the following morning, and the entire fax has been sent before the BYE was received. It is too late to send the BYE.

In the case where the telephone network cannot terminate the call, the server MUST return a "606 Not Acceptable" response to the BYE, along with a session description that indicates the telephone network session that is causing the problem.

Thus, in PINT, a "Not Acceptable" response MAY be returned both to INVITE and BYE requests. It indicates that some aspect of the session description makes the request unacceptable.

By allowing a server to return a "Not Acceptable" response to BYE requests, we are not changing its semantics, just enlarging its use.

A combination of Warning: headers and i= lines within the session

description can be used to indicate the precise nature of the problem.

Example:

```
SIP/2.0 606 Not Acceptable
From: ...
To: .......
.....
Warning: 399 pint.mycom.com Fax in progress, service cannot be
   aborted
Content-Type: application/sdp
Content-Length: ...
```



```
v=0
...
...
i=3 of 5 pages sent OK
c=TN  RFC2543  +12014064090
m=image 1 fax tif
a=fmtp:tif uri:http://tifsRus.com/yyyyyy.tif
```

Note that the server might return an updated session description within a successful response to a BYE as well. This can be used, for example, to indicate the actual start times and stop times of the telephone session, or how many pages were sent in the fax transmission.

The second issue concerns how long must a server keep call state after receiving a BYE. A question arises because other clients might still wish to send queries about the telephone network session that was the subject of the PINT transaction. Ordinary SIP semantics have three important implications for this situation:

1. A BYE indicates that the requesting client will clear out all call state as soon as it receives a successful response. A client SHOULD NOT send a SUBSCRIBE request after it has sent a BYE.

2. A server may return an Expires: header within a successful response to a BYE request. This indicates for how long the server will retain session state about the telephone network session. At any point during this time, a client may send a SUBSCRIBE request to the server to learn about the session state (although as explained in the previous paragraph, a client that has sent a BYE will not normally send a SUBSCRIBE).

3. When engaged in a SUBSCRIBE/NOTIFY monitoring session, PINT servers that send UNSUBSCRIBE to a URL listed in the Contact: header of a client

request SHOULD not clear session state until after the successful response to the UNSUBSCRIBE message is received. For example, it may be that the requesting client host is turned off (or in a low power mode) when the telephone service is executed (and is therefore not available at the location previously specified in the Contact: attribute) to receive the PINT server's UNSUBSCRIBE. Of course, it is possible that the UNSUBSCRIBE request will simply time out.

4. Examples of PINT Requests and Responses

4.1. A request to a call center from an anonymous user to receive a phone call.

```
C->S: INVITE  sip:R2C@pint.mailorder.com  SIP/2.0
      Via: SIP/2.0/UDP 169.130.12.5
      From: sip:anon-1827631872@chinet.net
      To: sip:+1-201-456-7890@iron.org;user=phone
      Call-ID: 19971205T234505.56.78@pager.com
      CSeq: 4711 INVITE
      Subject: Sale on Ironing Boards
      Content-type: application/sdp
      Content-Length: 174
```



```
      v=0
      o=- 2353687637 2353687637 IN IP4 128.3.4.5
      s=R2C
      i=Ironing Board Promotion
      e=anon-1827631872@chinet.net
      t=2353687637 0
      m=audio 1  voice -
      c=TN  RFC2543  +1-201-406-4090
```

In this example, the context that is required to interpret the To: address as a telephone number is not given explicitly; it is implicitly known to the R2C@pint.mailorder.com server. But the telephone of the person who wishes to receive the call is explicitly identified as an internationally significant E.164 number that falls within the North American numbering plan (because of the "+1" within the c= line).

4.2. A request from a non anonymous customer (John Jones) to receive a phone call from a particular sales agent (Mary James) concerning the defective ironing board that was purchased

```
C->S: INVITE  sip:marketing@pint.mailorder.com  SIP/2.0
      Via: SIP/2.0/UDP 169.130.12.5
```

```
       From: sip:john.jones.3@chinet.net
       To: sip:mary.james@mailorder.com
       Call-ID: 19971205T234505.56.78@pager.com
       CSeq: 4712 INVITE
       Subject: Defective Ironing Board - want refund
       Content-type: application/sdp
       Content-Length: 150

       v=0
       o=- 2353687640 2353687640 IN IP4 128.3.4.5
       s=marketing
       e=john.jones.3@chinet.net
       c= TN RFC2543  +1-201-406-4090
       t=2353687640 0
       m=audio 1  voice -
```

The To: line might include the Mary James's phone number instead of a email-like address. An implementation that cannot accept email-like URLs in the "To:" header must decline the request with a 606 Not Acceptable. Note that the sending PINT client "knows" that the PINT Gateway contacted with the "marketing@pint.mailorder.com" Request-URI is capable of processing the client request as expected. (see 3.5.5.1 for a discussion on this).

Note also that such a telephone call service could be implemented on the phone side with different details. For example, it might be that first the agent's phone rings, and then the customer's phone rings, or it might be that first the customer's phone rings and he hears silly music until the agent comes on line. If necessary, such service parameter details might be indicated in "a=" attribute lines within the session description. The specification of such attribute lines for service consistency is beyond the scope of the PINT 1.0 specifications.

4.3. A request from the same user to get a fax back on how to assemble the Ironing Board

```
C->S: INVITE  sip:faxback@pint.mailorder.com  SIP/2.0
       Via: SIP/2.0/UDP 169.130.12.5
       From: sip:john.jones.3@chinet.net
       To: sip:1-800-3292225K@steam.edu;user=phone;phone-context=+1
       Call-ID: 19971205T234505.66.79@chinet.net
       CSeq: 4713 INVITE
       Content-type: application/sdp
       Content-Length: 218
```

```
v=0
o=- 2353687660 2353687660 IN IP4 128.3.4.5
s=faxback
e=john.jones.3@chinet.net
t=2353687660 0
m=application 1 fax URI
c=TN  RFC2543  1-201-406-4091
a=fmtp:URI uri:http://localstore/Products/IroningBoards/2344.html
```

In this example, the fax to be sent is stored on some local server (localstore), whose name may be only resolvable, or that may only be reachable, from within the IP network on which the PINT server sits. The phone number to be dialled is a "local phone number" as well. There is no "phone-context" attribute, so the context (in this case, for which nation the number is "nationally significant") must be supplied by the faxback@pint.mailorder.com PINT server.

If the server that receives it does not understand the number, it SHOULD decline the request and include a "Network Address Not Understood" warning. Note that no "require" attribute was used here, since it is very likely that the request can be serviced even by a server that does not support the "require" attribute.

4.4. A request from same user to have that same information read out over the phone

```
C->S: INVITE  sip:faxback@pint.mailorder.com  SIP/2.0
      Via: SIP/2.0/UDP 169.130.12.5
      From: sip:john.jones.3@chinet.net
      To: sip:1-800-3292225@steam.edu;user=phone;phone-context=+1
      Call-ID: 19971205T234505.66.79@chinet.net
      CSeq: 4713 INVITE
      Content-type: application/sdp
      Content-Length: 220

      v=0
      o=- 2353687660 2353687660 IN IP4 128.3.4.5
      s=faxback
      e=john.jones.3@chinet.net
      t=2353687660 0
      m=application 1 voice URI
      c=TN  RFC2543  1-201-406-4090
      a=fmtp:URI uri:http://localstore/Products/IroningBoards/2344.html
```


4.5. A request to send an included text page to a friend's pager.
In this example, the text to be paged out is included in the request.

```
C->S: INVITE  sip:R2F@pint.pager.com  SIP/2.0
      Via: SIP/2.0/UDP 169.130.12.5
      From: sip:scott.petrack@chinet.net
      To: sip:R2F@pint.pager.com
      Call-ID: 19974505.66.79@chinet.net
      CSeq: 4714 INVITE
      Content-Type: multipart/related; boundary=--next

      ----next
      Content-Type: application/sdp
      Content-Length: 236
      v=0
      o=- 2353687680 2353687680 IN IP4 128.3.4.5
      s=R2F
      e=scott.petrack@chinet.net
      t=2353687680 0
      m=text 1 pager plain
      c= TN  RFC2543  +972-9-956-1867
      a=fmtp:plain spr:2@53655768


      ----next
      Content-Type: text/plain
      Content-ID: 2@53655768
      Content-Length:50

      Hi Joe! Please call me asap at 555-1234.

      ----next--
```

4.6. A request to send an image as a fax to phone number +972-9-956-1867

```
C->S: INVITE  sip:faxserver@pint.vocaltec.com  SIP/2.0
      Via: SIP/2.0/UDP 169.130.12.5
      From: sip:scott.petrack@chinet.net
      To: sip:faxserver@pint.vocaltec.com
      Call-ID: 19971205T234505.66.79@chinet.net
      CSeq: 4715 INVITE
      Content-type: application/sdp
      Content-Length: 267

      v=0
      o=- 2353687700 2353687700 IN IP4 128.3.4.5
      s=faxserver
      e=scott.petrack@chinet.net
      t=2353687700 0
      m=image  1 fax  tif gif
      c= TN  RFC2543  +972-9-956-1867
      a=fmtp:tif  uri:http://petrack/images/tif/picture1.tif
      a=fmtp:gif  uri:http://petrack/images/gif/picture1.gif
```

The image is available as tif or as gif. The tif is the preferred format. Note that the http server where the pictures reside is local, and the PINT server is also local (because it can resolve machine name "petrack")

4.7. A request to read out over the phone two pieces of content in sequence.
First some included text is read out by text-to-speech. Then some text that is stored at some URI on the internet is read out.

```
C->S: INVITE  sip:R2HC@pint.acme.com  SIP/2.0
      Via: SIP/2.0/UDP 169.130.12.5
      From: sip:scott.petrack@chinet.net
      To: sip:R2HC@pint.acme.com
      Call-ID: 19974505.66.79@chinet.net
      CSeq: 4716 INVITE
      Content-Type: multipart/related; boundary=next

      --next
      Content-Type: application/sdp
      Content-Length: 316
      v=0
      o=- 2353687720 2353687720 IN IP4 128.3.4.5
      s=R2HC
      e=scott.petrack@chinet.net

      c= TN  RFC2543  +1-201-406-4091
      t=2353687720 0
      m=text  1  voice  plain
      a=fmtp:plain   spr:2@53655768
      m=text  1 voice plain
      a=fmtp:plain  uri:http://www.your.com/texts/stuff.doc

      --next
      Content-Type: text/plain
      Content-ID: 2@53655768
      Content-Length: 172

      Hello!! I am about to read out to you the document you
      requested, "uri:http://www.your.com/texts/stuff.doc".
      We hope you like acme.com's new speech synthesis server.
      --next--
```

4.8. Request for the prices for ISDN to be sent to my fax machine

```
INVITE sip:R2FB@pint.bt.co.uk  SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
To: sip:0345-12347-01@pint.bt.co.uk;user=phone;phone-context=+44
From: sip:hank.wangford@newts.demon.co.uk
Call-ID: 19981204T201505.56.78@demon.co.uk
CSeq: 4716 INVITE
Subject: Price List
Content-type: application/sdp
Content-Length: 169
```



```
v=0
o=- 2353687740 2353687740 IN IP4 128.3.4.5
s=R2FB
i=ISDN Price List
e=hank.wangford@newts.demon.co.uk
t=2353687740 0
m=text 1  fax -
c=TN  RFC2543  +44-1794-8331010
```

4.9. Request for a callback

```
INVITE sip:R2C@pint.bt.co.uk  SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
To: sip:0345-123456@pint.bt.co.uk;user=phone;phone-context=+44
From: sip:hank.wangford@newts.demon.co.uk
Call-ID: 19981204T234505.56.78@demon.co.uk
CSeq: 4717 INVITE
Subject: It costs HOW much?
Content-type: application/sdp
Content-Length: 176

v=0
o=- 2353687760 2353687760 IN IP4 128.3.4.5
s=R2C
i=ISDN pre-sales query
e=hank.wangford@newts.demon.co.uk
c=TN  RFC2543  +44-1794-8331013
t=2353687760 0
m=audio 1  voice -
```

4.10.Sending a set of information in response to an enquiry

```
INVITE sip:R2FB@pint.bt.co.uk  SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
To: sip:0345-12347-01@pint.bt.co.uk;user=phone;phone-context=+44
From: sip:colin.masterton@sales.hh.bt.co.uk
```

```
Call-ID: 19981205T234505.56.78@sales.hh.bt.co.uk
CSeq: 1147 INVITE
Subject: Price Info, as requested
Content-Type: multipart/related; boundary=next

--next
Content-type: application/sdp
Content-Length: 325
v=0
o=- 2353687780 2353687780 IN IP4 128.3.4.5
s=R2FB
i=Your documents
e=colin.masterton@sales.hh.bt.co.uk
t=2353687780 0
m=application 1  fax octet-stream
c=TN  RFC2543  +44-1794-8331010
a=fmtp:octet-stream uri:http://www.bt.co.uk/imgs/pipr.gif opr:
  spr:2@53655768
```



```
--next
Content-Type: text/plain
Content-ID: 2@53655768
Content-Length: 352

Dear Sir,
  Thank you for your enquiry. I have checked availability in your
area, and we can provide service to your cottage. I enclose a
quote for the costs of installation, together with the ongoing
rental costs for the line. If you want to proceed with this,
please quote job reference isdn/hh/123.45.9901.
Yours Sincerely,
   Colin Masterton
--next--
```

Note that the "implicit" faxback content is given by an EMPTY opaque reference in the middle of the fmtp line in this example.

4.11.Sportsline "headlines" message sent to your phone/pager/fax

(i) phone

```
      INVITE sip:R2FB@pint.wwos.skynet.com  SIP/2.0
      Via: SIP/2.0/UDP 169.130.12.5
      To:
sip:1-900-123-456-7@wwos.skynet.com;user=phone;phone-context=+1
      From: sip:fred.football.fan@skynet.com
      Call-ID: 19971205T234505.56.78@chinet.net
```

```
      CSeq: 4721 INVITE
      Subject: Wonderful World Of Sports NFL Final Scores
      Content-type: application/sdp
      Content-Length: 220

      v=0
      o=- 2353687800 2353687800 IN IP4 128.3.4.5
      s=R2FB
      i=NFL Final Scores
      e=fred.football.fan@skynet.com
      c=TN  RFC2543 +44-1794-8331013
      t=2353687800 0
      m=audio 1 voice x-pay
      a=fmtp:x-pay opr:mci.com/md5:<crypto signature>
```

(ii) fax

```
      INVITE sip:R2FB@pint.wwos.skynet.com  SIP/2.0
      Via: SIP/2.0/UDP 169.130.12.5
      To: sip:1-900-123-456-7@wwos.skynet.com;user=phone;
          phone-context=+1
      From: sip:fred.football.fan@skynet.com
      Call-ID: 19971205T234505.56.78@chinet.net
      CSeq: 4722 INVITE
      Subject: Wonderful World Of Sports NFL Final Scores
      Content-type: application/sdp
      Content-Length: 217
```



```
      v=0
      o=- 2353687820 2353687820 IN IP4 128.3.4.5
      s=R2FB
      i=NFL Final Scores
      e=fred.football.fan@skynet.com
      c=TN  RFC2543 +44-1794-8331010
      t=2353687820 0
      m=text 1 fax x-pay
      a=fmtp:x-pay opr:mci.com/md5:<crypto signature>
```

(iii) pager

```
      INVITE sip:R2FB@pint.wwos.skynet.com  SIP/2.0
      Via: SIP/2.0/UDP 169.130.12.5
      To: sip:1-900-123-456-7@wwos.skynet.com;user=phone;
          phone-context=+1
      From: sip:fred.football.fan@skynet.com
      Call-ID: 19971205T234505.56.78@chinet.net
      CSeq: 4723 INVITE
```

```
Subject: Wonderful World Of Sports NFL Final Scores
Content-type: application/sdp
Content-Length: 219

v=0
o=- 2353687840 2353687840 IN IP4 128.3.4.5
s=R2FB
i=NFL Final Scores
e=fred.football.fan@skynet.com
c=TN  RFC2543 +44-1794-8331015
t=2353687840 0
m=text 1 pager x-pay
a=fmtp:x-pay opr:mci.com/md5:<crypto signature>
```

Note that these are all VERY similar.

4.12.Automatically giving someone a fax copy of your phone bill

```
INVITE sip:BillsRUs@pint.sprint.com SIP/2.0
Via: SIP/2.0/UDP 169.130.12.5
To: sip:+1-555-888-1234@fbi.gov;user=phone
From: sip:agent.mulder@fbi.gov
Call-ID: 19991231T234505.56.78@fbi.gov
CSeq: 911 INVITE
Subject: Itemised Bill for January 98
Content-type: application/sdp
Content-Length: 247
```



```
v=0
o=- 2353687860 2353687860 IN IP4 128.3.4.5
s=BillsRUs
i=Joe Pendleton's Phone Bill
e=agent.mulder@fbi.gov
c=TN  RFC2543  +1-202-833-1010
t=2353687860 0
m=text 1  fax x-files-id
a=fmtp:x-files-id opr:fbi.gov/jdcn-123@45:3des;base64,<signature>
```

Note: in this case the opaque reference is a collection of data used to convince the Executive System that the requester has the right to get this information, rather than selecting the particular content (the A party in the To: field of the SIP "wrapper" does that alone).

5. Security Considerations

5.1. Basic Principles for PINT Use

A PINT Gateway, and the Executive System(s) with which that Gateway is associated, exist to provide service to PINT Requestors. The aim of the PINT protocol is to pass requests from those users on to a PINT Gateway so an associated Executive System can service those requests.

5.1.1. Responsibility for service requests

The facility of making a GSTN-based call to numbers specified in the PINT request, however, comes with some risks. The request can specify an incorrect telephone of fax number. It is also possible that the Requestor has purposely entered the telephone number of an innocent third party. Finally, the request may have been intercepted on its way through any intervening PINT or SIP infrastructure, and the request may have been altered.

In any of these cases, the result may be that a call is placed incorrectly. Where there is intent or negligence, this may be construed as harrasment of the person incorrectly receiving the call. Whilst the regulatory framework for misuse of Internet connections differs throughout the world and is not always mature, the rules under which GSTN calls are made are much more settled. Someone may be liable for mistaken or incorrect calls.

Understandably, the GSTN Operators would prefer that this someone is not them, so they will need to ensure that any PINT Gateway and Executive System combination does not generate incorrect calls through some error in the Gateway or Executive system implementation or GSTN-internal communications fault. Equally, it is important that the Operator can show that they act only on requests that they have good reason to believe are correct. This means that the Gateway must not pass on requests unless it is sure that they have not been corrupted in transit from the Requestor.

If a request can be shown to have come from a particular Requestor and to have been acted on in good faith by the PINT service provider, then responsibility for making requests may well fall to the Requestor rather than the Operator who executed these requests.

Finally, it may be important for the PINT service provider to be able to show that they act only on requests for which they have some degree of assurance of origin. In many jurisdictions, it is a requirement on GSTN

Operators that they place calls only when they can, if required, identify the parties to the call (such as when required to carry out a Malicious Call Trace). It is at least likely that the provider of PINT services will have a similar responsibility placed on them.

It follows that the PINT service provider may require that the identity of the Requestor be confirmed. If such confirmation is not available, then they may be forced (or choose) not to provide service. This identification may require personal authentication of the Requesting User.

5.1.2. Authority to make requests

Where GSTN resources are used to provide a PINT service, it is at least possible that someone will have to pay for it. This person may not be the Requestor, as, for example, in the case of existing GSTN split-charging services like free phone in which the recipient of a call rather than the originator is responsible for the call cost.

This is not, of course, the only possibility; for example, PINT service may be provided on a subscription basis, and there are a number of other models. However, whichever model is chosen, there may be a requirement that the authority of a Requestor to make a PINT request is confirmed.

If such confirmation is not available, then, again, the PINT Gateway and associated Executive System may choose not to provide service.

5.1.3. Privacy

Even if the identity of the Requesting User and the Authority under which they make their request is known, there remains the possibility that the request is either corrupted, maliciously altered, or even replaced whilst in transit between the Requestor and the PINT Gateway.

Similarly, information on the Authority under which a request is made may well be carried within that request. This can be sensitive information, as an eavesdropper might steal this and use it within their own requests. Such authority SHOULD be treated as if it were financial information (such as a credit card number or PIN).

The data authorizing a Requesting User to make a PINT request should be known only to them and the service provider. However, this information may be in a form that does not match the schemes normally used within the Internet. For example, X.509 certificates[14] are commonly used for secured transactions on the Internet both in the IP Security Architecture[12] and in the TLS protocol[13], but the GSTN provider may only store an account code and PIN (i.e. a fixed string of numbers).

A Requesting User has a reasonable expectation that their requests for service are confidential. For some PINT services, no content is carried over the Internet; however, the telephone or fax numbers of the parties to a resulting service calls may be considered sensitive. As a result, it is likely that the Requestor (and their PINT service provider) will require that any request that is sent across the Internet be protected against eavesdroppers; in short, the requests SHOULD to be encrypted.

5.1.4. Privacy Implications of SUBSCRIBE/NOTIFY

Some special considerations relate to monitoring sessions using the SUBSCRIBE and NOTIFY messages. The SUBSCRIBE message that is used to register an interest in the disposition of a PINT service transaction uses the original Session Description carried in the related INVITE message. This current specification does not restrict the source of such a SUBSCRIBE message, so it is possible for an eavesdropper to capture an unprotected session description and use this in a subsequent SUBSCRIBE request. In this way it is possible to find out details on that transaction that may well be considered sensitive.

The initial solution to this risk is to recommend that a session description that may be used within a subsequent SUBSCRIBE message SHOULD be protected.

However, there is a further risk; if the origin-field used is "guessable" then it might be possible for an attacker to reconstruct the session description and use this reconstruction within a SUBSCRIBE message.

SDP (see section 6 of [2], "o=" field) does not specify the mechansim used to generate the sess-id field, and suggests that a method based on timestamps produced by Network Time Protocol [16] can be used. This is sufficient to guarantee uniqueness, but may allow the value to be guessed, particularly if other unprotected requests from the same originator are available.

Thus, to ensure that the session identifier is not guessable the techniques described in section 6.3 of [17] can be used when generating the origin-field for a session description to be used inside a PINT INVITE message. If all requests from (and responses to) a particular PINT requesting entity are protected, then this is not needed. Where such a situation is not assured, AND where session monitoring is supported, then a method by which an origin-field within a session description is not guessable SHOULD be used.

5.2. Registration Procedures

Any number of PINT Gateways may register to provide the same service; this is indicated by the Gateways specifying the same "userinfo" part in the To: header field of the REGISTER request. Whilst such ambiguity would be unlikely to occur with the scenarios covered by "core" SIP, it

is very likely for PINT; there could be any number of service providers all willing to support a "Request-To-Fax" service, for example.

Unless a request specifies the Gateway name explicitly, an intervening Proxy that acts on a registration database to which several Gateways have all registered is in a position to select from the registrands using whatever algorithm it chooses; in principle, any Gateway that has registered as "R2F" would be appropriate.

However, this opens up an avenue for attack, and this is one in which a "rogue" Gateway operator stands to make a significant gain. The standard SIP procedure for releasing a registration is to send a REGISTER request with a Contact field having a wildcard value and an expires parameter with a value of 0. It is important that a PINT Registrar uses authentication of the Registrand, as otherwise one PINT service provider would be able to "spoof" another and remove their registration. As this would stop the Proxy passing any requests to that provider, this would both increase requests being sent to the rogue and stop requests going to the victim.

Another variant on this attack would be to register a Gateway using a name that has been registered by another provider; thus a rogue Operator might register its Gateway as "R2C@pint.att.com", thereby hijacking requests.

The solution is the same; all registrations by PINT Gateways MUST be authenticated; this includes both new or apparent replacement registrations, and any cancellation of current registrations. This recommendation is also made in the SIP specification, but for the correct operation of PINT, it is very important indeed.

5.3. Security mechanisms and implications on PINT service

PINT is a set of extensions to SIP[1] and SDP[2], and will use the security procedures described in SIP. There are several implications of this, and these are covered here.

For several of the PINT services, the To: header field of SIP is used to identify one of the parties to the resulting service call. The PINT Request-To-Call service is an example. As mentioned in the SIP specification, this field is used to route SIP messages through an infrastructure of Redirect and Proxy server between the corresponding User Agent Servers, and so cannot be encrypted. This means that, although the majority of personal or sensitive data can be protected whilst in transit, the telephone (or fax) number of one of the parties

to a PINT service call cannot, and will be "visible" to any interception. For the PINT milestone services this may be acceptable, since the caller named in the To: service is typically a "well known" provider address, such as a Call Center.

Another aspect of this is that, even if the Requesting User does not consider the telephone or fax numbers of the parties to a PINT service to be private, those parties might. Where PINT servers have reason to believe this might be the case they SHOULD encrypt the request, even if the Requestor has not done so. This could happen, for example, if a Requesting User within a company placed a PINT request and this was carried via the company's Intranet to their Proxy/firewall and thence over the Internet to a PINT Gateway at another location.

If a request carries data that can be reused by an eavesdropper either to "spoof" the Requestor or to obtain PINT service by inserting the Requestor's authorization token into an eavesdropper's request, then this data MUST be protected. This is particularly important if the authorization token consists of static text (such as an account code and/or PIN).

One approach is to encrypt the whole of the request, using the methods described in the SIP specification. As an alternative, it may be acceptable for the authorization token to be held as an opaque reference (see section 3.4.2.3 and examples 4.11 and 4.12), using some proprietary scheme agreed between the Requestor and the PINT service provider, as long as this is resistant to interception and re-use. Also, it may be that the authorization token cannot be used outside of a request cryptographically signed by the Requestor; if so then this requirement can be relaxed, as in this case the token cannot be re-used by another. However, unless both the Requestor and the Gateway are assured that this is the case, any authorization token MUST be treated as sensitive, and so MUST be encrypted.

A PINT request may contain data within the SDP message body that can be used more efficiently to route that request. For example, it may be that one Gateway and Executive System combination cannot handle a request that specifies one of the parties as a pager, whilst another can. Both gateways may have registered with a PINT/SIP Registrar, and this information may be available to intervening PINT/SIP Proxies. However, if the message body is encrypted, then the request cannot be decoded at the Proxy server, and so Gateway selection based on contained information cannot be made there.

The result is that the Proxy may deliver the request to a Gateway that

cannot handle it; the implication is that a PINT/SIP Proxy SHOULD consider its choice for the appropriate Gateway subject to correction, and, on receiving a 501 or 415 rejection from the first gateway chosen, try another. In this way, the request will succeed if at all possible, even though it may be delayed (and tie up resources in the inappropriate Gateways).

This opens up an interesting avenue for Denial Of Service; sending a valid request that appears to be suitable for a number of different Gateways, and simply occupying those Gateways in decrypting a message requesting a service they cannot provide. As mentioned in section 3.5.5.1, the choice of service name to be passed in the userinfo portion of the SIP Request-URI is flexible, and it is RECOMMENDED that names be chosen that allow a Proxy to select an appropriate Gateway without having to examine the SDP body part. Thus, in the example given here, the service might be called "Request-To-Page" or "R2P" rather than the more general use of "R2F", if there is a possibility of the SDP body part being protected during transit.

A variation on this attack is to provide a request that is syntactically invalid but that, due to the encryption, cannot be detected without expending resources in decoding it. The effects of this form of attack can be minimised in the same way as for any SIP Invitation; the Proxy should detect the 400 rejection returned from the initial Gateway, and not pass the request onwards to another.

Finally, note that the Requesting User may not have a prior relationship with a PINT Gateway, whilst still having a prior relationship with the Operator of the Executive System that fulfils their request. Thus there may be two levels of authentication and authorization; one carried out using the techniques described in the SIP specification (for use between the Requestor and the Gateway), with another being used between the Requesting User or the Requestor and the Executive System.

For example, the Requesting User may have an account with the PINT service provider. That provider might require that requests include this identity before they will be convinced to provide service. In addition, to counter attacks on the request whilst it is in transit across the Internet, the Gateway may require a separate X.509-based certification of the request. These are two separate procedures, and data needed for the former would normally be expected to be held in opaque references inside the SDP body part of the request.

The detailed operation of this mechanism is, by definition, outside the scope of an Internet Protocol, and so must be considered a private

matter. However, one approach to indicating to the Requestor that such "second level" authentication or authorization is required by their Service Provider would be to ask for this inside the textual description carried with a 401 response returned from the PINT Gateway.

5.4. Summary of Security Implications

From the above discussion, PINT always carries data items that are sensitive, and there may be financial considerations as well as the more normal privacy concerns. As a result, the transactions MUST be protected from interception, modification and replay in transit.

PINT is based on SIP and SDP, and can use the security procedures outlined in [1] (sections 13 and 15). However, in the case of PINT, the SIP recommendation that requests and responses MAY be protected is not enough. PINT messages MUST be protected, so PINT Implementations MUST support SIP Security (as described in [1], sections 13 & 15), and be capable of handling such received messages.

In some configurations, PINT Clients, Servers, and Gateways can be sure that they operate using the services of network level security [13], transport layer security [12], or physical security for all communications between them. In these cases messages MAY be exchanged without SIP security, since all traffic is protected already. Clients and servers SHOULD support manual configuration to use such lower layer security facilities.

When using network layer security [13], the Security Policy Database MUST be configured to provide appropriate protection to PINT traffic. When using TLS, a port configured MUST NOT also be configured for non-TLS traffic. When TLS is used, basic authentication MUST be supported, and client-side certificates MAY be supported.

Authentication of the Client making the request is required, however, so if this is not provided by the underlying mechanism used, then it MUST be included within the PINT messages using SIP authentication techniques. In contrast with SIP, PINT requests are often sent to parties with which a prior communications relationship exists (such as a Telephone Carrier). In this case, there may be a shared secret between the client and the PINT Gateway. Such PINT systems MAY use authentication based on shared secrets, with HTTP "basic authentication". When this is done, the message integrity and privacy must be guaranteed by some lower layer mechanism.

There are implications on the operation of PINT here though. If a PINT

proxy or redirect server is used, then it must be able to examine the contents of the IP datagrams carried. It follows that an end-to-end approach using network-layer security between the PINT Client and a PINT Gateway precludes the use of an intervening proxy; communication between the Client and Gateway is carried via a tunnel to which any intervening entity cannot gain access, even if the IP datagrams are carried via this node. Conversely, if a "hop-by-hop" approach is used, then any intervening PINT proxies (or redirect servers) are, by implication, trusted entities.

However, if there is any doubt that there is an underlying network or transport layer security association in place, then the players in a PINT protocol exchange MUST use encryption and authentication techniques within the protocol itself. The techniques described in section 15 of RFC2543 MUST be used, unless there is an alternative protection scheme that is agreed between the parties. In either case, the content of any message body (or bodies) carried within a PINT request or response MUST be protected; this has implications on the options for routing requests via Proxies (see 5.3).

Using SIP techniques for protection, the Request-URI and To: fields headers within PINT requests cannot be protected. In the baseline PINT services these fields may contain sensitive information. This is a consideration, and if these data ARE considered sensitive, then this will preclude the sole use of SIP techniques; in such a situation, transport [12] or network layer [13] protection mechanisms MUST be used.

As a final point, this choice will in turn have an influence on the choice of transport layer protocol that can be used; if a TLS association is available between two nodes, then TCP will have to be used. This is different from the default behaviour of SIP (try UDP, then try TCP if that fails).

6. Deployment considerations and the Relationship PINT to I.N. (Informative)

6.1. Web Front End to PINT Infrastructure

It is possible that some other protocol may be used to communicate a Requesting User's requirements. Due to the high numbers of available Web Browsers and servers it seems likely that some PINT systems will use HTML/HTTP as a "front end". In this scenario, HTTP will be used over a

connection from the Requesting User's Web Browser (WC) to an Intermediate Web Server (WS). This will be closely associated with a PINT Client (using some unspecified mechanism to transfer the data from the Web Server to the PINT Client). The PINT Client will represent the Requesting User to the PINT Gateway, and thus to the Executive System that carries out the required action.

```
 [WC]------[WS]
           [PC]
             \
              \
             [PG]
             [XS]
```

Figure 2: Basic "Web-fronted" Configuration

6.2. Redirects to Multiple Gateways

It is quite possible that a given PINT Gateway is associated with an Executive System (or systems) that can connect to the GSTN at different places. Equally, if there is a chain of PINT Servers, then each of these intermediate or proxy servers (PP) may be able to route PINT requests to Executive Systems that connect at specific points to the GSTN. The result of this is that there may be more than one PINT Gateway or Executive System that can deal with a given request. The mechanisms by which the choice on where to deliver a request are outside the scope of this document.


```
 [WC]------[WS]                    [WC]------[WS]
           [PC]                              [PC]
             \                                 \
              \                                 \
             [PG]                              [PP]
    .........[XS].........                     /  \
    :                    :                    /    \
                                          [PG]    [PG]
                                          [XS]    [XS]
```

Figure 3: Multiple Access Configurations

However, there do seem to be two approaches. Either a Server that acts as a proxy or redirect will select the appropriate Gateway itself and will cause the request to be sent on accordingly, or a list of possible

Locations will be returned to the Requesting User from which they can select their choice.

In SIP, the implication is that, if a proxy cannot resolve to a single unique match for a request destination, then a response containing a list of the choices should be returned to the Requesting User for selection. This is not too likely a scenario within the normal use of SIP.

However, within PINT, such ambiguity may be quite common; it implies that there are a number of possible providers of a given service.

6.3. Competing PINT Gateways REGISTERing to offer the same service

With PINT, the registration is not for an individual but instead for a service that can be handled by a service provider. Thus, one can envisage a registration by the PINT Server of the domain telcoA.com of its ability to support the service R2C as "R2C@telcoA.com", sent to an intermediary server that acts as registrar for the "broker.telcos.com" domain from "R2C@pint.telcoA.com" as follows:

```
REGISTER sip:registrar@broker.telcos.com SIP/2.0
To: sip:R2C@pint.telcoA.com
From: sip:R2C@pint.telcoA.com
...
```

This is the standard SIP registration service.

However, what happens if there are a number of different Service Providers, all of whom support the "R2C" service? Suppose there is a PINT system at domain "broker.com". PINT clients requesting a Request-to-Call service from broker.com might be very willing to be redirected or proxied to any one of the various service providers that had previously registered with the registrar. PINT servers might also be interested in providing service for requests that did not specify the service provider explicitly, as well as those requests that were directed "at them".

To enable such service, PINT servers would REGISTER at the broker PINT server registrations of the form:

```
REGISTER sip:registrar@broker.com SIP/2.0
To: sip:R2C@broker.com
From: sip:R2C@pint.telcoA.com
```

When several such REGISTER messages appear at the registrar, each differing only in the URL in the From: line, the registrar has many possibilities, e.g.:

(i) it overwrites the prior registration for "R2C@broker.telcos.com" when the next comes in;
(ii) it rejects the subsequent registration for "R2C@broker.telcos.com";
(iii) it maintains all such registrations.

In this last case, on receiving an Invitation for the "general" service, either:

(iii.1) it passes on the invitation to all registered service providers, returning a collated response with all acceptances, using multiple Location: headers,

or

(iii.2) it silently selects one of the registrations (using, for example, a "round robin" approach) and routes the Invitation and response onwards without further comment.

As an alternative to all of the above approaches, it:
(iv) may choose to not allow registrations for the "general" service, rejecting all such REGISTER requests.

The algorithm by which such a choice is made will be implementation-dependent, and is outside the scope of PINT. Where a behaviour is to be defined by requesting users, then some sort of call processing language might be used to allow those clients, as a pre-service operation, to download the behaviour they expect to the server making such decisions. This, however, is a topic for other protocols, not for PINT.

6.4. Limitations on Available Information and Request Timing for SUBSCRIBE

A reference configuration for PINT is that service requests are sent, via a PINT Gateway, to an Executive System that fulfils the Service Control Function (SCF) of an Intelligent Network (see [11]). The success or failure of the resulting service call may be information available to the SCF and so may potentially be made available to the PINT Gateway. In terms of historical record of whether or not a service succeeded, a large SCF may be dealing with a million call attempts per hour. Given that volume of service transactions, there are finite limits beyond which it cannot store service disposition records; expecting to find out if a Fax was sent last month from a busy SCF is unrealistic.

Other status changes, such as that on completion of a successful service call, require the SCF to arrange monitoring of the service call in a way that the service may not do normally, for performance reasons. In most implementations, it is difficult efficiently to interrupt a service to change it once it has begun execution, so it may be necessary to have two different services; one that sets GSTN resources to monitor service call termination, and one that doesn't. It is unlikely to be possible to decide that monitoring is required once the service has started.

These factors can have implications both on the information that is potentially available at the PINT Gateway, and when a request to register interest in the status of a PINT service can succeed. The alternative to using a general SCF is to provide a dedicated Service Node just for PINT services. As this node is involved in placing all service calls, it is in a position to collect the information needed. However, it may well still not be able to respond successfully to a registration of interest in call state changes once a service logic program instance is running.

Thus, although a Requesting User may register an interest in the status of a service request, the PINT Gateway may not be in a position to comply with that request. Although this does not affect the protocol used between the Requestor and the PINT Gateway, it may influence the response returned. To avoid the problem of changing service logic once running, any registration of interest in status changes should be made at or before the time at which the service request is made.

Conversely, if a historical request is made on the disposition of a service, this should be done within a short time after the service has completed; the Executive System is unlikely to store the results of service requests for

long; these will have been processed as AMA (Automatic Message Accounting) records quickly, after which the Executive System has no reason to keep them, and so they may be discarded.

Where the PINT Gateway and the Executive System are intimately linked, the Gateway can respond to status subscription requests that occur while a service is running. It may accept these requests and simply not even try to query the Executive System until it has information that a service has completed, merely returning the final status. Thus the PINT Requestor may be in what it believes is a monitoring state, whilst the PINT Gateway has not even informed the Executive System that a request has been made. This will increase the internal complexity of the PINT Gateway in that it will have a complex set of interlocking state machines, but does mean that status registration and indication CAN be provided in conjunction with an I.N. system.

6.5. Parameters needed for invoking traditional GSTN Services within PINT

This section describes how parameters needed to specify certain traditional GSTN services can be carried within PINT requests.

6.5.1. Service Identifier

When a Requesting User asks for a service to be performed, he or she will, of course, have to specify in some way which service. This can be done in the URLs within the To: header and the Request-URI (see section 3.5.5.1).

6.5.2. A and B parties

With the Request-to-Call service, they will also need to specify the A and B parties they want to be engaged in the resulting service call. The A party could identify, for example, the Call Center from which they want a call back, whilst the B party is their telephone number (i.e. who the Call Center agent is to call).

The Request-to-Fax and Request-to-Hear-Content services require the B party to be specified (respectively the telephone number of the destination Fax machine or the telephone to which spoken content is to be delivered), but the A party is a Telephone Network based resource (either a Fax or speech transcoder/sender), and is implicit; the Requesting User does not (and cannot) specify it.

With the "Fax-Back" variant of the Request-to-Fax service, (i.e. where the content to be delivered resides on the GSTN) they will also have specify two parties. As before, the B party is the telephone number of the fax machine to which they want a fax to be sent. However, within this variant the A party identifies the "document context" for the GSTN-based document store from which a particular document is to be retrieved; the analogy here is to a GSTN user dialling a particular telephone number and then entering the document number to be returned using "touch tone" digits. The telephone number they dial is that of the document store or A party, with the "touch tone" digits selecting the document within that store.

6.5.3. Other Service Parameters

In terms of the extra parameters to the request, the services again differ. The Request-to-Call service needs only the A and B parties. Also it is convenient to assert that the resulting service call will carry voice, as the Executive System within the destination GSTN may be able to check that assertion against the A and B party numbers specified and may treat the call differently.

With the Request-to-Fax and Request-to-Hear-Content services, the source information to be transcoded is held on the Internet. That means either that this information is carried along with the request itself, or that a reference to the source of this information is given.

In addition, it is convenient to assert that the service call will carry fax or voice, and, where possible, to specify the format for the source information.

The GSTN-based content or "Fax-Back" variant of the Request-to-Fax service needs to specify the Document Store number and the Fax machine number to which the information is to be delivered. It is convenient to assert that the call will carry Fax data, as the destination Executive System may be able to check that assertion against the document store number and that of the destination Fax machine.

In addition, the document number may also need to be sent. This parameter is an opaque reference that is carried through the Internet but has significance only within the GSTN. The document store number and document number together uniquely specify the actual content to be faxed.

6.5.4. Service Parameter Summary

The following table summarises the information needed in order to specify fully the intent of a GSTN service request. Note that it excludes any other parameters (such as authentication or authorisation tokens, or Expires: or CallId: headers) that may be used in a request.

Service	ServiceID	AParty	BParty	CallFmt	Source	SourceFmt
R2C	x	x	x	voice	-	-
R2F	x	-	x	fax	URI/IL	ISF/ILSF
R2FB	x	x	x	fax	OR	-
R2HC	x	-	x	voice	URI/IL	ISF/ILSF

In this table, "x" means that the parameter is required, whilst "-" means that the parameter is not required.

The Services listed are Request-to-Call (R2C), Request-to-Fax (R2F), the GSTN-based content or "Fax-back" Variant of Request-to-Fax (R2FB), and Request-to-Hear-Content (R2HC).

The Call Format parameter values "voice" or "fax" indicate the kind of

service call that results.

The Source Indicator "URI/IL" implies either that the information is either an Internet source reference (a Universal Resource Identifier, or URI) or is carried "in-line" with the message. The Source indicator "OR" means that the value passed is an Opaque Reference that should be carried along with the rest of the message but is to be interpreted only within the destination (GSTN) context. As an alternative, it could be given as a "local" reference with the "file" style, or even using a partial reference with the "http" style. However, the way in which such a reference is interpreted is a matter for the receiving PINT Server and Executive System; it remains, in effect, an opaque reference.

The Source Format value "ISF/ILSF" means that the format of the source is specified either in terms of the URI or that it is carried "in-line". Note that, for some data, the format either can be detected by inspection or, if all else fails, can be assumed from the URI (for example, by assuming that the file extension part of a URL indicates the data type). For an opaque reference, the Source Format is not available on the Internet, and so is not given.

6.6. Parameter Mapping to PINT Extensions

This section describes the way in which the parameters needed to specify a GSTN service request fully might be carried within a "PINT extended" message. There are other choices, and these are not precluded. However, in order to ensure that the Requesting User receives the service that they expect, it is necessary to have some shared understanding of the parameters passed and the behaviour expected of the PINT Server and its attendant Executive System.

The Service Identifier can be sent as the userinfo element of the Request-URI. Thus, the first line of a PINT Invitation would be of the form:

```
INVITE <serviceID>@<pint-server>.<domain>  SIP/2.0
```

The A Party for the Request-to-Call and "Fax-back" variant of Request-to-Fax service can be held in the "To:" header field. In this case the "To:" header value will be different from the Request-URI. In the services where the A party is not specified, the "To:" field is free to repeat the value held in the Request-URI. This is the case for Request-to-Fax and Request-to-Hear-Content services.

The B party is needed in all these milestone services, and can be held

in the enclosed SDP sub-part, as the value of the "c=" field.

The call format parameter can be held as part of the "m=" field value. It maps to the "transport protocol" element as described in section 3.4.2 of this document.

The source format specifier is held in the "m=", as a type and either "-" or sub-type. The latter is normally required for all services except Request-to-Call or "Faxback", where the "-" form may be used. As shown earlier, the source format and source are not always required when generating requests for services. However, the inclusion in all requests of a source format specifier can make parsing the request simpler and allows for other services to be specified in the future, and so values are always given. The source format parameter is covered in section 3.4.2 as the "media type" element.

The source itself is identified by an "a=fmtp:" field value, where needed. With the exception of the Request-to-Call service, all invitations will normally include such a field. From the perspective of the SDP extensions, it can be considered as qualifying the media sub-type, as if to say, for example, "when I say jpeg, what I mean is the following".

In summary, the parameters needed by the different services are carried in fields as shown in the following table:

```
Service    Svc Param     PINT/SIP or SDP field used      Example value
-------    ---------     --------------------------      -------------

  R2C
           ServiceID:    <SIP Request-URI userinfo>      R2C
           BParty:       <SIP To: field>                 sip:123@p.com
           AParty:       <SDP c= field>                  TN RFC2543 4567
           CallFormat:   <SDP transport protocol
                              sub-field of m= field>     voice
           SourceFmt:    <SDP media type sub-field
                              of m= field>               audio
                         (--- only "-" sub-type
                              sub-field value used)      ---
           Source:       (--- No source specified)       ---

  R2F
           ServiceID:    <SIP Request-URI userinfo>      R2F
           BParty:       (--- SIP To: field not used) sip:R2F@pint.xxx.net
           AParty:       <SDP c= field>               TN RFCxxx +441213553
```

```
          CallFormat:  <SDP transport protocol
                            sub-field of m= field>      fax
          SourceFmt:   <SDP media type sub-field
                            of m= field>                image
                       <SDP media sub-type sub-field
                            of m= field>                jpeg
          Source:      <SDP a=fmtp: field qualifying
                            preceding m= field>     a=fmtp:jpeg<uri-ref>

  R2FB
          ServiceID:   <SIP Request-URI userinfo>       R2FB
          BParty:      <SIP To: field>               sip:1-730-1234@p.com
          AParty:      <SDP c= field>                TN RFCxxx +441213553
          CallFormat:  <SDP transport protocol
                            sub-field of m= field>      fax
          SourceFmt:   <SDP media type sub-field
                            of m= field>                image
                       <SDP media sub-type sub-field
                            of m= field>                jpeg
          Source:      <SDP a=fmtp: field qualifying
                            preceding m= field>      a=fmtp:jpeg opr:1234
```



```
R2HC
          ServiceID:   <SIP Request-URI userinfo>       R2HC
          BParty:      (--- SIP To: field not used) sip:R2HC@pint.ita.il
          AParty:      <SDP c= field>                TN RFCxxx +441213554
          CallFormat:  <SDP transport protocol
                            sub-field of m= field>      voice
          SourceFmt:   <SDP media type sub-field
                            of m= field>                text
                       <SDP media sub-type sub-field
                            of m= field>                html
          Source:      <SDP a=fmtp: field qualifying
                            preceding m= field>      a=fmtp:html<uri-ref>
```

7. Open Issues and Draft State

7.1. Open Issues

Thre are no current technical open issues.

7.2. Draft State

This draft reflects all changes resulting from the WG "last call" phase.

8. References

[1] M. Handley, E. Schooler, H. Schulzrinne, & J. Rosenberg,
"SIP: Session Initiation Protocol", RFC2543,
Internet Engineering Task Force, March 1999.

[2] M. Handley & V. Jacobsen,
"SDP: Session Description Protocol", RFC2327,
Internet Engineering Task Force, April 1998.

[3] N. Freed & N. Borenstein,
"Multipurpose Internet Mail Extensions (MIME)
Part One: Format of Internet Message Bodies",
RFC2045, November 1996.

[4] N. Freed & N. Borenstein,
"Multipurpose Internet Mail Extensions (MIME)
Part Two: Media Types",
RFC2046, November 1996.

[5] The Unicode Consortium,
"The Unicode Standard -- Version 2.0",
Addison-Wesley, 1996.

[6] ITU-T Study Group 2,
"E.164 - The International Public Network Numbering Plan",
ITU-T, June 1997.

[7] H. Lu et al,
"Toward the PSTN/Internet Inter-Networking--Pre-PINT
Implementations", Informational RFC2458,
Internet Engineering Task Force, Nov 1998.

[8] ITU-T Study Group XI,
"Q.763 - Formats and Codes for the ISDN User Part of SS No7"
ITU-T, August 1994.

[9] T. Berners-Lee, R. Fielding, & L. Masinter,
"Uniform Resource Identifiers (URI): Generic Syntax", RFC2396,
Internet Engineering Task Force, August 1998.

[10] D. Crocker,
"Standard for the format of ARPA Internet text messages",RFC822,
Internet Engineering Task Force, August 1982.

[11] ITU-T Study Group XI,
"Q.1204 - IN Distributed Functional Plane Architecture",
ITU-T, February 1994.

[12] T. Dierks & C. Allen,
"The TLS Protocol Version 1.0", RFC2246,
Internet Engineering Task Force, January 1999.

[13] S. Kent, R. Atkinson,
"Security Architecture for the Internet Protocol", RFC2401,
Internet Engineering Task Force, November 1998.

[14] R. Housley, W. Ford, W. Polk & D. Solo,
"Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC2459,
Internet Engineering Task Force, January 1999.
[15] D. Crocker & P. Overall,
"Augmented BNF for Syntax Specifications: ABNF", RFC2234,
Internet Engineering Task Force, November 1997.
[16] D. Mills, "Network Time Protocol (version 3) specification and implementation", RFC1305, Internet Engineering Task Force, March 1992.
[17] D. Eastlake, S. Crocker & J.Schiller,
"Randomness Recommendations for Security", Informational RFC 1305,
Internet Engineering Task Force, March 1992.
[18] P. Mockapetris,
"Domain Names - Implementation and Specification" RFC 1035,
Inernet Engineering Task Force November 1987.
[19] E. Levinson,
"The MIME Multipart/Related Content-type" RFC 2387,
Inernet Engineering Task Force August 1998.

9. Acknowledgements

The authors wish to thank the members of the PINT working group for comments that were helpful to the preparation of this specification. Ian Elz's comments were extremely useful to our understanding of internal PSTN operations. The SUBSCRIBE and NOTIFY requests were first suggested by Henning Schulzrinne and Jonathan Rosenberg. The suggestion to use an audio port of 0 to express that the phone is "on hold" (i.e. not receiving voice) is due to Ray Zibman. Finally, thanks to Bernie Hoeneisen for his close proofreading.

Appendix A: Collected ABNF for PINT Extensions

```
;; --(ABNF is specified in RFC 2234 [15])

;; --Variations on SDP definitions

connection-field    = ["c=" nettype space addrtype space
                        connection-address CRLF]
; -- this is the original definition from SDP, included for completeness
```

```
; -- the following are PINT interpretations and modifications

nettype = ("IN"/"TN")
; -- redefined as a superset of the SDP definition

addrtype = (INAddrType / TNAddrType)
; -- redefined as a superset of the SDP definition

INAddrType = ("IP4"/"IP6")
; -- this non-terminal added to hold original SDP address types

TNAddrType = ("RFC2543"/OtherAddrType)

OtherAddrType = (<X-Token>)
; -- X-token is as defined in RFC2045

addr = (<FQDN> / <unicast-address> / TNAddr)
; -- redefined as a superset of the original SDP definition
; -- FQDN and unicast address as specified in SDP

TNAddr = (RFC2543Addr/OtherAddr)
; -- TNAddr defined only in context of nettype == "TN"

RFC2543Addr = (INPAddr/LDPAddr)

INPAddr = "+" <POS-DIGIT> 0*(("-" <DIGIT>)/<DIGIT>)
; -- POS-DIGIT and DIGIT as defined in SDP

LDPAddr = <DIGIT> 0*(("-" <DIGIT>)/<DIGIT>)

OtherAddr = 1*<uric>
; -- OtherAdd defined in the context of OtherAddrType
; -- uric is as defined in RFC2396

media-field = "m=" media <space> port <space> proto
                   1*(<space> fmt) <CRLF>
; -- NOTE redefined as subset/relaxation of original SDP definition
; -- space and CRLF as defined in SDP

media = ("application"/"audio"/"image"/"text")
; -- NOTE redefined as a subset of the original SDP definition
; -- This could be any MIME discrete type; Only those listed are
; --  used in PINT 1.0
```



```
port = ("0" / "1")
```

```
; -- NOTE redefined from the original SDP definition;
; -- 0 retains usual sdp meaning of "temporarily no media"
; -- (i.e. "line is on hold")
; -- (1 means there is media)

proto = (INProto/TNProto)
; -- redefined as a superset of the original SDP definition

INProto = 1* (<alpha-numeric>)
; -- this is the "classic" SDP protocol, defined if nettype == "IN"
; -- alpha-numeric is as defined in SDP
..--
TNProto = ("voice"/"fax"/"pager")
; -- this is the PINT protocol, defined if nettype == "TN"

fmt = (<subtype> / "-")
; -- NOTE redefined as a subset of the original SDP definition
; -- subtype as defined in RFC2046, or "-". MUST be a subtype of type
held
; --  in associated media sub-field or the special value "-".

attribute-fields = *("a=" attribute-list <CRLF>)
; -- redefined as a superset of the definition given in SDP
; -- CRLF is as defined in SDP

attribute-list = 1(PINT-attribute / <attribute>)
; -- attribute is as defined in SDP

PINT-attribute = (clir-attribute / q763-nature-attribute /
                   q763plan-attribute / q763-INN-attribute /
                   phone-context-attribute / tsp-attribute /
                   pint-fmtp-attribute / strict-attribute)

clir-attribute = clir-tag ":" ("true" / "false")

clir-tag = "clir"

q763-nature-attribute = Q763-nature-tag ":" q763-natures

q763-nature-tag = "Q763-nature"

q763-natures = ("1" / "2" / "3" / "4")

q763-plan-attribute = Q763-plan-tag ":" q763-plans

q763-plan-tag = "Q763-plan"

q763-plans = ("1" / "2" / "3" / "4" / "5" / "6" / "7")
; -- of these, the meanings of 1, 3, and 4 are defined in the text
```

```
q763-INN-attribute = Q763-INN-tag ":" q763-INNs

q763-INN-tag = "Q763-INN"

q763-INNs = ("0" / "1")

phone-context-attribute = phone-context-tag ":" phone-context-ident

phone-context-tag = "phone-context"

phone-context-ident = network-prefix / private-prefix

network-prefix = intl-network-prefix / local-network-prefix

intl-network-prefix = "+" 1*<DIGIT>

local-network-prefix = 1*<DIGIT>

private-prefix = 1*excldigandplus 0*<uric>

excldigandplus = (0x21-0x2d,0x2f,0x40-0x7d))
..--
tsp-attribute = tsp-tag "=" provider-domainname

tsp-tag = "tsp"

provider-domainname = <domain>
; -- domain is defined in RFC1035

; -- NOTE the following is redefined relative to the normal use in SDP
pint-fmtp-attribute = "fmtp:" <subtype> <space> resolution
                        *(<space> resolution)
                        (<space> ";" 1(<attribute>) *(<space>
<attribute>))
; -- subtype as defined in RFC2046.
; -- NOTE that this value MUST match a fmt on the ultimately preceeding
; --  media-field
; -- attribute is as defined in SDP

resolution = (uri-ref / opaque-ref / sub-part-ref)

uri-ref = uri-tag ":" <URI-Reference>
; -- URI-Reference defined in RFC2396

uritag = "uri"

opaque-ref = opr-tag ":" 0*<uric>
```

```
opr-tag = "opr"
```



```
sub-part-ref = spr-tag ":" <Content-ID>
; -- Content-ID is as defined in RFC2046 and RFC822

spr-tag = "spr"

strict-attribute = "require:" att-tag-list

att-tag-list = 1(PINT-att-tag-list / <att-field> /
                    pint-fmtp-tag-list)
                  *(","
                    (PINT-att-tag-list / <att-field> /
                      pint-fmtp-tag-list)
                   )
; -- att-field as defined in SDP

PINT-att-tag-list = (phone-context-tag / clir-tag /
                       q763-nature-tag / q763-plan-tag /
                       q763-INN-tag)

pint-fmtp-tag-list = (uri-tag / opr-tag / spr-tag)

;; --Variations on SIP definitions

clir-parameter = clir-tag "=" ("true" / "false")

q763-nature-parameter = Q763-nature-tag "=" Q763-natures

q763plan-parameter = Q763-plan-tag "=" q763plans

q763-INN-parameter = Q763-INN-tag "=" q763-INNs

tsp-parameter = tsp-tag "=" provider-domainname

phone-context-parameter = phone-context-tag "=" phone-context-ident

SIP-param = ( <transport-param> / <user-param> / <method-param> /
                <ttl-param> / <maddr-param> / <other-param> )
; -- the values in this list are all as defined in SIP

PINT-param = ( clir-parameter / q763-nature-parameter /
                q763plan-parameter / q763-INN-parameter/
                tsp-parameter / phone-context-parameter )
```

```
URL-parameter = (SIP-param / PINT-param)
; -- redefined SIP's URL-parameter to include ones defined in PINT

Require-header = "require:" 1(required-extensions)
                            *("," required-extensions)
; -- NOTE this is redefined as a subset of the SIP definition
; -- (from RFC2543/section 6.30)

required-extensions = ("org.ietf.sip.subscribe" /
                       "org.ietf.sdp.require")
```


Appendix B: IANA Considerations

There are three kinds of identifier used in PINT extensions that SHOULD be registered with IANA, if a new value is specified. These are:

* Media Format sub-types, as described in section 3.4.2 of this document.
* Private Attributes as mentioned in section 3.4.3
* Private Phone Context values, as described in section 3.4.3.1.

It should be noted that private Address Types (in section 3.4.1) have been explicitly excluded from this process, as they must be in the form of an X-Token.

B.1. Media Format Sub-types

Taking these in turn, the media format sub-types are used within the PINT extensions to SDP to specify the attribute line that holds the data source definitions. In normal use, the values in this field are sub-types of MIME discrete types[4]. If a value other than an IANA-registered sub-type is to be used, then it should either be an X-Token (i.e. start with "X-") or it should be registered with IANA. if the intention is to describe a new MIME sub-type, then the procedures specified in RFC 2048 should be used. It is ASSUMED that any new MIME sub-type would follow the syntactic rules for interpretation of associated PINT fmtp lines defined in this document.

Note that, in keeping with the SDP description, such registrations SHOULD include the "proto" field values within which they are defined; however, it is appropriate to specify only that they can be used with "all values of TNProto".

Conversely, if the intent is to define a new way of including data source definitions within PINT, then it will be necessary to specify, in the documentation supporting any such new "PINT Media Format Sub-type"

registration, the syntax of the associated "fmtp" attribute line, as the identifier serves to indicate the interpretation that should be made of format specific attribute lines "tagged" with with such a sub-type.

If the fmtp interpretation follows the PINT default, then it is adequate to mention this in the defining document rather than repeating the syntax definition given here (although, in this case, it is unclear why such a new registration would be required). As before, the Media Format sub-type SHOULD specify the values of "proto" field within which it is defined, but this can be "all values of TNProto".

B.2. Private Attributes
Any proprietary attribute lines that are added may be registered with IANA using the procedures mentioned in [2]; the mechanism is the same as that used in SDP. If the attribute is defined for use only within PINT, then it may be approapriate to mention this in the supporting documentation. Note that, in the PINT 1.0 specification covered here, there is no mechanism to add such freshly registered attribute lines to a "require:" clause.

B.3. Private phone-contexts
Within the session description used for PINT requests, a phone-context attribute may be used to specify the prefix or context within which an associated telephone-number (in a connextion line) should be interpreted.

For "public" phone contexts the prefix to be used MUST start with either a DIGIT or a "+". Private phone contexts may be registered with IANA that do NOT start with either of these characters. Such a prefix may be useful to identify a private network, potentially with an associated numeric ID (see example 4 in section 3.4.3.1). In the example, the prefix acts as the context for X-acme.com's private network numbering plan.

It is recommended that any private context to be registered have the general form of a token including a domain name, optionally followed by a digit string or other token. The appropriate form of the initial token name space will be similar to that used for private or vendor registrations for sub-types (e.g. vnd.acme.com). However, note that the registration will be used to specify a customer's private network numbering plan format rather than being used generally for all of their equipment vendor's customer's; thus, fbi.gov would be appropriate, but lucent.com would not (unless the private network were to be that used by Lucent internally).

In addition, the supporting documentation MUST either declare that there is no associated token, or define the syntax by which that token can be parsed (e.g. vnd.fbi.gov <space> 1*DIGIT). Note that the registration describes a format, not a value range; it is sufficient that the private context can be parsed, without the value being interpreted.

In detail, the registration request SHOULD include:

* Kind of registration (i.e. private phone-context attribute to be used within the service description of PINT service requests)
* Contact details for the person responsible for the registration request (name, organisation, e-mail address, public telephone number)
* Private Prefix initial token name (e.g. vnd.fbi.gov)
* syntax for private context (e.g. "vnd.fbi.gov" <space> 1*DIGIT, or "vnd.gtn.gov.uk")
* Description of use (e.g. "This phone context declares an associated telephone number to be within the 'government telecommunications network'; the number is in an internal or private number plan form)
* Network Type and Address Type with which this private context is associated; If the "normal" telephone types (as specified in this document) are used, then the values would be shown as: "nettype=TN" , addrtype="RFC2543Addr". If, however, this context were to be used with another address type, then a reference to that address type name and the syntax of that address value would be required.

In short, this context is the telephone equivalent of a "Net 10" address space behind a NAT, and the initial name (and contact information) shows the context within which that address is valid. It also specifies the format for the network and address types (and address value syntax) with which this context is associated.

Of course, IANA may refer the requested registration to the IESG or an appropriate IETF working group for review, and may require revisions to be made before the registration is accepted.

Appendix C: Author's Addresses

Scott Petrack
MetaTel, Inc.
35 Rumford Avd.
Waltham, MA 02453
scott.petrack@metatel.com

+1 (781)-891-9000

Lawrence Conroy
Siemens Roke Manor Research
Roke Manor
Old Salisbury Lane
Romsey, Hampshire
U.K.   SO51 0ZN
lwc@roke.co.uk
+44 (1794) 833666