SIPPING Working Group
Internet-Draft
Expires: August 8, 2005

A. Allen
Research in Motion
J. Holm
Ericsson
T. Hallin
Motorola

February 7, 2005

Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the Open Mobile Alliance (OMA) Push to talk over Cellular (PoC)

draft-allen-sipping-poc-p-headers-01.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a set of private Session Initiation

Protocol(SIP) headers (P-headers) used by the Open Mobile Alliance (OMA),For Push to talk over Cellular (PoC) along with their applicability, which is limited to the OMA PoC application. The P-headers are used for requesting and indicating the alerting mode of the handset which is particular to the PoC application.

Table of Contents

1. Overall Applicability

The SIP extensions specified in this document make certain assumptions regarding network topology, and the availability of transitive trust. These assumptions are generally NOT APPLICABLE in the Internet as a whole. The mechanisms specified here were designed to satisfy the requirements specified by the Open Mobile Alliance for Push-to-talk over cellular for which either no general-purpose solution was found, where insufficient operational experience was available to understand if a general solution is needed, or where a more general solution is not yet mature. For more details about the assumptions made about these extensions, consult the Applicability subsection for each extension.

2. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [2].

3. Overview

The Open Mobile Alliance (OMA) (http://www.openmobilealliance.org) is specifying the Push-to-talk Over Cellular (PoC) service where SIP is the protocol used to establish half duplex media sessions across different participants. This document describes private extensions to address specific requirements of the PoC service and may not be applicable to the general Internet.

The PoC service allows a SIP UA (PoC terminal) to establish a session To one or more SIP UAs simultaneously, usually initiated by the initiating user pushing a button.

OMA has defined a collection of very stringent requirements in support of the PoC service. In order to provide the user with a satisfactory experience the initial session establishment from the time the user presses the button to the time they get an indication to speak must be minimized.

The PoC terminal may support such hardware capabilities as a speaker phone and/or headset and software that provide the capability for the user to configure the PoC terminal to accept the session initiations immediately and play out the media as soon as it is received without requiring the intervention of the called user. This mode of operation is known as Automatic Answer mode. The user may alternatively configure the PoC terminal to first alert the user and require the user to manually accept the session invitation before media is accepted. This mode of operation is known as Manual Answer

mode. The PoC terminal may support both or only one of these modes of operation. The user may change the Answer Mode (AM) configuration of the PoC terminal frequently based on their current circumstances and preference,(perhaps because the user is busy, or in a public area where she cannot use a speaker phone, etc).

The OMA PoC Architecture utilizes SIP servers within the network that may perform such roles as a conference focus [12], a RTP translator or a policy server. A possible optimization to minimize the delay in the providing of the caller with an indication to speak is for the SIP network server to perform buffering of media packets in order to provide an early or unconfirmed indication back to the caller and allow the caller to start speaking before the called PoC terminal has answered. An event package and mechanisms for a SIP UA to indicate its current answer mode to a SIP Server in order to enable buffering are defined in [4]. In addition, particularly when multiple domains are involved in the session more than one intermediate SIP server may be involved in the signaling path for the session and the server that performs the buffering may not be the server that has knowledge of the current answer mode of the SIP UA that is the final destination for the SIP INVITE request. A mechanism is therefore required to allow a terminal that acts as a SIP UA or a network based server that acts as a SIP UAC to indicate a preference to the final destination SIP UAS to answer in a particular mode and for an intermediary SIP UAS or proxy to relay the unconfirmed indication in a response back towards the originating SIP UAC.

The answer mode requested in the SIP INVITE request may be determined based on the preference of the calling user and/or the authorization policies of the called user and the currently known answer mode setting of the called user's terminal. In addition to the basic answer mode settings of the terminal a privileged caller may request a Manual Answer Override (MAO) to request that the called terminal answer automatically even when it is in the Manual-Answer mode. This mode is needed for emergency service and also some other dispatch applications.

This document proposes two new SIP header fields to support this optimization. One extension may be optionally included in a SIP INVITE request or a REFER that requests an INVITE to be sent by a SIP UAC to request that the terminating SIP UAS alert the user according to the mode indicated by the parameter contained in the header. The other extension may be optionally included in a response to a SIP INVITE request or in a NOTIFY sent as a result of a REFER that requests an INVITE to be sent to provide an indication from an intermediate node acting as a SIP proxy or back-to-back UA that it has information that hints that the terminating UA will likely answer automatically and therefore provides an unconfirmed indication back

towards the inviting SIP UA to transmit media prior to receiving a final response from the final destination of the SIP INVITE request. Each extension, is described in its own section below.

4. SIP Private Headers

4.1 The P-Alerting-Mode header

This extension allows a UAC to request that the terminating SIP UAS or group of UAS, alert the user according to the mode indicated by the parameter contained in the header when using the INVITE method to establish a session between two or more SIP UAs. It is possible that the INVITE request traverses one or more application servers that behave as SIP back-to-back UAs or proxies, as the INVITE request is routed to the final destination UA. The intermediate node application servers can modify the value of P-Alerting-Mode header or insert this header in the INVITE if it is not already present.

4.1.1 Requirements

The OMA PoC service has the following requirements for the answer mode requests:

REQ-AM1: It MUST be possible for a SIP UAC to request an automatic answer mode which allows the inviting SIP UA to send media to the invited PoC subscriber's SIP UA without any action by the invited PoC user.

REQ-AM2: It MUST be possible for a SIP UAC to request a manual answer mode which allows requires the invited PoC user to accept the invitation to the PoC half-duplex session before the inviting SIP UA is permitted to send media to the invited PoC subscriber's terminal.

REQ-AM3: It MUST be possible for a SIP UAC to request a manual answer override which allows an inviting PoC user to request to override an the invited PoC users manual answer settings.

REQ-AM4: It MUST be possible for an intermediary server (SIP Proxy or B2BUA) to validate that the invited SIP UAS current answer mode settings will support the specified requested answer mode from the inviting SIP UAC and if not modify it appropriately.

REQ-AM5: It MUST be possible for an intermediary server (SIP Proxy or B2BUA) to validate that the inviting user is authorized by the invited user to request the answer mode contained in the request from the inviting SIP UAC and if not modify it appropriately.

REQ-AM6: It MUST be possible for an intermediary server (SIP Proxy or

B2BUA) to add a request for a specific answer mode based on the current answer mode settings of the invited SIP UAS and any policy settings if no answer mode request was contained in the invitation.

REQ-AM7: It MUST be possible for a SIP UAC to request a specific answer mode when inviting a user using an INVITE.

REQ-AM8: It MUST be possible for a SIP UAC to request a specific answer mode when inviting a user using a REFER that request an INVITE to be sent.

4.1.2 Alternatives Considered for Selecting the Answer Mode

A number of alternatives to the P-Alerting-Mode header were considered.

There were proposals to add this information in the body of a SIP INVITE request, either in a separate multi-part body section or in the SDP body. - The choice of an SDP parameter was rejected because the answer mode attribute applies to the session and not to a media stream. - A separate multi-part body section was rejected because this would require the UAS to build a parser for a new sub-protocol when deciding when and how to accept or reject a session and also increase the overhead in the message.

There was a proposal to add a URI parameter to the request URI. This was rejected because the answer mode of the terminating party is not an attribute of the Request-URI, but is an attribute of the session.

There was a proposal to add it as a feature tag in the Accept-Contact header. This was rejected because it was not agreed that the answer mode is a different feature or capability of the UA, but is an attribute of the session and can be applied to many different features. There was also concern that frequent changes in the answer mode settings in the terminal and corresponding callee capabilities refresh registrations would provide a heavy load on the registrar.

The P-Alerting-Mode header was chosen because answer mode is an attribute of a session. As a header, SIP Proxies and B2BUA's can pass it on without needing to analyze the header or they can perform authorization checks before sending the header to a subsequent UAS.

4.1.3 Applicability statement for the P-Alerting-Mode header

The P-Alerting-Mode header is applicable in SIP networks where:

- o There are SIP UAs that support different modes of accepting session (Auto-answer and Manual-Answer;
- o The inviting UAC can, as an option request the terminating SIP UAS to automatically or manually accept the session;
- o Where there are intermediate network SIP servers that are trusted and have knowledge of the current answer mode Setting of the terminating UAS;
- o The intermediate network SIP servers can perform authorization of the privilege of the inviter to request the requested answer mode; and,
- o This mode of operation is most applicable in environments that where half-duplex communications is the primary mode for the media.

Such configurations are generally not applicable to the Internet as a whole where such trust relationships do not exist.

4.1.4 Usage of the P-Alerting-Mode header

The P-Alerting-Mode header field provides a mechanism to express the inviting party's preferences towards the alerting of the calling user. Therefore, this header field is a hint or preferences from the inviting party's preferences towards the alerting of the calling user. Therefore, this header field is a hint or preferences from the inviting party towards the called party. It is at the discretion of the called party UAS to accept this hint or not. For instance, a UAS can decide to ignore this header field. A UAC or proxy MAY insert a P-Alerting-Mode header field into an INVITE request or a REFER request when it is desired to request the final destination UAS to alert the user manually about the incoming session, or to accept the session automatically and start the receiving media packets without requiring the intervention of the user.

> The final destination UAS MAY be identified by the value of the Request-URI in the INVITE request, the value of the Refer-To header field in a REFER request or using the mechanisms specified in [15] or [16].

The header field value is populated with one of the enumeration values "Manual", "Auto" or "MAO". When the value is "Manual" the UAC or proxy is requesting the UAS to alert the user and wait for the user to accept the session before returning a 200 OK response for the INVITE request. Normally in this mode the destination UAS will return a 180 Ringing provisional response when alerting the user as per [1]. When the value is set to "Auto" the UAC is requesting the UAS to not alert the user, accept the session and automatically return a 200 OK response without alerting the user and without requiring the user to manually accept the session. Normally in this

mode the destination UAS will return a 200 OK response upon receiving the INVITE as per [1]. When the value is "MAO" the UAC or proxy is requesting the UAS to accept the session and return a 200 OK response without requiring the user to manually accept the session even if the mode of the destination UAS is set to normally alert the user and require Manual acceptance. The use of the "Auto" and "MAO" values will likely be subject to authorization by the destination UAS or an intermediate proxy or back-to-back UA that acts as an authorization policy server on behalf of the destination UAS.

4.1.4.1 Procedures at the UA

A UAC MAY insert a P-Alerting-Mode header field in an INVITE request or in a REFER request that requests another UA to send an INVITE request. A UAS can receive a P-Alerting-Mode header field in an INVITE request or a REFER request. If the UAS is the final destination of the request it MAY use the value of the P-Alerting-Mode header field to determine whether to first alert the user or accept the session automatically without requiring manual user acceptance. The semantics of the parameters are defined in 4.1.4. If the UAS cannot or does not accept the mode of session acceptance requested in the P-Alerting-Mode header field it can safely ignore this header field.

If the UA is an intermediate node and not the final destination of the request it MAY, when acting as a UAC, insert a P-Alerting-Mode header field into an INVITE request that corresponds with an INVITE request or REFER request received while acting as a UAS. Alternatively the intermediate node MAY, when acting as a UAC, change the value of the P-Alerting-Mode header field in the outgoing INVITE from that received in the corresponding INVITE or REFER when acting as a UAS. This functionality is normally performed as part of the authorization process for the P-Alerting-Mode header field parameter or when the intermediate node has some hint from the intended destination UA of its current alerting mode. An event package and mechanisms for a UA to communicate its current alerting mode to an intermediate node is defined in [4].

4.1.4.2 Procedures at the proxy server

A SIP proxy does not need to understand the semantics of the P-Alerting-Mode header field. As part of the regular SIP rules for unknown headers, a proxy will forward unknown headers.

A proxy MAY insert a P-Alerting-Mode header field into an INVITE Request or MAY change the value of the P-Alerting-Mode header field in an INVITE request. This functionality is normally performed as part of the authorization process for the P-Alerting-Mode header

field parameter or when the proxy has some hint from the intended destination UA of its current alerting mode. An event package and mechanisms for a UA to communicate its current alerting mode to a proxy is defined in [4].

4.2 The P-Answer-State header

This header field MAY be included in a response to a SIP INVITE request or in a NOTIFY request sent as a result of a REFER request to send an INVITE request The purpose of the header field is to provide an indication from an intermediate node acting as a SIP proxy or back-to-back UA that is has information that hints that the terminating UA identified in the Request-URI of the request will likely answer automatically and therefore provides an unconfirmed indication back towards the inviting SIP UA to transmit media prior to receiving a final response from the final destination of the SIP INVITE request.

4.2.1 Requirements

The OMA PoC service has initial setup performance requirements that can be met by an intermediate server (SIP B2BUA) spooling media from the inviting PoC subscriber until 1 one or more invited PoC subscribers have accepted the session. The specific requirements are:

REQ-AS1: An intermediate server MAY spool media from the inviting SIP UA until 1 one or more invited PoC SIP UAs haves accepted the invite.

REQ-AS2: An intermediate server that is capable of spooling media MAY accept an invite request from an inviting SIP UAC even if no invited SIP UAS has accepted the invite request if it has a hint that the invited SIP UAC is likely to accept the request without requiring user intervention.

REQ-AS3: An intermediate server or proxy that is incapable of spooling media or does not wish to, but has a hint that the invited SIP UAC is likely to accept the request MUST be able to indicate back to another intermediate server that can spool media SHOULD only accept the invite request if that it has some indication hint that one or more invited PoC SIP UAs is likely to accept the invite request without requiring user intervention.

REQ-AS4: An intermediate server that is willing to spool media from the inviting SIP UA until one or more invited SIP UAs have accepted the invite SHOULD indicate that it is spooling media to the inviting SIP UAC.

4.2.2 Alternatives Considered

In order to meet REQ-AS3, an intermediate server needs to receive an indication back that the invited SIP UA is likely to accept the invite request without requiring user intervention. In this case, the intermediate server or proxy that has a hint that the invited SIP UAC is likely to accept the request can include an answer state indication in the 183 Session Progress or 200 OK response.

A number of alternatives were considered for the intermediate server to inform the another intermediate server or the inviting SIP UAC of the invited PoC SIP UAs answer mode settings.

One suggestion proposal was to create a unique reason-phrase in the 183 and 200 OK response. This was rejected because the reason phrases are normally intended for human readers and not meant to be parsed by servers for special syntactic and semantic meaning.

Another suggestion proposal was to use a Reason header in the 183 and 200 OK response. This was rejected because this would be inconsistent with the intended use of the reason header and its usage is not defined for these response codes would have required creating and registering a new protocol identifier.

Another suggestion proposal was to use a feature-tag in the returned Contact header. This was rejected because it was not a different feature, but is an attribute of the session and can be applied to many different features for the same reasons that the use of a feature-tag was rejected in 4.1.2.

Another suggestion proposal was to use a new SDP attribute. The choice of an SDP parameter was rejected because the answer state applies to the session and not to a media stream.

The P-Answer-State header was chosen to give additional information about the state of the SIP session progress and acceptance. Even though the UAC sees that its SDP offer has been answered and accepted, the header lets the UAC know whether invited PoC subscriber has accepted the invite or just an intermediary has done the acceptance.

4.2.3 Applicability statement for the P-Answer-State header

The P-Answer-State header is applicable in the following

circumstances:

- In networks where there are UAs that engage in half-duplex communication where there is not the possibility for the invited user to verbally acknowledge the answering of the session as is normal in full duplex communication;
- Where the invited UA may automatically accept the session without manual acceptance;
- The network also contains intermediate network SIP servers that are trusted;
- The intermediate network SIP servers have knowledge of the current answer mode setting of the terminating UAS; and,
- The intermediate network SIP servers can provide buffering of the media in order to reduce the time for the inviting user to send media.

Such configurations are generally not applicable to the internet as a whole where such trust relationships do not exist.

4.2.4 Usage of the P-Answer-State header

A UAS or proxy MAY insert a P-Answer-State header field in any 1XX or 2XX response that is allowed to contain an SDP answer in response to an SDP offer contained in an INVITE as specified in [13]. Typically the P-Answer-State header field is inserted in either a 183 Session Progress or a 200 OK response. A UA that receives a REFER request to send an INVITE MAY also insert a P-Answer-State header field in a NOTIFY request it sends as a result of the implicit subscription created by the REFER request.

When the P-Answer-State header field contains the parameter "Unconfirmed" the UAC or proxy is indicating that it has information that hints that the final destination UAS for the INVITE request is likely to automatically accept the session but that this is unconfirmed and it is possible that the final destination UAS will first alert the user and require manual acceptance of the session or not accept the session request. This is referred to here as an "unconfirmed response". When the P-Answer-State header field contains the parameter "Confirmed" the UAC or proxy is indicating that the destination UAS has accepted the session and is ready to receive media. The parameter value of "Confirmed" has the usual semantics of an SDP answer and is included for completeness. The usual end to end SDP answer response semantics are referred to here as a "confirmed response".

4.2.4.1 Procedures at the UA

A UAS MAY insert a P-Answer-State header field in any 1XX or 2XX

response that is allowed to contain an SDP answer in response to an SDP offer contained in an INVITE request as specified in [13]. A response containing the P-Answer-State header field containing the parameter "Unconfirmed" MAY or MAY NOT contain an SDP answer. If the response contains an SDP answer then the sending UA MUST be ready to receive media as specified in [13].

A UAC that receives a 1XX or 2XX response containing a P-Answer-State header field containing the parameter "Unconfirmed" and an SDP answer MAY send media as specified in [13], however there is no guarantee that the media will be received by the final recipient. How a UAC confirms whether the media was or was not received by the final destination when it his received a 2XX "unconfirmed response" is application specific and outside of the scope of this document. If the application is a conference then the mechanism specified in [13] could be used to determine that the invited user joined. Alternatively a BYE request could be sent or the media could be placed on hold if the final destination UAS does not accept the session.

An intermediate node that acts as a back-to-back UA and returns a 1XX or 2XX response in response to an INVITE request MAY insert a P-Answer-State header field containing the parameter "Unconfirmed" in the response if it has not yet received a "confirmed response" from the final destination UA. If the intermediate node UAS also includes SDP in the response along with a P-Answer-State header field containing the parameter "Unconfirmed" the intermediate node MUST be ready to receive media as specified in [13] and MAY buffer any media it receives until it receives a "confirmed response" from the final destination UA or until the buffer is full. Such an intermediate node may insert an SDP answer in the response it generates even if the "unconfirmed response" it received did not contain an SDP answer.

An intermediate node that acts as a back-to-back UA and receives a REFER request to send an INVITE request to another UA as specified in [11] MAY insert a P-Answer-State header field containing the parameter "Unconfirmed" in the initial NOTIFY request sent in response to the REFER request if it has not yet received a "confirmed response" from the final destination UA and it has information that hints that the final destination UAS for the INVITE is likely to automatically accept the session. If the REFER was sent as part of an existing dialog established by an INVITE request and for which there has been a successful SDP offer-answer exchange according to [13] the intermediate node MUST be ready to receive media as specified in [13] and MAY buffer any media it receives until it receives a "confirmed response" from the final destination UA or until its buffer is full.

An intermediate node that acts as a back-to-back UA and receives a 1XX or 2XX response in response to an INVITE request containing a P-Answer-State header field in the response SHOULD include the P-Answer-State header field unmodified in the 1XX or 2XX response it sends as a result of receiving that response. If the intermediate node that acts as a back-to-back UA sends a NOTIFY request according to [11] then the intermediate node UAC SHOULD include the P-Answer-State header field unmodified in the sipfrag of the response included in the body of the NOTIFY request.

A UAC that receives a 1XX or 2XX response without a P-Answer-State Header or containing a P-Answer-State header field containing the parameter "Confirmed" SHALL treat it as a "confirmed response". If the UAS knows that the final destination UA is now ready to accept media and the UAS previously sent an "Unconfirmed response" the UAS SHOULD insert a P-Answer-State header field containing the parameter "Confirmed" in the response.

An intermediate node that acts as a back-to-back UA that previously sent an initial NOTIFY request containing a P-Answer-State header field containing the parameter "Unconfirmed" that subsequently receives a "confirmed response" without a P-Answer-State header field in response to the INVITE request sent as a result of the REFER request SHOULD include a P-Answer-State header containing the parameter "Confirmed" in the subsequent NOTIFY request generated as a result of the "confirmed response".

If the UAS knows that the final destination UA is ready to accept media and the UAS did not previously send an "Unconfirmed response" the UAS MAY insert a P-Answer-State header field containing the parameter "Confirmed" in the response.

If an intermediate node that acts as a back-to-back UA and sends an INVITE request in response to a REFER request learns by receiving a "confirmed response" that the final destination UA is ready to accept media and the back-to-back UA did not previously include a P-Answer-State header containing the parameter "Unconfirmed" in the initial NOTIFY request sent in response to the REFER request then the back-to-back UA MAY insert a P-Answer-State header field containing the parameter "Confirmed" in the response if the "confirmed response" does not contain a P-Answer-State header.

A UA that receives in response to a REFER request a NOTIFY request request containing a P-Answer-State header field containing the parameter "Unconfirmed" as either a SIP header or contained in a sipfrag in the body of the NOTIFY request received on a pre-existing dialog that was established by an INVITE request and for which there has been a successful SDP offer-answer exchange according to [13]

then the UA MAY send media, however there is no guarantee that the media will be received by the final recipient that was indicated in the Refer-To header in the original REFER request.

4.2.4.2 Procedures at the proxy server

SIP proxy servers do not need to understand the semantics of the P-Answer-State header field. As part of the regular SIP rules for unknown headers, a proxy will forward unknown headers. A proxy MAY insert a P-Answer-State header field in a 1XX response that it originates compliant with [1] or add it to a 2XX response that contains an SDP answer in response to an SDP offer contained in an INVITE request as specified in [13].

A proxy that returns a 1XX response in response to an INVITE request MAY insert a P-Answer-State header field containing the parameter "Unconfirmed" in the response if it has not yet received a "confirmed response" from the final destination UA.

A proxy that receives a 1XX or 2XX response without a P-Answer-State Header or containing a P-Answer-State header field containing the parameter "Confirmed" SHALL for the purposes of this document treat it as a "confirmed response".

If the proxy knows that the final destination UA is now ready to accept media and the proxy previously sent an "Unconfirmed response" the proxy SHOULD insert a P-Answer-State header field containing the parameter "Confirmed" in the response.

If the proxy knows that the final destination UA is ready to accept media and the proxy did not previously send an "Unconfirmed response" the proxy MAY insert a P-Answer-State header field containing the parameter "Confirmed" in the response.

5. Formal Syntax

All of the mechanisms specified in this document are described in both prose and an augmented Backus-Naur Form (BNF) defined in RFC 2234 [3]. Further, several BNF definitions are inherited from SIP and are not repeated here. Implementers need to be familiar with the notation and contents of SIP [1] and RFC 2234 [3] to understand this document.

5.1 P-Alerting-Mode header syntax

The syntax of the P-Alerting-Mode header is described as follows:

```
P-Alerting-Mode        = "P-Alerting-Mode" HCOLON alerting-type
```

```
alerting-type          = "Manual" / "Auto" / "MAO"
```

5.2 P-Answer-State header syntax

The syntax of the P-Answer-State header is described as follows:

```
P-Answer-State          = "P-Answer-State" HCOLON answer-type
answer-type             = "Confirmed" / "Unconfirmed"
```

5.3 Table of new headers

Table 1 extends the headers defined in this document to Table 2 in SIP [1], section 7.1 of the SIP-specific event notification [6], tables 1 and 2 in the SIP INFO method [8], tables 1 and 2 in Reliability of provisional responses in SIP [7], tables 1 and 2 in the SIP UPDATE method [9], tables 1 and 2 in the SIP extension for Instant Messaging [10], and table 1 in the SIP REFER method [11]:

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG	SUB
P-Alerting-Mode	R	am	-	-	-	o	-	-	-
P-Answer-State	1xx,2xx	a	-	-	-	o	-	-	-

Header field	where	NOT	PRA	INF	UPD	MSG	REF
P-Alerting-Mode	R	-	-	-	-	-	o
P-Answer-State	R	o	-	-	-	-	-

Table 1: Header field support

6. Security Considerations

6.1 P-Alerting-Mode

The P-Alerting-Mode header requests that the destination UA behave in the way requested in this header. Although the destination UA does not have to accept what is requested the impact of an unauthorized intermediate attacker modifying this header or an unauthorized user sending an INVITE including the values "Auto" or "MAO" in this header could violate the privacy of the called user as a speaker phone may be engaged by the terminal and the callers voice may be heard by anyone in the vicinity. An INVITE request containing the P-Alerting-Mode header with the values "Auto" or "MAO" SHOULD be authenticated and authorized to ensure that the sender has the permission to trigger the callers terminal in an Auto-Answer mode of

operation. The authorization MAY be performed by the destination UA or by a trusted intermediate node that performs authorization policy on behalf of the called party. When an intermediate node is used to perform such authorization it is RECOMMENDED that this extension is used in a secured trusted environment where transitive trust exists between the proxies and UAs if end-to-end protection is not used at the SIP layer.

An eavesdropper cannot gain any useful information by obtaining the contents of this header.

6.2 P-Answer-State

The information returned in the P-Answer-State header is not viewed as particularly sensitive. Rather, it is informational in nature, providing an indication to the UAC that delivery of any media sent as a result of an answer in this response is not guaranteed. An eavesdropper cannot gain any useful information by obtaining the contents of this header.

If end-to-end protection is not used at the SIP layer, it is possible for proxies between the UAs to remove the header or modify the contents of the header value. This attack either denies the caller the knowledge that the callee has yet to be contacted or falsely indicates that the callee has yet to be contacted when they have already answered. It is therefore RECOMMENDED that this extension is used in a secured trusted environment where transitive trust exists between the proxies and UAs if end-to-end protection is not used at the SIP layer.

7. IANA Considerations

This document defines two private SIP extension header fields (beginning with the prefix "P-") based on the registration procedures defined in RFC 3427 [5].

The following extensions are registered as private extension header fields:

```
RFC Number:         [To be added by the RFC Editor]
Header Field Name:  P-Alerting-Mode
Compact Form:       none
```

```
RFC Number:         [To be added by the RFC Editor]
Header Field Name:  P-Answer-State
Compact Form:       none
```

Person to Contact: Andrew Allen, aallen@rim.com

8. draft-allen-sipping-poc-p-headers-01

Version 01 includes changes based on comments from the SIPPING chairs and members of the OMA PoC WG. Functions for the proxy role were added and requirements and alternatives considered sections included.

9. Acknowledgments

The authors would like to thank Miguel Garcia-Martin and the OMA POC Working Group members for their comments and support of this document.

10. References

10.1 Normative References

[1] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

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

[3] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

10.2 Informative References

[4] Garcia-Martin, M., "A Session Initiation Protocol (SIP) Event Package and Data Format for Incoming Session Barring and Answer Mode in support for the Push-to-talk Over Cellular (PoC) service", Internet-Draft draft-garcia-sipping-poc-isb-am-01, December 2004.

[5] Mankin, A., Bradner, S., Mahy, R., Willis, D., Ott, J. and B. Rosen, "Change Process for the Session Initiation Protocol (SIP)", BCP 67, RFC 3427, December 2002.

[6] Roach, A., "Session Initiation Protocol (SIP)-Specific Event Notification", RFC 3265, June 2002.

[7] Rosenberg, J. and H. Schulzrinne, "Reliability of Provisional Responses in Session Initiation Protocol (SIP)", RFC 3262, June 2002.

[8] Donovan, S., "The SIP INFO Method", RFC 2976, October 2000.

[9] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, October 2002.

[10] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C. and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

[11] Sparks, R., "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003.

[12] Rosenberg, J., "A Framework for Conferencing with the Session Initiation Protocol", Internet-Draft draft-ietf-sipping-conferencing-framework-03, October 2004.

[13] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[14] Rosenberg, J., "A Session Initiation Protocol (SIP) Event Package for Conference State", Internet-Draft draft-ietf-sipping-conference-package-08, December 2004.

[15] Camarillo, G. and A. Johnston, "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)", Internet-Draft draft-ietf-sipping-uri-list-conferencing-02, December 2004.

[16] Camarillo, G., "Refering to Multiple Resources in the Session Initiation Protocol (SIP)", Internet-Draft draft-ietf-sipping-multiple-refer-02, December 2004.

Authors' Addresses

Andrew Allen
Research in Motion
122 West John Carpenter Parkway, Suite 430
Irving, Texas 75039
USA

Email: aallen@rim.com

Jan Holm
Ericsson
Gotalandsvagen 220
Stockholm 612526
Sweden

Email: Jan.Holm@ericsson.com

Tom Hallin
Motorola
1501 W SHURE DRIVE
ARLINGTON HEIGHTS IL 60004
USA

Email: thallin@motorola.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.