Internet Engineering Task Force (IETF)
Request for Comments: 7315
Obsoletes: 3455
Category: Informational
ISSN: 2070-1721

R. Jesske
Deutsche Telekom
K. Drage
Alcatel-Lucent
C. Holmberg
Ericsson

July 2014

Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP

Abstract

This document describes a set of private header (P-header) Session Initiation Protocol (SIP) fields used by the 3GPP, along with their applicability, which is limited to particular environments. The P-header fields are used for a variety of purposes within the networks that the partners implement, including charging and information about the networks a call traverses. This document obsoletes RFC 3455.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7315.

Table of Contents

1. Overall Applicability 3
2. Conventions 3
3. Overview 3
4. SIP Private Header Fields 4
4.1. The P-Associated-URI Header Field 4
4.1.1. Applicability Statement for the P-Associated-URI Header Field 5
4.1.2. Usage of the P-Associated-URI Header Field 5
4.2. The P-Called-Party-ID Header Field 6
4.2.1. Applicability Statement for the P-Called-Party-ID Header Field 10
4.2.2. Usage of the P-Called-Party-ID Header Field 11
4.3. The P-Visited-Network-ID Header Field 12
4.3.1. Applicability Statement for the P-Visited-Network-ID Header Field 12
4.3.2. Usage of the P-Visited-Network-ID Header Field 13
4.4. The P-Access-Network-Info Header Field 17
4.4.1. Applicability Statement for the P-Access-Network-Info Header Field 18
4.4.2. Usage of the P-Access-Network-Info Header 18
4.5. The P-Charging-Function-Addresses Header Field 19
4.5.1. Applicability Statement for the P-Charging-Function-Addresses Header Field 20
4.5.2. Usage of the P-Charging-Function-Addresses Header Field 21
4.6. The P-Charging-Vector Header Field 23
4.6.1. Applicability Statement for the P-Charging-Vector Header Field 25
4.6.2. Usage of the P-Charging-Vector Header Field 25
4.6.3. Usage of the transit-ioi 27
4.6.4. Usage of the related-icid 28

5. Formal Syntax 28
5.1. P-Associated-URI Header Syntax 29
5.2. P-Called-Party-ID Header Syntax 29
5.3. P-Visited-Network-ID Header Syntax 29
5.4. P-Access-Network-Info Header Syntax 29
5.5. P-Charging-Function-Addresses Header Syntax 31
5.6. P-Charging-Vector Header Syntax 32
5.7. New Headers 33
6. Security Considerations 33
6.1. P-Associated-URI Header Field 33
6.2. P-Called-Party-ID Header Field 34
6.3. P-Visited-Network-ID Header Field 34
6.4. P-Access-Network-Info Header Field 35
6.5. P-Charging-Function-Addresses Header Field 36
6.6. P-Charging-Vector Header Field 36
7. IANA Considerations 37
8. Contributors and Acknowledgements 38
9. References 39
9.1. Normative References 39
9.2. Informative References 39
Appendix A. Changes from RFC 3455 41

1. Overall Applicability

The SIP extensions specified in this document make certain assumptions regarding network topology, linkage between SIP and lower layers, and the availability of transitive trust. These assumptions apply only to private networks and are not appropriate for use in an Internet environment. The mechanisms specified here were designed to satisfy the requirements specified in the 3GPP Release 5 requirements on SIP [RFC4083] for which either no general-purpose solution was planned (where insufficient operational experience was available to understand if a general solution would be needed) or for which 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 [RFC2119].

3. Overview

The 3GPP uses SIP as the protocol to establish and tear down multimedia sessions in the context of its IP Multimedia Subsystem (IMS), as described in the 3GPP TS 23.228 [TS23.228] and 3GPP TS

24.229 [TS24.229]. RFC 3455 [RFC3455] defines SIP private header extensions (referred to as P-headers) that are required by the 3GPP specification. Note that the requirements for these extensions are documented in RFC 4083 [RFC4083]. This document obsoletes RFC 3455 [RFC3455]. This document updates existing P-header descriptions to address additional requirements that are needed for 3GPP Release 11. Each of the P-headers is described in the sections below.

4. SIP Private Header Fields

4.1. The P-Associated-URI Header Field

This extension allows a registrar to return a set of associated URIs for a registered SIP address-of-record. We define the P-Associated-URI header field, used in the 200 (OK) response to a REGISTER request. The P-Associated-URI header field contains the set of associated URIs that are associated with the registered address-of-record.

In addition to the address-of-record, an associated URI is a URI that the service provider has allocated to a user. A registrar contains information that allows zero or more URIs to be associated with an address-of-record. Usually, all these URIs (the address-of-record and the associated URIs) are allocated for the usage of a particular user. This extension to SIP allows the User Agent Client (UAC) to know, upon a successful authenticated registration, which other URIs, if any, the service provider has associated with an address-of-record URI.

Note that, in standard SIP usage [RFC3261], the registrar does not register the associated URIs on behalf of the user. Only the address-of-record that is present in the To header field of the REGISTER is registered and bound to the contact address. The only information conveyed is that the registrar is aware of other URIs that can be used by the same user.

A situation may be possible, however, in which an application server (or even the registrar itself) registers any of the associated URIs on behalf of the user by means of a third-party registration. However, this third-party registration is out of the scope of this document. A UAC MUST NOT assume that the associated URIs are registered.

If a UAC wants to check whether any of the associated URIs is registered, it can do so by mechanisms specified outside this document, e.g., the UA MAY send a REGISTER request with the To header field value set to any of the associated URIs and without a Contact header field. The 200 (OK) response will include a Contact header

field with the list of addresses-of-record that have been registered with contact addresses. If the associated URI is not registered, the UA MAY register it prior to its utilization.

4.1.1. Applicability Statement for the P-Associated-URI Header Field

The P-Associated-URI header field is applicable in SIP networks where the SIP provider allows a set of identities that a user can claim (in header fields like the From header field) in requests that the UA generates. Furthermore, it assumes that the provider knows the entire set of identities that a user can legitimately claim and that the user is willing to restrict its claimed identities to that set. This is in contrast to normal SIP usage, where the From header field is explicitly an end-user-specified field.

4.1.2. Usage of the P-Associated-URI Header Field

The registrar inserts the P-Associated-URI header field into the 200 (OK) response to a REGISTER request. The header field value is populated with a list of URIs that are associated to the address-of-record.

If the registrar supports the P-Associated-URI header field extension and there is at least one associated URI, then the registrar MUST insert the P-Associated-URI header field in all the 200 (OK) responses to a REGISTER request. The absence of a P-Associated-URI header field indicates that there are no associated URIs for the registered address-of-record.

4.1.2.1. Procedures at the UA

A UAC may receive a P-Associated-URI header field in the 200 (OK) response for a REGISTER request. The presence of a header field in the 200 (OK) response for a REGISTER request implies that the extension is supported at the registrar.

The header field value contains a list of one or more associated URIs to the address-of-record. The UAC MAY use any of the associated URIs to populate the From header field value, or any other SIP header field value that provides information of the identity of the calling party, in a subsequent request.

The UAC MAY check whether or not the associated URI is registered. This check can be done, e.g., by populating the To header field value in a REGISTER request sent to the registrar and without a Contact header field. The 200 (OK) response will include a Contact header field with the list of address-of-record that have been registered

with contact addresses. As described in SIP [RFC3261], the 200 (OK) response may contain a Contact header field with zero or more values (zero meaning the address-of-record is not registered).

4.1.2.2. Procedures at the Registrar

A registrar that receives and authorizes a REGISTER request MAY associate zero or more URIs with the registered address-of-record.

If the address-of-record under registration does not have any associated URIs, the P-Associated-URI header field SHALL NOT be included.

Otherwise, a registrar that supports this specification MUST include a P-Associated-URI header field in the 200 (OK) response to a REGISTER request that contains a contact header. The header field MUST be populated with a comma-separated list of URIs that are associated to the address-of-record under registration.

4.1.2.3. Procedures at the Proxy

This header is not intended to be used by proxies -- a proxy does not add, read, modify, or delete the header field; therefore, any proxy MUST relay this header field unchanged.

4.2. The P-Called-Party-ID Header Field

A proxy server inserts a P-Called-Party-ID header field, typically in an INVITE request, en route to its destination. The header is populated with the Request-URI received by the proxy in the request. The User Agent Server (UAS) identifies to which address-of-record, out of several registered addresses-of-record, the invitation was sent (for example, the user may be simultaneously using one personal SIP URI and one business SIP URI to receive invitation to sessions). The UAS can use the information to render different distinctive audiovisual alerting tones, depending on the URI used to receive the invitation to the session.

Users in the 3GPP IP Multimedia Subsystem (IMS) may get one or several SIP URIs (address-of-record) to identify the user. For example, a user may get one business SIP URI and one personal SIP URI. As an example of utilization, the user may make available the business SIP URI to coworkers and may make available the personal SIP URI to members of the family.

At a certain point in time, both the business SIP URI and the personal SIP URI are registered in the SIP registrar, so both URIs can receive invitations to new sessions. When the user receives an invitation to join a session, he/she should be aware of which of the registered SIP URIs this session was sent to.

This requirement is stated in the 3GPP Release 5 requirements on SIP [RFC4083].

The problem arises during the terminating side of a session establishment. At that time, the SIP proxy that is serving a UA gets an INVITE request, and the SIP server retargets the SIP URI that is present in the Request-URI, and replaces that SIP URI with the SIP URI published by the user in the Contact header field of the REGISTER request at registration time.

One can argue that the To header field conveys the semantics of the called user, and therefore, this extension to SIP is not needed. Although the To header field in SIP may convey the called party ID in most situations, there are two particular cases when the above assumption is not correct:

1. The session has been forwarded, redirected, etc., by previous SIP proxies, before arriving to the proxy that is serving the called user.

2. The UAC builds an INVITE request and the To header field is not the same as the Request-URI.

The problem of using the To header field is that this field is populated by the UAC and not modified by proxies in the path. If the UAC, for any reason, did not populate the To header field with the address-of-record of the destination user, then the destination user is not able to distinguish to which address-of-record the session was destined.

Another possible solution to the problem is built upon the differentiation of the Contact header field value between different address-of-record at registration time. The UA can differentiate each address-of-record it registers by assigning a different Contact header field value. For example, when the UA registers the address-of-record sip:id1, the Contact header field value can be sip:id1@ua, while the registration of the address-of-record sip:id2 can be bound to the Contact header field value sip:id2@ua.

The solution described above assumes that the UA explicitly registers each of its addresses-of-record, and therefore, it has full control over the contact address values assigned to each registration.

However, if the UA does not have full control of its registered addresses-of-record, because of, e.g., a third-party registration, the solution does not work. This may be the case of the 3GPP registration, where the UA may have previously indicated to the network, by means outside of SIP, that some other addresses-of-record may be automatically registered when the UA registers a particular address-of-record. The requirement is covered in the 3GPP Release 5 requirements on SIP [RFC4083].

In the next paragraphs, we show an example of the problem, in the case in which there has been some sort of call forwarding in the session, so that the UAC is not aware of the intended destination URI in the current INVITE request.

We assume that a UA is registering to its proxy (P1).

```
  Scenario                      UA --- P1

       F1 Register UA -> P1
            REGISTER sip:example.com SIP/2.0
            Via: SIP/2.0/UDP 192.0.2.4:5060;branch=z9hG4bKnashds7
            To: sip:user1-business@example.com
            From: sip:user1-business@example.com;tag=456248
            Call-ID: 843817637684230998sdasdh09
            CSeq: 1826 REGISTER
            Contact: <sip:user1@192.0.2.4>
```

The user also registers his personal URI to his/her registrar.

```
       F2 Register UA -> P1
            REGISTER sip:example.com SIP/2.0
            Via: SIP/2.0/UDP 192.0.2.4:5060;branch=z9hG4bKnashdt8
            To: sip:user1-personal@example.com
            From: sip:user1-personal@example.com;tag=346249
            Call-ID: 2Q3817637684230998sdasdh10
            CSeq: 1827 REGISTER
            Contact: <sip:user1@192.0.2.4>
```

Later, the proxy/registrar (P1) receives an INVITE request from another proxy (P2) destined to the user's business SIP address-of-record. We assume that this INVITE request has undergone some sort of forwarding in the past, and as such, the To header field is not populated with the SIP URI of the user. In this case, we assume that the session was initially addressed to sip:other-user@othernetwork.com. The SIP server at othernetwork.com has forwarded this session to sip:user1-business@example.com.

```
   Scenario                      UA --- P1 --- P2

  F3 Invite P2 -> P1
       INVITE sip:user1-business@example.com SIP/2.0
       Via: SIP/2.0/UDP 192.0.2.20:5060;branch=z9hG4bK03djaoe1
       To: sip:other-user@othernetwork.com
       From: sip:another-user@anothernetwork.com;tag=938s0
       Call-ID: 843817637684230998sdasdh09
       CSeq: 101 INVITE
```

The proxy P1 retargets the user and replaces the Request-URI with the SIP URI published during registration time in the Contact header field value.

```
  F4 Invite P1 -> UA
       INVITE sip:user1@192.0.2.4 SIP/2.0
       Via: SIP/2.0/UDP 192.0.2.10:5060;branch=z9hG4bKg48sh128
       Via: SIP/2.0/UDP 192.0.2.20:5060;branch=z9hG4bK03djaoe1
       To: sip:other-user@othernetwork.com
       From: sip:another-user@anothernetwork.com;tag=938s0
       Call-ID: 843817637684230998sdasdh09
       CSeq: 101 INVITE
```

When the UAS receives the INVITE request, it cannot determine whether it got the session invitation due to his registration of the business or the personal address-of-record. Neither the UAS nor proxies / application servers can provide this user a service based on the destination address-of-record of the session.

We solve this problem by allowing the proxy that is responsible for the home domain (as defined in SIP) of the user to insert a P-Called-Party-ID header field that identifies the address-of-record to which this session is destined.

If this SIP extension is used, the proxy serving the called user will get the message flow F5, it will populate the P-Called-Party-ID header field in message flow F6 with the contents of the Request-URI in F4. This is show in flows F5 and F6 below:

```
F5 Invite P2 -> P1
     INVITE sip:user1-business@example.com SIP/2.0
     Via: SIP/2.0/UDP 192.0.2.20:5060;branch=z9hG4bK03djaoe1
     To: sip:other-user@othernetwork.com
     From: sip:another-user@anothernetwork.com;tag=938s0
     Call-ID: 843817637684230998sdasdh09
     CSeq: 101 INVITE

F6 Invite P1 -> UA
     INVITE sip:user1@192.0.2.4 SIP/2.0
     Via: SIP/2.0/UDP 192.0.2.10:5060;branch=z9hG4bKg48sh128
     Via: SIP/2.0/UDP 192.0.2.20:5060;branch=z9hG4bK03djaoe1
     To: sip:other-user@othernetwork.com
     From: sip:another-user@anothernetwork.com;tag=938s0
     Call-ID: 843817637684230998sdasdh09
     P-Called-Party-ID: <sip:user1-business@example.com>
     CSeq: 101 INVITE
```

When the UA receives the INVITE request F6, it can determine the intended address-of-record of the session and apply whatever service is needed for that address-of-record.

4.2.1. Applicability Statement for the P-Called-Party-ID Header Field

The P-Called-Party-ID header field is applicable when the UAS needs to be aware of the intended address-of-record that was present in the Request-URI of the request, before the proxy retargets to the contact address. The UAS may be interested in applying different audiovisual alerting effects or other filtering services, depending on the intended destination of the request. It is especially valuable when the UAS has registered several addresses-of-record to his registrar, and therefore, the UAS is not aware of the address-of-record that was present in the INVITE request when it hit his proxy/registrar, unless this extension is used.

P-Called-Party-ID header field and the History-Info header field: At the time RFC 3455 [RFC3455] was written, the History-Info header field was a long way from specification. This header has now been specified and approved in RFC 7044 [RFC7044]. It is acknowledged that the History-Info header field will provide equivalent coverage to that of the P-Called-Party-ID header field. However, the P-Called-Party-ID header field is used entirely within the 3GPP system and does not appear to SIP entities outside that of a single 3GPP operator.

4.2.2. Usage of the P-Called-Party-ID Header Field

The P-Called-Party-ID header field provides proxies and the UAS with the address-of-record that was present in the Request-URI of the request, before a proxy retargets the request. This information is intended to be used by subsequent proxies in the path or by the UAS.

Typically, a SIP proxy inserts the P-Called-Party-ID header field prior to retargetting the Request-URI in the SIP request. The header field value is populated with the contents of the Request-URI, prior to replacing it with the contact address.

4.2.2.1. Procedures at the UA

A UAC MUST NOT insert a P-Called-Party-ID header field in any SIP request or response.

A UAS may receive a SIP request that contains a P-Called-Party-ID header field. The header field will be populated with the address-of-record received by the proxy in the Request-URI of the request, prior to its forwarding to the UAS.

The UAS MAY use the value in the P-Called-Party-ID header field to provide services based on the called party URI, such as, e.g., filtering of calls depending on the date and time, distinctive presentation services, distinctive alerting tones, etc.

4.2.2.2. Procedures at the Proxy

A proxy that has access to the contact information of the user can insert a P-Called-Party-ID header field in any of the requests indicated in Section 5.7. When included, the proxy MUST populate the header field value with the contents of the Request-URI present in the SIP request that the proxy received.

It is necessary that the proxy that inserts the P-Called-Party-ID header field has information about the user, in order to prevent a wrong delivery of the called party ID. This information may, for example, have been learned through a registration process.

A proxy or application server that receives a request containing a P-Called-Party-ID header field MAY use the contents of the header field to provide a service to the user based on the URI of that header field value.

A SIP proxy MUST NOT insert a P-Called-Party-ID header field in REGISTER requests.

4.3. The P-Visited-Network-ID Header Field

3GPP networks are composed of a collection of so-called home networks, visited networks, and subscribers. A particular home network may have roaming agreements with one or more visited networks. The effect of this is that when a mobile terminal is roaming, it can use resources provided by the visited network in a transparent fashion.

One of the conditions for a home network to accept the registration of a UA roaming to a particular visited network, is the existence of a roaming agreement between the home and the visited network. There is a need to indicate to the home network which network is the visited network that is providing services to the roaming UA.

3GPP user agents always register to the home network. The REGISTER request is proxied by one or more proxies located in the visited network towards the home network. For the sake of a simple approach, it seems sensible that the visited network includes an identification that is known to the home network. This identification should be globally unique, and it takes the form of a quoted-text string or a token. The home network may use this identification to verify the existence of a roaming agreement with the visited network, and to authorize the registration through that visited network.

Note that P-Visited-Network-ID information reveals the location of the user, to the level of the coverage area of the visited network. For a national network, for example, P-Visited-Network-ID would reveal that the user is in the country in question.

4.3.1. Applicability Statement for the P-Visited-Network-ID Header Field

The P-Visited-Network-ID header field is applicable whenever the following circumstances are met:

1. There is transitive trust in intermediate proxies between the UA and the home network proxy via established relationships between the home network and the visited network, supported by the use of standard security mechanisms, e.g., IPsec, Authentication and Key Agreement (AKA), or Transport Layer Security (TLS).

2. An endpoint is using resources provided by one or more visited networks (a network to which the user does not have a direct business relationship).

3. A proxy that is located in one of the visited networks wants to be identified at the user’s home network.

4. There is no requirement that every visited network need be identified at the home network. Those networks that want to be identified make use of this extension. Those networks that do not want to be identified do nothing.

5. A commonly pre-agreed text string or token identifies the visited network at the home network.

6. The UAC sends a REGISTER request or dialog-initiating request (e.g., INVITE request) or a standalone request outside a dialog (e.g., OPTIONS request) to a proxy in a visited network.

7. The request traverses, en route to its destination, a first proxy located in the visited network and a second proxy located in the home network or its destination is the registrar in the home network.

8. The registrar or home proxy verifies and authorizes the usage of resources (e.g., proxies) in the visited network.

The P-Visited-Network-ID header field assumes that there is trust relationship between a home network and one or more transited visited networks. It is possible for other proxies between the proxy in the visited network that inserts the header, and the registrar or the home proxy, to modify the value of P-Visited-Network-ID header field. Therefore, intermediaries participating in this mechanism MUST apply a hop-by-hop integrity-protection mechanism such as IPsec or other available mechanisms in order to prevent such attacks.

4.3.2. Usage of the P-Visited-Network-ID Header Field

The P-Visited-Network-ID header field is used to convey to the registrar or home proxy in the home network the identifier of a visited network. The identifier is a text string or token that is known by both the registrar or the home proxy at the home network and the proxies in the visited network.

Typically, the home network authorizes the UA to roam to a particular visited network. This action requires an existing roaming agreement between the home and the visited network.

While it is possible for a home network to identify one or more visited networks by inspecting the domain name in the Via header fields, this approach has a heavy dependency on DNS. It is an option for a proxy to populate the Via header field with an IP address, for example, and in the absence of a reverse DNS entry, the IP address will not convey the desired information.

Any SIP proxy in the visited network that receives any of the requests indicated in Section 5.7 MAY insert a P-Visited-Network-ID header field when it forwards the request. In case a REGISTER request or other request is traversing different administrative domains (e.g., different visited networks), a SIP proxy MAY insert a new P-Visited-Network-ID header field if the request does not contain a P-Visited-Network-ID header field with the same network identifier as its own network identifier (e.g., if the request has traversed other different administrative domains).

Note also that, there is no requirement for this header field value to be readable in the proxies. Therefore, a first proxy MAY insert an encrypted header field that only the registrar can decrypt. If the request traverses a second proxy located in the same administrative domain as the first proxy, the second proxy may not be able to read the contents of the P-Visited-Network-ID header field. In this situation, the second proxy will consider that its visited network identifier is not already present in the value of the header field, and therefore, it will insert a new P-Visited-Network-ID header field value (hopefully with the same identifier that the first proxy inserted, although perhaps, not encrypted). When the request arrives at the registrar or proxy in the home network, it will notice that the header field value is repeated (both the first and the second proxy inserted it). The decrypted values should be the same, because both proxies where part of the same administrative domain. While this situation is not desirable, it does not create any harm at the registrar or proxy in the home network.

The P-Visited-Network-ID header field is normally used at registration. However, this extension does not preclude other usages. For example, a proxy located in a visited network that does not maintain registration state MAY insert a P-Visited-Network-ID header field into any standalone request outside a dialog or a request that creates a dialog. At the time of writing this document, the only requests that create dialogs are INVITE requests [RFC3261], SUBSCRIBE requests [RFC6665], and REFER requests [RFC3515].

In order to avoid conflicts with identifiers, especially when the number of roaming agreements between networks increase, care must be taken when selecting the value of the P-Visited-Network-ID header field. The identifier MUST be globally unique to avoid duplications. Although there are many mechanisms to create globally unique identifiers across networks, one such mechanism is already in operation, and that is DNS. The P-Visited-Network-ID header field does not have any connection to DNS, but the values in the header field can be chosen from the DNS entry representing the domain name of the network. This guarantees the uniqueness of the value.

4.3.2.1. Procedures at the UA

In the context of the network to which the header fields defined in this document apply, a User Agent has no knowledge of the P-Visited-Network-ID when sending the REGISTER request. Therefore, UACs MUST NOT insert a P-Visited-Network-ID header field in any SIP message.

4.3.2.2. Procedures at the Registrar and Proxy

A SIP proxy that is located in a visited network MAY insert a P-Visited-Network-ID header field in any of the requests indicated in Section 5.7. The header field MUST be populated with the contents of a text string or a token that identifies the administrative domain of the network where the proxy is operating towards the user's home network.

A SIP proxy or registrar which is located in the home network can use the contents of the P-Visited-Network-ID header field as an identifier of one or more visited networks that the request traversed. The proxy or registrar in the home network may take local-policy-driven actions based on the existence (or nonexistence) of a roaming agreement between the home and the visited networks. This means, for instance, the authorization of the actions of the request is based on the contents of the P-Visited-Network-ID header field.

A SIP proxy that is located in the home network MUST delete this header field when forwarding the message outside the home network administrative domain, in order to retain the user's privacy.

A SIP proxy that is located in the home network SHOULD delete this header field when the home proxy has used the contents of the header field or the request is routed based on the called party's identification, even when the request is not forwarded outside the home network administrative domain.

Note that a received P-Visited-Network-ID from a UA is not allowed and MUST be deleted when the request is forwarded.

4.3.2.3. Examples of Usage

We present an example in the context of the scenario shown in the following network diagram:

This example shows the message sequence for a REGISTER transaction originating from UA eventually arriving at the REGISTRAR. P1 is an outbound proxy in the visited network for UA. In this case, P1 inserts the P-Visited-Network-ID header field. Then, P1 routes the REGISTER request to REGISTRAR via P2.

Message sequence for REGISTER using P-Visited-Network-ID header field:

```
F1 Register UA -> P1
     REGISTER sip:example.com SIP/2.0
     Via: SIP/2.0/UDP 192.0.2.4:5060;branch=z9hG4bKnashds7
     To: sip:user1-business@example.com
     From: sip:user1-business@example.com;tag=456248
     Call-ID: 843817637684230998sdasdh09
     CSeq: 1826 REGISTER
     Contact: <sip:user1@192.0.2.4>
```

In flow F2, proxy P1 adds its own identifier in a quoted string to the P-Visited-Network-ID header field.

```
F2 Register P1 -> P2
     REGISTER sip:example.com SIP/2.0
     Via: SIP/2.0/UDP p1@visited.net;branch=z9hG4bK203igld
     Via: SIP/2.0/UDP 192.0.2.4:5060;branch=z9hG4bKnashd8
     To: sip:user1-personal@example.com
     From: sip:user1-personal@example.com;tag=346249
     Call-ID: 2Q38176376842309 98sdasdh10
     CSeq: 1826 REGISTER
     Contact: <sip:user1@192.0.2.4>
     P-Visited-Network-ID: "Visited network number 1"
```

Finally, in flow F3, proxy P2 decides to insert its own identifier, derived from its own domain name to the P-Visited-Network-ID header field.

```
F3 Register P2 -> REGISTRAR
     REGISTER sip:example.com SIP/2.0
     Via: SIP/2.0/UDP p2@other.net;branch=z9hG4bK2bndnvk
     Via: SIP/2.0/UDP p1@visited.net;branch=z9hG4bK203igld
     Via: SIP/2.0/UDP 192.0.2.4:5060;branch=z9hG4bKnashd8
     To: sip:user1-personal@example.com
     From: sip:user1-personal@example.com;tag=346249
     Call-ID: 2Q38176376842309 98sdasdh10
     CSeq: 1826 REGISTER
     Contact: <sip:user1@192.0.2.4>
     P-Visited-Network-ID: other.net,"Visited network number 1"
```

4.4. The P-Access-Network-Info Header Field

This section describes the P-Access-Network-Info header field. This header field is useful in SIP-based networks that also provide Layer 2 (L2) / Layer 3 (L3) connectivity through different access technologies. SIP UAs may use this header field to relay information about the access technology to proxies that are providing services. The serving proxy may then use this information to optimize services for the UA. For example, a 3GPP UA may use this header field to pass information about the access network such as radio access technology and radio cell identity to its home service provider.

For the purpose of this extension, we define an access network as the network providing the L2/L3 IP connectivity, which, in turn, provides a user with access to the SIP capabilities and services provided.

In some cases, the SIP server that provides the user with services may wish to know information about the type of access network that the UA is currently using. Some services are more suitable or less suitable depending on the access type, and some services are of more value to subscribers if the access network details are known by the SIP proxy that provides the user with services.

In other cases, the SIP server that provides the user with services may simply wish to know crude location information in order to provide certain services to the user. For example, many of the location-based services available in wireless networks today require the home network to know the identity of the cell the user is being served by.

Some regulatory requirements exist mandating that for cellular radio systems, the identity of the cell where an emergency call is established is made available to the emergency authorities.

The SIP server that provides services to the user may desire to have knowledge about the access network. This is achieved by defining a new private SIP extension header field, P-Access-Network-Info header field. This header field carries information relating to the access network between the UAC and its serving proxy in the home network.

A proxy providing services based on the P-Access-Network-Info header field must consider the trust relationship to the UA or outbound proxy including the P-Access-Network-Info header field.

4.4.1. Applicability Statement for the P-Access-Network-Info Header Field

This mechanism is appropriate in environments where SIP services are dependent on SIP elements knowing details about the IP and lower-layer technologies used by a UA to connect to the SIP network. Specifically, the extension requires that the UA know the access technology it is using, and that a proxy desires such information to provide services. Generally, SIP is built on the everything over IP and IP over everything principle, where the access technology is not relevant for the operation of SIP. Since SIP systems generally should not care or even know about the access technology, this SIP extension is not for general SIP usage.

The information revealed in the P-Access-Network-Info header field is potentially very sensitive. Proper protection of this information depends on the existence of specific business and security relationships amongst the proxies that will see SIP messages containing this header field. It also depends on explicit knowledge of the UA of the existence of those relationships. Therefore, this mechanism is only suitable in environments where the appropriate relationships are in place, and the UA has explicit knowledge that they exist.

4.4.2. Usage of the P-Access-Network-Info Header

When a UA generates a SIP request or response that it knows is going to be securely sent to its SIP proxy that is providing services, the UA inserts a P-Access-Network-Info header field into field the SIP message. This header contains information on the access network that the UA is using to get IP connectivity. The header is typically ignored by intermediate proxies between the UA and the SIP proxy that is providing services. The proxy providing services can inspect the header and make use of the information contained there to provide appropriate services, depending on the value of the header. Before proxying the request onwards to an untrusted administrative network domain, this proxy strips the header from the message.

Additionally, the first outbound proxy, if in possession of appropriate information, can also add a P-Access-Network-Info header field with its own information.

4.4.2.1. UA Behavior

A UA that supports this extension and is willing to disclose the related parameters MAY insert the P-Access-Network-Info header field in any SIP request or response.

The UA inserting this information MUST have a trust relationship with the proxy that is providing services to protect its privacy by deleting the header before forwarding the message outside of the proxy's domain. This proxy is typically located in the home network.

In order to avoid the deletion of the header, there MUST also be a transitive trust in intermediate proxies between the UA and the proxy that provides the services. This trust is established by business agreements between the home network and the access network, and generally supported by the use of standard security mechanisms, e.g., IPsec, AKA, and TLS.

4.4.2.2. Proxy Behavior

A proxy MUST NOT modify the value of the P-Access-Network-Info header field.

A proxy in possession of appropriate information about the access technology MAY insert a P-Access-Network-Info header field with its own values. A proxy sending towards an untrusted entity MUST remove any P-Access-Network-Info header field containing a "network-provided" value.

A proxy that is providing services to the UA, can act upon any information present in the P-Access-Network-Info header field value, if is present, to provide a different service depending on the network or the location through which the UA is accessing the server. For example, for cellular radio access networks, the SIP proxy located in the home network MAY use the cell ID to provide basic localized services.

A proxy that provides services to the user is typically located in the home network and is therefore trusted. It MUST delete the header when the SIP signaling is forwarded to a SIP server located in an untrusted administrative network domain. The SIP server providing services to the UA uses the access network information that is of no interest to other proxies located in different administrative domains.

4.5. The P-Charging-Function-Addresses Header Field

3GPP has defined a distributed architecture that results in multiple network entities becoming involved in providing access and services. There is a need to inform each SIP proxy involved in a transaction about the common charging functional entities to receive the generated charging records or charging events.

The solution provided by 3GPP is to define two types of charging functional entities: Charging Collection Function (CCF) and Event Charging Function (ECF). CCF is used for offline charging (e.g., for postpaid account charging). ECF is used for online charging (e.g., for pre-paid account charging). There may be more than a single instance of CCF and ECF in a network, in order to provide redundancy in the network. In case there are more than a single instance of either the CCF or the ECF addresses, implementations SHOULD attempt sending the charging data to the ECF or CCF address, starting with the first address of the sequence (if any) in the P-Charging-Function-Addresses header field. If the first address of the sequence is not available, then the next address (ccf-2 or ecf-2) MUST be used if available. The CCF and ECF addresses MAY be passed during the establishment of a dialog or in a standalone transaction. More detailed information about charging can be found in 3GPP TS 32.240 [TS32.240] and 3GPP TS 32.260 [TS32.260].

We define the SIP private header field P-Charging-Function-Addresses header field. A proxy MAY include this header field, if not already present, in either the initial request or response for a dialog or in the request and response of a standalone transaction outside a dialog. When present, only one instance of the header MUST be present in a particular request or response.

The mechanisms by which a SIP proxy collects the values to populate the P-Charging-Function-Addresses header field values are outside the scope of this document. However, as an example, a SIP proxy may have preconfigured these addresses or may obtain them from a subscriber database.

4.5.1. Applicability Statement for the P-Charging-Function-Addresses Header Field

The P-Charging-Function-Addresses header field is applicable within a single private administrative domain where coordination of charging is required, for example, according to the architecture specified in 3GPP TS 32.240 [TS32.240].

The P-Charging-Function-Addresses header field is not included in a SIP message sent outside of the own administrative domain. The header is not applicable if the administrative domain does not provide a charging function.

The P-Charging-Function-Addresses header field is applicable whenever the following circumstances are met:

1. A UA sends a REGISTER or dialog-initiating request (e.g., INVITE request) or a standalone transaction request outside a dialog to a proxy located in the administrative domain of a private network.

2. A registrar, proxy, or UA that is located in the administrative domain of the private network wants to generate charging records.

3. A registrar, proxy, or UA that is located in the private network has access to the addresses of the charging function entities for that network.

4. There are other proxies that are located in the same administrative domain of the private network and that generate charging records or charging events. The proxies want to send, by means outside SIP, the charging information to the same charging collecting entities than the first proxy.

4.5.2. Usage of the P-Charging-Function-Addresses Header Field

A SIP proxy that receives a SIP request MAY insert a P-Charging-Function-Addresses header field prior to forwarding the request, if the header was not already present in the SIP request. The header filed contains one or more parameters that contain the hostnames or IP addresses of the nodes that are willing to receive charging information.

A SIP proxy that receives a SIP request that includes a P-Charging-Function-Addresses header field can use the hostnames or IP addresses included in the value, as the destination of charging information or charging events. The means to send those charging information or events are outside the scope of this document, and usually, do not use SIP for that purpose.

4.5.2.1. Procedures at the UA

This document does not specify any procedure at the UA located outside the administrative domain of a private network, with regard to the P-Charging-Function-Addresses header field. Such UAs need not understand this header.

However, it might be possible that a UA is located within the administrative domain of a private network (e.g., a Public Switched Telephone Network (PSTN) gateway, or conference mixer), and it may have access to the addresses of the charging entities. In this case,

a UA MAY insert the P-Charging-Function-Addresses header field in a SIP request or response when the next hop for the message is a proxy or UA located in the same administrative domain. Similarly, such a UA MAY use the contents of the P-Charging-Function-Addresses header field in communicating with the charging entities.

4.5.2.2. Procedures at the Proxy

A SIP proxy that supports this extension and receives a request or response without the P-Charging-Function-Addresses header field MAY insert a P-Charging-Function-Addresses header field prior to forwarding the message. The header is populated with a list of the addresses of one or more charging entities where the proxy should send charging-related information.

If a proxy that supports this extension receives a request or response with the P-Charging-Function-Addresses header field, it MAY retrieve the information from the header field to use with application-specific logic, i.e., charging. If the next hop for the message is within the administrative domain of the proxy, then the proxy SHOULD include the P-Charging-Function-Addresses header field in the outbound message. However, if the next hop for the message is outside the administrative domain of the proxy, then the proxy MUST remove the P-Charging-Function-Addresses header field.

4.5.2.3. Examples of Usage

We present an example in the context of the scenario shown in the following network diagram:

In this scenario, we assume that P1 and P2 belong to the same administrative domain.

The example below shows the message sequence for an INVITE transaction originating from UA1 and eventually arriving at UA2. P1 is an outbound proxy for UA1. In this case, P1 inserts charging information. Then, P1 routes the request via P2 to UA2.

Message sequence for INVITE using P-Charging-Function-Addresses header field:

```
F1 Invite UA1 -> P1
   INVITE sip:ua2@home1.net SIP/2.0
   Via: SIP/2.0/UDP 192.0.2.4:5060;branch=z9hG4bKnashds7
   To: sip:ua2@home1.net
   From: sip:ua1@home1.net;tag=456248
   Call-ID: 843817637684230998sdasdh09
   CSeq: 18 INVITE
   Contact: sip:ua1@192.0.2.4

F2 Invite P1 -> P2
   INVITE sip:ua2@home1.net SIP/2.0
   Via: SIP/2.0/UDP p1@home1.net:5060;branch=z9hG4bK34ghi7ab04
   Via: SIP/2.0/UDP 192.0.2.4:5060;branch=z9hG4bKnashds7
   To: sip:ua2@home1.net
   From: sip:ua1@home1.net;tag=456248
   Call-ID: 843817637684230998sdasdh09
   CSeq: 18 INVITE
   Contact: sip:ua1@192.0.2.4
   P-Charging-Function-Addresses:
                             ccf=192.0.8.1; ecf=192.0.8.3,
                             ccf-2=192.0.8.2; ecf-2=192.0.8.4
```

Now both P1 and P2 are aware of the IP addresses of the entities that collect charging record or charging events. Both proxies can send the charging information to the same entities.

4.6. The P-Charging-Vector Header Field

3GPP has defined a distributed architecture that results in multiple network entities becoming involved in providing access and services. Operators need the ability and flexibility to charge for the access and services as they see fit. This requires coordination among the network entities (e.g., SIP proxies), which includes correlating charging records generated from different entities that are related to the same session.

The correlation information includes, but is not limited to, a globally unique charging identifier that makes the billing effort easy.

A charging vector is defined as a collection of charging information. The charging vector MAY be filled in during the establishment of a dialog or standalone transaction outside a dialog. The information inside the charging vector MAY be filled in by multiple network entities (including SIP proxies) and retrieved by multiple network

entities. There are three types of correlation information to be transferred: the IMS Charging Identity (ICID) value, the address of the SIP proxy that creates the ICID value, and the Inter Operator Identifier (IOI).

ICID is a charging value that identifies a dialog or a transaction outside a dialog. It is used to correlate charging records. ICID MUST be a globally unique value. One way to achieve globally uniqueness is to generate the ICID using two components: a locally unique value and the hostname or IP address of the SIP proxy that generated the locally unique value.

The IOI identifies both the originating and terminating networks involved in a SIP dialog or transaction outside a dialog. There MAY be an IOI generated from each side of the dialog to identify the network associated with each side.

Additionally, in a multi-network environment, one or more transit IOI identifiers MAY be included along the path of the SIP dialog or transaction outside a dialog. Due to network policy, a void value MAY be included instead of the transit network name. The void value is used to indicate that a transit network appeared but due to operator policy the network name is not shown.

Furthermore, in a multi-service provider environment, one or more transit IOIs MAY be included along the path of the SIP dialog or transaction outside a dialog. Due to service provider policy, a void value MAY be included instead of the transit service provider. The void value is used to indicate that a transit appeared but due to service provider policy the service provider name is not shown.

There is also expected to be access network charging information, which consists of network-specific identifiers for the access level (e.g., Universal Mobile Telecommunications System (UMTS) radio access network or IEEE 802.11b). The details of the information for each type of network are not described in this memo.

We define the SIP private header P-Charging-Vector header field. A proxy MAY include this header, if not already present, in either the initial request or response for a dialog, or in the request and response of a standalone transaction outside a dialog. When present, only one instance of the header MUST be present in a particular request or response.

The mechanisms by which a SIP proxy collects the values to populate the P-Charging-Vector header field are outside the scope of this document.

4.6.1. Applicability Statement for the P-Charging-Vector Header Field

The P-Charging-Vector header field is applicable within a single private administrative domain or between different administrative domains where there is a trust relationship between the domains.

The P-Charging-Vector header field is not included in a SIP message sent to another network if there is no trust relationship. The header is not applicable if the administrative domain manages charging in a way that does not require correlation of records from multiple network entities (e.g., SIP proxies).

The P-Charging-Vector header field is applicable whenever the following circumstances are met:

1. A UA sends a REGISTER or dialog-initiating request (e.g., INVITE) or mid-dialog request (e.g., UPDATE) or a standalone transaction request outside a dialog to a proxy located in the administrative domain of a private network.

2. A registrar, proxy, or UA that is located in the administrative domain of the private network wants to generate charging records.

3. A proxy or UA that is located in the administrative domain of the private network has access to the charging correlation information for that network.

4. Optionally, a registrar, proxy, or UA that is part of a second administrative domain in another private network, whose SIP requests and responses are traversed through, en route to/from the first private network, wants to generate charging records and correlate those records with those of the first private network. This assumes that there is a trust relationship between both private networks.

4.6.2. Usage of the P-Charging-Vector Header Field

The P-Charging-Vector header field is used to convey charging-related information, such as the globally unique IMS Charging Identity (ICID) value.

Typically, a SIP proxy that receives a SIP request that does not contain a P-Charging-Vector header field MAY insert it, with those parameters that are available at the SIP proxy.

A SIP proxy that receives a SIP request that contains a P-Charging-Vector header field can use the values, such as the globally unique ICID, to produce charging records.

4.6.2.1. Procedures at the UA

This document does not specify any procedure at a UA located outside the administrative domain of a private network (e.g., PSTN gateway or conference mixer), with regard to the P-Charging-Vector header field. UAs need not understand this header.

However, it might be possible that a UA be located within the administrative domain of a private network (e.g., a PSTN gateway, or conference mixer), and it may interact with the charging entities. In this case, a UA MAY insert the P-Charging-Vector header field in a SIP request or response when the next hop for the message is a proxy or UA located in the same administrative domain. Similarly, such a UA MAY use the contents of the P-Charging-Vector header field in communicating with the charging entities.

4.6.2.2. Procedures at the Proxy

A SIP proxy that supports this extension and receives a request or response without the P-Charging-Vector header field MAY insert a P-Charging-Vector header field prior to forwarding the message. The header is populated with one or more parameters, as described in the syntax, including but not limited to, a globally unique charging identifier.

If a proxy that supports this extension receives a request or response with the P-Charging-Vector header field, it MAY retrieve the information from the header value to use with application-specific logic, i.e., charging. If the next hop for the message is within the trusted domain, then the proxy SHOULD include the P-Charging-Vector header field in the outbound message. If the next hop for the message is outside the trusted domain, then the proxy MAY remove the P-Charging-Function-Addresses header field.

Per local application-specific logic, the proxy MAY modify the contents of the P-Charging-Vector header field prior to sending the message.

4.6.2.3. Examples of Usage

We present an example in the context of the scenario shown in the following network diagram:

This example shows the message sequence for an INVITE transaction originating from UA1 and eventually arriving at UA2. P1 is an outbound proxy for UA1. In this case, P1 inserts charging information. Then, P1 routes the call via P2 to UA2.

Message sequence for INVITE using P-Charging-Vector header field:

```
F1 Invite UA1 -> P1
     INVITE sip:joe@example.com SIP/2.0
     Via: SIP/2.0/UDP 192.0.2.4:5060;branch=z9hG4bKnashds7
     To: sip:joe@example.com
     From: sip:ua1@home1.net;tag=456248
     Call-ID: 843817637684230998sdasdh09
     CSeq: 18 INVITE
     Contact: sip:ua1@192.0.2.4

F2 Invite P1 -> P2
     INVITE sip:joe@example.com SIP/2.0
     Via: SIP/2.0/UDP P1@home1.net:5060;branch=z9hG4bK34ghi7a
     Via: SIP/2.0/UDP 192.0.2.4:5060;branch=z9hG4bKnashds7
     To: sip:joe@example.com
     From: sip:ua1@home1.net;tag=456248
     Call-ID: 843817637684230998sdasdh09
     CSeq: 18 INVITE
     Contact: sip:ua1@192.0.2.4
     P-Charging-Vector: icid-value=1234bc9876e;
                        icid-generated-at=192.0.6.8;
                        orig-ioi=home1.net
```

4.6.3. Usage of the transit-ioi

The transit-ioi is added to the P-Charging-Vector header field when traversing transit networks. It is allowed to have multiple transit-ioi values within one SIP message or response. The values within the response are independent from the values set up within the request.

The element could be added either by a transit network itself or by the succeeding network at the entry point where the preceding network is known. Based on network policy, a void value can be used.

Depending on the call scenario, each transit network can add either a transit network name or a void value. However, it cannot be guaranteed that all the values that are added will appear within the P-Charging-Vector header field.

Some networks can screen the P-Charging-Vector header field and delete transit-ioi values, e.g., networks not supporting this value. There are scenarios where the appearance of the transit-ioi values of all networks is needed to have a correct end-to-end view.

The policies of adding, modifying, and deleting transit-ioi values are out of the scope of this document.

The transit-ioi contains an indexed value that MUST be incremented with each value added to the P-Charging-Vector header field.

A void value has no index. By adding the next value, the index has to be incremented by the number of void entries +1.

4.6.3.1. Procedures at the Proxy

Procedures described within Section 4.5.2.2 apply. A transit-ioi MAY be added or modified by a proxy. A deletion of the transit-ioi or a entry within the tranist-ioi could appear depending on the network policy and trust rules. This is also valid by replacing the transit-ioi with a void value.

4.6.4. Usage of the related-icid

4.6.4.1. Procedures at the UA

The UAS acting as a B2BUA MAY add the related-icid into the P-Charging-Vector header field into SIP request or SIP responses. For example, the UAS can include the related-icid in a response to an INVITE request when the received INVITE request creates a new call leg towards the same remote end. The value of the related-icid is the icid value of the original dialog towards the remote end.

4.6.4.2. Procedures at the Proxy

Procedures described within Section 4.5.2.2 apply. A related-icid and "related-icid-generated-at" MAY be added or modified by a proxy. A deletion of the elements could appear depending on the network policy and trust rules.

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 5234 [RFC5234]. Further, several BNF definitions are inherited from SIP and are not repeated here. Implementors need to be familiar with the notation and contents of SIP [RFC3261] and [RFC5234] to understand this document.

5.1. P-Associated-URI Header Syntax

The syntax of the P-Associated-URI header field is described as follows:

```
P-Associated-URI       = "P-Associated-URI" HCOLON
                         [p-aso-uri-spec]
                         *(COMMA p-aso-uri-spec)
p-aso-uri-spec         = name-addr *(SEMI ai-param)
ai-param               = generic-param
```

5.2. P-Called-Party-ID Header Syntax

The syntax of the P-Called-Party-ID header field is described as follows:

```
P-Called-Party-ID      = "P-Called-Party-ID" HCOLON
                         called-pty-id-spec
called-pty-id-spec     = name-addr *(SEMI cpid-param)
cpid-param             = generic-param
```

5.3. P-Visited-Network-ID Header Syntax

The syntax of the P-Visited-Network-ID header field is described as follows:

```
P-Visited-Network-ID   = "P-Visited-Network-ID" HCOLON
                          vnetwork-spec
                          *(COMMA vnetwork-spec)
vnetwork-spec          = (token / quoted-string)
                          *(SEMI vnetwork-param)
vnetwork-param         = generic-param
```

5.4. P-Access-Network-Info Header Syntax

The syntax of the P-Access-Network-Info header field is described as follows:

```
P-Access-Network-Info  = "P-Access-Network-Info" HCOLON
                          access-net-spec *(COMMA access-net-spec)
access-net-spec        = (access-type / access-class)
                         *(SEMI access-info)
access-type            = "IEEE-802.11" / "IEEE-802.11a" /
                         "IEEE-802.11b" / "IEEE-802.11g" /
                         "IEEE-802.11n" /
                         "IEEE-802.3" / "IEEE-802.3a" /
                         "IEEE-802.3ab" / "IEEE-802.3ae" /
                         "IEEE-802.3ak" / "IEEE-802.3ah" /
```

```
                              "IEEE-802.3aq" / "IEEE-802.3an" /
                              "IEEE-802.3e" / "IEEE-802.3i" /
                              "IEEE-802.3j" / "IEEE-802.3u" /
                              "IEEE-802.3y" / "IEEE-802.3z" /
                              "3GPP-GERAN" /
                              "3GPP-UTRAN-FDD" / "3GPP-UTRAN-TDD" /
                              "3GPP-E-UTRAN-FDD" / "3GPP-E-UTRAN-TDD" /
                              "3GPP2-1X-Femto" / "3GPP2-UMB" /
                              "3GPP2-1X-HRPD" / "3GPP2-1X" /
                              "ADSL" / "ADSL2" / "ADSL2+" / "RADSL" /
                              "SDSL" / "HDSL" / "HDSL2" / "G.SHDSL" /
                              "VDSL" / "IDSL" /
                              "DOCSIS" / "GSTN" / "GPON" / " XGPON1" /
                              "DVB-RCS2" / token
      access-class           = "3GPP-GERAN" /  "3GPP-UTRAN" /
                               "3GPP-E-UTRAN" / "3GPP-WLAN" /
                               "3GPP-GAN" / "3GPP-HSPA" /
                               "3GPP2" / token
      access-info            = cgi-3gpp / utran-cell-id-3gpp /
                               dsl-location / i-wlan-node-id /
                               ci-3gpp2 / eth-location /
                               ci-3gpp2-femto / fiber-location /
                               np / gstn-location /local-time-zone /
                               dvb-rcs2-node-id / extension-access-info
      np                     = "network-provided"
      extension-access-info  = gen-value
      cgi-3gpp               = "cgi-3gpp" EQUAL
                                   (token / quoted-string)
      utran-cell-id-3gpp     = "utran-cell-id-3gpp" EQUAL
                                   (token / quoted-string)
      i-wlan-node-id         = "i-wlan-node-id" EQUAL
                                   (token / quoted-string)
      dsl-location           = "dsl-location" EQUAL
                                   (token / quoted-string)
      eth-location           = "eth-location" EQUAL
                                   (token / quoted-string)
      fiber-location         = "fiber-location" EQUAL
                                   (token / quoted-string)
      ci-3gpp2               = "ci-3gpp2" EQUAL
                                   (token / quoted-string)
      ci-3gpp2-femto         = "ci-3gpp2-femto" EQUAL
                                    (token / quoted-string)
      gstn-location          = "gstn-location" EQUAL
                                    (token / quoted-string)
      dvb-rcs2-node-id       = "dvb-rcs2-node-id" EQUAL
                                     quoted-string
      local-time-zone        = "local-time-zone"  EQUAL
                                    quoted-string
```

```
      operator-specific-GI   = "operator-specific-GI" EQUAL
                                    (token / quoted-string)
      utran-sai-3gpp         = "utran-sai-3gpp" EQUAL
                                    (token / quoted-string)
```

The access-info MAY contain additional information relating to the access network. The values for "cgi-3gpp", "utran-cell-id-3gpp", "i-wlan-node-id", "dsl-location", "ci-3gpp2", "ci-3gpp2-femto", and "gstn-location" are defined in 3GPP TS 24.229 [TS24.229].

5.5. P-Charging-Function-Addresses Header Syntax

The syntax for the P-Charging-Function-Addresses header field is described as follows:

```
  P-Charging-Addresses = "P-Charging-Function-Addresses" HCOLON
                          charge-addr-params *(COMMA charge-addr-params)
  charge-addr-params   = charge-addr-param *(SEMI charge-addr-param)
  charge-addr-param    = ccf / ecf / ccf-2 /ecf-2 / generic-param
  ccf                  = "ccf" EQUAL gen-value
  ecf                  = "ecf" EQUAL gen-value
  ccf-2                = "ccf-2" EQUAL gen-value
  ecf-2                = "ecf-2" EQUAL gen-value
```

The P-Charging-Function-Addresses header field contains one or two addresses of the ECF (ecf and ecf-2) or CCF (ccf and ccf-2). The first address of the sequence is ccf or ecf. If the first address of the sequence is not available, then the next address (ccf-2 or ecf-2) MUST be used if available.

5.6. P-Charging-Vector Header Syntax

The syntax for the P-Charging-Vector header field is described as follows:

```
P-Charging-Vector  = "P-Charging-Vector" HCOLON icid-value
                          *(SEMI charge-params)
charge-params      = icid-gen-addr / orig-ioi / term-ioi /
                     transit-ioi / related-icid /
                     related-icid-gen-addr / generic-param
icid-value               = "icid-value" EQUAL gen-value
icid-gen-addr            = "icid-generated-at" EQUAL host
orig-ioi                 = "orig-ioi" EQUAL gen-value
term-ioi                 = "term-ioi" EQUAL gen-value
transit-ioi              = "transit-ioi" EQUAL transit-ioi-list
transit-ioi-list         = DQUOTE transit-ioi-param
                              *(COMMA transit-ioi-param) DQUOTE
transit-ioi-param        = transit-ioi-indexed-value /
                           transit-ioi-void-value
transit-ioi-indexed-value = transit-ioi-name "."
                                       transit-ioi-index
transit-ioi-name         = ALPHA *(ALPHA / DIGIT)
transit-ioi-index        = 1*DIGIT
transit-ioi-void-value   = "void"
related-icid             = "related-icid" EQUAL gen-value
related-icid-gen-addr    = "related-icid-generated-at" EQUAL host
```

The P-Charging-Vector header field contains icid-value as a mandatory parameter. The icid-value represents the IMS charging ID, and contains an identifier used for correlating charging records and events. The first proxy that receives the request generates this value.

The icid-gen-addr parameter contains the hostname or IP address of the proxy that generated the icid-value.

The orig-ioi and term-ioi parameters contain originating and terminating interoperator identifiers. They are used to correlate charging records between different operators. The originating IOI represents the network responsible for the charging records in the originating part of the session or standalone request. Similarly, the terminating IOI represents the network responsible for the charging records in the terminating part of the session or standalone request.

The transit-ioi parameter contains values with each of them, respectively, representing a transit interoperator identifier. It is used to correlate charging records between different networks. The transit-ioi represents the network responsible for the records in the transit part of the session or standalone request.

The related-icid parameter contains the icid-value of a related charging record when more than one call leg is associated with one session. This optional parameter is used for correlation of charging information between two or more call legs related to the same remote-end dialog.

The related-icid-gen-addr parameter contains the hostname or IP address of the proxy that generated the related-icid.

Applications using the P-Charging-Vector header field within their own applicability are allowed to define generic-param extensions without further reference to the IETF specification process.

5.7. New Headers

The P-Associated-URI header field can appear in SIP REGISTER method and 2xx resonses. The P-Called-Party-ID header field can appear in SIP INVITE, OPTIONS, PUBLISH, SUBSCRIBE, and MESSAGE methods and all responses. The P-Visited-Network-ID header field can appear in all SIP methods except ACK, BYE, and CANCEL and all responses. The P-Access-Network-Info header field can appear in all SIP methods except ACK and CANCEL. The P-Charging-Vector header field can appear in all SIP methods except CANCEL. The P-Charging-Function-Addresses header field can appear in all SIP methods except ACK and CANCEL.

6. Security Considerations

6.1. P-Associated-URI Header Field

The information returned in the P-Associated-URI header field is not viewed as particularly sensitive. Rather, it is simply informational in nature, providing openness to the UAC with regard to the automatic association performed by the registrar. If end-to-end protection is not used at the SIP layer, it is possible for proxies between the registrar and the UA to modify the contents of the header value.

The lack of encryption, either end-to-end or hop-by-hop, may lead to leak some privacy regarding the list of authorized identities. For instance, a user who registers an address-of-record of sip:user1@example.com may get another SIP URI associated as sip:first.last@example.com returned in the P-Associated-URI header field value.

An eavesdropper could possibly collect the list of identities a user is registered. This can have privacy implications. To mitigate this problem, this extension SHOULD only be used in a secured environment, where encryption of SIP messages is provided either end-to-end or hop-by-hop and where a trust relationship equivalent with that defined in RFC 3325 [RFC3325] between entities exists. That is, the privacy of the user relies on the other entities in the session not disclosing information that they have learned about the user.

While the P-Associated-URI header field value allows the implicit registration of a bundle of URIs with one REGISTER Message, the impact of security using the P-Associated-URI header field is no higher than using separate REGISTER messages for each of the URIs.

6.2. P-Called-Party-ID Header Field

Due to the nature of the P-Called-Party-ID header field, this header does not introduce any significant security concern. It is possible for an attacker to modify the contents of the header. However, this modification will not cause any harm to the session establishment.

An eavesdropper could possibly collect the list of identities a user has registered. This can have privacy implications. To mitigate this problem, this extension SHOULD only be used in a secured environment, where encryption of SIP messages is provided either end-to-end or hop-by-hop.

Normally, within a 3GPP environment, the P-Called-Party-ID is not sent towards end users but may be exchanged between carriers where other security mechanisms than SIP encryption are used.

6.3. P-Visited-Network-ID Header Field

The P-Visited-Network-ID header field assumes that there is trust relationship between a home network and one or more transited visited networks. It is possible for other proxies between the proxy in the visited network that inserts the header, and the registrar or the home proxy, to modify the value of P-Visited-Network-ID header field. Therefore, intermediaries participating in this mechanism MUST apply a hop-by-hop integrity-protection mechanism such as IPsec or other available mechanisms in order to prevent such attacks.

6.4. P-Access-Network-Info Header Field

A Trust Domain is formally defined in RFC 3324 [RFC3324]. For the purposes of this document, we refer to the 3GPP trust domain as the collection of SIP proxies and application servers that are operated by a 3GPP network operator and are compliant with the requirements expressed in 3GPP TS 24.229 [TS24.229].

This extension assumes that the access network is trusted by the UA (because the UA's home network has a trust relationship with the access network), as described earlier in this document.

This extension assumes that the information added to the header by the UAC should be sent only to trusted entities and MUST NOT be used outside of the trusted administrative network domain.

The SIP proxy that provides services to the user, utilizes the information contained in this header to provide additional services and UAs are expected to provide correct information. However, there are no security problems resulting from a UA inserting incorrect information. Networks providing services based on the information carried in the P-Access-Network-Info header field will therefore need to trust the UA sending the information. A rogue UA sending false access network information will do no more harm than to restrict the user from using certain services.

The mechanism provided in this document is designed primarily for private systems like 3GPP. Most security requirements are met by way of private standardized solutions.

For instance, 3GPP will use the P-Access-Network-Info header field to carry relatively sensitive information like the cell ID. Therefore, the information MUST NOT be sent outside of the 3GPP domain.

The UA is aware -- if it is a 3GPP UA -- that it is operating within a trusted domain.

The 3GPP UA is aware of whether or not a secure association to the home network domain for transporting SIP signaling is currently available, and, as such, the sensitive information carried in the P-Access-Network-Info header field MUST NOT be sent in any initial unauthenticated and unprotected requests (e.g., REGISTER).

Any UA that is using this extension and is not part of a private trusted domain should not consider the mechanism as secure, and, as such, MUST NOT send sensitive information in the P-Access-Network-Info header field.

Any proxy that is operating in a private trust domain where the P-Access-Network-Info header field is supported is REQUIRED to delete the header, if it is present, from any message prior to forwarding it outside of the trusted domain.

A proxy receiving a message containing the P-Access-Network-Info header field from an untrusted entity is not able to guarantee the validity of the contents. Thus, this content SHOULD be deleted based on local policy.

6.5. P-Charging-Function-Addresses Header Field

It is expected as normal behavior that proxies within a closed network will modify the values of the P-Charging-Function-Addresses header field and insert it into a SIP request or response. However, the proxies that share this information MUST have a trust relationship.

If an untrusted entity were inserted between trusted entities, it could potentially substitute a different charging function address. Therefore, an integrity-protection mechanism such as IPsec or other available mechanisms MUST be applied in order to prevent such attacks. Since each trusted proxy MAY need to view or modify the values in the P-Charging-Function-Addresses header field, the protection should be applied on a hop-by-hop basis.

6.6. P-Charging-Vector Header Field

It is expected as normal behavior that proxies within a closed network will modify the values of the P-Charging-Vector header field and insert it into a SIP request or response. However, these proxies that share this information MUST have a trust relationship.

If an untrusted entity were inserted between trusted entities, it could potentially interfere with the charging correlation mechanism. Therefore, an integrity-protection mechanism such as IPsec or other available mechanisms MUST be applied in order to prevent such attacks. Since each trusted proxy MAY need to view or modify the values in the P-Charging-Vector header field, the protection should be applied on a hop-by-hop basis.

7. IANA Considerations

This document defines several private SIP extension header fields (beginning with the prefix "P-").

This document obsoletes [RFC3455] but uses the same SIP header field names. The references in the "Header Fields" registry and "Header Field Parameters and Parameter Values" registry have been updated to [RFC3455] to this document.

The following extensions are registered as private extension header fields:

```
Header Field Name:  P-Associated-URI
Compact Form:       none
Reference:          RFC 7315

Header Field Name:  P-Called-Party-ID
Compact Form:       none
Reference:          RFC 7315

Header Field Name:  P-Visited-Network-ID
Compact Form:       none
Reference:          RFC 7315

Header Field Name:  P-Access-Network-Info
Parameter Name:     ci-3gpp
Parameter Name:     ci-3gpp2
Parameter Name:     ci-3gpp2-femto
Parameter Name:     dsl-location
Parameter Name:     dvb-rcs2-node-id
Parameter Name:     eth-location
Parameter Name:     fiber-location
Parameter Name:     gstn-location
Parameter Name:     i-wlan-node-id
Parameter Name:     local-time-zone
Parameter Name:     operator-specific-GI
Parameter Name:     utran-cell-id-3gpp
Parameter Name:     utran-sai-3gpp
Compact Form:       none
Reference:          RFC 7315
```

Header Field Name:	P-Charging-Function-Addresses
Parameter Name:	ccf
Parameter Name:	ccf-2
Parameter Name:	ecf
Parameter Name:	ecf-2
Compact Form:	none
Reference:	RFC 7315

Header Field Name:	P-Charging-Vector
Parameter Name:	icid-value
Parameter Name:	icid-generated-at
Parameter Name:	orig-ioi
Parameter Name:	related-icid
Parameter Name:	related-icid-generated-at
Parameter Name:	term-ioi
Parameter Name:	transit-ioi
Compact Form:	none
Reference:	RFC 7315

8. Contributors and Acknowledgements

The authors would like to thank James Yu and Atle Monrad for their extensive review, Dean Willis for his expert review, and Mary Barnes for the proto review. The authors would like to acknowledge the constructive feedback and contributions provided by Peter Leis, Joergen Axell, and Jan Holm.

The extensions described in [RFC3455] were originally specified in several documents. Miguel Garcia-Martin authored the P-Associated-URI, P-Called-Party-ID, and P-Visited-Network-ID header fields. Duncan Mills authored the P-Access-Network-Info header. Eric Henrikson authored the P-Charging-Function-Addresses and P-Charging-Vector headers. Rohan Mahy assisted in the incorporation of these extensions into a single document.

The listed authors of [RFC3455] were Miguel Garcia-Martin, Eric Henrikson and Duncan Mills.

The [RFC3455] authors thanked Andrew Allen, Gabor Bajko, Gonzalo Camarillo, Keith Drage, Georg Mayer, Dean Willis, Rohan Mahy, Jonathan Rosenberg, Ya-Ching Tan, and the 3GPP CN1 WG members for their comments on [RFC3455].

9. References

9.1. Normative References

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

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

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

[TS24.229] 3GPP, "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", 3GPP TS 24.229 12.4.0, March 2014.

9.2. Informative References

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

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[RFC3455] Garcia-Martin, M., Henrikson, E., and D. Mills, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)", RFC 3455, January 2003.

[RFC3515] Sparks, R., "The Session Initiation Protocol (SIP) Refer Method", RFC 3515, April 2003.

[RFC4083] Garcia-Martin, M., "Input 3rd-Generation Partnership Project (3GPP) Release 5 Requirements on the Session Initiation Protocol (SIP)", RFC 4083, May 2005.

[RFC6665] Roach, A., "SIP-Specific Event Notification", RFC 6665, July 2012.

[RFC7044] Barnes, M., Audet, F., Schubert, S., van Elburg, J., and C. Holmberg, "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 7044, February 2014.

[TS23.228] 3GPP, "P Multimedia Subsystem (IMS); Stage 2", 3GPP TS 23.228 12.4.0, March 2014.

[TS32.240] 3GPP, "Telecommunication management; Charging management; Charging architecture and principles", 3GPP TS 32.240 12.3.0, March 2013.

[TS32.260] 3GPP, "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging", 3GPP TS 32.260 10.3.0, April 2011.

Appendix A. Changes from RFC 3455

1. Procedures for the P-Associated-URI header field at a proxy. RFC 3455 indicates that it defines no procedures for the P-Associated-URI header field at a proxy. What is implicitly meant here is that the proxy does not add, read, modify, or delete the header; therefore, RFC 3261 proxy procedures only apply to the header.

2. P-Called-Party-ID header field and the History-Info header field: At the time RFC 3455 was written, the History-Info header field was a long way from specification. This header has now been specified and approved in RFC 7044. It is acknowledged that the History-Info header field will provide equivalent coverage to that of the P-Called-Party-ID header field. However, the P-Called-Party-ID header field is used entirely within the 3GPP system and does not appear to SIP entities outside that of a single 3GPP operator.

3. Procedures at the UA for the P-Charging-Function Addresses header field: The text in Section 4.5.2.1 of RFC 3455 does not adequately take into account procedures for UAs located inside the private network, e.g., as gateways and such that may play a full part in network charging procedures. Section 4.5.2.1 is replaced with new text.

4. The text in Section 4.6.2.1 of RFC 3455 does not adequately take into account procedures for UAs located inside the private network, e.g., as gateways and such that may play a full part in network charging procedures. Section 4.6.2.1 is now replaced with new text.

5. Recognition of additional values of access technology in the P-Access-Network-Info header field (Section 4.4): A number of new access technologies are contemplated in 3GPP, and the reuse of IMS to support Next Generation Networks (NGN) is also resulting in new access technologies. Values for access technologies are defined explicitly in RFC 3455, and no IANA procedures are defined to maintain a separate registry. In particular, the new values: "IEEE 802.11", "IEEE-802.11g", "IEEE-802.11n", "ADSL" / "ADSL2", "ADSL2+", "RADSL", "SDSL", "HDSL", "HDSL2", "G.SHDSL", "VDSL", "IDSL", "IEEE-802.3", "IEEE-802.3a", "IEEE-802.3e", "IEEE-802.3i", "IEEE-802.3j", "IEEE-802.3u", "IEEE-802.3ab", "IEEE-802.3ae", "IEEE-802.3ak", "IEEE-802.3aq", "IEEE-802.3an", "IEEE-802.3y", "IEEE-802.3z", and "IEEE-802.3y" are defined.

6. Replacement of existing value of access technology in the P-Access-Network-Info header field (Section 4.4): The value of "3GPP-CDMA2000" was replaced long ago in 3GPP2 by three new values: "3GPP2-1X", "3GPP2-1X-HRPD", and "3GPP2-UMB". It is not believed that there was any deployment of the "3GPP-CDMA2000" value.

7. Network-provided P-Access-Network-Info header field: The P-Access-Network-Info header field may additionally be provided by proxies within the network. This does not impact the values provided by a UA; rather, the header is repeated. Such values are identified by the string "network-provided". A special class of values are defined for use here, as the same granularity of values may not be possible as for those available from the UA: "3GPP-GERAN", "3GPP-UTRAN", "3GPP-WLAN", "3GPP-GAN", and "3GPP-HSPA". Outbound proxies remove P-Access-Network-Info header fields containing the "network-provided" value.

8. Definition of additional parameters to the P-Charging-Vector header field: Section 5.6 of RFC 3455 defines the syntax of the P-Charging-Vector header field. Additional parameters were considered too application specific for specification in RFC 3455, but it was acknowledged that they would exist, and indeed additional specification of such parameters, relating to specific access technologies, has occurred in 3GPP. Therefore, this update states that applications using the P-Charging-Vector header field within their own applicability are allowed to define generic-param extensions without further reference to the IETF specification process.

9. In Section 5.7, it was added that the P-Called-Party-ID can appear in the PUBLISH method.

10. Referencing: RFC 3427 was deleted from the References section as it was not used within the document. Various informative references have now been published as RFCs and have been updated to include the appropriate RFC number. References to 3GPP TS 32.200 were replaced by references to 3GPP TS 32.240 [TS32.240], which is the successor specification. References to 3GPP TS 32.225 were replaced by references to 3GPP TS 32.260 [TS32.260], which is the successor specification. The referencing style was changed to symbolic references. Dates have been removed from all 3GPP references (i.e., latest version applies).

11. Various editorial changes in alignment with style used in RFC 3261 such as placing response code text in parentheses and using words "request" and "response" in association with method names have been applied.

Authors' Addresses

Roland Jesske
Deutsche Telekom
Heinrich-Hertz-Strasse 3-7
Darmstadt 64307
Germany

Phone: +4961515812766
EMail: r.jesske@telekom.de

Keith Drage
Alcatel-Lucent
Quadrant, StoneHill Green, Westlea
Swindon, Wilts
UK

EMail: drage@alcatel-lucent.com

Christer Holmberg
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: christer.holmberg@ericsson.com