SIMPLE
Internet-Draft
Expires: April 4, 2005

H. Khartabil
E. Leppanen
M. Lonnfors
J. Costa-Requena
Nokia

October 4, 2004

Functional Description of Event Notification Filtering
draft-ietf-simple-event-filter-funct-03

Status of this Memo

Copyright Notice

Abstract

The SIP event notification framework describes the usage of the Session Initiation Protocol (SIP) for subscriptions and notifications of changes to a state of a resource. The document does not describe a mechanism of how filtering of event notification information can be achieved.

This document describes the operations a subscriber performs in order to define filtering rules associated with event notification information. The handling of responses to subscriptions carrying filtering rules and the handling of notifications with filtering rules applied to them is described. The document also describes how the notifier behaves when receiving such filtering rules and how a notification is constructed.

Table of Contents

1. Conventions

In this document, the key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and 'OPTIONAL' are to be interpreted as described in RFC 2119 [1] and indicate requirement levels for compliant implementations.

"Content" refers to the XML document that appears in a notification reflecting the state of a resource.

2. Introduction

SIP event notification is described in [3]. It defines a general framework for sending subscriptions and receiving notifications in SIP based systems. It introduces the concept of event packages, which are concrete applications of the general event framework to a specific usage of events.

Filtering is a mechanism for controlling the content of event notifications. Additionally, the subscriber may specify the rules for when a notification should be sent to it. The filtering mechanism is expected to be particularly valuable to users of mobile wireless access devices. The characteristics of the devices typically include high latency, low bandwidth, low data processing capabilities, small display, and limited battery power. Such devices can benefit from the ability to filter the amount of information generated at the source of the event notification. However, implementers need to be aware of the computational burden on the source of the event notification. This is discussed further in Section 7.

It is stated in [3] that the notifier may send a NOTIFY at any time, but typically it is sent when the state of the resource changes. It also states that the notifications would contain the complete and current state of the resource authorized for a certain subscriber to see. The format of such resource state information is package specific. In this memo, we assume that the NOTIFY for any package contains an XML document.

This document presents a mechanism for filtering whereby a subscriber describes its preference of when notifications are to be sent to it and what they are to contain. It also describes how the notifier functions when generating notifications by taking into account filters and default functionality of the package/service.

The XML format for defining the filter is described in [5]. The creator of the filter MUST ensure that the XML document inserted as the SUBSCRIBE request body is well-formed and valid. The creator

MUST NOT insert any extension elements or attributes into the XML document unless it has access to the extension schema and can validate the XML document. The XML document consumer MAY validate the XML document according the schemas, including extension schemas, it has access to that are applicable to this XML document.

3. Client Operation

3.1 Transport Mechanism

Transportation of the filter to the server is achieved by inserting the XML document, as defined in [5], in the body of the SUBSCRIBE request. Alternatively, the XML document can be uploaded to the server using means outside the scope of this document.

3.2 SUBSCRIBE Bodies

SIP entities compliant with this specification MUST support the content type 'application/simple-filter+xml'.

3.3 Subscriber Generating SUBSCRIBE Requests

This section presents additional functionality required from the subscriber when filters are used in the bodies of the SUBSCRIBE requests. Normal operations of services, e.g., as defined in [7], [9] and [4] are otherwise followed.

As defined in [3], the SUBSCRIBE message MAY contain a body. This body would serve the purpose of carrying filtering information. Honouring those filters is at the discretion of the notifier and might depend on local policies.

No content in the body of a SUBSCRIBE indicates to the notifier that no filter is being requested so that the notifier is instructed to send all the NOTIFY requests using the notifier's own or service specific policy. Note that e.g. in the list case [4] the filter might have been uploaded to the server beforehand (by means outside the scope of this document).

If the body of the SUBSCRIBE includes the filter, the body MUST be of the MIME-Type 'application/simple-filter+xml'.

3.3.1 Structure of a Filter

Multiple filters MAY be included in one SUBSCRIBE. This is achieved by including multiple <filter> elements in the filter [5]. Each <filter> element may include a URI attribute.

A SUBSCRIBE request destined to a list URI [4] MAY include multiple filters specific to individual resources. This is achieved by including multiple <filter> elements with different URIs of resources in each of those elements. This resource specific filter overrides any list specific filter, if any. The list specific filter may or may not include a URI.

Furthermore, regardless whether the SUBSCRIBE is destined to a list URI or not, there can only be one filter applicable to a single resource or domain within a single SUBSCRIBE. I.e. Each filter within a subscription MUST uniquely identify one resource or one domain.

3.3.2 Request-URI vs. Filter URI

The URI in the filter defines the target resource, e.g. in the Presence service case; it is the presentity's presence information to which the filter is applied. The subscriber MAY choose to leave the URI in the filter undefined. If the URI is not defined within the filter, the filter applies to the resource identified in the Request-URI. Similarly, the subscriber MAY define a filter URI. If the Request-URI is a list URI [4], the filter URI MUST be the list URI, a sub-list URI or resource who's URI is one of the URIs that result from a lookup, by an RLS, on the Request-URI. If not, the filter may be ignored or may be rejected. URI matching is done according to the matching rules defined for a particular scheme (SIP URI matching rules are defined in RFC3261 [2].

A filter may also be addressed to a domain using the "domain" attribute instead of the "uri" attribute. In this case, the filter applies to resources in that domain. This can be used when a subscription is for a resource that is an event list with many resources from differing domains. If an individual resource specific filter is present along with the domain filter, this resource specific filter overrides any domain specific filter, if any.

3.3.3 Changing Filters within a Dialog

The client MAY reset or change the filter by re-issuing a new SUBSCRIBE request within the existing dialog. A SUBSCRIBE within the exiting dialog that does not contain a filter is assumed to maintain existing filters. This means that filters are persistent and are only explicitly removed.

A client requiring removal of a filter may do so by using the 'remove="true"' attribute as defined in [5].

In the case the URI in the filter is that of a list, a client may

override the existing filter with a filter for an individual resource, that is part of the list subscribed to earlier, by issuing a new SUBSCRIBE within the existing dialog and including a filter specific for that individual resource. The new filter need not include the original filter since a filter is only removed in the manner indicated above.

A filter is replaced by the client re-issuing the filter using the same filter ID and replacing the contents of the filter. Replacing a filter by changing the filter ID and keeping the resource URI is considered an error since this causes the server to assume that two filters are placed for the same resource.

3.3.4 Subscriber Interpreting SIP responses

The SUBSCRIBE request will be confirmed with a final response. A 200-class responses indicate that the subscription has been accepted, and that a NOTIFY will be sent immediately. A "200" response indicates that the subscription has been accepted and the filter is accepted. A "202" response merely indicates that the subscription has been understood, the content type has been accepted, and that authorization may or may not have been granted. A "202" response also indicates that the filter has not been accepted yet. The acceptance of the filter MAY arrive in a subsequent NOTIFY.

A non-200 class final responses indicate that no subscription or dialog has been created, and no subsequent NOTIFY message will be sent. All non-200 class final responses have the same meanings and handling as described in [2] and [3].

Specifically, a "415" response indicates that the MIME type 'application/simple-filter+xml' is not understood by the notifier. A "488" response indicates that the content type (filter) is understood but some aspects of it were either not understood or not accepted.

3.4 Subscriber Processing of NOTIFY Requests

If the 2xx response was returned for the SUBSCRIBE, the NOTIFY that follows MAY contain a body that describes the present state of the resource after the filters have been applied.

If the NOTIFY indicates that a subscription has been terminated [3], the subscription is assumed to be terminated. Behaviour in such events is also described in [3].

If the subscription is indicated as active, NOTIFY requests are handled as described in package specific documents and [3].

4. Resource List Server Behaviour

The Resource List Server is defined in [4]. This section describes how such entity behaves in the presence of a filter in a subscription to a list.

4.1 Request-URI vs. Filter URI

If the URI is not defined within the filter, the filter applies to the resource list identified in the Request-URI of the SUBSCRIBE request. This results in the filter being applied to all the notifications that the RLS issues to this subscription. The same processing applies to a filter that defines a URI that matches the request-URI of the SUBSCRIBE request. I.e. The filter applies to all notifications that the RLS issues to this subscription.

If the URI indicated by the filter is for one resource whose URI is one of the URIs that result from a lookup, by the RLS, on the Request-URI, the filter for that particular resource is extracted and propagated in the SUBSCRIBE request sent to that resource. It is possible to have more than one filter in a SUBSCRIBE request body, and therefore a filter specific to a resource MUST be extracted and only that is propagated. For example, if the Request-URI in a SUBSCRIBE has the value "sip:mybuddies@mydomain.com" where "bob@mydomain.com" is a resource belonging to that list, and the URI in a filter is "sip:bob@mydomain.com", the filter specific for Bob is extracted and placed in the body of the SUBSCRIBE sent to "bob@mydomain.com".

If the URI indicated by the filter is for one resource whose URI is NOT under the RLS administrative control, the RLS propagates the filter to all the fanned out subscriptions sent to destinations outside the administrative domain of the RLS. This is to accommodate the scenario where the subscriber knows that there are sub-lists in the event list that are under a different administrative domain than where the original subscription was sent to, and the subscriber wishes to set a filter for a resource in that sub-list.

If the URI indicated by the filter is for one resource whose URI is under the RLS administrative control but is not part of the resource list that the subscription was addressed to, the filter is not propagated. In this case, it is the RLS responsibility to make sure than this filter is applied to notifications issued, if information about that resource is present.

For example: If we have 2 lists, each located on its own RLS:

List1 (list1@example1.com) on RLS1 has: bob@example1.com

list2@example2.com

List2 on RLS2 has: alice@example2.com sarah@example1.com
(Note: list2 is a resource in list1)

RLS1 receives the following SUBSCRIBE request (the SUBSCRIBE is for addressed to list1 and contains 2 filters: one for sarah@example1.com and the other for alice@example2.com):

```
SUBSCRIBE sip:List1@example1.com SIP/2.0
...
<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
    <ns-binding prefix="pidf" urn="urn:ietf:params:xml:ns:pidf"/>
  </ns-bindings>
  <filter id="999" uri="sip:sarah@example1.com">
    <what>
      <include type="namespace">
        urn:ietf:params:xml:ns:pidf</include>
      <exclude>
        //pidf:tuple/pidf:note</exclude>
    </what>
  </filter>
  <filter id="8439" uri="sip:alice@example2.com">
    <what>
      <include>
        //pidf:tuple/pidf:status/pidf:basic</include>
    </what>
  </filter>
</filter-set>
```

RLS1 fans out subscriptions to resources on list1. The text above suggests that if a filter is destined to a resource that is not part of the list and is outside the administrative domain of an RLS, then that filter is propagated. The rest are consumed. In our example, only the filter to alice@example2.com is propagated since example2.com is not under the administrative domain of RLS1. The filter to sarah@example1.com is consumed, and RLS1 needs to apply that filter to notifications it receives.

URI matching is done according to the matching rules defined for a particular scheme (SIP URI matching rules are defined in RFC3261 [2].

A filter may also be addressed to a domain using the "domain"

attribute instead of the "uri" attribute. In this case, the filter applies to resources in that domain and the RLS MUST NOT apply filters to any notifications it sends, but instead MUST forward the filter with all fanned out subscriptions to the notifiers.

As indicated in Section 3.3.1, multiple filters can be present in a SUBSCRIBE request. Filters can also be added or modified as indicated in Section 3.3.3. In such circumstances, an RLS MUST check that there are no filters addressed to the same resource or domain and if so, it MUST reject the SUBSCRIBE request with a "488" error response.

4.2 Changing Filters within a Dialog

If an RLS receives a subscription refresh request with no filters specified (empty payload), the RLS assumes that the client does not wish to update the filters. If an RLS receives a subscription refresh with a filter containing the 'remove="true"' attribute as defined in [5], the RLS assumes that the client is removing that filter identified by the filter ID.

If an RLS receives a subscription refresh request with a filter that already exists (i.e. having the same filter ID), the RLS interprets it as a replacement of the existing filter. Replacing a filter by changing the filter ID and keeping the resource URI is considered an error since this causes the RLS to assume that two filters are placed for the same resource.

5. Server Operation

5.1 NOTIFY Bodies

SIP entities compliant with this specification MUST support content-type 'application/simple-filter+xml'.

5.2 Notifier Processing SUBSCRIBE Requests

This section presents additional functionality required from the notifier when filters are used in the bodies of the SUBSCRIBE requests. Normal package specific functionality are otherwise followed.

The notifier will examine the Content-Type header field and will return a 415 response if it does not understand the content type 'application/simple-filter+xml'.

A 200-class responses indicate that the subscription has been accepted, and the NOTIFY will be sent immediately. A "200" response

indicates that the subscription has been accepted, the user is authorized and the filter is accepted. A "202" response merely indicates that the subscription has been understood, but the authorization may or may not have been granted. A "202" response also indicates that the filters have not been accepted yet. The acceptance of the filters MAY arrive in a subsequent NOTIFY.

Procedures described in section Section 5.4 are followed if an error is encountered.

As indicated in Section 3.3.1, multiple filters can be present in a SUBSCRIBE request. Filters can also be added or modified as indicated in Section 3.3.3. In such circumstances, a server MUST check that there are no filters addressed to the same resource or domain and if so, it MUST reject the SUBSCRIBE request with a "488" error response.

5.2.1 Request-URI vs. Filter URI

The subscriber may have chosen to leave the URI in the filter undefined. If the URI is not defined within the filter, the filter applies to the resource identified in the Request-URI.

Similarly, the subscriber may have chosen to include a URI in the filter. In this case, the filter applies to all notifications sent with content associated with the resource with that URI, for this subscription. If the Request-URI and the URI in the filter mismatch, the filter may be ignored or may be rejected. URI matching is done according to the matching rules defined for a particular scheme (SIP URI matching rules are defined in RFC3261 [2].

A filter may also be addressed to a domain using the "domain" attribute instead of the "uri" attribute. In this case, the filter applies to resources in that domain. The notifier MUST NOT apply filters to any notifications it sends if the domain is not that of its own, and MUST ignore it. Notifiers belonging to the domain MUST apply the filter to all notifications it sends for that subscription, unless policy dictates otherwise.

5.2.2 Changing Filters within a Dialog

If a server receives a subscription refresh request with no filters specified (empty payload), it assumes that the client does not wish to update the filters. If it receives a subscription refresh with a filter containing the 'remove="true"' attribute as defined in [5], the server assumes that the client is removing that filter identified by the filter ID.

If the server receives a subscription refresh request with a filter that already exists (i.e. having the same filter ID), it interprets it as a replacement of the existing filter. Replacing a filter by changing the filter ID and keeping the resource URI is considered an error since this causes the server to assume that two filters are placed for the same resource.

5.3 Notifier Generating NOTIFY Requests

Upon receiving the SUBSCRIBE with the filter, the notifier SHOULD retain the filter as long as the subscription persists. The filter MAY be incorporated within an existing subscription (in an active dialog) by sending a re-SUBSCRIBE that includes the filter in the body.

If the response sent to the SUBSCRIBE was a "202" and the "202" was chosen because the filter could not be accepted that time, the NOTIFY MAY be used to terminate the subscription if the filter was found unacceptable.

As described in [3], the NOTIFY message MAY contain a body that describes the state of the resource. This body is in one of the formats listed in the Accept header field of the SUBSCRIBE, or the package specific default if the Accept header field is omitted.

5.3.1 Generation of NOTIFY Contents

If the NOTIFY being sent is the immediate one sent after a 2xx response to the original SUBSCRIBE, its contents MUST be populated according to the filter unless the processing of the filters will take too long or the NOTIFY request is following a "202" response to the SUBSCRIBE request and is terminating the subscription. In the case that the fliter is taking too long to process, the NOTIFY request being sent may be empty or may be populated with a pre-configured value as authorised to that subscriber. If applying the filter results in no content to be delivered, the NOTIFY MUST be sent with empty contents.

The input to the content filter is a package specific XML document, e.g. [6] and [8] derived according to the package specific specifications, ([7] and [9]).

The content is filtered according to the expressions in the <what> element of the filter. The expression indicates the delivered XML elements and/or attributes. Prefixes of the namespaces of the items of the XML document to be filtered must be expanded before applying the filter to the items.

The expression directly states the XML elements and attributes to be delivered in the NOTIFY, along with their values. In addition to the selected contents also the namespaces of all the selected items are included in the NOTIFY. The XML elements and/or attributes indicated by the expression in the <what> element must be items that the subscriber is authorised to see. If not, the notifier policy dictates the behaviour of the notifier (notifier can either ignore the filter, parts of the filter, or reject the filter completely). Implementers need to carefully consider such an implementation decision; the subscriber may not be aware of the authorised contents and therefore most likely will include a filter requesting unauthorised contents. It is therefore RECOMMENDED that notifiers just ignore the parts of the filter where it is requesting unauthorised info. I.e. The filter in the <filter> element where the unauthorised contents are requested is ignored. If polite blocking is used by the notifier, the notifier may choose to ignore the filter, by choosing to deliver notifications containing bogus information in the unauthorised elements or attributes.

The resultant XML document MUST be well formed and valid according to the XML schema. This means that all mandatory elements and attributes along with their values MUST be included in the XML document regardless of the expression. In other words, if the results of applying a filter on an XML document is a non-valid XML document, the notifier MUST add elements and attributes, along with their values, from the original XML document into the newly formulated one in order for it to be a valid one.

5.3.2 Handling of Notification Triggering Rules

There can be several <trigger> elements inside one <filter> element. If the criteria for any of the <trigger> elements are satisfied, a NOTIFY SHOULD be generated.

The items (XML elements and/or attributes) indicated by the expression in the <changed> element, <added> element or <removed> element must be items that the subscriber is authorised to access. If not, the notifier policy dictates the behaviour of the notifier (notifier can either ignore the filter, parts of the filter, or reject the filter completely).

5.4 Handling Abnormal Cases

In case of an invalid filter definition where the XML document of the filter is not aligned with the XML schema of the filter format[5], the notifier rejects the SUBSCRIBE request with a "488" response. A Warning header field in the response may give better indication why the filters were not accepted. If the subscription was accepted with

a "202" response but the invalid filter was discovered after that, a NOTIFY with a subscription-state of value 'terminated' is sent. An event-reason-value "badfilter", introduced here, of subexp-params [3] MAY be included.

In case of an erroneous expression in the filter definition the notifier either ignores the filter definition or terminates the subscription.

If a <what> or <trigger> element is empty, the notifier proceeds as if the element did not exist.

6. Examples

The following chapters include filtering examples for Presence and Watcher Information. The format of filter is according to [5].

6.1 Presence Specific Examples

This chapter describes three use cases where the presence information filtering solution is utilised [7]. In the first use case the watcher is interested in getting messaging specific information of a certain presentity. In the second use case the watcher is interested in getting information about the communication means and contact addresses the presentity is currently available for communication on. The third case shows how a presentity can request triggers to receive notifications

Below is the Presentity's presence information in PIDF [6]. It includes two tuples: one for the instant messaging and another for the voice related information.

```
<?xml version="1.0" encoding="UTF-8"?>
      <presence xmlns="urn:ietf:params:xml:ns:pidf"
                        xmlns:rpid="urn:ietf:params:ns:rpid-tuple"
                        entity="sip:presentity@domain.com">
         <tuple id="432sd">
            <status>
               <basic>closed</basic>
            </status>
            <rpid:class>im</rpid:class>
            <contact>im:presentity@domain.com</contact>
         </tuple>
         <tuple id="thr76jk">
            <status>
               <basic>open</basic>
            </status>
            <rpid:class>voice</rpid:class>
            <contact>tel:2224055555@domain.com</contact>
         </tuple>
      </presence>
```

6.1.1 Subscriber Requests Messaging Related Information

The subscriber initiates a subscription to the presentity's messaging (MMS, IM and SMS) related presence information. The subscription includes the content limiting filter.

The filtered content is indicated with an expression. This expression selects the <basic> element and all the parent elements (this means the status, tuple and its root element), the <class> element and the <contact> element. The filter is: <class> elements that have values beginning with "MMS", "SMS" or "IM".

In this case, the notification includes the contents of the tuple that has the value "IM" in its <label> element.

SUBSCRIBE request from the subscriber including filter:

```
SUBSCRIBE sip:presentity@domain.com
Via: SIP/2.0/TCP 10.0.0.1:5060;branch=xjfdsjfk
To: <sip:presentity@domain.com>
From: <sip:watcher@domain.com>;tag:12341111
Call-ID: 121212@10.0.0.1
Cseq: 1 SUBSCRIBE
Expires: 3600
Event: Presence
Contact: <sip:watcher@client.domain.com>
Content-Type: application/simple-filter+xml
```

```
   Content-Length: ...

   <?xml version="1.0" encoding="UTF-8"?>
   <filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
     <ns-bindings>
       <ns-binding prefix="pidf" urn="urn:ietf:params:xml:ns:pidf"/>
       <ns-binding prefix="rpid"
                           urn="urn:ietf:params:xml:ns:pidf:rpid-tuple"/>
     </ns-bindings>
     <filter id="123" uri="sip:presentity@domain.com">
       <what>
         <include type="xpath">
           //pidf:tuple[rpid:class="IM" or rpid:class="SMS"
           or rpid:class="MMS"]/pidf:status/pidf:basic
       </include>
       <include type="xpath">
         //pidf:tuple[rpid:class="IM" or rpid:class="SMS"
         or rpid:class="MMS"]/rpid:class
       </include>
       <include type="xpath">
         //pidf:tuple[rpid:class="IM" or rpid:class="SMS"
         or rpid:class="MMS"]/pidf:contact
       </include>
       </what>
     </filter>
   </filter-set>

   Notification to the subscriber:

   NOTIFY sip:watcher@client.domain.com SIP/2.0
   Via: SIP/2.0/TCP presence.domain.com:5060;branch=xjfder
   To: <sip:watcher@domain.com>;tag:12341111
   From: <sip:presentity@domain.com>;tag:232321
   Call-ID: 121212@10.0.0.1
   Cseq: 1 NOTIFY
   Event: Presence
   Subscription-State: active; expires=3599
   Contact: sip:presentity@server.domain.com
   Content-Type: application/pidf+xml
   Content-Length: ...

   <?xml version="1.0" encoding="UTF-8"?>
      <presence xmlns="urn:ietf:params:xml:ns:pidf"
      xmlns:rpid="urn:example-com:ietf:params:ns:rpid-tuple"
      entity="sip:presentity@domain.com">
         <tuple id="432sd">
            <status>
               <basic>closed</basic>
```

```
            </status>
            <rpid:class>im</rpid:class>
            <contact>im:presentity@domain.com</contact>
          </tuple>
        </presence>
```

6.1.2 Subscriber Fetches Information about "Open" Communication Means

The subscriber makes a subscription to the presentity's available communication means. The subscription includes the content limiting filter.

The filtered content is indicated with an expression. This expression selects the <basic> element and all the parent elements (this means the status, tuple and its root element), the <class> element and the <contact> element. The filter is: the <basic> element's value is "Open". There is also a need to indicate that only the tuples which have contact address information are selected.

In this case the notification returns the contents of the tuple that has both the value "open" inside the <status> element and the existing <contact> elements.

SUBSCRIBE request from the subscriber including filter:

```
SUBSCRIBE sip:presentity@domain.com SIP/2.0
Via: SIP/2.0/TCP 10.0.0.1:5060;branch=xjfdsjfk
To: <sip:presentity@domain.com>
From: <sip:watcher@domain.com>;tag:12341111
Call-ID: 121212@10.0.0.1
Cseq: 1 SUBSCRIBE
Expires: 3600
Event: Presence
Contact: <sip:watcher@client.domain.com>
Content-Type: application/simple-filter+xml
Content-Length: ...

<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
    <ns-binding prefix="pidf" urn="urn:ietf:params:xml:ns:pidf"/>
  </ns-bindings>
  <filter id="123" uri="sip:presentity@domain.com">
    <what>
      <include type="xpath">
        //pidf:tuple/pidf:status[pidf:basic="open"]/pidf:basic
      </include>
```

```
        <include type="xpath">
          //pidf:tuple[pidf:status/pidf:basic="open"]/rpid:class
        </include>
        <include type="xpath">
          //pidf:tuple[pidf:status/pidf:basic="open"]/pidf:contact
        </include>
      </what>
    </filter>
  </filter-set>
```

Notification to the subscriber:

```
NOTIFY sip:watcher@client.domain.com SIP/2.0
Via: SIP/2.0/TCP presence.domain.com:5060;branch=xjfder
To: <sip:watcher@domain.com>;tag:12341111
From: <sip:presentity@domain.com>;tag:232321
Call-ID: 121212@10.0.0.1
Cseq: 1 NOTIFY
Event: Presence
Subscription-State: active; expires=3599
Contact: sip:presentity@server.domain.com
Content-Type: application/pidf+xml
Content-Length: ...

<?xml version="1.0" encoding="UTF-8"?>
   <presence xmlns="urn:ietf:params:xml:ns:pidf"
   xmlns:rpid="urn:example-com:ietf:params:ns:rpid-tuple"
   entity="sip:presentity@domain.com">
      <tuple id="thr76jk">
         <status>
            <basic>open</basic>
         </status>
            <rpid:class>voice</rpid:class>
            <contact>tel:2224055555@domain.com</contact>
      </tuple>
   </presence>
```

6.1.3 Subscriber Requests Notifications when Presentity's Status Changes

The subscriber subscribes to the presentity, specifying in the filter that it wants notifications only when the <basic>element has changed to value 'open'

SUBSCRIBE request from the subscriber including filter:

```
SUBSCRIBE sip:presentity@domain.com
Via: SIP/2.0/TCP 10.0.0.1:5060;branch=xjfdsjfk
To: <sip:presentity@domain.com>
From: <sip:watcher@domain.com>;tag:12341111
Call-ID: 121212@10.0.0.1
Cseq: 1 SUBSCRIBE
Expires: 3600
Event: Presence
Contact: <sip:watcher@client.domain.com>
Content-Type: application/simple-filter+xml
Content-Length: ...

<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
    <ns-binding prefix="pidf" urn="urn:ietf:params:xml:ns:pidf"/>
    <ns-binding prefix="rpid"
                        urn="urn:ietf:params:xml:ns:pidf:rpid-tuple"/>
  </ns-bindings>
  <filter id="123" uri="sip:presentity@domain.com">
    <trigger>
      <changed from="closed" to="open">
        //pidf:presence/pidf:tuple/pidf:status/pidf:basic
      </changed>
    </trigger>
  </filter>
</filter-set>
```

Assuming a 2nd PIDF document is created with both tuples having status of closed:

```
<?xml version="1.0" encoding="UTF-8"?>
   <presence xmlns="urn:ietf:params:xml:ns:pidf"
   xmlns:rpid="urn:example-com:ietf:params:ns:rpid-tuple"
   entity="sip:presentity@domain.com">
      <tuple id="432sd">
         <status>
         <basic>closed</basic>
         </status>
            <rpid:class>im</rpid:class>
            <contact>im:presentity@domain.com</contact>
      </tuple>
      <tuple id="thr76jk">
         <status>
            <basic>closed</basic>
         </status>
         <rpid:class>voice</rpid:class>
         <contact>tel:2224055555@domain.com</contact>
```

```
         </tuple>
      </presence>
```

A NOTIFY is not sent to the subscriber in this case.

Now, a 3rd PIDF document is created when IM status changes to OPEN:

```
<?xml version="1.0" encoding="UTF-8"?>
   <presence xmlns="urn:ietf:params:xml:ns:pidf"
   xmlns:rpid="urn:example-com:ietf:params:ns:rpid-tuple"
   entity="sip:presentity@domain.com">
      <tuple id="432sd">
         <status>
            <basic>open</basic>
         </status>
         <rpid:class>im</rpid:class>
         <contact>im:presentity@domain.com</contact>
      </tuple>
      <tuple id="thr76jk">
         <status>
            <basic>closed</basic>
         </status>
         <rpid:class>voice</rpid:class>
         <contact>tel:2224055555@domain.com</contact>
      </tuple>
   </presence>
```

Notification to the subscriber is sent in this case:

```
NOTIFY sip:watcher@client.domain.com SIP/2.0
Via: SIP/2.0/TCP presence.domain.com:5060;branch=xjfder
To: <sip:watcher@domain.com>;tag:12341111
From: <sip:presentity@domain.com>;tag:232321
Call-ID: 121212@10.0.0.1
Cseq: 1 NOTIFY
Event: Presence
Subscription-State: active; expires=3599
Contact: sip:presentity@server.domain.com
Content-Type: application/pidf+xml
Content-Length: ...

<?xml version="1.0" encoding="UTF-8"?>
   <presence xmlns="urn:ietf:params:xml:ns:pidf"
   xmlns:rpid="urn:example-com:ietf:params:ns:rpid-tuple"
   entity="sip:presentity@domain.com">
      <tuple id="432sd">
         <status>
```

```
            <basic>closed</basic>
         </status>
         <rpid:class>im</rpid:class>
         <contact>im:presentity@domain.com</contact>
      </tuple>
      <tuple id="thr76jk">
         <status>
            <basic>open</basic>
         </status>
         <rpid:class>voice</rpid:class>
         <contact>tel:2224055555@domain.com</contact>
      </tuple>
   </presence>
```

6.2 Watcher Information Specific Examples

The examples in this section use the winfo template-package with the presence event package [9].

Watcher information to a Presentity:

```
<?xml version="1.0"?>
  <watcherinfo xmlns="urn:ietf:params:xml:ns:watcherinfo"
version="0" state="full">
  <watcher-list resource="sip:presentity@domain.com"
                package="presence">
      <watcher status="active"
         id="sr8fdsj"
         duration-subscribed="509"
         expiration="20"
         event="approved">sip:watcherA@example.com"</watcher>
      <watcher status="pending"
         id="sr8fdsj"
         duration-subscribed="501"
         expiration="100"
         event="subscribe">sip:watcherB@example.com"</watcher>
      <watcher status="terminated"
         id="sr8fdsj"
         duration-subscribed="500"
         expiration="0"
         event="rejected">sip:watcherC@example.com"</watcher>
      <watcher status="active"
         id="sr8fdsj"
         duration-subscribed="20"
         expiration="30"
         event="approved">sip:watcherD@domain.com"</watcher>
  </watcher-list>
```

```
        </watcherinfo>
```

6.2.1 Watcher Subscriber Makes Subscription to Get All the Information about Active Watchers

SUBSCRIBE request from the presentity including the filter:

```
SUBSCRIBE sip:presentity@domain.com
Via: SIP/2.0/TCP 10.0.0.1:5060;branch=xjfdsjfk
To: <sip:presentity@domain.com>
From: <sip:presentity@domain.com>;tag:12341111
Call-ID: 121212@10.0.0.1
Cseq: 1 SUBSCRIBE
Expires: 3600
Event: Presence.winfo
Contact: sip:presentity@client.domain.com
Content-Type: application/simple-filter+xml
Content-Length: ...

<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
    <ns-binding prefix="wi"
                        urn="urn:ietf:params:xml:ns:watcherinfo"/>
  </ns-bindings>
  <filter id="123" uri="sip:presentity@domain.com">
    <what>
      <include>
        /watcherinfo/watcher-list[@package="presence"]/
        watcher[@status="active"]
      </include>
</what>
</filter>
</filter-set>
```

Notification to the subscriber:

```
NOTIFY sip:presentity@client.domain.com SIP/2.0
Via: SIP/2.0/TCP presence.domain.com:5060;branch=xjfder
To: sip:presentity@domain.com;tag:12341111
From: sip:presentity@domain.com;tag:232321
Call-ID: 121212@10.0.0.1
Cseq: 1 NOTIFY
Contact: sip:presentity@server.domain.com
Event: Presence.winfo
```

```
Content-Type: application/watcherinfo+xml
Content-Length: ...

<?xml version="1.0"?>
  <watcherinfo xmlns="urn:ietf:params:xml:ns:watcherinfo"
version="0" state="full">
  <watcher-list resource="sip:presentity@domain.com"
                package="presence">
      <watcher status="active"
         id="sr8fdsj"
         duration-subscribed="509"
         expiration="20"
         event="approved">sip:watcherA@example.com"</watcher>
      <watcher status="active"
         id="sr8fdsj"
         duration-subscribed="20"
         expiration="30"
         event="approved">sip:watcherD@domain.com"</watcher>
  </watcher-list>
  </watcherinfo>
```

6.2.2 Watcher Subscriber Requests Information of Watchers with Specific Subscription Duration Conditions

SUBSCRIBE request from the presentity including the filter:

```
SUBSCRIBE sip:presentity@domain.com
Via: SIP/2.0/TCP 10.0.0.1:5060;branch=xjfdsjfk
To: <sip:presentity@domain.com>;tag:12341111
From: <sip:presentity@domain.com>
Call-ID: 121212@10.0.0.1
Cseq: 1 SUBSCRIBE
Expires: 0
Event: Presence.winfo
Contact: <sip:presentity@client.domain.com>
Content-Type: application/simple-filter+xml
Content-Length: ...

<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-filter">
  <ns-bindings>
    <ns-binding prefix="wi"
                      urn="urn:ietf:params:xml:ns:watcherinfo"/>
  </ns-bindings>
  <filter id="123" uri="sip:presentity@domain.com">
    <what>
```

```
        <include>
          /watcherinfo/watcher-list[@package="presence"]/
          watcher[@duration-subscribed>500]
        </include>
      </what>
    <filter>
  </filter-set>
```

Notification to the subscriber:

```
NOTIFY sip:presentity@client.domain.com SIP/2.0
Via: SIP/2.0/TCP presence.domain.com:5060;branch=xjfder
To: sip:presentity@domain.com;tag:12341111
From: sip:presentity@domain.com;tag:232321
Call-ID: 121212@10.0.0.1
Cseq: 1 NOTIFY
Contact: sip:presentity@server.domain.com
Event: Presence.winfo

Content-Type: application/watcherinfo+xml
Content-Length: ...

<?xml version="1.0"?>
  <watcherinfo xmlns="urn:ietf:params:xml:ns:watcherinfo"
version="0" state="full">
  <watcher-list resource="sip:presentity@domain.com"
                package="presence">
      <watcher status="active"
         id="sr8fdsj"
         duration-subscribed="509"
         expiration="20"
         event="approved">sip:watcherA@example.com"</watcher>
      <watcher status="pending"
         id="sr8fdsj"
         duration-subscribed="501"
         expiration="100"
         event="subscribe">sip:watcherB@example.com"</watcher>
  </watcher-list>
  </watcherinfo>
```

6.2.3 Watcher Subscriber Requests Specific Watcher Info On Specific Triggers

This filter selects watcher information notifications [8] to be sent when the pending subscription status has changed from 'pending' to 'terminated'. In the notification, only the watchers that have a status of 'terminated' and an event of 'rejected' are included.

SUBSCRIBE request from the Watcher Subscriber including the filter:

```
SUBSCRIBE sip:presentity@domain.com
Via: SIP/2.0/TCP 10.0.0.1:5060;branch=xjfdsjfk
To: <sip:presentity@domain.com>;tag:12341111
From: <sip:presentity@domain.com>
Call-ID: 121212@10.0.0.1
Cseq: 1 SUBSCRIBE
Expires: 0
Event: Presence.winfo
Contact: <sip:presentity@client.domain.com>
Content-Type: application/simple-filter+xml
Content-Length: ...

<?xml version="1.0" encoding="UTF-8"?>
<filter-set xmlns="urn:ietf:params:xml:ns:simple-winfo-filter">
  <ns-bindings>
    <ns-binding prefix="wi"
                        urn="urn:ietf:params:xml:ns:watcherinfo"/>
  </ns-bindings>
  <filter id="123" uri="sip:presentity@domain.com">
    <what>
      <include>
        /watcherinfo/watcher-list[@package="presence"]/
        watcher[@status="terminated" and @event="rejected"]
      </include>
    </what>
    <trigger>
      <changed from="pending"
                                           to="terminated">
        //@status
      </changed>
    </trigger>
  </filter>
</filter-set>
```

A 2nd Winfo document is created due to some change:

```
 <?xml version="1.0"?>
     <watcherinfo xmlns="urn:ietf:params:xml:ns:watcherinfo"
   version="0" state="full">
     <watcher-list resource="sip:presentity@domain.com"
                   package="presence">
         <watcher status="active"
            id="sr8fdsj"
            duration-subscribed="509"
            expiration="20"
            event="approved">sip:watcherA@example.com</watcher>
```

```
            <watcher status="terminated"
               id="sr8fdsj"
               duration-subscribed="501"
               expiration="100"
               event="rejected">sip:watcherB@example.com"</watcher>
            <watcher status="terminated"
               id="sr8fdsj"
               duration-subscribed="500"
               expiration="0"
               event="rejected">sip:watcherC@example.com"</watcher>
            <watcher status="active"
               id="sr8fdsj"
               duration-subscribed="20"
               expiration="30"
               event="approved">sip:watcherD@domain.com"</watcher>
        </watcher-list>
         </watcherinfo>
```

Notification to the subscriber, taking into account the <trigger> and <what> elements:

```
NOTIFY sip:presentity@client.domain.com SIP/2.0
Via: SIP/2.0/TCP presence.domain.com:5060;branch=xjfder
To: sip:presentity@domain.com;tag:12341111
From: sip:presentity@domain.com;tag:232321
Call-ID: 121212@10.0.0.1
Cseq: 1 NOTIFY
Contact: sip:presentity@server.domain.com
Event: Presence.winfo

Content-Type: application/watcherinfo+xml
Content-Length: ...

<?xml version="1.0"?>
  <watcherinfo xmlns="urn:ietf:params:xml:ns:watcherinfo"
version="0" state="full">
  <watcher-list resource="sip:presentity@domain.com"
                package="presence">
      <watcher status="terminated"
         id="sr8fdsj"
         duration-subscribed="501"
         expiration="100"
         event="rejected">sip:watcherB@example.com"</watcher>
      <watcher status="terminated"
         id="sr8fdsj"
         duration-subscribed="500"
         expiration="0"
         event="rejected">sip:watcherC@example.com"</watcher>
```

```
    </watcher-list>
    </watcherinfo>
```

7. Security Considerations

The presence of filters in the body in a SIP message has a significant effect on the ways in which the request is handled at a server. As a result, it is especially important that messages containing this extension be authenticated and authorized.

Processing of requests and looking up filters requires set operations and searches, which can require some amount of computation. This enables a DoS attack whereby a user can send requests with substantial numbers messages with large contents, in the hopes of overloading the server. To counter this, the server can establish a limit on the number of occurrences of the <what>, <changed>, <added> and <removed> elements allowed in the filters. A default limit of 40 is RECOMMENDED, however, servers may raise or lower the limit depending upon their specific engineered capacity.

Requests can reveal sensitive information about a UA's capabilities. If this information is sensitive, it SHOULD be encrypted using SIP S/MIME capabilities. All package specific security measures MUST be followed.

Propagating filters in SUBSCRIBE requests to foreign domains reveals sensitive information about a user's resource lists. It is therefore required that an RLS does not forward a filter if that filter is addressed to a resource that is under the administrative domain of the RLS, but is not on the resource list. Section 4.1 shows an example where such a scenario can occur.

It is important to note that a flitered document located at a subscriber may project false reality. For example, if a subscriber asked to be notified when a resource has changed his presence state from closed to open but not from open to closed, then the subscriber may afterwards be under the false impression that the resource's presence state is open even long after the resource has changed it to closed. Therefore, subscribers need to be sure what they put in a filter, understand what they asked for and be prepared to be out of sync with the real state of a resource.

8. IANA Considerations

A new event-reason-value "badfilter" is defined to represent the event where the filter is not well formed and/or not accepted. No IANA registration is required for this value.

9. Acknowledgements

The authors would like to thank George Foti, Tim Moran, Sreenivas Addagatla, Juha Kalliokulju, Jari Urpalainen and Mary Barnes for their valuable input.

10. References

10.1 Normative References

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

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

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

[4] Roach, A., "A Session Initiation Protocol (SIP) Event Notification Extension for Collections", draft-ietf-simple-event-list-01.txt, March 2003.

[5] Khartabil, H., "An Extensible Markup Language (XML) Based Format for Event Notification Filtering", draft-ietf-simple-filter-format-00.txt, June 2004.

10.2 Informative References

[6] Sugano, H., "CPIM Presence Information Data Format", draft-ietf-impp-cpim-pidf-08.txt, May 2003.

[7] Rosenberg, J., "Session Initiation Protocol (SIP) Extensions for Presence", RFC 3856, July 2004.

[8] Rosenberg, J., "An Extensible Markup Language (XML) Based Format for Watcher Information", RFC 3858, July 2004.

[9] Rosenberg, J., "A Watcher Information Event Template-Package for SIP", RFC 3857, July 2004.

Authors' Addresses

Hisham Khartabil
Nokia
P.O. Box 321
Helsinki
Finland

Phone: +358 7180 76161
EMail: hisham.khartabil@nokia.com

Eva Leppanen
Nokia
P.O BOX 785
Tampere
Finland

Phone: +358 7180 77066
EMail: eva-maria.leppanen@nokia.com

Mikko Lonnfors
Nokia
Itamerenkatu 00180
Helsinki
Finland

Phone: + 358 50 4836402
EMail: mikko.lonnfors@nokia.com

Jose Costa-Requena
Nokia
P.O. Box 321
FIN-00045 NOKIA GROUP
FINLAND

Phone: +358 71800 8000
EMail: jose.costa-requena@nokia.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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