VoIP 프레즌스 서비스에 적용 가능한 XCAP 기반 권한관리기법 설계*

이태진, 원용근, 임채태, 원유재
한국정보보호진흥원
tjlee@kisa.or.kr, ygwon@kisa.or.kr, chtim@kisa.or.kr, yjwon@kisa.or.kr

A Design on XCAP based Authorization Management applicable to VoIP based Presence Services

Taijin Lee, Yonggeun Won, Chate Im, Youjae Won
Korea Information Security Agency

요 약

SIP 기반 프레즌스 서비스는 향후 유비쿼터스 시대의 상황인지형 서비스를 비롯한 다양한 곳에 응용될 수 있는 핵심서비스이다. 또한 프레즌스 서비스는 개인의 프라이버시 문제를 다루기 때문에, 권한관리를 위해 draft로 제시되어 있는 XCAP 기반 기술이 주요 이슈로 대두되고 있다. 그러나, 현재 프레즌스 기반 구조를 활용한 응용서비스 모델이 제시되어 있지 않으며, XCAP 기반 권한관리 기술이 적용된 사례가 나와있지 않다. 본 논문에서는 VoIP에 적용 가능한 프레즌스 서비스 모델을 선정하고, 서비스 개발을 위한 프레즌스 기반구조의 적용방법, XCAP 기반 권한관리 기술의 적용방안을 설계하였다. 본 논문을 통해 중요한 서비스로 인식되면서도 마땅한 서비스가 발굴되지 않은 현실에서, 프레즌스 기반 서비스 개발 및 XCAP 기반 권한관리 기술개발을 위한 참조모델로 활용할 수 있다. 특히, 보안에 민감한 프라이버시 정보를 다루는 프레즌스 서비스 보호를 위해 XCAP 기반기술은 반드시 필요하며, 임의의 응용서비스에 독립적으로 적용할 수 있는 XCAP 기반기술의 특징을 고려하면 더욱 큰 의미를 지닌다.

1. 서 론

1)

최근 SIP을 활용한 서비스가 IETF, 3GPP등을 통해 표준화가 활발히 진행되고 있으며, 이러한 서비스 중 대표적인 것 중의 하나가 프레즌스 서비스이다. 프레즌스 서비스는 향후 유비쿼터스시대의 상황인지형 서비스를 비롯한 다양한 곳에서 사용될 것으로 예상된다. IETF SIMPLE WG은 프레즌스 서비스에 대한 표준화 작업을 활발히 진행하고 있다.

프레즌스 서비스의 대표적인 예는 IM(Instant Messenger)에서 Buddy의 현재 상태정보를 확인할 수 있는 것이 있으며, 이러한 프레즌스 정보는 위치, 시간에 대한 정보 뿐 아니라 혈압 등을 체크할 수 있는 센서정보, 임의로 설정할 수 있는 상태정보 등을 포함하여, 향후 서비스가 개발될 것으로 예상된다.

한편, 프레즌스 정보는 주로 개인의 프라이버시에 관한 정보를 다루기 때문에, 악의적인 사용자에게 노출되면 다양한 피해가 발생할 수 있다. 이에 따라 프레즌스 정보에 대한 XCAP 기반 권한관리 기술이 현재 draft로 제안되어 있는 상태이다. XCAP 기반 권한관리 기술은 프레즌스 정보를 제공하는 Presentity가 자신의 프레즌스 정보를 누구에게, 어떤 정보를 줄 것인지를 XCAP 서버에 설정한다. 이후, 프레즌스 정보를 제공받기를 원하는 Watcher의 요청이 있을때, 프레즌스 서버는 XCAP 서버를 통해 권한이 있는지 확인하고, 권한이 있을 경우 프레즌스 정보를 Watcher에게 제공한다.

그러나, 현재 IM 외에 마땅한 프레즌스 서비스 모델이 제시되어 있지 않고, XCAP 기반 권한 관리기술이 draft로 제시되었으나, 이를 프레즌스 기반 응용서비스에의 적용방안이 나와있지 않다. 본 논문에서는 VoIP에 적용 가능한 프레즌스 서비스 모델을 제안하며, 서비스 모델에 XCAP 기반 권한관리 기법의 적용방안을 제시한다. 본 논문을 통해 중요한 서비스로 인식되면서도 마땅한 서비스가 발굴되지 않은 현실에서, 프레즌스 기반 서비스 개발 및 XCAP 기반 권한관리 기술개발을 위한 참조모델로 활용할 수 있다.

본 논문의 구성은 다음과 같다. 2절에서는 관련 기술 동향을 소개하고, 3절에서는 VoIP에 적용 가능한 프레즌스 서비스 모델을 선정하고, XCAP 기반 권한관리기법을 설계하였다. 4절에서는 본 논문에서 제안한 VoIP 프레즌스 서비스의 동작 시나리오에 따른 상세설계를 기술하였으며, 5절에서는 결론을 맺는다.

* 본 연구는 정보통신부 및 정보통신연구진흥원의IT 신성장동력핵심기술개발사업의 일환으로 수행하였음 [2006-S-043-02, VoIP 정보보호기술]

2. 관련기술 연구동향

2.1 프레즌스 서비스 모델

프레즌스 서비스는 자신의 정보를 제공하는 Presentity와 Presentity의 정보를 얻는 Watcher, 프레즌스 정보를 관리하는 PA(Presence Agent), 권한설정을 위해 사용되는 RH(Rule Holder)로 구성된다. 프레즌스 서비스는 향후 유비쿼터스시대의 상황인지형 서비스를 비롯한 다양한 곳에서 사용될 것으로 예상된다 아래는 IETF SIMPLE WG에서 표준화 작업을 추진하고 있는 SIP 기반 프레즌스 서비스 모델을 나타낸다

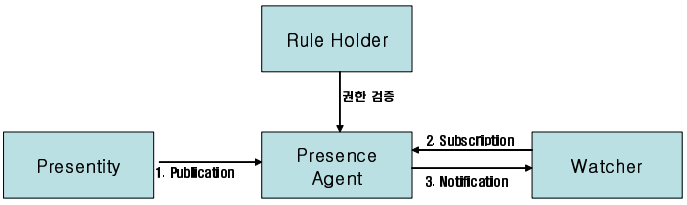

그림 1. 프레즌스 서비스 모델

Presentity는 자신의 프레즌스 정보제공을 위해 확장된 SIP PUBLISH를 사용하며[11], Watcher는 이 정보를 요청 및 수신하기위해 SIP SUBSCRIBE, NOTIFY 메소드를 사용한다[12]. 한편 프레즌스 정보를 표현하기 위해 PIDF(Presence Information Data Format) 포맷을 사용하며[4], 다양한 프레즌스 정보를 표현하기 위해 개발된 RPID(Rich Presence Extension to the Presence Information Data Format)등을 사용할 수 있다[5]. 또한 프레즌스 기반의 다양한 서비스를 개발하기 위해 리소스 리스트를 관리하는 기법[6,7]과 자신의 프레즌스 정보를 요청하는 Watcher들을 관리하는 기법 등이 표준화되어 있다[9,10].

2.2 XCAP을 이용한 권한관리 기술

XCAP(XML Configuration Access Protocol)은 XML과 HTTP 프로토콜을 기반으로 프레즌스 정보에 대한 권한관리를 위해 사용되는 프로토콜이다[1]. XCAP Client는 자신의 프레즌스 정보를 요청하는 Watcher에 대한 권한을 생성/수정/삭제할 수 있으며, XCAP Server는 설정된 권한정보 관리 및 Watcher 요청에 응답한다. 프레즌스 기반 다양한 응용서비스는 고유한AUID(Application Unique ID)를 통해 구분되므로, XCAP을 이용한 권한관리는 모든 응용서비스 개발에 공통적으로 활용할 수 있다. 아래 그림은 XCAP 권한관리 프로토콜을 나타낸다.

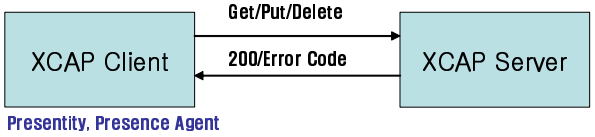

그림 2. XCAP 기반 권한관리 기술

XCAP Client는 자신의 프레즌스 정보를 열람하고자 하는 Watcher들에 대한 권한설정 정보를XCAP Server에 저장하거나 삭제, 조회를 요청하고, XCAP Server는 이에 대한 응답 메시지를 보낸다 XCAP 기반 권한관리를 위해 HTTP GET, PUT, DELETE 메소드가 사용된다.

- GET : XCAP Client 권한정보 조회
- PUT : XCAP Client 권한정보 생성 및 수정
- DELETE : XCAP Client 권한정보 삭제

2.3 XCAP을 이용한 권한관리 문서포맷

XCAP을 이용한 프레즌스 권한관리 정보는XML로 기술되며, 기본적으로 "urn:ietf:xml:ns:pres-rules" 스키마를 따르고 있으며[2], "urn:ietf:params:xml:ns:common-policy" 등 다른 스키마를 추가로 사용하여 세부적인 권한관리가 가능하다[3]. XCAP을 이용한 권한관리 문서는 아래와 같이 기술된다.

표 1. XCAP 기반 권한관리 문서 포맷

```
<ruleset>
<rule id='a'>
 <conditions>
  <identity>
   <one id="sip:bob@example.com"/>
  </identity>
 </conditions>
 <actions>
  <sub-handling>Allow</sub-handling>
 </actions>
 <transformations>
   <provide-services>
    <service-uri-scheme>sip</service-uri-scheme>
    <service-uri-scheme>mailto</service-uri-scheme>
   </provide-services>
   <provide-persons>
    <all-persons/>
   </provide-persons>
 </transformations>
</rule>
</ruleset>
```

먼저 <ruleset>은 권한관리에 사용되는 여러 개의 <rule>을 기술할 수 있으며, 각각의 <rule>은 <conditions>, <actions>, <transformations>로 구성되어 있다. <conditions>는 Rule이 적용되는 대상을 나타내는데, 특정대상을 지정하거나, 권한을 가질 수 있는 시간, 위치 등의 정보를 세부적으로 기술할 수 있다 <actions>는 권한을 가진 대상에 대해서 어떤 권한을 줄 것인지 기술하며, <transformations>는 해당 권한에 대한 정보 제공범위 등이 포함된다 [표 1]은 bob@example.com에게 sip, mail 등에 대한 프레즌스 정보를 제공한다는 권한이 기술되어 있다.

3. VoIP 프레즌스 서비스 선정 및 구현을 위한 XCAP 기반 권한관리 기술 설계

앞서 논의한 바와 같이, 프레즌스 서비스에 대한 논의

는 활발히 이루어지고 있으나, 실제 개발된 서비스 사례가 거의 없다. 본 절에서는 VoIP를 대상으로 실제 적용 가능한 프레즌스 서비스 모델을 선정하고, 구현을 위해 필요한 XCAP 기반 권한관리기술에서의 고려사항 및 서비스 시나리오를 도출한다

3.1 VoIP 프레즌스 서비스 주요기능

VoIP 프레즌스 서비스 모델은 다음과 같다. VoIP 단말은 자신의 Buddy 목록을 볼 수 있는 화면을 가지고 있으며, 각각의 Buddy가 전화를 받을 수 있는지, 없는지에 대한 프레즌스 정보가 제공된다. 따라서 본 서비스를 통해 전화통화를 하지 않고도 상대방이 전화를 받을 수 있는지, 없는지 알 수 있는 장점이 있다. 또한, 부가기능으로 수신자가 전화를 받을 수 없는 상황일지라도, 발신자가 긴급 상황일때는 동적으로 전화를 받을 수 있는 상태로 표시되는 기능도 추가하였다. 본 서비스의 주요기능은 다음과 같다.

표 2. VoIP 프레즌스 서비스 주요기능

o 대 상 A : Presentity(통화가능 여부에 대한 프레즌스 정보제공) B : Watcher(A에게 전화를 걸기전에, A가 전화를 받을 수 있는지에 대한 프레즌스 정보 수신) o 주요 기능 1) 업무시간에, B가 A의 프레즌스 정보를 확인할 때, “통화가능”으로 표시 2) 업무시간외에, B가 A의 프레즌스 정보를 확인할 때, “통화불가”로 표시 3) 업무시간외에, B가 긴급통화를 위해 A의 프레즌스 정보를 확인할 때, “통화가능”으로 표시

[표 2]는 B가 A와 통화를 하지 않고도, A가 전화를 받을 수 있는지, 없는지에 대한 정보를 알 수 있는 서비스를 나타낸다. 본 서비스에서는 업무시간을 기준으로 “통화가능”, “통화불가” 정보를 설정했으나, 이는 요구하는 서비스 기능에 따라 확장하여 다양한 프레즌스 정보를 표현할 수 있다.

3.2 프레즌스 서비스 설계를 위한 고려사항

앞서 본 논문에서 새롭게 제안한 VoIP 프레즌스 서비스 모델을 선정하였다. 여기서는 실제 구현에 앞서 XCAP 기반 권한관리 기법을 적용하기 위해 고려해야 할 사항을 기술한다. 크게 보면, 1) 제공해야 하는 프레즌스 정보가 무엇인지 분석하고, 2) 프레즌스 정보를 누구에게 어떤 범위의 정보를 제공하는지 고려해야 한다.

1) 프레즌스 정보 식별

본 서비스에서 A는 통화가능, 통화불가에 관한 상태정보, B는 긴급상황인지 아닌지에 대한 상태정보를 제공한다. A와 B의 상태정보는 확장된 프레즌스 정보를 표현할 수 있는 RPID 스펙에 있는 <sphere> 엘리먼트를 사용한다[5].

2) 권한정보 설정

본 서비스에서는 업무시간과 B의 상태에 따라 A의 상태정보를 볼 수 있는 권한이 달라진다. 업무시간과 관련한 권한설정은 Common Policy 스펙에 있는 <validity> 엘리먼트를 사용하고[3], 프레즌스 정보 제공범위에 대해서는 Presence Authorization Rules 스펙에 있는 <provide-sphere> 엘리먼트를 사용한다[2].

위 시나리오에 따라 권한관리 로직을 정리하면 다음과 같다.

표 3. 권한관리 로직

Watcher의 현재상태 (Sphere)	프레즌스 정보요청 시간 (Validity)	프레즌스 정보 제공여부 (Actions)	프레즌스정보 제공범위 (Transformations)
normal	업무시간중	Allow	""통화가능“
normal	업무시간외	Deny	“통화불가”
emergency	any	Allow	“통화가능”

3.3 서비스 시나리오

위 내용을 바탕으로 VoIP 프레즌스 서비스 전체 시나리오를 구성하면 다음과 같다.

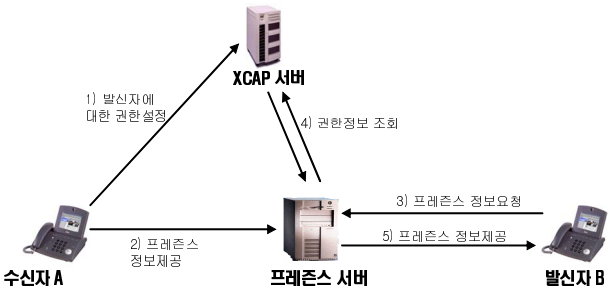

그림 3. 서비스 시나리오

1) 수신자 A는 자신의 통화가능여부에 관한 프레즌스 정보를 볼 수 있는 대상에 대한 권한을XCAP 서버를 통해 설정한다[표 3].
2) A는 근무시간에는 “통화가능”, 근무시간외에는 “통화불가”의 정보를 프레즌스 서버에 보낸다
3) 발신자 B는 수신자 A와 통화할 수 있는지 확인하기 위해 A의 프레즌스 정보를 프레즌스 서버에게 요청한다
4) 프레즌스 서버는 XCAP 서버에게 발신자 B가 권한이 있는지 확인한다.
5) 권한이 있을 경우, 프레즌스 서버는 발신자 B에게 수신자 A의 프레즌스 정보를 제공한다

지금까지 VoIP 프레즌스 서비스 주요기능 및 고려사항, 동작 시나리오를 살펴보았다. 다음절에서는 이를 구

현하기 위한 상세설계 내용을 기술한다

4. XCAP 기반 권한관리 기법 상세설계

본 절에서는 XCAP 기반 권한관리 기법에 대한 상세설계를 [그림 3]의 동작 시나리오에 따라 기술하였다

4.1 Watcher B에 대한 XCAP 기반 권한정보 설정

우선, 프레즌스 정보를 제공하는 Presentity A는 자신에게 전화를 걸 수 있는 B를 포함한 Watcher들에 대한 권한설정을 한다. A는 통신 프로토콜로 HTTP PUT 메소드를 사용하며, 문서포맷은 앞서 논의된 pres-rules와 common policy 스키마를 사용하여 XCAP 서버에게 전송한다. 해당화일이 없을 경우 새롭게 생성이 되며, 이미 있을 경우 기존에 설정된 권한설정 파일을 덮어쓰게 된다. 한편, 권한설정 정보를 조회할 때는HTTP GET, 삭제할 때는 HTTP DELETE 메소드를 사용한다. 본 시나리오에 따른 XCAP 기반 권한설정 정보는 다음과 같다.

표 4. XCAP을 통한 권한설정

```
HTTP PUT
 /pres-rules/users/A/pres-rules.xml
 HTTP/1.1
 Accept: */*
 Accept-Language : ko
 If-Match : "kkll"
 Content-Type : application/pres-rules+xml
 Host : xcap.kisa.or.kr

<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
   xmlns="urn:ietf:params:xml:ns:pres-rules"
   xmlns="http://www.w3.org/2001/XMLSchema-instance">
<rule id="a">
 <conditions>
  <sphere>emergency</sphere>
 </conditions>
 <actions>allow</actions>
 <transformations>
  <provide-sphere>TRUE</provide-sphere>
 </transformations>
</rule>

<rule id="b">
 <conditions>
  <validity>
     <from>2007-03-29T09:00:00+01:00</from>
     <to>2007-03-29T18:00:00+01:00</to>
  </validity>
 </conditions>
 <actions>allow</actions>
 <transformations>
    <provide-sphere>TRUE</provide-sphere>
 </transformations>
</rule>
</ruleset>
```

첫 번째 Rule은 정보를 요청한 Watcher B의 상태정보가 emergency일 경우, Presentity A의 프레즌스 정보열람을 허용하며, A의 Sphere 정보를 제공한다는 의미이며, 두 번째 Rule은 업무시간에 해당하는 오전 9시부터 오후 6시 사이에 A의 프레즌스 정보를 요청하는 B에게는 A의 정보열람을 허용하며, A의 Sphere 정보를 제공한다는 의미이다. 따라서 업무시간 이외에 A의 프레즌스 정보를 요청하면, 해당되는 권한이 없어 프레즌스 정보를 제공받을 수 없게 된다.

4.2 Presentity A 정보를 프레즌스 서버에게 제공

업무시간에 따라 Presentity A는 “통화가능”, “통화불가”에 해당하는 프레즌스 정보를 SIP PUBLISH 메소드를 통해 프레즌스 서버에게 제공한다[11]. 프레즌스 정보는 앞서 논의된대로, PIDF의 확장된 스펙인 RPID에서 정의하고 있는 <sphere> 엘리먼트를 사용한다.

표 5. SIP PUBLISH를 통한 Presentity 정보 제공

```
PUBLISH sip:A@kisa.or.kr SIP/2.0
Via : SIP/2.0/TCP/ watcherhost.kisa.or.kr;branch=xxx
From : <sip:A@kisa.or.kr>;tag=ccc
To : <sip:A@kisa.or.kr>
Call-ID : 1111@watcherhost.kisa.or.kr
CSeq : 1 SUBSCRIBE
Max-Forwards : 70
Event : Presence
Accept : application/pidf+xml
Contact : <sip:A@kisa.or.kr>
Expires : 600
Content-Length:...

<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
          xmlns="urn:ietf:params:xml:ns:pidf:rpid">
<tuple id="aa">
 <status><basic>open </basic> </status>
 <rpid:sphere>통화가능</rpid:sphere>
 <contact>im:A@kisa.or.kr</contact>
</tuple>
</presence>
```

4.3 Presentity A에 대한 정보요청

Watcher B는 Presentity A에게 전화를 걸기전에, A가 전화를 받을 수 있는지 확인하기 위해A에 대한 프레즌스 정보를 프레즌스 서버에게 요청한다. 이를 위해 SIP SUBSCRIBE 메소드를 사용한다[12].

표 6. SIP SUBSCRIBE을 통한 Presentity A 정보 요청

```
SUBSCRIBE sip:B@kisa.or.kr SIP/2.0
Via : SIP/2.0/TCP/ watcherhost.kisa.or.kr;branch=xxx
From : <sip:Br@kisa.or.kr>;tag=ccc
To : <sip:B@kisa.or.kr>
Call-ID : 1111@watcherhost.kisa.or.kr
CSeq : 1 SUBSCRIBE
Max-Forwards : 70
Event : Presence
Accept : application/pidf+xml
Contact : <sip:B@kisa.or.kr>
Expires : 600
Content-Length:0
```

4.4 XCAP 서버를 통한 권한정보 조회

프레즌스 서버는 Watcher B에게 Presentity A의 프레즌스 정보 제공여부를 결정하기 위해XCAP 서버에게 문의한다. 여기서 문의하는 방법은 표준에 명시되지 않았으나, 다음과 같은 방법을 생각해볼 수 있다.

- 프레즌스 서버와 XCAP 서버가 권한관리 정보에 대한 데이터베이스를 공유하는 방법
- XCAP Client(Presentity)가 XCAP 서버에 설정된 권한조회를 위해 HTTP GET 메소드를 사용하는 것과 마찬가지로, 프레즌스 서버도 HTTP GET 메소드를 사용하는 방법
- 권한정보가 변경될때마다 XCAP 서버는 프레즌스 서버로 알려주는 방법

4.5 Presentity A의 프레즌스 정보 제공

프레즌스 서버는 Watcher B에게 SIP NOTIFY 메소드를 통해 Presentity A에 대한 프레즌스 정보를 제공한다 [12].

5. 결 론

지금까지 VoIP 서비스에 적용 가능한 프레즌스 서비스 모델을 선정하고, XCAP 기반 권한관리 기술의 적용 방안을 제시하였다. 본 논문을 통해 중요한 서비스로 인식되면서도 마땅한 서비스가 발굴되지 않은 현실에서, 프레즌스 기반 서비스 개발 및 XCAP 기반 권한관리 기술개발에 대한 참조모델로 활용할 수 있다. 특히, 보안에 민감한 프라이버시 정보를 다루는 프레즌스 서비스 보호를 위해 XCAP 기반기술은 반드시 필요하며, 임의의 응용서비스에 독립적으로 적용할 수 있는 XCAP 기반기술의 특징을 고려하면 더욱 큰 의미를 지닌다.

본 논문에서는 기본적인 프레즌스 정보에 대한 권한관리 기법을 설계하였다. 성공적인 프레즌스 서비스 상용화를 위해서는 복잡한 프레즌스 정보에 대한 권한관리, 리소스리스트에 대한 권한관리, Watcher에 대해 중복된 Rule이 적용될 때의 Rule Combine 알고리즘 등에 대한 참조모델이 개발되어야 한다. 또한, 프레즌스 서비스는 개인의 프라이버시 정보를 다루고 있어 보안에 민감하므로, 서비스 개발 뿐 아니라 프레즌스 서비스에 대한 정보보호요구사항 분석 및 보안 프레임워크를 개발하여 안전한 서비스 환경이 구축되도록 유도하는 것이 필요하다.

참고 문헌

[1] IETF, draft-ietf-simple-xcap-12.txt, "The Extensible Markup Language (XML) Configuration Access Protocol(XCAP)", 2006

[2] IETF, draft-ietf-simple-presence-rules-09, "Presence Authorization Rules", 2007

[3] IETF, "Common Policy : A Document Format for Expressing Privacy Preferences", RFC 4745, 2007

[4] IETF, "Presence Information Data Format (PIDF)", RFC 3863, 2004

[5] IETF, "RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)", RFC 4480, 2006

[6] IETF, "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists", RFC 4662, 2006

[7] IETF, draft-ietf-simple-xcap-list-usage-05, "Extensible Markup Language (XML) Formats for Representing Resource Lists", 2005

[8] IETF, "A Presence Event Package for the Session Initiation Protocol (SIP)", RFC 3856, 2004

[9] IETF, "A Watcher Information Event Template-Package for the Session Initiation Protocol, RFC 3857, 2004

[10] IETF, "An Extensible Markup Language (XML) Based Format for Watcher Information", RFC 3858, 2004

[11] IETF, "Session Initiation Protocol(SIP) Extension for Event State Publication", RFC 3903

[12] IETF, "Session Initiation Protocol(SIP) - Specific Event Notification", RFC 3265