XCON
Internet-Draft
Expires: March 10, 2005

H. Khartabil
A. Niemi
Nokia

September 9, 2004

Privileges for Manipulating a Conference Policy
draft-ietf-xcon-conference-policy-privileges-00

Status of this Memo

Copyright Notice

Abstract

The Conference Policy is defined as the complete set of rules for a particular conference manipulated by the conference policy server. The Conferece Policy Control Protocol (CPCP) is the protocol used by client to manipulate the conference policy. This document specifies an Extensible Markup Language (XML) Schema that enumerates the conference policy meta data that enable a user to assign privileges to users that enables them to read and/or manipulate parts of or the entire conference policy.

Table of Contents

1. Introduction

The Conference Policy Control Protocol (CPCP) [1]specifies an Extensible Markup Language (XML) Schema that enumerates the conference policy data elements that enable a user to define a conference policy. It, however, does not define user privileges (who is allowed to read or modify certain parts or all of a conference policy).

In many cases, the creator of the conference policy is the sole user with access rights to the conference policy and other users do not have any rights to view nor modify the document. However, there is a need for different privileges to exist where users can modify certain parts of the conference policy XML document. This document specifies an Extensible Markup Language (XML) Schema that enumerates the conference policy meta data that enable such privileges to exist.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [3].

3. Terminology

This document uses terminology from [13]. Some additional definitions are introduced in [1], including the defintion of a privileged user.

4. Structure of a Conference Policy Privileges XML Document

The conference policy privileges document is an XML [4] document that MUST be well-formed and MUST be valid. The Conference policy privelges documents MUST be based on XML 1.0 and MUST be encoded using UTF-8. This specification makes use of XML namespaces for identifying conference policy privileges documents and document fragments. The namespace URI for elements defined by this specification is a URN [6], using the namespace identifier 'ietf' defined by [7] and extended by [8]. This URN is:

```
urn:ietf:params:xml:ns:privileges
```

4.1 MIME Type for CPCP XML Document

The MIME type for the CPCP XML document is "application/privileges+xml".

4.2 Privileges Root

A conference policy privileges document begins with the root element tag <privileges>. Other elements from different namespaces MAY be present for the purposes of extensibility. Elements or attributes from unknown namespaces MUST be ignored.

A user may create a new conference policy privieleges at the CPS by placing a new conference policy document at the CPS. Depending on server policy and user privileges, the CPS may accept the creation. Only the creator of the conference can create a conference policy privileges document for that conference policy.

A conference that exists without a conference policy privileges document allows all privileges to the creator of the conference policy only. A conference policy privielges document can be deleted permanently by removing the conference policy document from the CPS. When the user deletes a conference policy document, the user SHOULD also delete the conference policy privielges document associated with the deleted conference. A CPS may apply local policy in determining when and if to delete the conference policy privielges document if it has not been removed after a the conference policy document was deleted.

4.3 XML Document Description

4.3.1 Conference Policy Privileges

One of the key components of the conference policy privileges document is the set of authorization rules that specify who is allowed to read and manipulate a conference policy. The unordered list of authorization rules together define the conference policy privileges in the form of an authorization policy.

The <xml-document-rules> element appears after the root element and contains the mandatory "uri" attribute. This attributes carries the URI of the conference policy document that the privileges defines within it apply to.

The conference policy privileges are enclosed in the <xml-document-rules> element are formatted according to the XML schema defined in the common policy framework [2]. In the <xml-document-rules> element, there can be multiple rules, each rule is represented by the <rule> element, each of which consist of three parts: conditions, actions and transformations. Conditions determine whether a particular rule applies to a request. Each action or transformation in the applied rule is a positive grant of permission to the conference policy user. The details of each specific element

and attribute is described in [2].

Asking the conference policy server to allow certain users to manipulate the conference policy is achieved by modifying an existing authorization rule or creating a new one.

If the conference is long-lasting, it is possible that new rules are added all the time but old rules are almost never removed (some of them are overwritten, though). This leads easily to the situation that the conference policy meta data contains many unnecessary rules which are not really needed anymore. Therefore, there is a need to delete rules. This can be achieved by removing that portion of the policy.

Conflicting rules may exist (for example, both allowed and blocked action is defined for same target). The common policy directives [2] dictate the behaviour in such situations.

This section outlines the new conditions, actions and transformations for conference policy privileges.

4.3.1.1 Conditions

4.3.1.1.1 Validity

The <validity> element, as defined in the common policy framework [2], expresses the rule validity period by two attributes, a starting and a ending time. Times are expressed in XML dateTime format. Expressing the lifetime of a rule implements a garbage collection mechanism. A rule maker might not have always access to the conference policy server to remove some rules which grant permissions. Hence this mechanisms allows to remove or invalidate granted permissions automatically without further interaction between the rule maker and the conference policy server.

To give a real life example, there are often meetings where users can have access to modify the dial-out list from 10 minutes before the conference starts until 10 mintues after the conference starts. One rules can be set in this scenario. The following example demostrates this. The meeting starts at 9:30 and ends at 12:30. A manager with identity "manager@example.com can read and modify the dial-out list betweem 8:50 and 9:40. After that time until the conference ends, the manager can only read the dial-out-list

```
<rule id="1">
  <conditions>
     <validity>
      <from>2004-12-17T08:50:00-05:00</from>
      <to>2004-12-17T09:40:00-05:00</to>
    </validity>
   <identity>
      <id>manager@example.com</id>
    </identity>
  </conditions>
  <actions>
    <allow-modify-dol>allow</allow-modify-dol>
  </actions>
  <transformations/>
</rule>
<rule id="2">
  <conditions>
    <identity>
      <id>manager@example.com</id>
    </identity>
  </conditions>
  <actions>
    <allow-read-dol>allow</allow-read-dol>
  </actions>
  <transformations/>
</rule>
...
<time>
  <occurrence>
    <mixing-start-time required-participant="participant">
      2004-12-17T09:30:00-05:00</mixing-start-time>
    <mixing-stop-time required-participant="none">
      2004-12-17T12:30:00-05:00</mixing-stop-time>
  </occurrence>
</time>
```

4.3.1.1.2 Identity

The <identity> element is already defined in the common policy framework [2]The presence of the <identity> element is a condition requires any identity within it to be authenticated before a rule is applied to it. This includes the <id> element (Section 4.3.1.1.2.1), the <any> element (Section 4.3.1.1.2.2), the <external-list> element (Section 4.3.1.1.2.3), their exceptions, and any future extension that carries an identity. The absence of the <identity> element with in a condition indicated that the rule applies to all unauthenticated

identities. That is participants that have provided no authenticated identity to the conference focus.

4.3.1.1.2.1 Interpreting the <id> Element

As earlier indicated, the <identity> element is already defined in the common policy framework [2]. However, the rules for interpreting the identities in <id> elements are left for each application to define separately. This document, however, does not define the rules for interpreting identities in <id> elements in conferencing applications since those interpretation rules are signalling protocol specific.

OPEN ISSUE: Do we need to state more than this? How are identities derived from users that join using POTS, H.323, etc.?

4.3.1.1.2.2 Matching Any Identity

The <any> element is used to match any participant. This allows a conference priveleges to be open to any authenticated user. Just as for the <domain> element in <identity> element, The <any> element contains a list of <except> elements and allows to implement a simple blacklist mechanism. The <except> element contains the identity. It differs from the <domain> element in that the domain part is needed in the identity since it has not domain to refer to.

4.3.1.1.2.3 Matching Identities in External Lists

The <external-list> element can be used to match those participants that are part of a resource list that is created externally. The use of <external-list> is similar to that defined in Section x of [1].

4.3.1.2 Actions

4.3.1.2.1 Modifying Conference setting

The <allow-modify-settings> element represents a boolean action. If set to TRUE, the identity is allowed to modify the conference settings in the conference policy. If set to FALSE, any modifications to the conference settings are rejected.

If this element is undefined it has a value of FALSE, causing the modifications to be rejected.

4.3.1.2.2 Modifying Conference Information

The <allow-modify-information> element represents a boolean action.

If set to TRUE, the identity is allowed to modify the conference information in the conference policy. If set to FALSE, any modifications to the conference information are rejected.

If this element is undefined it has a value of FALSE, causing the modifications to be rejected.

4.3.1.2.3 Modifying Conference Time

The <allow-modify-time> element represents a boolean action. If set to TRUE, the identity is allowed to modify the conference time in the conference policy. If set to FALSE, any modifications to the conference time are rejected.

If this element is undefined it has a value of FALSE, causing the modifications to be rejected.

4.3.1.2.4 Modifying Authorization rules

The <allow-modify-authorization-rules> element represents a boolean action. If set to TRUE, the identity is allowed to modify the authorization rules of a conference in the conference policy. If set to FALSE, any modifications to the rules are rejected.

If this element is undefined it has a value of FALSE, causing the modifications to be rejected.

4.3.1.2.5 Modifying Conference Dial-out List

The <allow-modify-dol> element represents a boolean action. If set to TRUE, the identity is allowed to modify the conference dial-out list in the conference policy. If set to FALSE, any modifications to the dial-out list are rejected.

If this element is undefined it has a value of FALSE, causing the modifications to be rejected.

4.3.1.2.6 Modifying Conference Refer List

The <allow-modify-rl> element represents a boolean action. If set to TRUE, the identity is allowed to modify the conference refer list in the conference policy. If set to FALSE, any modifications to the refer list are rejected.

If this element is undefined it has a value of FALSE, causing the modifications to be rejected.

4.3.1.2.7 Modifying Conference media streams

The <allow-modify-ms> element represents a boolean action. If set to TRUE, the identity is allowed to modify the conference media streams in the conference policy. If set to FALSE, any modifications to the media streams are rejected.

If this element is undefined it has a value of FALSE, causing the modifications to be rejected.

4.3.1.2.8 Creating Sidebars

The <allow-modify-sidebar> element represents a boolean action. If set to TRUE, the identity is allowed to create and manipulate a sidebar by creating and modifying a <sidebar> element in a conference policy. If set to FALSE, any sidebar creation and manipulation is rejected.

If this element is undefined it has a value of FALSE, causing the modifications to be rejected.

4.3.1.2.9 Modifying Conference Dial-in List

The conference dial-in list is virtual and is not represented by a physical list in the conference policy. It is rather a collection of authorization rules that allow users to join a conference. The <allow-modify-dil> element represents a boolean action. If set to TRUE, the identity is allowed to create an authorization rule in the conference policy that give a user a join handling of "allow". If set to FALSE, any modifications to authorization rules are rejected.

If this element is undefined it has a value of FALSE, causing the modifications to be rejected.

4.3.1.2.10 Reading Conference setting

The <allow-read-settings> element represents a boolean action. If set to TRUE, the identity is allowed to read the conference settings in the conference policy. If set to FALSE, any attempts to read the conference settings are rejected.

If this element is undefined it has a value of FALSE, causing the read requests to be rejected.

4.3.1.2.11 Reading Conference Information

The <allow-read-information> element represents a boolean action. If set to TRUE, the identity is allowed to read the conference

information in the conference policy. If set to FALSE, any attempts to read the conference information are rejected.

If this element is undefined it has a value of FALSE, causing the read requests to be rejected.

4.3.1.2.12 Reading Conference Time

The <allow-read-time> element represents a boolean action. If set to TRUE, the identity is allowed to read the conference time in the conference policy. If set to FALSE, any attempts to read the conference time are rejected.

If this element is undefined it has a value of FALSE, causing the read requests to be rejected.

4.3.1.2.13 Reading Authorization rules

The <allow-read-authorization-rules> element represents a boolean action. If set to TRUE, the identity is allowed to read the authorization rules of a conference in the conference policy. If set to FALSE, any attempts to read the rules are rejected.

If this element is undefined it has a value of FALSE, causing the read requests to be rejected.

4.3.1.2.14 Reading Conference Dial-out List

The <allow-read-dol> element represents a boolean action. If set to TRUE, the identity is allowed to read the conference dial-out list in the conference policy. If set to FALSE, any attempts to read the dial-out list are rejected.

If this element is undefined it has a value of FALSE, causing the read requests to be rejected.

4.3.1.2.15 REading Conference Refer List

The <allow-read-rl> element represents a boolean action. If set to TRUE, the identity is allowed to read the conference refer list in the conference policy. If set to FALSE, any attempts to read the refer list are rejected.

If this element is undefined it has a value of FALSE, causing the read requests to be rejected.

4.3.1.2.16 Reading Conference media streams Information

The <allow-read-ms> element represents a boolean action. If set to TRUE, the identity is allowed to read the conference media streams information in the conference policy. If set to FALSE, any attempts to read the media streams information are rejected.

If this element is undefined it has a value of FALSE, causing the read requests to be rejected.

4.3.1.2.17 Reading Sidebar Information

The <allow-read-sidebar> element represents a boolean action. If set to TRUE, the identity is allowed to read side bar inforation in the conference policy, indicating how many sidebars are currently in a conference. If set to FALSE, any attempts to read sidebar information is rejected.

If this element is undefined it has a value of FALSE, causing the modifications to be rejected.

4.3.1.2.18 Reading Conference Dial-in List

The Dial-in List is defined in Section 4.3.1.2.9. If set to TRUE, the identity is allowed to read authorizations rule in the conference policy that give a user a join handling of "allow". If set to FALSE, any attempts to read such rules are rejected.

If this element is undefined it has a value of FALSE, causing the read requests to be rejected.

4.3.1.3 Transformations

No transformations are defined at this time.

4.4 XML Schema

```
   <?xml version="1.0" encoding="UTF-8"?>
   <xs:schema targetNamespace="urn:ietf:params:xml:ns:privileges"
xmlns="urn:ietf:params:xml:ns:privileges" xmlns:xs="http://www.w3.org/2001/
XMLSchema" elementFormDefault="qualified">
        <!-- This import brings in the XML language attribute xml:lang-->
        <xs:import namespace="http://www.w3.org/XML/1998/namespace"
schemaLocation="http://www.w3.org/2001/xml.xsd"/>
        <xs:element name="privileges">
                <xs:complexType>
                        <xs:sequence>
                                <xs:element name="xml-document-rules"
```

```
type="XMLDocument"/>
                        </xs:sequence>
                </xs:complexType>
```

```
        </xs:element>
        <xs:complexType name="XMLDocument">
                <xs:sequence>
                        <xs:element name="rule" type="ruleType" minOccurs="0"
maxOccurs="unbounded"/>
                </xs:sequence>
                <xs:attribute name="uri" type="xs:string" use="required"/>
        </xs:complexType>
        <xs:complexType name="ruleType">
                <xs:sequence>
                        <xs:element name="conditions" minOccurs="0">
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element ref="condition"
minOccurs="0" maxOccurs="unbounded"/>
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="actions" minOccurs="0">
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element ref="action"
minOccurs="0" maxOccurs="unbounded"/>
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element name="transformations" minOccurs="0">
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element
ref="transformation" minOccurs="0" maxOccurs="unbounded"/>
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                </xs:sequence>
                <xs:attribute name="id" type="xs:string" use="required"/>
        </xs:complexType>
        <xs:element name="condition" abstract="true"/>
        <xs:element name="action" abstract="true"/>
        <xs:element name="transformation" abstract="true"/>
        <xs:element name="validity" substitutionGroup="condition">
                <xs:complexType>
                        <xs:all>
                                <xs:element name="from" type="xs:dateTime"/>
                                <xs:element name="to" type="xs:dateTime"/>
                        </xs:all>
                </xs:complexType>
        </xs:element>
        <xs:element name="identity" substitutionGroup="condition">
                <xs:complexType>
                        <xs:choice>
                                <xs:element name="id" type="xs:string"
maxOccurs="unbounded"/>
```

```
                                <xs:sequence>
                                        <xs:element name="domain"
type="xs:string"/>
                                        <xs:sequence minOccurs="0">
                                                <xs:element name="except"
type="xs:string" maxOccurs="unbounded"/>
                                        </xs:sequence>
                                </xs:sequence>
                                <xs:sequence>
                                        <xs:element name="any"
type="xs:string"/>
                                        <xs:sequence minOccurs="0">
                                                <xs:element name="except"
type="xs:string" maxOccurs="unbounded"/>
                                        </xs:sequence>
                                </xs:sequence>
                                <xs:sequence>
                                        <xs:element name="external-list"
type="xs:string"/>
                                        <xs:sequence minOccurs="0">
                                                <xs:element name="except"
type="xs:string" maxOccurs="unbounded"/>
                                        </xs:sequence>
                                </xs:sequence>
                        </xs:choice>
                </xs:complexType>
        </xs:element>
        <xs:element name="allow-modify-settings" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-modify-information" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-modify-time" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-modify-authorization-rules" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-modify-dol" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-modify-rl" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-modify-ms" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-modify-sidebar" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-modify-dil" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-read-settings" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-read-information" type="xs:boolean"
```

```
substitutionGroup="action"/>
        <xs:element name="allow-read-time" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-read-authorization-rules" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-read-dol" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-read-rl" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-read-ms" type="xs:boolean"
substitutionGroup="action"/>
        <xs:element name="allow-read-sidebar" type="xs:boolean"
substitutionGroup="action"/>
   </xs:schema>
```

5. Examples

5.1 A Simple Conference Policy Privileges Document

The following document dictates that Bob and Alice are allowed to read and modify the conference settings at "http://xcap.example.com/services/conferences/users/Alice/conference.xml" why John can only read the dial-out list.

```
   <?xml version="1.0" encoding="UTF-8"?>
   <privileges xmlns="urn:ietf:params:xml:ns:privileges" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
        <xml-document-rules uri="http://xcap.example.com/services/conferences/
users/Alice/conference.xml">
                <rule id="1">
                        <conditions>
                                <identity>
                                        <id>bob@example.com</id>
                                        <id>alice@example.com</id>
                                </identity>
                        </conditions>
                        <actions>
                                <allow-modify-settings>true</allow-modify-
settings>
                                <allow-read-settings>true</allow-read-settings>
                        </actions>
                        <transformations/>
                </rule>
                <rule id="2">
                        <conditions>
                                <identity>
                                        <id>john@example.com</id>
                                </identity>
                        </conditions>
                        <actions>
                                <allow-read-dol>true</allow-read-dol>
                        </actions>
                        <transformations/>
                </rule>
        </xml-document-rules>
   </privileges>
```

6. Security Considerations

A conference document may contain information that is highly sensitive. Its delivery to the conference server needs to happen strictly, paying special attention to integrity and confidentiality. Reading the document is also a security concern since the conference policy contains sensitive information like the topic of the conference, who is allowed to join and the URIs of the users that can participate.

Manipulations of the conference policy have similar security issues.

Users with relevant privileges can manipulate parts of the conference policy giving themselves and others privileges to manipulate the conference policy, including the dial-out list and the security level settings for a conference. This can happen because the conference policy itself carries the identities and the authorization rules that apply to those identities. Those authorization rules carry the privileges that certain identities have. If an unauthorized user gets access to this document (pretending to be someone else), s/he can manipulate those rules giving himself and other unauthorized users access to the conference policy. S/he can also manipulate other parts of the conference policy under a false identity. Some of the things that a malicious user can do include: denying users certain privileges, giving himself floor moderation, removing users from lists, removing rules for certain identities, giving privileges to other malicious users, changing the media streams and changing conference time. Therefore, it is very important that only authorized clients are able to manipulate the conference policy. Any conference policy transport protocol MUST provide authentication, confidentiality and integrity.

In the case that XCAP is used to create and manipulate a conference policy, the XCAP base specification mandates that all XCAP servers MUST implement HTTP Authentication: Basic and Digest Access Authentication [14]. Furthermore, XCAP servers MUST implement HTTP over TLS [15]. It is recommended that administrators of XCAP servers use an HTTPS URI as the XCAP root services URI, so that the digest client authentication occurs over TLS. By using these means, XCAP client and server can ensure the confidentiality and integrity of the XCAP created conference policy document and its manipulation operations, and that only authorized clients are allowed to perform them.

7. IANA Considerations

7.1 application/privileges+xml MIME TYPE

MIME media type: application

MIME subtype name: privileges+xml

Mandatory parameters: none

Optional parameters: Same as charset parameter application/xml as specified in RFC 3023 [5].

Encoding considerations: Same as encoding considerations of application/xml as specified in RFC 3023 [5].

Security considerations: See section 10 of RFC 3023 [5] and section Section 7 of this document.

Interoperability considerations: none.

Published specification: This document.

Applications which use this media type: This document type has been used to support conference policy manipulation for SIP based conferencing.

Additional information:

Magic number: None

File extension: .cl or .xml

Macintosh file type code: "TEXT"

Personal and email address for further information: Hisham Khartabil (hisham.khartabil@nokia.com)

Intended Usage: COMMON

Author/change controller: The IETF

7.2 URN Sub-Namespace Registration for urn:ietf:params:xml:ns:privileges

This section registers a new XML namespace, as per guidelines in URN document [8].

URI: The URI for this namespace is urn:ietf:params:xml:ns:privileges.

Registrant Contact: IETF, XCON working group, Hisham Khartabil (hisham.khartabil@nokia.com)

XML:

```
BEGIN
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
     "http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
 <meta http-equiv="content-type"
   content="text/html;charset=iso-8859-1"/>
 <title>Conference Policy Namespace</title>
</head>
<body>
  <h1>Namespace for Conference Policy</h1>
  <h2>application/conference-policy+xml</h2>
  <p>See <a href="[[[URL of published RFC]]]">RFCXXXX</a>.</p>
</body>
</html>
END
```

8. Acknowledgements

The authors would like to thank Hannes Tschofenig, Aki Niemi, Alan Johnston, and the IETF XCON working group for their feedback and suggestions.

9 Normative References

[1] Khartabil, H., Koskelainen, P. and A. Niemi, "The Conference Policy Control Protocol (CPCP)", Internet-Draft I-D.draft-ietf-xcon-cpcp, September 2004.

[2] Schulzrinne, H., Tschofenig, H., Cuellar, J., Polk, J. and J. Rosenberg, "Common Policy", Internet-Draft I-D.ietf-geopriv-common-policy, February 2004.

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

[4] Bray, T., Paoli, J., Sperberg-McQueen, C. and E. Maler, "Extensible Markup Language (XML) 1.0 (Second Edition)", W3C REC REC-xml-20001006, October 2000.

[5] Murata, M., Laurent, S. and D. Kohn, "XML Media Types", RFC 3023, January 2001.

[6] Moats, R., "URN Syntax", RFC 2141, May 1997.

[7] Moats, R., "A URN Namespace for IETF Documents", RFC 2648,

August 1999.

[8] Mealling, M., "The IETF XML Registry", RFC 3688, January 2004.

[9] Koskelainen, P. and H. Khartabil, "Requirements for conference policy control protocol", draft-ietf-xcon-cpcp-req-01 (work in progress), January 2004.

[10] Johnston, A. and O. Levin, "Session Initiation Protocol Call Control - Conferencing for User Agents", draft-ietf-sipping-cc-conferencing-03 (work in progress), February 2004.

[11] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", draft-ietf-simple-xcap-02 (work in progress), February 2004.

[12] Rosenberg, J., "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Usage for Presence Lists", draft-ietf-simple-xcap-list-usage-02 (work in progress), February 2004.

[13] Rosenberg, J., "A Framework for Conferencing with the Session Initiation Protocol", draft-ietf-sipping-conferencing-framework-01 (work in progress), October 2003.

[14] Franks, J., "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[15] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

Authors' Addresses

Hisham Khartabil
Nokia
P.O. Box 321
Helsinki FIN-00045
Finland

EMail: hisham.khartabil@nokia.com

Aki Niemi
Nokia
P.O. Box 100
NOKIA GROUP, FIN 00045
Finland

Phone: +358 50 389 1644
EMail: aki.niemi@nokia.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

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