

XCON WG
Internet-Draft
Expires: July 19, 2004

P. Koskelainen
H. Khartabil
Nokia
January 19, 2004

**Requirements for Conference Policy Control Protocol
draft-ietf-xcon-cpcp-reqs-01**

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on July 19, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

The conference policy server allows clients to manipulate and interact with the conference policy. One mechanism to manipulate the policy is to use conference policy control protocol (CPCP). This document gives the requirements for CPCP.

Table of Contents

1.	Introduction	3
2.	Conventions Used in This Document	4
3.	Terminology	5
4.	Integration with Floor Control	6
5.	Conference Policy Data Model	7
6.	CPCP Requirements	8
6.1	Conference creation, termination and joining	8
6.2	Manipulating general conference attributes	8
6.3	Authentication and Security	9
6.4	Application and media manipulation	9
6.5	ACL manipulation	9
6.6	Floor control	10
6.7	Inviting and ejecting users	11
6.8	User Privileges	11
6.9	General Protocol Requirements	11
7.	Changes since draft-ietf-xcon-cpcp-reqs-00	13
8.	Acknowledgements	14
	Normative References	15
	Informative References	16
	Authors' Addresses	16
	Intellectual Property and Copyright Statements	17

1. Introduction

The conferencing framework document [3] describes the overall architecture, terminology, and protocol components needed for multi-party conferencing. It defines a logical function called a conference policy server (CPS) which can store and manipulate rules associated with participation in a conference. These rules include directives on the lifespan of the conference, who can and cannot join the conference, definitions of roles available in the conference and the responsibilities associated with those roles.

The conference policy control protocol (CPCP) is a client-server protocol that can be used by users to manipulate the rules associated with the conference.

The conference policy is represented by a URI. There is a unique conference policy for each conference. The conference policy URI points to a conference policy server which can manipulate that conference policy.

Conferencing framework describes also conference notification service that is a logical function provided by the focus. It means that the focus can act as a notifier, accepting subscriptions to the conference state.

Note that CPCP is not the only mechanism to manipulate conference policy, but other mechanisms exists as well, such as Web interface.

This document can be used with other documents, such as Conferencing framework document [3]. Moreover, [5] and [7] give useful background information about conferencing and floor control.

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. Terminology

This document uses the definitions from [\[3\]](#).

Additional definitions:

ACL

Access control list (ACL) defines users who can join a conference. Users may have allow, blocked or pending status in the list. Each conference has its own ACL.

Moderator

A special (privileged) role for a user that is allowed to manipulate conference policy and override policy decisions made by other users.

Floor control

Floor control is a mechanism that enables applications or users to gain safe and mutually exclusive or non-exclusive access to the shared object or resource in a conference.

Privilege

A privilege is a right to perform a manipulation operation in a conference. It is user permission such as the right to modify ACL or expel users.

4. Integration with Floor Control

Floor control is an optional feature often used by conferencing applications. It enables applications or users to gain safe and mutually exclusive or non-exclusive input access to a shared object or resource. We define a floor as the temporary permission for a conference participant to access or manipulate a specific shared resource or group of resources.

We assume that the ability of users to create floors is governed by the conference policy. Conference user may use floor control protocol (see e.g. [6]) or some other mechanism to request floors.

The conference policy also defines the floor control policy (e.g. moderator-controlled or server grants the floor randomly) and the floor moderator, if the floor policy is moderator-controlled.

The privileged user in a conference (such as the creator) can remove the floor at any time by modifying the conference policy (so that the resources are no longer floor- controlled), or change the floor chair.

The floor moderator just controls the access to the floor, according to the floor policy, defined by the conference policy at a time when the floor is created.

5. Conference Policy Data Model

Conference policy data is relatively static. It is not updated frequently as e.g. participant list is not part of conference policy. Users with sufficient privileges are able to manipulate conference policy. For example, a user with sufficient privileges may manipulate conference's access control list by adding a user into the ACL allowed list.

6. CPCP Requirements

This section describes requirements for the conference policy control protocol (CPCP).

6.1 Conference creation, termination and joining

REQ-A1: It MUST be possible to create a new conference addressable by a URI.

REQ-A2: It MUST be possible to associate policy attributes to a conference URI.

REQ-A3: It MUST be possible to reserve a conference URI for future use with or without associating policy attributes to it.

REQ-A4: It MUST be possible for a privileged user to read conference policy for a given conference URI, during and before joining the conference.

REQ-A5: It MUST be possible to delete existing conference policy. This results in terminating the conference, deleting conference URI and releasing all resources associated with it.

REQ-A6: It MUST be possible to anonymously participate in a conference.

REQ-A7: It MUST NOT be possible for a user to authenticate himself as an anonymous user.

Note: A conference focus must not accept users to authenticate themselves with a username "anonymous" (like in Digest authentication).

REQ-A8: It MUST be possible to assign multiple conference URIs to a conference, one for each session signaling protocol scheme that the conference server supports.

6.2 Manipulating general conference attributes

REQ-B1: It MUST be possible to set, modify and delete a conference Subject.

REQ-B2: It MUST be possible to set, modify and delete conference URI display name.

REQ-B3: It MUST be possible to set, modify and delete conference creator information (as is seen e.g. in SDP o line).

REQ-B4: It MUST be possible to set, modify and delete conference URI link for more information (as used e.g. in SDP u line).

REQ-B5: It MUST be possible to set, modify and delete conference host contact information (as used e.g. in SDP e and p lines).

REQ-B6: It MUST be possible to set, modify and delete short conference session description (as used e.g. in SDP i line). This can be per session or per media.

REQ-B7: It MUST be possible to set, modify and delete the parameter for max number of conference participants. This defines the maximum number of participants present at the same time.

REQ-B8: It MUST be possible to hide conference related information from non-privileged users.

Note: This defines the level of visibility of the basic conference information (e.g. visible only to participants). This feature may be needed e.g. in search operations.

REQ-B9: It MUST be possible to set, modify and delete conference Keywords.

Note: (This may be useful e.g. for search engines).

6.3 Authentication and Security

REQ-C1: It MUST be possible to define appropriate authentication for joining users.

6.4 Application and media manipulation

REQ-D1: It MAY be possible to define media policy within conference policy.

REQ-D2: It MUST be possible to define the media types for the conference.

Note: This means MIME main types, such as audio and video. The conference server can use this information e.g when placing m lines in SIP/SDP dial-outs.

6.5 ACL manipulation

REQ-E1: It MUST be possible to define which users are not allowed to join the conference.

REQ-E2: It MUST be possible to define which users are not allowed to join a conference in a single operation.

REQ-E3: It MUST be possible to define which users are allowed to join the conference.

REQ-E4: It MUST be possible to define which users are allowed to join a conference in a single operation.

REQ-E5: It MUST be possible to define which users are places into pending list, waiting for further approval e.g. from moderator.

REQ-E6: It MUST be possible to use wildcards in ACL (such as sip:*@example.com is allowed to join).

REQ-E7: ACL conflicts MUST be solved in a well-defined way (e.g. what if user appears both in blocked list and in allowed list) e.g. by mandating the order in which ACL definitions are evaluated (e.g. most specific expression first).

REQ-E8: Conference MUST have default policy for those users that no matching rule is found in ACL.

REQ-E9: It MUST be possible to allow and disallow anonymous membership in a conference.

6.6 Floor control

REQ-F1: It MUST be possible to define whether floor control is in use or not.

REQ-F2: It MUST be possible to define the algorithm to be used in granting the floor.

Note: Example algorithms might be e.g. moderator-controlled, FCFS, random.

REQ-F3: It MUST be possible to define how many users can have the floor at the same time.

REQ-F4: It MUST be possible to have one floor for one or more media types.

REQ-F5: It MUST be possible to have multiple floors in a conference.

REQ-F6: It MUST be possible to define whether a floor is moderator-controlled or not.

REQ-F7: If the floor is moderator-controlled, it MUST be possible to assign and replace the floor moderator.

6.7 Inviting and ejecting users

REQ-G1: It MUST be possible to define a dial-out list of users that the conference focus invites.

REQ-G2: It MUST be possible to set a dial-out list in a single operation.

REQ-G3: It MUST be possible to expel users from a currently occurring conference.

REQ-G4: It MUST be possible to expel many users in a single operation.

REQ-G5: It MUST be possible to define list of users who the focus should refer to the conference (so that the referred users will dial in the conference).

REQ-G6: It MUST be possible to set the list of referred users in a single operation.

6.8 User Privileges

REQ-H1: It MUST be possible to give a privilege to a user.

REQ-H2: It MUST be possible to give privileges to many users in a single operation.

REQ-H3: It MUST be possible to remove a privilege from a user.

REQ-H4: It MUST be possible to remove privileges from many users in a single operation.

REQ-H5: It MUST be possible to define users who are allowed to subscribe to the conference event package [\[4\]](#)

REQ-H6: It MUST be only be possible for a users with sufficient privileges to manipulate conference policy.

Note: For example, the creator of the conference may manipulate conference policy.

6.9 General Protocol Requirements

REQ-CP-1: Protocol behaviour: CPCP protocol MUST be a reliable

client-server protocol. Hence, it MUST have a positive response indicating that the request has been received, or error response if an error has occurred.

REQ-CP-2: Manipulations of the policy collection MUST exhibit the ACID property; that is, they MUST be atomic, be consistent, durable, and operate independently.

REQ-CP-3: It MAY be possible for the client to batch multiple operations (such as add a user to ACL blocked list, or remove a user from ACL allowed list) into a single request that is processed atomically.

REQ-CP-4: It MUST be possible for the server to authenticate the client.

REQ-CP-5: It MUST be possible for the client to authenticate the server.

REQ-CP-6: It MUST be possible for message integrity to be ensured between the client and the server.

REQ-CP-7: It MUST be possible for privacy to be ensured between the client and server.

7. Changes since [draft-ietf-xcon-cpcp-reqs-00](#)

- floor control aligned with floor control requirements document
- removed the concept of hidden user
- anonymous membership modified
- removed "inactive"
- added media type requirement (e.g. audio, video)

8. Acknowledgements

The authors would like to thank Eric Burger, Keith Drage, Brian Rosen, Xiaotao Wu, Henning Schulzrinne, Simo Veikkolainen and IETF conferencing design team for their feedback.

Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), BCD 14, March 1997.
- [2] Rosenberg et al., J., "SIP: Session Initiation Protocol", [RFC 3261](#), June 2002.
- [3] Rosenberg, J., "A Framework for Conferencing with the Session Initiation Protocol", [draft-rosenberg-sipping-conferencing-framework-01](#) (work in progress), February 2003.
- [4] Rosenberg, J., "A Session Initiation Protocol (SIP) Event Package for Conference State", [draft-ietf-sipping-conference-package-01](#) (work in progress), June 2003.

Informative References

- [5] Koskelainen, P., Schulzrinne, H. and X. Wu, "Additional Requirements to Conferencing", October 2002.
- [6] Wu, X., Schulzrinne, H. and P. Koskelainen, "Use of SIP and SOAP for conference floor control", January 2003.
- [7] Koskelainen, P., Schulzrinne, H. and X. Wu, "A sip-based conference control framework", Nossdav'2002 Miami Beach, May 2002.

Authors' Addresses

Petri Koskelainen
Nokia
P.O. Box 100 (Visiokatu 1)
Tampere FIN-33721
Finland

EMail: petri.koskelainen@nokia.com

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

EMail: hisham.khartabil@nokia.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Acknowledgement

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