

Simple Policy Control Protocol over TCP/IP

```
<!-- --> <!-- --> <!-- --> <!-- body { font-family: verdana, charcoal, helvetica, arial,
sans-serif; font-size: small ; color: #000000 ; background-color: #ffffff ; } .title { color:
#990000; font-size: x-large ; font-weight: bold; text-align: right; font-family: helvetica,
monaco, "MS Sans Serif", arial, sans-serif; background-color: transparent; }
.filename { color: #666666; font-size: 18px; line-height: 28px; font-weight: bold;
text-align: right; font-family: helvetica, arial, sans-serif; background-color:
transparent; } td.rfcbug { background-color: #000000 ; width: 30px ; height: 30px ;
text-align: justify; vertical-align: middle ; padding-top: 2px ; } td.rfcbug span.RFC {
color: #666666; font-weight: bold; text-decoration: none; background-color: #000000
; font-family: monaco, charcoal, geneva, "MS Sans Serif", helvetica, verdana,
sans-serif; font-size: x-small ; } td.rfcbug span.hotText { color: #ffffff; font-weight:
normal; text-decoration: none; text-align: center ; font-family: charcoal, monaco,
geneva, "MS Sans Serif", helvetica, verdana, sans-serif; font-size: x-small ;
background-color: #000000; } A { font-weight: bold; } A:link { color: #990000;
background-color: transparent ; } A:visited { color: #333333; background-color:
transparent ; } A:active { color: #333333; background-color: transparent ; } p {
margin-left: 2em; margin-right: 2em; } p.copyright { font-size: x-small ; } p.toc {
font-size: small ; font-weight: bold ; margin-left: 3em ;} span.emph { font-style: italic; }
span.strong { font-weight: bold; } span.verb { font-family: "Courier New", Courier,
monospace ; } ol.text { margin-left: 2em; margin-right: 2em; } ul.text { margin-left:
2em; margin-right: 2em; } li { margin-left: 3em; } pre { margin-left: 3em; color:
#333333; background-color: transparent; font-family: "Courier New", Courier,
monospace ; font-size: small ; } h3 { color: #333333; font-size: medium ; font-family:
helvetica, arial, sans-serif ; background-color: transparent; } h4 { font-size: small;
font-family: helvetica, arial, sans-serif ; } table.bug { width: 30px ; height: 15px ; }
td.bug { color: #ffffff ; background-color: #990000 ; text-align: center ; width: 30px ;
height: 15px ; } td.bug A.link2 { color: #ffffff ; font-weight: bold; text-decoration: none;
font-family: monaco, charcoal, geneva, "MS Sans Serif", helvetica, sans-serif;
font-size: x-small ; background-color: transparent } td.header { color: #ffffff; font-size:
x-small ; font-family: arial, helvetica, sans-serif; vertical-align: top; background-color:
#666666 ; width: 33% ; } td.author { font-weight: bold; margin-left: 4em; font-size:
x-small ; } td.author-text { font-size: x-small; } table.data { vertical-align: top ;
border-collapse: collapse ; border-style: solid solid solid solid ; border-color: black
black black black ; font-size: small ; text-align: center ; } table.data th { font-weight:
bold ; border-style: solid solid solid solid ; border-color: black black black black ; }
```

```
table.data td { border-style: solid solid solid solid ; border-color: #333333 #333333  
#333333 #333333 ; } hr { height: 1px } -->
```

Table of contents

13

Simple Policy Control Protocol over TCP/IP

1.

TOC	
Network Working Group	R. Hedberg
Internet-Draft	Stockholm University
Expires: July 1, 2004	January 2004

Simple Policy Control Protocol over TCP/IP

draft-hedberg-spocp-tcp-00

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/1id-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 1, 2004.

Copyright Notice

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

Table of Contents

- [1.](#) Abstract
- [2.](#) Protocol implementation
- [3.](#) Security considerations
- [§](#) References
- [§](#) Author's Address
- [A.](#) Simple examples
- [§](#) Intellectual Property and Copyright Statements

TOC

1. Abstract

The SPOCP protocol has been described in [\[SPOCP\]](#). The description is done in general terms and is not done in such a way that implementers can directly implement the protocol. To make that possible there has to be a mapping defined between the more abstract description and a bits on the wire description. This document represents one possible mapping.

[TOC](#)

2. Protocol implementation

We have chosen a very simple base for our approach: namely to use as a common structure tuples, consisting of a length and a value (LV). The format of the length part is the printable representation of the length and the value is then a variable length value field. The border between the length and the value is denoted by a ':' (0x3A) .

So, the string "foobar" would be represented by the LV "6:foobar".

The reason for choosing this format is of course that the Spocp server must anyway be able to parse canonical S-expressions [\[SPOCP Sexp\]](#) and there for already has the capability to parse LV's. So no extra code is needed for decoding this format. The other benefit is that the server and the client, after having read a couple of bytes of a command or response from the net, knows how many bytes it must read before it has all the information. For the client if a multipart response is received there is no length field telling how big the combined length of all the parts is. Each part is coded separately.

More general, a protocol operations in SPOCP which consists of a operand and a set of zero or more arguments will be represented using the format:

```
L(L'Operand' *L'arg')
```

For example (using the canonical s-expression representation) the permission check:

```
QUERY (4:http(4:page10:index.html)(6:action3:GET)(6:user1d4:olav))
```

Would be represented as

```
70:5:QUERY60:(4:http(4:page10:index.html)(6:action3:GET)(6:user1d4:olav))
```

The server is quiet unless the client sends a query. That is, no initial greeting is sent from the server.

Note: As of this moment there is no default SPOCP port defined.

[TOC](#)

3. Security considerations

This document is about how the SPOCP protocol is to be coded on the wire. Security concerns with the protocol itself and the usage of a generalized access control service is delt with in [\[SPOCP\]](#) and [\[SPOCP Sexp\]](#).

Simple Policy Control Protocol over TCP/IP

[TOC](#)

References

[SPOCP Sexp]	Hedberg, R. and O. Bandmann , "Restricted S-expressions for usage in a generalized access control service".
[SPOCP]	Hedberg, R. , "The Simple Policy Control Protocol".

[TOC](#)

Author's Address

	Roland Hedberg
	Stockholm University
	Kasamark 114
	Umea 90586
	Sweden
Phone:	+46 90 147275
E-Mail:	roland@it.su.se

[TOC](#)

Appendix A. Simple examples

C: marks what the client sends and S: the replies from the server.

Adding a new rule:

```
C: 49:3:ADD41:(4:http(4:page)(6:action3:GET)(6:userid))S: 9:3:2002:Ok
```

A typical query session:

```
C:  
70:5:QUERY60:(4:http(4:page10:index.html)(6:action3:GET)(6:user4:olav))S:  
9:3:2002:OkC: 8:6:LOGOUTS: 10:3:2033:Bye
```

If the client wants to keep the connection open in order to send more queries it just does not send and LOGOUT command.

[TOC](#)

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.

Acknowledgment

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