

RAP Working Group  
Internet Draft  
Expires August 23, 2001

L-N. Hamer  
B. Kosinski  
B. Gage  
Nortel Networks  
February 23, 2001

## **Session Authorization for RSVP**

[draft-hkg-rap-rsvp-authsession-00.txt](#)

### Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#) [1].

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>

The distribution of this memo is unlimited. This memo is filed as [<draft-hkg-rap-rsvp-authsession-00.txt>](#), and expires August 23, 2001. Please send comments to the authors.

### Copyright Notice

Copyright (C) The Internet Society (2001). All Rights Reserved.

### Abstract

This document describes the representation of session authorization information in the POLICY\_DATA object [[POL-EXT](#)] for supporting policy-based per-session authorization and admission control in RSVP. The goal of session authorization is to allow the exchange of information between network elements in order to authorize the use of resources for a service and to co-ordinate actions between the signaling and transport planes. This document describes how a process on a system authorizes the reservation of resources by a host and then provides that host with a session authorization policy element which can be inserted into the RSVP PATH message to facilitate proper and secure reservation of those resources within the network. We describe the encoding of media authorization information as RSVP policy elements and provide details relating to

operations, processing rules and error scenarios.

Expires August 2001

[Page 1]

## **1. 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](#)].

## **2. Introduction**

RSVP [[RFC-2205](#)] is a resource reservation setup protocol designed for an integrated services [[RFC-1633](#)] or DiffEdge [[RFC-2998](#)] Internet. The RSVP protocol is used by a host to request specific qualities of service from the network for particular application data streams or flows. RSVP is also used by routers to deliver quality-of-service (QoS) requests to all nodes along the path(s) of the flows and to establish and maintain state to provide the requested service. RSVP requests will generally result in resources being reserved in each node along the data path. RSVP allows users to obtain preferential access to network resources, under the control of an admission control mechanism. Such admission control is often based on user or application identity [[I-REP](#)], however, it is also valuable to provide the ability for per-session admission control.

In order to allow for per-session admission control, it is necessary to provide a mechanism for ensuring an RSVP request from a host has been properly pre-authorized before allowing the reservation of resources. In order to meet this requirement, there must be information in the RSVP message which may be used to verify the validity of the RSVP request. This may be done by providing the host with a token upon authorization which may be inserted into the RSVP PATH message and verified by the network.

We describe the session authorization element (AUTH\_SESSION) contained in the POLICY\_DATA object. The user process must obtain an AUTH\_SESSION object from an authorizing entity, which it may then pass to the RSVP process (service) on the originating host. The RSVP service then inserts the AUTH\_SESSION object into the RSVP PATH message to allow verification of the network resource request. Network elements, such as routers, verify the request and then admit the RSVP message based on admission policy.

[S-AUTH] describes a framework in which a session authorization policy element may be utilized to contain information relevant to the network's decision to grant a reservation request.

Expires August 2001

[Page 2]

### **3. Policy Element for Session Authorization Data**

#### **3.1 Policy Data Object Format**

POLICY\_DATA objects contain policy information and are carried by RSVP messages. A detail description of the format of POLICY\_DATA object can be found in "RSVP Extensions for Policy Control" [POL-EXT].

#### **3.2 Session Authorization Data Policy Element**

In this section we describe a policy element (PE) called session authorization data (AUTH\_SESSION). The AUTH\_SESSION policy element contains a list of fields which describe the session, along with other attributes.

```
+-----+-----+-----+-----+
| Length                | P-Type = AUTH_SESSION |
+-----+-----+-----+-----+
// Session Authorization Attribute List      //
```

##### **Length**

The length of the policy element (including the Length and P-Type) is in number of octets (MUST be in multiples of 4) and indicates the end of the session authorization information block.

##### **P-Type (Session Authorization Type)**

The Policy element type (P-type) of this element. The Internet Assigned Numbers Authority (IANA) acts as a registry for policy element types for identity as described in [POL-EXT]. The definition for AUTH\_SESSION is currently to be defined.

##### **Session Authorization Attribute List**

The session authorization attribute list is a collection of objects which describes the session and provides other information necessary to verify the RSVP request.

#### **3.3 Session Authorization Attributes**

A session authorization attribute may contain a variety of information and has both an attribute type and subtype. The attribute itself MUST be a multiple of 4 octets in length, and any attributes that are not a multiple of 4 octets long MUST be padded to a 4-octet boundary.

Expires August 2001

[Page 3]

```

+-----+-----+-----+-----+
| Length           | S-Type |SubType |
+-----+-----+-----+-----+
| Value ...
+-----+-----+-----+-----+

```

### Length

The length field is two octets and indicates the actual length of the attribute (including Length, S-Type and SubType fields) in number of octets. The length does NOT include any bytes padding to the value field to make the attribute a multiple of 4 octets long.

### S-Type

Session authorization attribute type (S-Type) field is one octet. IANA SHALL act as a registry for S-Types as described in [section 7](#), IANA Considerations. Initially, the registry contains the following S-Types:

- |   |                   |   |
|---|-------------------|---|
| 1 | AUTH_ENT_ID       | The unique identifier of the entity which authorized the session.         |
| 2 | AUTH_ENT_CRED     | The credentials of the authorizing entity, such as a digital certificate. |
| 3 | SESSION_ID        | Unique identifier for this session.                                       |
| 4 | SOURCE_ADDR       | Address specification for the session originator.                         |
| 5 | DEST_ADDR         | Address specification for the session end-point.                          |
| 6 | START_TIME        | The starting time for the session.  |
| 7 | END_TIME          | The end time for the session.   |
| 8 | RESOURCES         | The resources which the user is authorized to request.                    |
| 9 | DIGITAL_SIGNATURE | Digital signature of the session authorization policy element.            |

### SubType

Session authorization attribute sub-type is one octet in length. The value of the SubType depends on the S-Type.

Value

The attribute specific information.

Expires August 2001

[Page 4]



### 3.3.1 Authorizing Entity Identifier

AUTH\_ENT\_ID is used to identify the entity which authorized the initial service request and generated the session authorization policy element. The AUTH\_ENT\_ID may be represented in various formats, and the SubType is used to define the format for the ID. The format for AUTH\_ENT\_ID is as follows:

```
+-----+-----+-----+-----+
| Length      |S-Type|SubType|
+-----+-----+-----+-----+
| OctetString ...
+-----+-----+-----+-----+
```

#### Length

Length of the attribute, which MUST be  $\geq 4$ .

#### S-Type

AUTH\_ENT\_ID

#### SubType

The following sub-types for AUTH\_ENT\_ID are defined. IANA SHALL act as a registry for AUTH\_ENT\_ID sub-types as described in [section 7](#), IANA Considerations. Initially, the registry contains the following sub-types of AUTH\_ENT\_ID:

- |   |               |  |
|---|---------------|--|
| 1 | IPV4_ADDRESS  | IPv4 address   |
| 2 | IPV6_ADDRESS  | IPv6 address   |
| 3 | FQDN          | Fully Qualified Domain Name  |
| 4 | ASCII_DN      | X.500 Distinguished name as defined in <a href="#">RFC-1779</a> as an ASCII string.  |
| 5 | UNICODE_DN    | X.500 Distinguished name as defined in <a href="#">RFC-1779</a> as a UNICODE string. |
| 6 | URI           | Universal Resource Identifier, as defined in <a href="#">RFC-2396</a> .              |
| 7 | KRB_PRINCIPAL | Kerberos principal name as defined in <a href="#">RFC-1510</a> .                     |

#### OctetString

Contains the authorizing entity identifier.

Expires August 2001

[Page 5]

### 3.3.2 Authorizing Entity Credentials

AUTH\_ENT\_CRED contains the credentials of the authorizing entity, which can then be used by the network to ensure that the entity which generated this session authorization policy element is a valid trusted entity.

```
+-----+-----+-----+-----+
| Length      |S-Type|SubType|
+-----+-----+-----+-----+
| OctetString ...
+-----+-----+-----+-----+
```

Length

Length of the attribute, which MUST be  $\geq 4$ .

S-Type

AUTH\_ENT\_CRED

SubType

The type of credentials contained in this attribute. IANA SHALL act as a registry for AUTH\_ENT\_CRED sub-types as described in [section 7](#), IANA Considerations. Initially, the registry contains the following sub-types:

- |   |              |   |
|---|--------------|---|
| 1 | ASCII_ID     | The authorizing entity identification in a plain ASCII text string.   |
| 2 | UNICODE_ID   | The authorizing entity identification in a plain UNICODE text string. |
| 3 | X509_V3_CERT | A chain of authorizing entity's X.509 V3 digital certificates.        |
| 4 | PGP_CERT     | The PGP digital certificate of the authorizing entity.                |

OctetString

Contains the authorizing entity credentials.

### 3.3.3 Session Identifier

SESSION\_ID is a unique identifier for this session. It may be used for a number of purposes, including replay detection, or even mapping this request to a policy decision entry made by the authorizing entity.

```
+-----+-----+-----+-----+
| Length      |S-Type|SubType|
+-----+-----+-----+-----+
```

```
+-----+-----+-----+-----+
| OctetString ...
+-----+-----+-----+-----+
```

**Length**

Length of the attribute, which MUST be  $\geq 4$ .

**S-Type**

SESSION\_ID

**SubType**

The following sub-types for SESSION\_ID are defined. IANA SHALL act as a registry for SESSION\_ID sub-types as described in [section 7](#), IANA Considerations. Initially, the registry contains the following sub-types of SESSION\_ID:

- |   |            |   |
|---|------------|---|
| 1 | ASCII_ID   | Simple plain ASCII string identifier.   |
| 2 | UNICODE_ID | Simple plain UNICODE string identifier. |
| 3 | OCTET_ID   | Raw octet string identifier.            |

**OctetString**

Contains the actual session identifier.

**3.3.4 Source Address**

SOURCE\_ADDR is used to identify the source address specification of the authorized session. This S-Type MAY be useful in some scenarios to make sure the resource request has been authorized for that particular source IP address and/or port.

```

+-----+-----+-----+-----+
| Length      |S-Type |SubType|
+-----+-----+-----+-----+
| OctetString ...
+-----+-----+-----+-----+
```

**Length**

Length of the attribute, which MUST be  $\geq 4$ .

**S-Type**

SOURCE\_ADDR

**SubType**

The following sub types for SOURCE\_ADDR are defined. IANA SHALL act as a registry for SOURCE\_ADDR sub-types as described in [section 7](#), IANA Considerations. Initially, the registry contains the following sub types for SOURCE\_ADDR:

- |   |              |              |
|---|--------------|--------------|
| 1 | IPV4_ADDRESS | IPv4 address |
| 2 | IPV6_ADDRESS | IPv6 address |

Expires August 2001

[Page 7]

- |   |          |                        |
|---|----------|------------------------|
| 3 | UDP_PORT | UDP port specification |
| 4 | TCP_PORT | TCP port specification |

OctetString

The OctetString contains the source address information.

### **3.3.5 Destination Address**

DEST\_ADDR is used to identify the destination address of the authorized session. This S-Type MAY be useful in some scenarios to make sure the resource request has been authorized for that particular destination IP address and/or port.

```

+-----+-----+-----+-----+
| Length      |S-Type |SubType|
+-----+-----+-----+-----+
| OctetString ...
+-----+-----+-----+-----+

```

Length

Length of the attribute, which MUST be >= 4.

S-Type

DEST\_ADDR

SubType

The following sub types for DEST\_ADDR are defined. IANA SHALL act as a registry for DEST\_ADDR sub-types as described in [section 7](#), IANA Considerations. Initially, the registry contains the following sub types for DEST\_ADDR:

- |   |              |                        |
|---|--------------|------------------------|
| 1 | IPV4_ADDRESS | IPv4 address           |
| 2 | IPV6_ADDRESS | IPv6 address           |
| 3 | UDP_PORT     | UDP port specification |
| 4 | TCP_PORT     | TCP port specification |

OctetString

The OctetString contains the destination address specification.

### **3.3.6 Start time**

START\_TIME is used to identify the start time of the authorized session. This S-Type MAY be useful in some scenarios to specify a start time for the authorized session.

Expires August 2001

[Page 8]



```

+-----+-----+-----+-----+
| Length      |S-Type |SubType|
+-----+-----+-----+-----+
| OctetString ...
+-----+-----+-----+-----+

```

**Length**

Length of the attribute, which MUST be  $\geq 4$ .

**S-Type**

START\_TIME

**SubType**

The following sub types for START\_TIME are defined. IANA SHALL act as a registry for START\_TIME sub-types as described in [section 7](#), IANA Considerations. Initially, the registry contains the following sub types for START\_TIME:

- |   |               |   |
|---|---------------|---|
| 1 | NTP_TIMESTAMP | NTP Timestamp Format as defined in <a href="#">RFC-1305</a> . |
|---|---------------|---|

**OctetString**

The OctetString contains the start time.

**[3.3.7](#) End time**

END\_TIME is used to identify the end time of the authorized session. This S-Type MAY be useful in some scenarios to specify a end time for the authorized session.

```

+-----+-----+-----+-----+
| Length      |S-Type |SubType|
+-----+-----+-----+-----+
| OctetString ...
+-----+-----+-----+-----+

```

**Length**

Length of the attribute, which MUST be  $\geq 4$ .

**S-Type**

END\_TIME

**SubType**

The following sub types for END\_TIME are defined. IANA SHALL act as a registry for END\_TIME sub-types as described in [section 7](#), IANA Considerations. Initially, the registry contains the following sub types for END\_TIME:

- |   |               |                                    |
|---|---------------|------------------------------------|
| 1 | NTP_TIMESTAMP | NTP Timestamp Format as defined in |
|---|---------------|------------------------------------|

[RFC-1305](#).

Expires August 2001

[Page 9]

OctetString

The OctetString contains the end time.

### **3.3.8 Resources Authorized**

RESOURCES is used to define the characteristics of the authorized session. This S-Type MAY be useful in some scenarios to specify the specific resources authorized to ensure the request fits the authorized specifications.

```
+-----+-----+-----+-----+
| Length      |S-Type|SubType|
+-----+-----+-----+-----+
| OctetString ...
+-----+-----+-----+-----+
```

Length

Length of the attribute, which MUST be  $\geq 4$ .

S-Type

RESOURCES

SubType

The following sub-types for RESOURCES are defined. IANA SHALL act as a registry for RESOURCES sub-types as described in [section 7](#), IANA Considerations. Initially, the registry contains the following sub types for RESOURCES:

- |             |  |
|-------------|--|
| 1 BANDWIDTH | Maximum bandwidth (kbps) authorized.                                       |
| 2 FLOW_SPEC | Flow spec specification as defined in <a href="#">RFC-2205</a> .           |
| 3 SDP       | SDP Media Descriptor as defined in <a href="#">RFC-2327</a> .              |
| 4 DSCP      | Differentiated services codepoint as defined in <a href="#">RFC-2474</a> . |

OctetString

The OctetString contains the resources specification.

### **3.3.9 Digital Signature**

The DIGITAL\_SIGNATURE attribute contains the digital signature of the AUTH\_SESSION policy element and signs all the data in the policy element up to the DIGITAL\_SIGNATURE. If the DIGITAL\_SIGNATURE attribute has been included in the AUTH\_SESSION policy element, it MUST be the last attribute in the list.

A summary of DIGITAL\_SIGNATURE attribute format is described below.

Expires August 2001

[Page 10]

```

+-----+-----+-----+-----+
| Length      |S-Type |SubType|
+-----+-----+-----+-----+
| OctetString ...
+-----+-----+-----+-----+

```

**Length**

Length of the attribute, which MUST be  $\geq 4$ .

**S-Type**

DIGITAL\_SIGNATURE

**SubType**

The following sub-types for DIGITAL\_SIGNATURE are defined. IANA SHALL act as a registry for DIGITAL\_SIGNATURE sub-types as described in [section 7](#), IANA Considerations. Initially, the registry contains the following sub types for DIGITAL\_SIGNATURE:

- |   |           |   |
|---|-----------|---|
| 1 | DSA_SHA1  | DSA signature using SHA1 [ <a href="#">X.509</a> ]. |
| 2 | RSA_SHA1  | RSA signature using SHA1 [ <a href="#">X.509</a> ]. |
| 3 | RSA_MD5   | RSA signature using MD5 [ <a href="#">X.509</a> ].  |
| 4 | HMAC_SHA1 | HMAC with SHA1 [ <a href="#">RFC 2104</a> ].        |
| 5 | HMAC_MD5  | HMAC with MD5 [ <a href="#">RFC 2104</a> ].         |

**OctetString**

OctetString contains the digital signature of the AUTH\_SESSION.

**[4. Framework](#)**

[S-AUTH] describes a framework in which the session authorization policy element may be utilized to transport information for use in authorizing resource reservation for media flows.

**[5. Message Processing Rules](#)****[5.1 Message Generation \(RSVP Host\)](#)**

An RSVP message is created as specified in [[RFC-2205](#)] with following modifications.

1. RSVP message MUST contain at most one AUTH\_SESSION policy element.

Expires August 2001

[Page 11]

2. A Session Authorization policy element (AUTH\_SESSION) is created and the IdentityType field is set to indicate the identity type in the policy element. Only the required Session Authorization attributes are added.
3. POLICY\_DATA object (containing the AUTH\_SESSION policy element) is inserted in the RSVP message in the appropriate place.

## **5.2 Message Reception (Router)**

RSVP message is processed as specified in [[RFC-2205](#)] with following modifications.

1. If router is policy aware then it SHOULD send the RSVP message to the PDP and wait for response. If the router is policy unaware then it ignores the policy data objects and continues processing the RSVP message.
2. Reject the message if the response from the PDP is negative.
3. Continue processing the RSVP message.

## **5.3 Authorization (Router/PDP)**

1. Retrieve the AUTH\_SESSION policy element. Check the PE type field and return an error if the identity type is not supported.
2. Verify the authorizing entity credentials and message integrity.
  - Pre-shared key authentication: Get entity ID, identify appropriate pre-shared key for the authorizing entity, and validate signature.
  - Public Key: Validate the certificate chain against trusted Certificate Authority (CA) and validate the message signature using the public key.
  - Kerberos Ticket: Request a ticket for the authorizing entity from the local KDC. Use the ticket to access the authorizing entity and obtain authentication data for the message (e.g. the signing key) or the data itself.
3. Verify the requested QoS does not exceed the authorized QoS.

Expires August 2001

[Page 12]



## **6. Error Signaling**

If PDP fails to verify the AUTH\_SESSION policy element then it MUST return policy control failure (Error Code = 02) to the PEP. The error values are described in [[RFC-2205](#)] and [[POL-EXT](#)]. Also PDP SHOULD supply a policy data object containing an AUTH\_DATA Policy Element with A-Type=POLICY\_ERROR\_CODE containing more details on the Policy Control failure [[I-REP](#)]. The PEP will include this Policy Data object in the outgoing RSVP Error message.

## **7. IANA Considerations**

Following the policies outlined in [[IANA-CONSIDERATIONS](#)], session authorization attribute types (S-Type) in the range 0-127 are allocated through an IETF Consensus action, S-Type values between 128-255 are reserved for Private Use and are not assigned by IANA.

Following the policies outlined in [[IANA-CONSIDERATIONS](#)], AUTH\_ENT\_ID, AUTH\_ENT\_CRED, SESSION\_ID, START\_TIME, STOP\_TIME, SOURCE\_IP, DEST\_IP, RESOURCES and DIGITAL\_SIGNATURE SubType values in the range 0-127 are allocated through an IETF Consensus action, SubType values between 128-255 are reserved for Private Use and are not assigned by IANA.

## **8. Security Considerations**

The purpose of this draft is to describe a mechanism for media authorization to prevent theft of service. It does not cover other possible security breaches such as IP spoofing.

## **9. Acknowledgments**

We would like to thank Francois Audet, Don Wade, Hamid Syed, Matt Broda, and many others for their valuable comments.

In addition, we would like to thank S. Yadav, et al, for their efforts on [RFC 2752](#), as this document borrows heavily from their work.

## **10. References**

- |          |   |
|----------|---|
| [I-REP]  | S. Yadav et al, "Identity Representation for RSVP", Internet-draft, <a href="#">draft-ietf-rap-rsvp-newidentity-01.txt</a> , January 2000 |
| [S-AUTH] | Hamer, L-N. and Gage, B, "Framework for session setup with media authorization",  |

Internet-Draft,  
[draft-hamer-rap-session-auth-00.txt](#),  
February 2001.

Expires August 2001

[Page 13]

- [ASCII] Coded Character Set -- 7-Bit American Standard Code for Information Interchange, ANSI X3.4-1986.
- [IANA-CONSIDERATIONS] Alvestrand, H. and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 2434](#), October 1998.
- [POL-EXT] Herzog, S., "RSVP Extensions for Policy Control", [RFC 2750](#), January 2000.
- [POL-FRAME] Yavatkar, R., Pendarakis, D. and R. Guerin, "A Framework for Policy-based Admission Control RSVP", [RFC 2753](#), January 2000.
- [RFC-1305] Mills, David L., "Network Time Protocol (Version 3) Specification, Implementation, and Analysis", [RFC 1305](#), March 1992.
- [RFC-1510] Kohl, J. and C. Neuman, "The Kerberos Network Authentication Service (V5)", [RFC 1510](#), September 1993.
- [RFC-1633] Braden, R., Clark, D., Shenker, S., "Integrated Services in the Internet Architecture: An Overview", [RFC 1633](#), June 1994.
- [RFC-1779] Killie, S., "A String Representation of Distinguished Names", [RFC 1779](#), March 1995.
- [RFC-2205] Braden, R., Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification", [RFC 2205](#), September 1997.
- [RFC-2209] Braden, R. and L. Zhang, "Resource ReSerVation Protocol (RSVP) - Version 1 Message Processing Rules", [RFC 2209](#), September 1997.
- [RFC-2327] Handley, M., Jacobson, V., "SDP: Session Description Protocol", [RFC 2327](#), April 1998.
- [RFC-2396] Berners-Lee, T., Fielding, R., Irvine, U.C., Masinter, L., "Uniform Resource Identifiers (URI): Generic Syntax", [RFC 2396](#), August 1998.
- [RFC-2474] Nichols, K., Blake, S., Baker, F., Black, D., "Definition of the Differentiated Services

Field (DS Field) in the IPv4 and IPv6  
Headers", [RFC 2474](#), December 1998.

Expires August 2001

[Page 14]

- [RFC-2998]                Bernet, Y., Ford, P., Yavatkar, R., Baker, F., Zhang, L., Speer, M., Braden, R., Davie, B., Wroclawski, J., Felstaine, E., "A Framework for Integrated Services Operation over Diffserv Networks", [RFC 2998](#), November 2000.
- [UNICODE]                The Unicode Consortium, "The Unicode Standard, Version 2.0", Addison-Wesley, Reading, MA, 1996.
- [X.509]                  Housley, R., Ford, W., Polk, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", [RFC 2459](#), January 1999.
- [X.509-ITU]                ITU-T (formerly CCITT) Information technology - Open Systems Interconnection - The Directory: Authentication Framework Recommendation X.509 ISO/IEC 9594-8

## **11. Author Information**

Louis-Nicolas Hamer  
Nortel Networks  
Ottawa, Canada  
EEmail: [nhamer@nortelnetworks.com](mailto:nhamer@nortelnetworks.com)

Brett Kosinski  
Nortel Networks  
Ottawa, Canada  
EEmail: [brettk@nortelnetworks.com](mailto:brettk@nortelnetworks.com)

Bill Gage  
Nortel Networks  
Ottawa, Canada  
EEmail: [gageb@nortelnetworks.com](mailto:gageb@nortelnetworks.com)

## **12. Full Copyright Statement**

Copyright (C) The Internet Society (2001). 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 organisations, 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.

#### Expiration Date

This memo is filed as <[draft-hkg-rap-rsvp-authsession-00.txt](#)>, and expires August 23, 2001.

Expires August 2001

[Page 15]