RAP Working Group
Internet-Draft
Obsoletes: 2752
Expires January 2002

R. Hess, Ed.
S. Yadav
R. Yavatkar
Intel
R. Pabbati
P. Ford
T. Moore
Microsoft
S. Herzog
IPHighway

July 2001

Identity Representation for RSVP

draft-ietf-rap-rsvp-better-identity-01.txt

Status of this Memo

Copyright Notice

Abstract

This document describes the representation of identity information in POLICY_DATA objects [POL-EXT] for supporting policy based admission control in RSVP [RFC 2205]. The goal of identity representation is

to allow a process on a system to securely identify the owner and the application of the communicating process (e.g. user id) and to convey this information in RSVP PATH or RESV messages in a secure manner. We describe the encoding of identities as a RSVP policy element. We describe the processing rules to generate identity policy elements for multicast merged flows. Subsequently, we describe representations of user identities for Kerberos and public-key based authentication mechanisms. In summary we describe the use of this identity information in an operational setting.

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 protocol designed for an integrated services Internet [RFC 1633]. A host uses RSVP to request a specific quality of service (QoS) from the network for a particular application's data flows. RSVP is also used by routers to deliver QoS requests to all nodes along the path(s) of the flows and to establish and maintain state in order to provide the requested service. RSVP requests will generally result in resources being reserved in each node along the data path. RSVP allows particular users to obtain preferential access to network resources, under the control of an admission control mechanism. Permission to make a reservation is based both upon the availability of the requested resources along the data path and upon satisfaction of policy rules. Providing policy based admission control mechanism based on user or application identity is one of the primary requirements of RSVP.

In order to solve these problems and implement identity based policy control it is necessary to identify the user or application making the RSVP request.

This document proposes a mechanism for sending identification information in an RSVP message, thereby enabling authorization decisions to be based on policy and identity.

We describe the authentication policy element (AUTH_DATA) contained in a POLICY_DATA object [POL-EXT]. A user process generates an AUTH_DATA policy element and hands it off to a policy aware RSVP service on the originating host. The RSVP service encapsulates the AUTH_DATA policy element into a POLICY_DATA object. It then inserts this object into the RSVP PATH or RESV message to permit identification of the owner (e.g. user or application) making the

request for network resources. Policy aware RSVP systems, also referred to by this memo as Policy Enforcement Points (PEPs), forward the policy elements to their Policy Decision Points (PDPs) [POL-FRAME].

Each PDP along the data path authenticates the request using the credentials present in the AUTH_DATA policy element. The PDP makes an admission policy decision along with other policy decisions as warranted by policy configuration. The admit or deny decision is returned to the PEP, who either installs the necessary RSVP state or rejects the RSVP request. Furthermore, with an admit decision, the PDP also returns to the PEP a new policy element list in which exists a new AUTH_DATA policy element amongst other possible policy elements. This new AUTH_DATA contains the identity credentials of this PDP for authentication by the next PDP in the data path. The PEP forwards the RSVP message with the new policy elements to the next RSVP hop. In this manner, network resources can be allocated or reserved based on policy and identity.

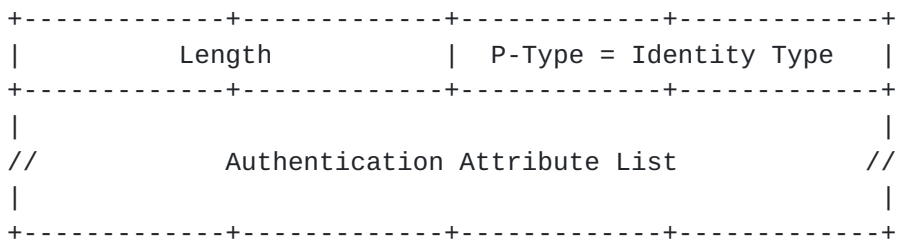
3. Policy Element for Authentication Data

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 the POLICY_DATA object can be found in "RSVP Extensions for Policy Control" [POL-EXT].

3.2. Authentication Data Policy Element

In this section, we describe a policy element (PE) called authentication data (AUTH_DATA). AUTH_DATA policy elements contain a list of authentication attributes.



Length: 16 bits

The length of the policy element (including the Length and P-Type fields) in number of octets (MUST be a multiple of 4) and indicates the end of the authentication attribute list.

P-Type (Identity Type): 16 bits

Type of identity information contained in this Policy Element supplied as the Policy Element Type (P-Type). The Internet Assigned Numbers Authority (IANA) acts as a registry for Policy

Element Types for identity as described in the [POL-EXT].

Initially, the registry contains the following P-Types for identity:

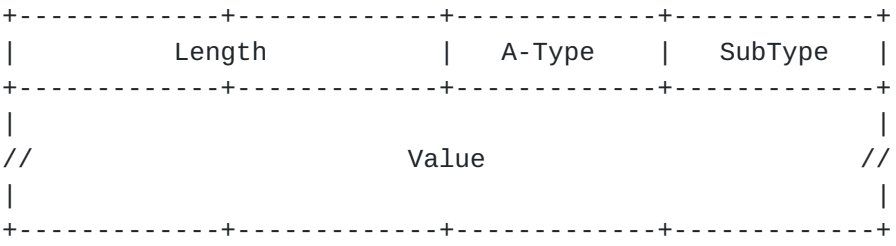
2	AUTH_USER	Authentication scheme to identify users
3	AUTH_APP	Authentication scheme to identify applications

Authentication Attribute List: Variable length

Authentication attributes contain information specific to the authentication method and the type of AUTH_DATA. The policy element definition [POL-EXT] provides the mechanism for grouping a collection of authentication attributes.

3.3. Authentication Attributes

Authentication attributes MUST be encoded as a multiple of 4 octets; attributes that are not a multiple of 4 octets long MUST be padded to a 4-octet boundary.



Length: 16 bits

The length field indicates the actual length of the attribute (including the Length and A-Type fields) in number of octets. The length does not include any octet padding to the Value field to make the attribute a multiple of 4 octets long.

A-Type: 8 bits

Authentication attribute type (A-Type) field is one octet. IANA acts as a registry for A-Types as described in the section 9, IANA Considerations. Initially, the registry contains the following A-Types:

1	POLICY_LOCATOR	Unique string for locating the admission policy (such as X.500 DN described in [RFC 1779]).
2	CREDENTIAL	User credential such as a Kerberos ticket, or a digital certificate.

	Application credential such as an application ID.

3	DIGITAL_SIGNATURE	Digital signature of the authentication data policy element.
4	POLICY_ERROR_OBJECT	Detailed information on policy failures.

SubType: 8 bits

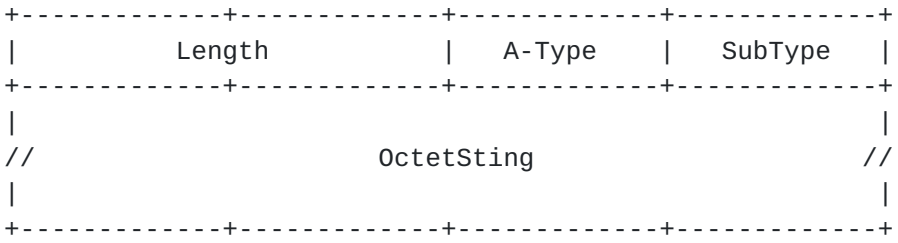
Authentication attribute sub-type field is one octet. Value of SubType depends on A-type.

Value: Variable length

The value field contains the attribute specific information.

3.3.1. POLICY_LOCATOR A-Type

POLICY_LOCATOR is used to locate the admission policy for the user or application. Distinguished Name (DN) is unique for each User or application hence a DN is used as for the policy locator.



Length: 16 bits

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

A-Type: 8 bits

This field MUST contain the value POLICY_LOCATOR.

SubType: 8 bits

The following SubTypes for POLICY_LOCATOR are defined. IANA acts As a registry for POLICY_LOCATOR SubTypes as described in Section 9, IANA Considerations. Initially, the registry contains the following SubTypes for POLICY_LOCATOR:

1	ASCII_DN	OctetString contains the X.500 DN as described in the RFC 1779 as an ASCII string.
2	UNICODE_DN	OctetString contains the X.500 DN

described in the RFC 1779 as an UNICODE string.

3	ASCII_DN_ENCRYPT	OctetString contains the encrypted X.500 DN. The Kerberos session key or digital certificate private key is used for encryption. For Kerberos encryption the format is the same as returned from gss_seal [RFC 1509].
4	UNICODE_DN_ENCRYPT	OctetString contains the encrypted UNICODE X.500 DN. The Kerberos session key or digital certificate private key is used for encryption. For Kerberos encryption the format is the same as returned from gss_seal [RFC 1509].

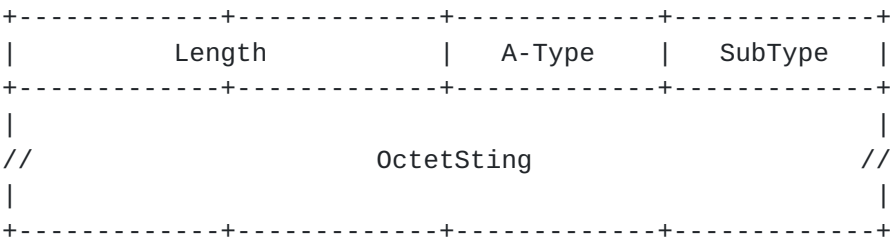
OctetString: Variable length

The OctetString field contains the DN.

3.3.2. CREDENTIAL A-Type

CREDENTIAL indicates the credentials of the user or application to be authenticated. For Kerberos authentication method the CREDENTIAL object contains the Kerberos session ticket. For public-key based authentication this field contains a digital certificate.

A summary of the CREDENTIAL attribute format is shown below. The fields are transmitted from left to right.



Length: 16 bits

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

A-Type: 8 bits

This field MUST contain the value CREDENTIAL.

SubType: 8 bits

IANA acts as a registry for CREDENTIAL SubTypes as described in Section 9, IANA Considerations. Initially, the registry contains the following SubTypes for CREDENTIAL:

1	ASCII_ID	OctetString contains user or application identification in a plain ASCII text string.
2	UNICODE_ID	OctetString contains user or application identification in a plain UNICODE text string.
3	KERBEROS_TKT	OctetString contains a Kerberos ticket.
4	X509_V3_CERT	OctetString contains a X.509 V3 digital certificate [X.509].
5	PGP_CERT	OctetString contains a PGP digital certificate.

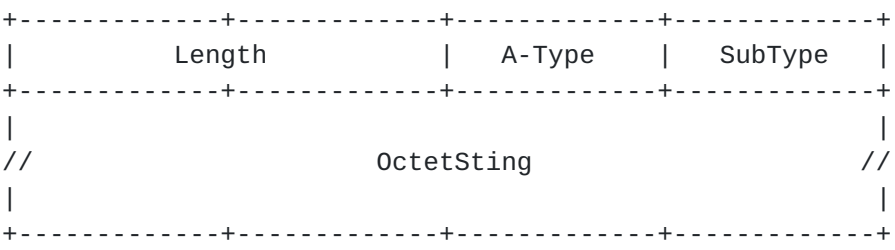
OctetString: Variable length

The OctetString contains the user or application credentials.

3.3.3. DIGITAL_SIGNATURE A-Type

The DIGITAL_SIGNATURE attribute MUST be the last attribute in the attribute list and contains the digital signature of the AUTH_DATA policy element. The digital signature signs all data in the AUTH_DATA policy element up to, but not including, the DIGITAL_SIGNATURE. The algorithm used to compute the digital signature depends on the authentication method specified by the CREDENTIAL SubType field.

A summary of DIGITAL_SIGNATURE attribute format is described below.



Length: 16 bits

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

A-Type: 8 bits

This field MUST contain the value DIGITAL_SIGNATURE.

SubType: 8 bits

No SubTypes for DIGITAL_SIGNATURE are currently defined. This

field MUST be set to 0.

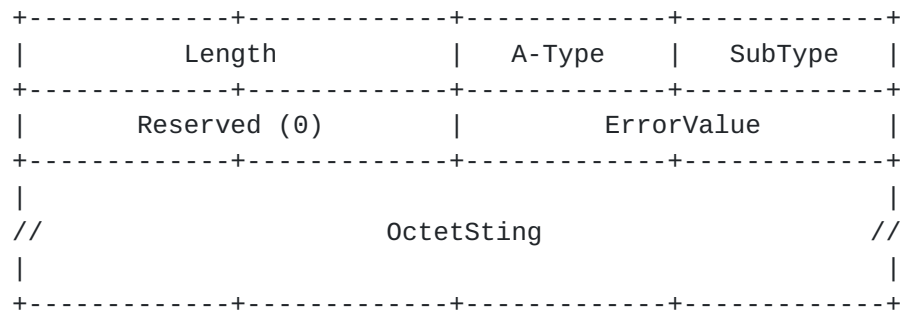
OctetString: Variable length

OctetString contains the digital signature of the AUTH_DATA.

3.3.4. POLICY_ERROR_CODE A-Type

This attribute is used to carry any specific policy control errors generated by a node when processing/validating an Authentication Data Policy Element. When a RSVP policy node (local policy decision point or remote PDP) encounters a request that fails policy control due to its Authentication Policy Element, it SHOULD add a POLICY_ERROR_CODE containing additional information about the reason the failure occurred into the policy element. This will then cause an appropriate PATH_ERROR or RESV_ERROR message to be generated with the policy element and appropriate RSVP error code in the message, which is returned to the request's source.

The AUTH_DATA policy element in a PATH or RSVP message SHOULD NOT contain the POLICY_ERROR_OBJECT attribute. These are only inserted into PATH_ERROR and RESV_ERROR messages when generated by policy aware intermediate nodes.



Length: 16 bits

Length of the attribute, which MUST be >= 8.

A-Type: 8 bits

This field MUST contain the value POLICY_ERROR_CODE

SubType: 8 bits

No SubTypes for POLICY_ERROR_CODE are currently defined. This field MUST be set to 0.

Reserved: 16 bits

This field MUST be set to 0.

ErrorValue: 16 bits

A 16-bit code containing the reason that the Policy Decision Point failed to process the policy element. IANA acts as a registry for ErrorValues as described in Section 9, IANA Considerations. The following values have been defined.

1	ERROR_NO_MORE_INFO	No information is available.
2	UNSUPPORTED_CREDENTIAL_TYPE	This type of credentials is not supported.
3	INSUFFICIENT_PRIVILEGES	The credentials do not have sufficient privilege.
4	EXPIRED_CREDENTIAL	The credential has expired.
5	IDENTITY_CHANGED	Identity has changed.

OctetString: Variable length

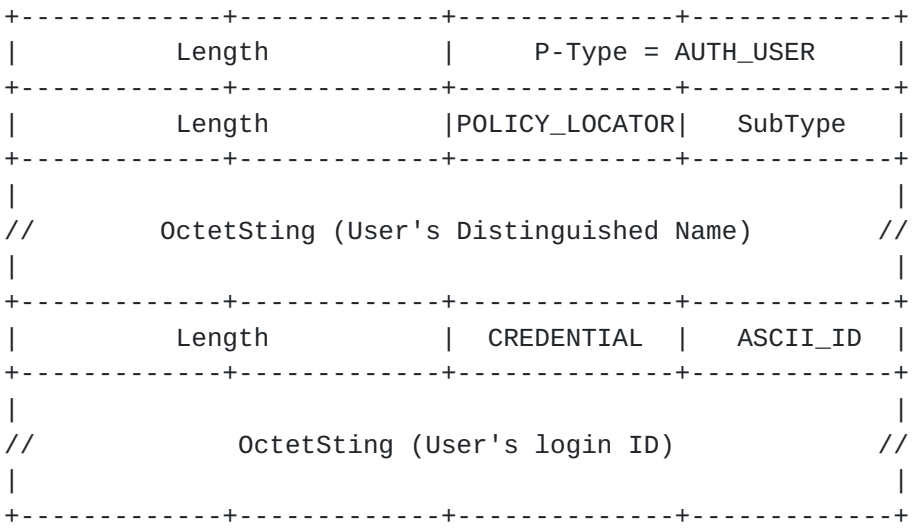
The OctetString field contains information from the Policy Decision Point that MAY contain additional information about the policy failure. For example, it may include a human readable message in the ASCII text.

4. Authentication Data Formats

Authentication attributes are grouped together in a policy element to represent the identity credentials.

4.1. Simple User Authentication

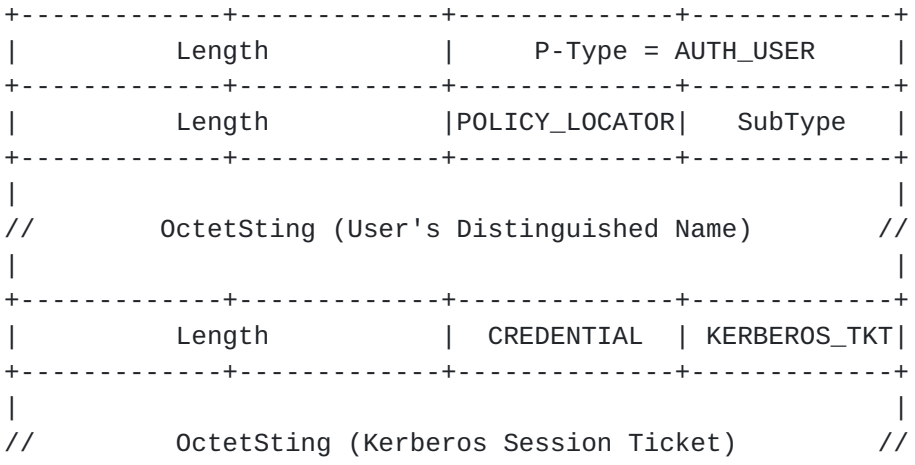
In the simple user authentication method, the user's login ID, in either plain ASCII or UNICODE text, is encoded as a CREDENTIAL attribute. A summary of the simple user AUTH_DATA policy element is shown below.

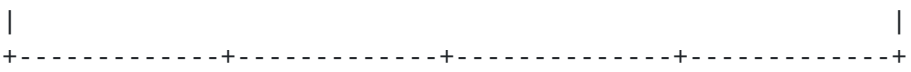


4.2. Kerberos User Authentication

Kerberos [RFC 1510] authentication utilizes a trusted third party, the Kerberos Distribution Center (KDC), to provide for authentication of the user to a policy aware network element. For this method of authentication to work, a KDC must be present, and both the host and the policy aware network element (re: PDP) implement the Kerberos authentication protocol.

An example of a user Kerberos AUTH_DATA policy element is shown below.





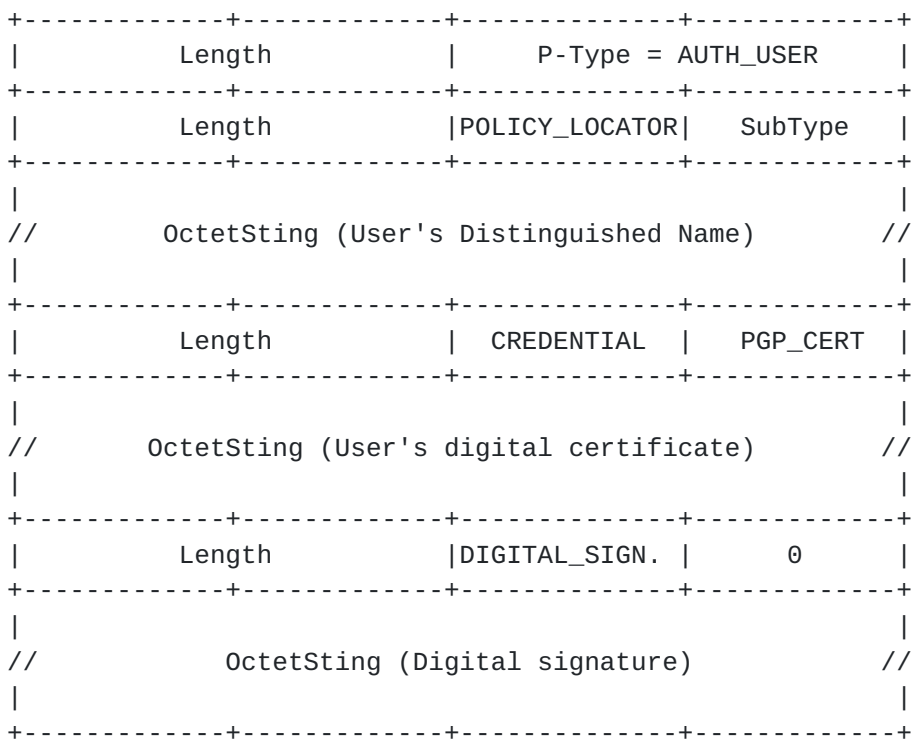
4.2.1. Operational Setting using Kerberos Identities

A policy aware RSVP enabled host is configured to construct and insert AUTH_DATA policy objects into RSVP messages that designate use of the Kerberos authentication method (KERBEROS_TKT). Upon a RSVP session initialization, the initiating application, be it a user and/or an application, contacts the KDC to obtain a Kerberos ticket for the next policy aware RSVP system or its PDP on the data path. The identity of the next hop may have been statically configured, learned via DHCP or maintained in a directory service. Once the ticket is acquired, the host constructs a Kerberos AUTH_DATA policy object, encapsulates it into a RSVP message, and sends it to the next hop RSVP system. Once received by the PDP, the Kerberos ticket is used to authenticate the user and/or application initiating the RSVP session.

4.3. Public-Key Based User Authentication

In the public-key based user authentication method, the digital certificate is encoded as the user's and/or application's credentials. The digital signature is used for authenticating the user and/or application.

An example of a user public-key AUTH_DATA policy element is show below.



4.3.1. Operational Setting for Public-Key Based Authentication

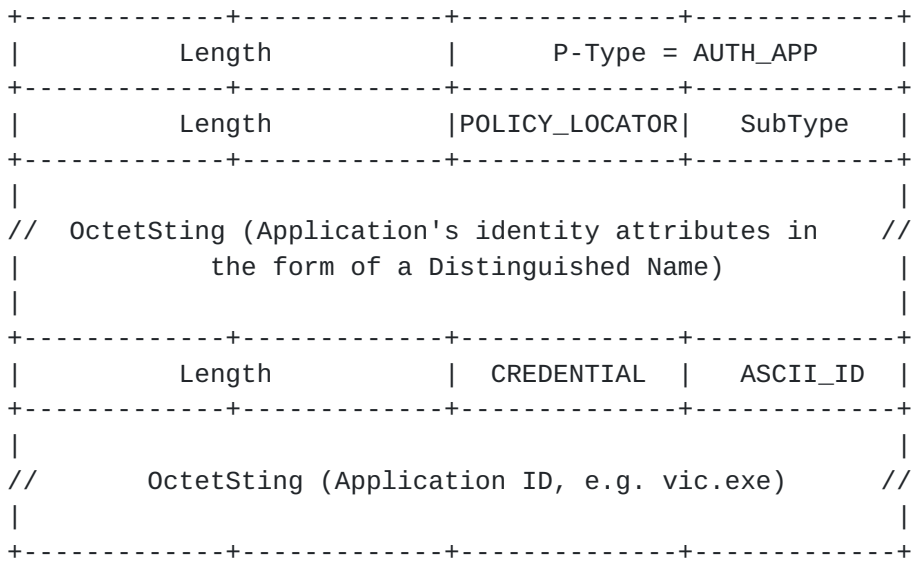
Public-key based authentication assumes the following:

- RSVP service requestors have a pair of keys, one private and one public.
- The private key is secured with the user.
- Public keys are stored in digital certificates. A trusted third party, the certificate authority (CA), issues these digital certificates upon request.
- The PDP has the ability to verify digital certificates.

A policy aware RSVP enabled host is configured to construct and insert AUTH_DATA policy objects into RSVP messages that designate use of a public-key authentication method. When constructing the AUTH_DATA policy element, the host uses the user's private key to generate the digital signature. The host then encapsulates the AUTH_DATA policy object into a RSVP message and sends it to the next hop RSVP system. Once received by the PDP, authentication of the user is accomplished by verifying the digital signature using the user's public key stored in the digital certificate.

4.4. Simple Application Authentication

The application authentication method encodes the application identification such as an executable filename as plain ASCII or UNICODE text.



5. AUTH_DATA Construction at Intermediary PDP Nodes

As described in Section 2, each PDP along the data path constructs a new AUTH_DATA for the next PDP. More specifically, generation of the user AUTH_DATA policy element follows these rules:

1. For unicast RSVP sessions, the user policy locator is copied from the previous hop. For authentication credentials, the PDP uses its own instead of the previous hop's.

2. For multicast messages, the PDP discards data from the previous hop and uses its own policy locator and authentication credentials instead.

For application AUTH_DATA policy elements, the PDP follows these rules:

1. For unicast sessions, the application AUTH_DATA is copied from the previous hop.

2. For multicast messages the application AUTH_DATA is either the first application AUTH_DATA in the message or chosen by the PDP.

6. Message Processing Rules

6.1. Message Generation

A RSVP message is created by a policy aware RSVP host as specified in [RFC 2205] and [POL-EXT] with the following modifications.

1. A RSVP message MAY contain multiple AUTH_DATA policy elements in one or more POLICY_DATA objects.

2. When an AUTH_DATA PE is created, the P-Type field is set to indicate the identity type, e.g. user. The DN is inserted as a POLICY_LOCATOR attribute. Authentication credentials such as a Kerberos ticket or a digital certificate are inserted as a CREDENTIAL attribute.

3. The AUTH_DATA PE is encapsulated into a POLICY_DATA object as described in [POL-EXT]. The INTEGRITY option of a POLICY_DATA object SHOULD be included if protection against corruption and replay attacks is desired [POLICY-MD5].

4. The policy object is inserted into the RSVP message at the appropriate place.

6.2. Message Reception

RSVP messages are processed as specified by [RFC 2205] with the following modifications.

1. If a RSVP system is policy unaware, it MUST ignore any policy data objects it finds in a RSVP message [POL-EXT]. Processing of the RSVP message occurs normally as specified in [RFC 2205] and [POL-EXT].

   If a RSVP system is policy aware, that is, it is also a policy enforcement point (PEP), then it SHOULD send the policy elements from the POLICY_DATA objects to its PDP (or LDP, as appropriate) and wait for a response.

2. Reject the RSVP message if the response from the PDP is negative. Otherwise, continue processing the RSVP message.

6.3. Authentication

1. The PDP retrieves the AUTH_DATA PE from the list of policy elements. Check the P-Type field and return an error if the identity type is unsupported (see Section 7).

2. Verify user credentials. If the authentication method is unsupported, return an error as described in Section 7.

   - For simple authentication, this means validating the user ID or executable name.

   - For the Kerberos method, use the enclosed Kerberos ticket to validate the user.

   - For the public-key method, first, validate the digital certificate that should have been issued by a trusted certificate authority. Then, retrieve the user's public key from the certificate, and verify the digital signature.

7. Error Signaling

If the PDP fails to verify the AUTH_DATA policy element, then it MUST return a policy control failure (Error Code = 02) to the PEP. The error values are described in [RFC 2205] and [POL-EXT]. Furthermore, the PDP SHOULD supply a policy data object containing an AUTH_DATA PE with a POLICY_ERROR_CODE attribute containing more details on the policy control failure (see Section 3.3.4). The PEP will include this policy data object in the outgoing RSVP Error message.

8. IANA Considerations

Following the policies outlined in [IANA-CONSIDERATIONS], Standard RSVP Policy Elements (P-type values) are assigned by IETF Consensus action as described in [POL-EXT].

P-Type AUTH_USER is assigned the value 2. P-Type AUTH_APP is assigned the value 3.

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

A-Type POLICY_LOCATOR is assigned the value 1. A-Type CREDENTIAL is assigned the value 2. A-Type DIGITAL_SIGNATURE is assigned the value 3. A-Type POLICY_ERROR_OBJECT is assigned the value 4.

Following the policies outlined in [IANA-CONSIDERATIONS], POLICY_LOCATOR SubType values in the range 0-127 are allocated through an IETF Consensus action, POLICY_LOCATOR SubType values between 128-255 are reserved for Private Use and are not assigned by IANA.

POLICY_LOCATOR SubType ASCII_DN is assigned the value 1, SubType UNICODE_DN is assigned the value 2, SubType ASCII_DN_ENCRYPT is assigned the value 3 and SubType UNICODE_DN_ENCRYPT is assigned the value 4.

Following the policies outlined in [IANA-CONSIDERATIONS], ErrorValue assignments for the POLICY_ERROR_CODE attribute are assigned by IETF Consensus action.

The ErrorValue ERROR_NO_MORE_INFO is assigned the value 1, UNSUPPORTED_CREDENTIAL_TYPE is assigned the value 2, INSUFFICIENT_PRIVILEGES is assigned the value 3, EXPIRED_CREDENTIAL is assigned the value 4, and the ErrorValue IDENTITY_CHANGED is assigned the value 5.

Following the policies outlined in [IANA-CONSIDERATIONS], CREDENTIAL SubType values in the range 0-127 are allocated through an IETF Consensus action, CREDENTIAL SubType values between 128-255 are reserved for Private Use and are not assigned by IANA.

CREDENTIAL SubType ASCII_ID is assigned the value 1, SubType UNICODE_ID is assigned the value 2, SubType KERBEROS_TKT is assigned the value 3, SubType X509_V3_CERT is assigned the value 4, SubType PGP_CERT is assigned the value 5.

9. Security Considerations

The purpose of this memo is to describe a mechanism to authenticate RSVP requests based on user identity in a secure manner. The INTEGRITY Option of a RSVP POLICY_DATA object can be used to protect the policy object containing user identity information from corruption or replay attacks [POLICY-MD5]. Combining a policy object containing the AUTH_DATA policy element and an INTEGRITY option with an RSVP's INTEGRITY Object can result in a secure admission control mechanism that enforces authentication based on both the identity of the user and the identity of the originating node.

Simple authentication does not contain credentials that can be securely authenticated and is inherently less secured.

The Kerberos authentication mechanism is reasonably well secured.

User authentication using a public-key certificate is known to provide the strongest security.

10. Acknowledgments

We would like to thank Andrew Smith, Bob Lindell and many others for their valuable comments on this memo.

11. References

[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] Hess, R., Ed., and Herzog, S., "RSVP Extensions for Policy Control", work in progress, draft-ietf-rap-new-rsvp-ext-00.txt, June 2001.

[POL-FRAME] Yavatkar, R., Pendarakis, D. and R. Guerin, "A Framework for Policy-based Admission Control RSVP", RFC 2753, January 2000.

[POLICY-MD5] Hess, R., "Cryptographic Authentication for RSVP POLICY_DATA Objects", work in progress, draft-ietf-rap-auth-policy-data-01.txt, July 2001.

[RFC 1510] Kohl, J. and C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

[RFC 1704] Haller, N. and R. Atkinson, "On Internet Authentication", RFC 1704, October 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 2119] Bradner, S., "Key Words for use in RFCs to Indicate Requirement Levels," RFC 2119, March 1997.

[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

12. Author Information

Rodney Hess
Intel, BD1
28 Crosby Drive
Bedford, MA 01730

EMail: rodney.hess@intel.com

Satyendra Yadav
Intel, JF3-206
2111 NE 25th Avenue
Hillsboro, OR 97124

EMail: Satyendra.Yadav@intel.com

Raj Yavatkar
Intel, JF3-206
2111 NE 25th Avenue
Hillsboro, OR 97124

Email: Raj.Yavatkar@intel.com

Ramesh Pabbati
Microsoft
1 Microsoft Way
Redmond, WA 98054

Email: rameshpa@microsoft.com

Peter Ford
Microsoft
1 Microsoft Way
Redmond, WA 98054

Email: peterf@microsoft.com
Tim Moore
Microsoft
1 Microsoft Way
Redmond, WA 98054

Email: timmoore@microsoft.com

Shai Herzog
IPHighway, Inc.
55 New York Avenue
Framingham, MA 01701

Email: herzog@iphighway.com

Appendix A: Revision History

Revision 01

1. Corrected an error in the processing of Kerberos credentials in AUTH_DATA policy objects by the PDP (Section 4.2.1 and Section 6.3).

2. Corrected the length of the ErrorValue field for a POLICY_ERROR_OBJECT attribute (Section 3.3.4).

3. Specified the IANA considerations for ErrorValue in Section 3.3.4 and Section 9.

4. Expanded Section 2, Introduction.

5. Rewrote the text for Section 5 to better follow Section 2.

6. Updated Step 3 in Section 6.1 to correctly reflect how security issues are addressed.

Revision 00

1. Updated the Security Considerations Section to correctly reflect how various security issues are addressed.

Full Copyright Statement

Acknowledgement

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