Y.Bernet, Microsoft
R. Pabbati, Microsoft

Internet Draft October, 1999
Document: draft-ietf-rap-rsvp-appid-00.txt expires April, 2000

Application and Sub Application Identity Policy Element for Use with RSVP

Status of this Memo

1. Abstract

RSVP [RFC 2205] signaling messages typically include policy data objects, which in turn contain policy elements. Policy elements may describe user and/or application information, which may be used by RSVP aware network elements to apply appropriate policy decisions to a traffic flow. This informational draft details the usage of policy elements that provide application information.

2. Overview

RSVP aware network elements may act as policy enforcement points (PEPs). These work together with policy decision points (PDPs) to

enforce QoS policy. Briefly, PEPs extract policy information from RSVP signaling requests and compare the information against information stored in a policy database or directory. A policy decision is made based on the results of the comparison.

One type of policy information describes the application on behalf of which an RSVP signaling request is generated. When application policy information is available, network administrators are able to manage QoS based on application type. So for example, a network administrator may establish a policy that prioritizes known mission critical applications over games.

We propose a hierarchical structure for application policy elements. Specifically, the highest level of the hierarchy specifies an application name. The next level specifies a version. At the next level, an arbitrary number of sub-applications may be specified. An example of a sub-application is 'print data'.

In this draft, we show the structure of the application policy element. We also propose keywords for the various levels of the hierarchy. However, we do not enumerate values for applications, version numbers or sub-applications. Such an enumeration is beyond the scope of this draft.

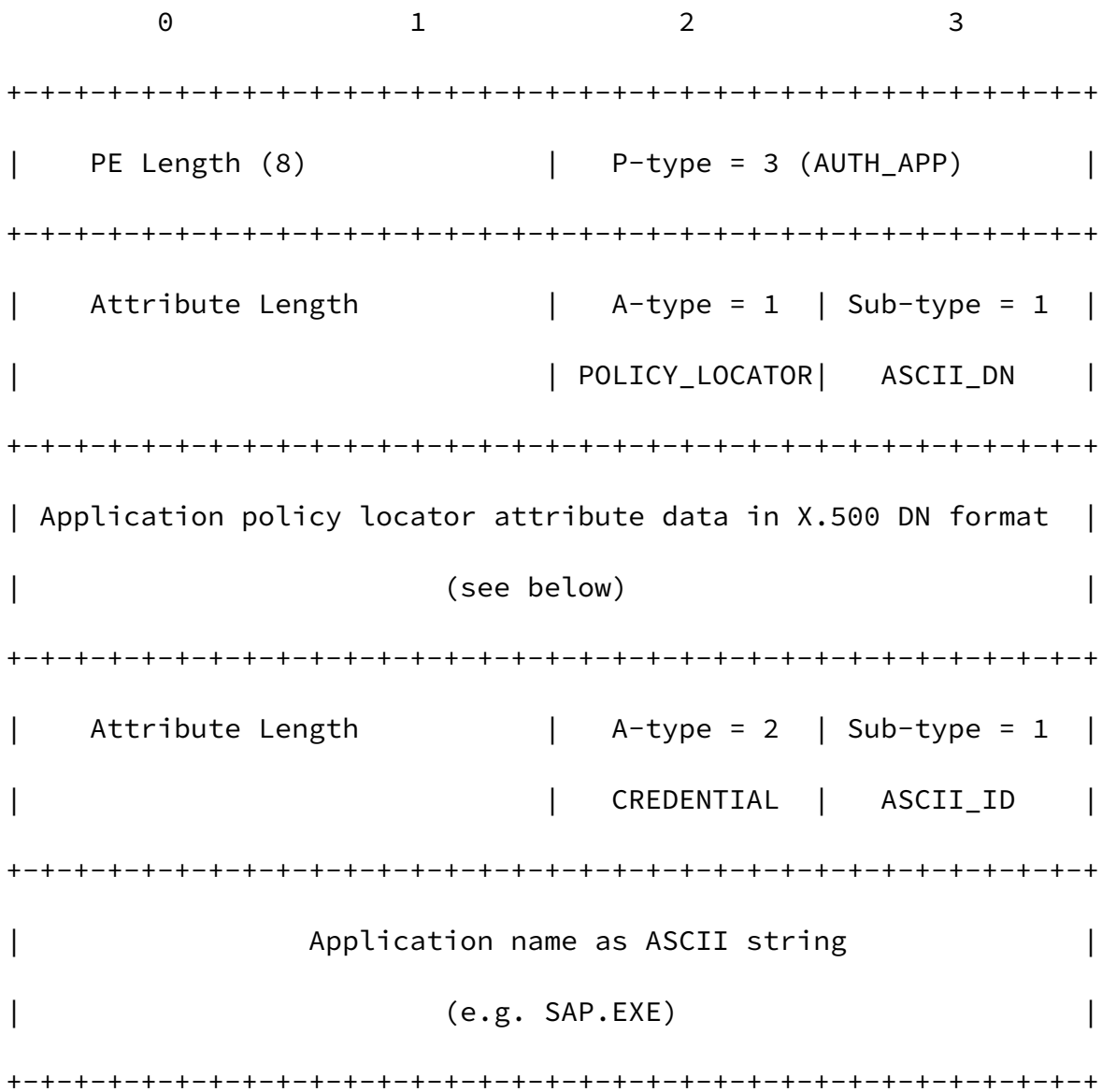
3. Application Policy Element Structure

General application policy elements are defined in [identity]. These are policy elements with a P-type of AUTH_APP (value 3). Following the policy element header is a list of authentication attributes.

The first authentication attribute should be of the A-type POLICY_LOCATOR (value 1). The sub-type of the POLICY_LOCATOR attribute should be of type ASCII_DN (value 1) [RFC 1779]. The actual attribute data is formatted as an X.500 distinguished name (DN), representing the application, version number and sub-application.

The second authentication attribute should be of the A-type CREDENTIAL (value 2). The sub-type of the CREDENTIAL attribute is of type ASCII_ID. The actual attribute data is an ASCII string representing the application name.

This structure is illustrated in the following diagram:


0 1 2 3
PE Length (8)
P-type = 3 (AUTH_APP)
Attribute Length
A-type = 1
POLICY_LOCATOR
Sub-type = 1
ASCII_DN
Application policy locator attribute data in X.500 DN format
(see below)
Attribute Length
A-type = 2
CREDENTIAL
Sub-type = 1
ASCII_ID
Application name as ASCII string
(e.g. SAP.EXE)

The policy locator attribute for an application policy element is conformant with the X.500 DN format[RFC 1779]. We propose the following keywords:

Key	Attribute
APP	Application Name
VER	Application Version Number
SAPP	Sub Application

The following is an example of a conformant policy locator:

APP=SAP, VER=1.1, SAPP=Print

4. Security Considerations

The proposed simple policy element does not guarantee that element is indeed associated with the application it claims to be associated with. In order to provide such guarantees, it is necessary to sign applications. Signed application policy elements may be proposed at a future date. Note that typically, the application policy element will be included in an RSVP message with an encrypted and authenticated user policy element. A level of security is provided by trusting the application policy element only if the user policy element is trusted.

All RSVP integrity considerations apply to the message containing the application policy element.

5. References

[RFC2205] Braden, B., et al., "Resource Reservation Protocol (RSVP) - Version 1 Functional Specification", RFC 2205, September 1997.

[RFC-1779], Kille, S., A String Representation of Distinguished Names, March 1995

[identity] Yadav, S., Yavatkar, R., Pabbati, R., Ford, P., Moore, T., Herzog, S., "Identity Representation for RSVP", Internet Draft, February 1999.

6. Acknowledgments

Thanks to Tim Moore and Shai Mohaban for their input.

7. Author's Addresses

Bernet, Yoram
Microsoft
One Microsoft Way,
Redmond, WA 98052
Phone: (425) 936-9568
Email: yoramb@microsoft.com

Pabbati, Ramesh
One Microsoft Way,
Redmond, WA 98052
Email: rameshpa@microsoft.co

This draft expires April, 2000