Network Working Group
Request for Comments: 2872
Category: Standards Track

Y. Bernet
R. Pabbati
Microsoft

June 2000

Application and Sub Application Identity Policy Element for Use with RSVP

Status of this Memo

Copyright Notice

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 [RFC2119].

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 memo details the usage of policy elements that provide application information.

1. 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 by a PDP in a (possibly remotely located) 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.

This memo describes a structure for a policy element that can be used to identify application traffic flows. The policy element includes a number of attributes, one of which is a policy locator. This policy locator includes the following hierarchically ordered sub-elements (in descending levels of hierarchy):

1. identifier that uniquely identifies the application vendor
2. identifier of the application
3. version number of the application
4. sub-application identifier

An arbitrary number of sub-application identifiers may be included in the policy locator. An example of such an identifier is 'print transaction'.

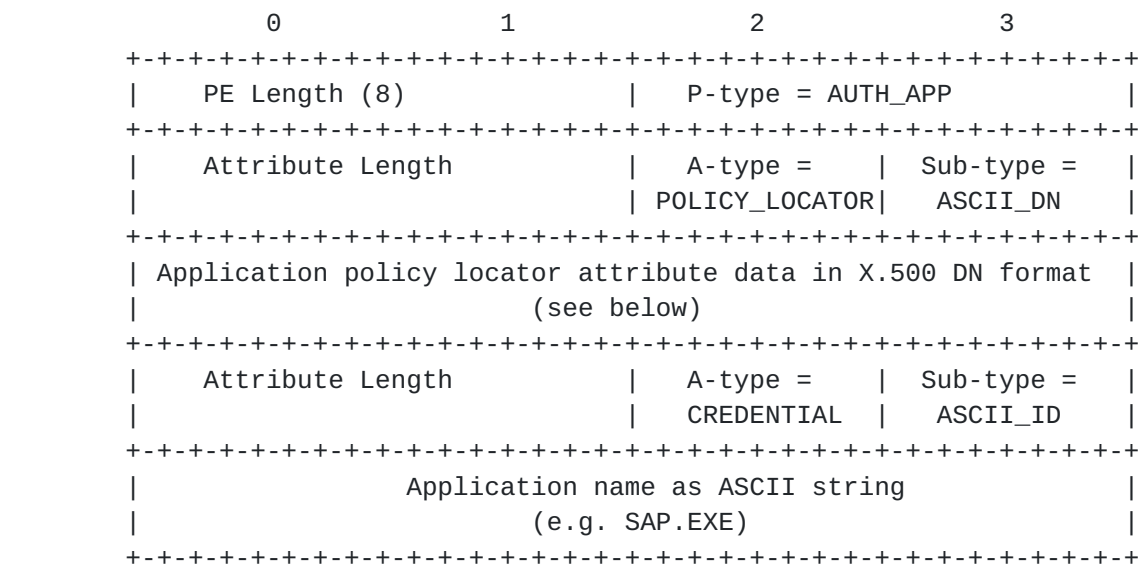
This memo specifies the structure of the application policy element and proposes keywords for the sub-elements at each level of the hierarchy. It does not enumerate specific values for the sub-elements: such an enumeration is beyond the scope of this memo.

2. Simple Application Identity Policy Element Structure

General application identity policy elements are defined in [RFC2752]. These are policy elements with a P-type of AUTH_APP. Following the policy element header is a list of authentication attributes.

The first authentication attribute is of the A-type POLICY_LOCATOR. The sub-type of the POLICY_LOCATOR attribute is of type ASCII_DN [RFC1779] or UNICODE_DN. The actual attribute data is formatted as an X.500 distinguished name (DN), representing a globally unique identifier, the application, version number and sub-application in a hierarchical structure. The POLICY_LOCATOR attribute contains keywords as described in section 2. For further details on the format of the POLICY_LOCATOR attribute, see [RFC2752].

The second authentication attribute is of the A-type CREDENTIAL. The sub-type of the CREDENTIAL attribute is of type ASCII_ID or UNICODE_ID. The actual attribute data is an ASCII or Unicode string representing the application name. This structure is illustrated in the following diagram:



The following keywords are recommended although others MAY be used:

Key	Attribute
GUID	Globally Unique Identifier (optional)
APP	Application Name
VER	Application Version Number
SAPP	Sub Application (optional)

The following are examples of conformant policy locators:

"APP=SAP, VER=1.1, SAPP=Print"

"GUID=http://www.microsoft.com/apps, APP=MyApplication, VER=1.2.3"

The APP, VER and SAPP attributes SHOULD describe the application to a human reader in as unique and unambiguous a way as possible. The GUID attribute MAY be used when absolute uniqueness of application identification is required and its contents MUST be an identifier from a globally-unique source (e.g. domain names as assigned by the corresponding registration authorities). Note that publication of the chosen identifiers in a suitable format is strongly encouraged.

3. 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.

4. References

[RFC2205] Braden, R., Zhang, L., Berson, L., Herzog, S. and S. Jamin, "Resource Reservation Protocol (RSVP) - Version 1 Functional Specification", RFC 2205, September 1997.

[RFC1779] Kille, S., "A String Representation of Distinguished Names", RFC 1779, March 1995.

[RFC2752] Yadav, S., Yavatkar, R., Pabbati, R,. Ford, P., Moore, T. and S. Herzog, "Identity Representation for RSVP", RFC 2752, January 2000.

[ASCII] Coded Character Set -- 7-Bit American Standard Code for Information Interchange, ANSI X3.4-1986.

[UNICODE] The Unicode Consortium, "The Unicode Standard, Version 2.0", Addison-Wesley, Reading, MA, 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

5. Acknowledgments

Thanks to Tim Moore, Shai Mohaban, Andrew Smith, Ulrich Homann and other contributors to the IETF's RAP WG for their input.

6. Authors' Addresses

Yoram Bernet
Microsoft
One Microsoft Way
Redmond, WA 98052

Phone: (425) 936-9568
EMail: yoramb@microsoft.com

Ramesh Pabbati
One Microsoft Way
Redmond, WA 98052

EMail: rameshpa@microsoft.com

7. Full Copyright Statement

Acknowledgement

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