

Network Working Group
Internet Draft
Intended status: Informational
Expires: November 2010

J. Howlett
JANET(UK)
May 25, 2010

**A RADIUS attribute for SAML constructs
draft-howlett-radius-saml-attr-00.txt**

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

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 November 25, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Abstract

This document defines the SAML-Construct attribute using the Remote Authentication Dial In User Service (RADIUS). This attribute is used for encapsulating Security Assertion Mark-up Language (SAML) constructs.

Table of Contents

1. Introduction.....	2
2. Conventions used in this document.....	2
3. SAML-Construct Attribute.....	2
4. Security Considerations.....	3
5. IANA Considerations.....	3
6. References.....	5
6.1. Normative References.....	5
6.2. Informative References.....	5
7. Acknowledgments.....	5

[1. Introduction](#)

This document defines the SAML-Construct attribute for the Remote Authentication Dial In User Service (RADIUS). This attribute encapsulates Security Assertion Mark-up Language (SAML) constructs.

[2. 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](#) [[RFC2119](#)].

[3. SAML-Construct Attribute](#)

This attribute contains a SAML [[Core](#)] construct. This attribute MAY be used with any AAA protocol that makes use of RADIUS attributes, such as RADIUS [[RFC2865](#)] or DIAMETER [[RFC3588](#)].

Where multiple SAML-Construct attributes are included in an AAA protocol message (for example, a RADIUS packet), the Construct field of the attributes are to be concatenated to form a SAML construct.

A summary of the SAML-Construct format is shown below. The fields are transmitted from left to right.


```

      0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Type      |      Length      |      MT      |      Construct...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Type

TBD

Length

>=4

Construct Type (CT)

The Construct Type field is a one octet enumerated field. It takes an integer value denoting the type of SAML construct in the Construct field.

TBD SAML Request protocol element

TBD SAML Response protocol element

All other values are reserved for IANA allocation subject to the provisions of [section 5](#).

Construct

The Construct field is one or more octets. It contains a SAML construct (for example, as defined in [SAMLCore]). If larger than a single attribute, the SAML construct data MUST be split on 253-octet boundaries over as many attributes as necessary. On reception, the SAML construct is reconstructed by concatenating the contents of all SAML-Construct attributes.

[4. Security Considerations](#)

TODO

[5. IANA Considerations](#)

The following numbers have been assigned in the RADIUS Attribute Types registry.

A new RADIUS Attribute Type: SAML-Construct (TDB)

The enumerated values of the newly registered RADIUS Attribute Type as defined in this document were assigned at the same time as the new Attribute Type.

For the SAML-Construct Attribute:

TBD SAML Request protocol element

TBD SAML Response protocol element

Assignments of additional enumerated values for the RADIUS attributes defined in this document are to be processed as described in [[RFC3575](#)], subject to the additional requirements of a published specification.

6. References

6.1. Normative References

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

6.2. Informative References

[Core] Cantor, S., Kemp, J., Philpott, R., and E. Maler, "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard saml-core-2.0-os, March 2005.

[RFC2865] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), June 2000.

[RFC3575] Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)", [RFC 3575](#), July 2003.

[RFC3588] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol", [RFC 3588](#), September 2003.

7. Acknowledgments

TODO

Copyright (c) 2010 IETF Trust and the persons identified as authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted pursuant to, and subject to the license terms contained in, the Simplified BSD License set forth in [Section 4.c](#) of the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>).

Authors' Addresses

Josh Howlett
JANET(UK)

Email: josh.howlett@ja.net