

Internet Engineering Task Force	K. Hazelton, Ed.
Internet-Draft	University of Wisconsin-Madison
Intended status: Informational	September 20, 2017
Expires: March 24, 2018	

Scratchpad Version SAML vocabulary extension for OTTO

otto-saml-1.0

Abstract

This specification describes a method for packaging information about SAML-based federations, and establishing mechanisms for its validation. It includes term definitions which appear in the current JSON-LD context for the OTTO 1.0 specification.

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on March 24, 2018.

Copyright Notice

Copyright (c) 2017 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 (<https://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.

Table of Contents

1. [Introduction](#)
2. [Requirements Language](#)
3. [Notational Conventions](#)
4. [OTTO SAML Vocabulary Extension](#)
 - 4.1. [SAML Entity](#)
 - 4.2. [SAML SSO Endpoint](#)
 - 4.3. [SAML SSO Extensions](#)
 - 4.4. [SAML Service Provider Endpoint](#)
 - 4.5. [SAML Identity Provider Endpoint](#)
5. [Acknowledgements](#)
6. [IANA Considerations](#)
7. [Security Considerations](#)
8. [References](#)
 - 8.1. [Normative References](#)
 - 8.2. [Informative References](#)
- [Author's Address](#)

1. Introduction

The Open Trust Taxonomy for Federation Operators ("OTTO") defines an extension mechanism to allow the community to add functionality in a community compatible way. This specification was developed to enable OTTO federations to support SAML-based identity services, and defines all the terms used in the JSON-LD context file which the extension covers.

2. Requirements Language

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](#).

3. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\]](#).

Unless otherwise noted, all protocol properties and values are case sensitive.

4. OTTO SAML Vocabulary Extension

4.1. SAML Entity

Property	Expected Type	Description
Entity	Otto:Entity	Elements that are common to both SAML Entities and Otto Entities
Refeds Entity Category	URI	URI identifier for a formal Refeds Entity Category (e.g., Research and Scholarship)
SSO Endpoint	SAML SSO Endpoint	The characteristics of this endpoint as a party to Single Sign-On

SAML Entity

4.2. SAML SSO Endpoint

Property	Expected Type	Description
Keys	Key Descriptor element or array of Key Descriptor elements as defined in [SAML:Metadata]	Public Keys for use in signing and encryption
Extensions	SAML Metadata Extensions or array of Extensions	Extensions to the basic SAML Metadata Schema

SAML SSO Endpoint

4.3. SAML SSO Extensions

Property	Expected Type	Description
UI metadata	SAML UI Metadata	descriptive information about the SSO User Interface

SAML SSO Extension

4.4. SAML Service Provider Endpoint

Property	Expected Type	Description
SAML SSO Endpoint	SAML SSO Endpoint	SSO Endpoint elements shared by both IdPs and SPs
SP SSO Descriptor	SP SSO Descriptor	elements unique to the SAML SP entity
Discovery Responses	DiscoveryResponse or array of DiscoveryResponses	URL(s) of the SSO Endpoints associated with this SAML Entity
Assertion Consumers	Assertion Consumer element or array of Assertion Consumer elements as defined in [SAML:Metadata]	URLs and type of endpoint that will be consuming attributes
Attribute Consumer	Attribute Consumer element as defined in [SAML:Metadata]	Name and descriptive label for the service that will be consuming attributes
Requested Attributes	List of attributes as defined in [SAML:Metadata]	Friendly name and name format of requested attributes

SAML Service Provider Endpoint

4.5. SAML Identity Provider Endpoint

Property	Expected Type	Description
SAML SSO Endpoint	SAML SSO Endpoint	SSO Endpoint elements shared by both IdPs and SPs
Single Sign-on Service	SAML SSO Service Element	SSO Service elements specific to SAML Identity Providers
More TBD

SAML Identity Provider Endpoint

5. Acknowledgements

TBD

6. IANA Considerations

This memo includes no request to IANA.

7. Security Considerations

TBD

8. References

8.1. Normative References

[RFC2119] Bradner, S., "[Key words for use in RFCs to Indicate Requirement Levels](#)", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.

8.2. Informative References

[RFC6749] Hardt, D., "[The OAuth 2.0 Authorization Framework](#)", RFC 6749, DOI 10.17487/RFC6749, October 2012.

Author's Address

Keith Hazelton (editor)
University of Wisconsin-Madison
1210 W Dayton St.
Madison, Wisconsin 53706
US
Phone: +1 608 262 0771
Email: hazelton@wisc.edu