Document	Group Representative Information Exchange
Identifier	https://wiki.federationer.internetstiftelsen.se/x/BICFAg
Version	V1.0.0
Last modified	2023-08-21
Pages	6
Status	Draft
License	Creative Commons BY-SA 3.0

Group Representative Information Exchange

Stefan Halén

Abstract

This document defines an approach for representing and exchanging information about group representatives and their associated Security Assertion Markup Language (SAML) entities. This document introduces a comprehensive JSON schema that guides the inclusion of essential attributes and facilitating metadata security through JSON Web Signature (JWS). Additionally, the specification introduces the concept of extracting URLs from the AdditionalMetadataLocation element within SAML metadata, allowing for enhanced metadata sharing and representation.

Contents

1 Introduction

This document aims to establish a standardized mechanism for extracting a URL from the AdditionalMetadataLocation element within Security Assertion Markup Language (SAML) metadata. The AdditionalMetadataLocation element serves as a means to include supplementary metadata, enhancing the comprehension and interoperability of the involved entities within a federation.

The URL, obtained using the AdditionalMetadataLocation function, points to a JSON Web Signature (JWS) [1] adhering to the guidelines outlined in this . The JWS serves the purpose of disclosing the organizations represented by a group representative. Essentially, an entity within SAML metadata, owned by a group representative, references a JSON structure through a URL provided by the AdditionalMetadataLocation element. This structure details all organizations under representation.

By enabling the extraction and utilization of information from the AdditionalMetadataLocation element, this document enhances the overall utility and flexibility of SAML metadata, allowing for a more comprehensive representation of group representatives and their associated entities.

2 Terminology and Typographical Conventions

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 [2]

Text in Italics is non-normative. All other text is normative unless otherwise stated.

2.1 Definition of terminology

Group Representative: An authorized entity acting on behalf of a group or organization.

SAML Entity: An entity participating in the Security Assertion Markup Language (SAML) framework.

Constituents: The organizations or members represented by the group representative within the SAML metadata.

3 Metadata Claims

This section defines the set of claims that can be included in the metadata.

version: (REQUIRED) Schema version follows semantic versioning (https://semver.org)

cache_ttl: (REQUIRED) How long (in seconds) to cache metadata.

iat: (REQUIRED) Identifies the time on which the signature was issued. Its value MUST be a number containing a NumericDate value.

exp: (REQUIRED) Identifies the expiration time on and after which the signature and federation metadata are no longer valid. The expiration time of the federation metadata MUST be set to the value of exp. Its value MUST be a number containing a NumericDate value.

iss: (REQUIRED) URI that identifies the publisher of the metadata.

entities: (REQUIRED) List of entities (see Entities)

3.1 Entities

Each entity in the entities list consists of:

entity_id: (REQUIRED) The URI identifying the corresponding SAML entity. The entity is owned by the group representative and functions as the hub for its relationship with associated constituents and organizational representation.

Example: “https://idp1.example.com”

constituents: (REQUIRED) List of constituents (see Constituents)

3.2 Constituents

organization_id: (REQUIRED) Unique identifier of the organization represented by the group representative.

Example: “SE1122334455”

organization_name: (REQUIRED) Name of the organization represented by the group representative.

Example: “Example Org”

3.3 Metadata Example

```
{
    "iss": "https://my-domain.example.com",
    "exp": 1693056343,
    "iat": 1692192343,
    "version": "1.0.0",
    "cache_ttl": 3600,
    "entities": [{
        "entity_id": "https://idp1.example.com",
        "constituents": [{
            "organization_id": "SE1122334455",
            "organization_name": "Example Org One"
        }, {
            "organization_id": "SE6677889900",
            "organization_name": "Example Org Two"
        }]
    }]
}
```

4 Metadata Signing

The metadata is signed using JSON Web Signature (JWS) and published using JWS JSON Serialization. It is RECOMMENDED that metadata signatures are created with algorithm ECDSA using P-256 and SHA-256 (“ES256”) as defined in [3].

4.1 Signature Protected Headers

alg: (REQUIRED) Identifies the algorithm used to generate the JWS signature [@!RFC7515], section 4.1.1.

x5t#S256: (REQUIRED) The x5t#S256 claim is utilized to identify the signing key used for signing the JWS. The value MUST correspond to the fingerprint of a key found in the SAML metadata of the entity.

4.2 Header Example

The following is a non-normative example of a header statement

```
{
    "alg": "ES256",
    "x5t#S256": "3z1Tl22dleJP-nLX-8bKN1x6duPmP1IaEhgtPnq8TP4"
}
```

5 JSON Schema

The metadata JSON schema (in YAML format) Version: 1.0.0

```
---
# JSON Schema for Group Representative Entities
# Version: 1.0.0

$schema: "http://json-schema.org/draft-07/schema#"
title: "Group Representative Information Exchange"
type: object
additionalProperties: true
properties:
  iss:
    title: "Issuer"
    type: string
    format: uri
    description: "An URI that identifies the issuer of the data."
    example: "https://my-domain.example.com"
  exp:
    title: "Expiration Time"
    type: integer
    pattern: "^\\d{10}$"
    description: "The expiration timestamp of the data in NumerDate format."
    example: 1693056343
  iat:
    title: "Issued Time"
    type: integer
    pattern: "^\\d{10}$"
    description: >
      "The timestamp indicating when the data was issued in NumericDate format."
    example: 1692192343
  version:
    title: "Version"
    type: string
    pattern: "^\\d+\\.\\d+\\.\\d+$"
    description: "The version of the data, following semantic versioning."
    example: "1.0.0"
  cache_ttl:
    title: "Cache TTL"
    type: integer
    description: "The time-to-live (TTL) duration for caching the data in seconds."
    example: 3600
  entities:
    title: "Entities"
    type: array
    description: "An array of entities represented by the group representative."
    items:
      type: object
      properties:
        entity_id:
          title: "Entity ID"
          type: string
          format: uri
          description: "The unique identifier of the entity."
          example: "https://idp1.example.com"
        constituents:
          title: "Constituents"
          type: array
          description: "An array of constituents associated with the entity."
          items:
            type: object
            properties:
              organization_id:
                title: "Organization ID"
                type: string
                pattern: ^[A-Z]{2}\d{10}$
                description: >
                  "The unique identifier of the organization represented by
                  the Group Representative."
                example: "SE1122334455"
              organization_name:
                title: "Organization Name"
                type: string
                description: >
                  "The name of the organization represented by the Group
                  Representative."
                example: "Example Org"
            required: ["organization_id", "organization_name"]
      required: ["entity_id", "constituents"]
required: ["iss", "exp", "iat", "version", "cache_ttl", "entities"]
```

6 References

[1] M.B. Jones, J. Bradley, N. Sakimura, JSON Web Signature (JWS), RFC 7515; RFC Editor, 2015. https://doi.org/10.17487/RFC7515.

[2] S. Bradner, Key words for use in RFCs to indicate requirement levels, RFC Editor; Internet Requests for Comments; RFC Editor, 1997. http://www.rfc-editor.org/rfc/rfc2119.txt.

[3] M.B. Jones, JSON Web Algorithms (JWA), RFC 7518; RFC Editor, 2015. https://doi.org/10.17487/RFC7518.