OAuth Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 10, 2017

C. Smith
T. Hardjono
MIT

February 6, 2017

JSON Web Document (JWD)
draft-smith-oauth-json-web-document-00

Abstract

JSON Web Document (JWD) is a means of representing optionally signed and/or encrypted JSON content suitable for storage, retrieval, transmission, and display in a graphical user interface. The content of a JWD is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure.

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 [RFC2119].

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 http://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 August 10, 2017.

Copyright Notice

Table of Contents

1. Introduction

JWD introduces a new set of serializations to JWS and JWE called the Document Serializations. These serializations follow the form of the JSON Serialization and Flattened JSON Serialization described in JWS Section 7.2 [1], except that the payload, integrity-protected header, and non-integrity-protected header contents are all represented as unencoded JSON values and MUST NOT be base64url-encoded.

Signatures present in the data structure MUST be base64url-encoded. Signatures are computed using base64url-encoded JSON values for the payload and integrity-protected headers as in JWS. For a given payload and JOSE Header, the signature(s) of a JWD MUST be identical to signatures computed for semantically equivalent JWT serializations.

2. Terminology

This specification uses terms defined in the JSON Web Token [JWT], JSON Web Signature [JWS], and JSON Web Encryption [JWE] specifications.

These terms are defined by this specification:

JSON Web Document (JWD)

A data structure representing a digitally signed, MACed, or encrypted JSON document.

JWS Document Serialization

A representation of the JWD as a JSON document. Unlike the JWS JSON Serialization, the JWS Document Serialization represents the JWS Payload and integrity-protected JOSE Header parameters as unencoded JSON values. This representation simplifies storage and retrieval of signed content with document stores and search engines, as well as display in applications.

3. JWS Document Serialization

```
{
  "payload": <payload contents>,
  "signatures": [
    {
      "protected": <integrity-protected header 1 contents>,
      "header": <non-integrity-protected header 1 contents>,
      "signature": "<signature 1 contents>"
    },
    ...
    {
      "protected": <integrity-protected header N contents>,
      "header": <non-integrity-protected header N contents>,
      "signature": "<signature N contents>"
    }
  ]
}
```

Figure 1

4. JWS Flattened Document Serialization

```
{
    "payload": <payload contents>,
    "protected": <integrity-protected header contents>,
    "header": <non-integrity-protected header contents>,
    "signature": "<signature contents>"
}
```

Figure 2

5. IANA Considerations

TBD

6. Security Considerations

TBD

7. Acknowledgements

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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <http://www.rfc-editor.org/info/rfc7515>.

[RFC7516] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015, <http://www.rfc-editor.org/info/rfc7516>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <http://www.rfc-editor.org/info/rfc7519>.

8.2. URIs

[1] https://tools.ietf.org/html/rfc7515#section-7.2

Appendix A. Example Signed JWD

```
{
  "protected": {
    "alg": "ES512",
    "jku": "https://example.com/jwks"
  },
  "payload": {
    "a": "Please don't BASE64URL encode me!",
    "b": "I need to be indexed!",
    "c": "I need to be rendered!"
  },
  "signature": ""
}
```

Figure 3

Authors' Addresses

Christian Smith
MIT

Email: csmth@mit.edu

Thomas Hardjono
MIT

Email: hardjono@mit.edu