Abstract

The JSON Web Signature JSON Serialization (JWS-JS) is a means of representing content secured with digital signatures or Message Authentication Codes (MACs) using JavaScript Object Notation (JSON) data structures. This specification describes a means of representing secured content as a JSON data object (as opposed to the JWS specification, which uses a compact serialization with a URL-safe representation). It enables multiple digital signatures and/or MACs to be applied to the same content (unlike JWS). Cryptographic algorithms and identifiers used with this specification are described in the separate JSON Web Algorithms (JWA) specification. The JSON Serialization for related encryption functionality is described in the separate JSON Web Encryption JSON Serialization (JWE-JS) 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 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 April 18, 2013.

Copyright Notice

Copyright (c) 2012 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.

Table of Contents

1. Introduction
   1.1. Notational Conventions
2. Terminology
3. JSON Serialization
4. Example JWS-JS
5. IANA Considerations
1. Introduction

The JSON Web Signature JSON Serialization (JWS-JS) is a format for representing content secured with digital signatures or Message Authentication Codes (MACs) as a JavaScript Object Notation (JSON) object. It enables multiple digital signatures and/or MACs to be applied to the same content (unlike JWS [JWS]). The digital signature and MAC mechanisms used are independent of the type of content being secured, allowing arbitrary content to be secured. Cryptographic algorithms and identifiers used with this specification are described in the separate JSON Web Algorithms (JWA) [JWA] specification. The JSON Serialization for related encryption functionality is described in the separate JSON Web Encryption JSON Serialization (JWE-JS) [JWE-JS] specification.

1.1. Notational 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 Key words for use in RFCs to Indicate Requirement Levels [RFC2119].

2. Terminology

This specification uses the same terminology as the JSON Web Signature (JWS) [JWS] specification.

3. JSON Serialization

The JSON Serialization represents secured content as a JSON object with a recipients member containing an array of per-recipient information and a payload member containing a shared Encoded JWS Payload value. Each member of the recipients array is a JSON object with a header member containing an Encoded JWS Header value and a signature member containing an Encoded JWS Signature value.

Unlike the compact serialization used by JWSs, content using the JSON Serialization MAY be secured with more than one digital signature and/or MAC value. Each is represented as an Encoded JWS Signature value in the signature member of an object in the recipients array. For each, there is an Encoded JWS Encoded Header value in the header member of the same object in the recipients array. This specifies the digital signature or MAC applied to the Encoded JWS Header value and the shared Encoded JWS Payload value to create the JWS Signature value. Therefore, the syntax is:

```json
{"recipients": [
    {"header": "<header 1 contents>",
     "signature": "<signature 1 contents>"},
    ...
    {"header": "<header N contents>",
     "signature": "<signature N contents>"}],
```
The contents of the Encoded JWS Header, Encoded JWS Payload, and Encoded JWS Signature values are exactly as specified in JSON Web Signature (JWS) [JWS]. They are interpreted and validated in the same manner, with each corresponding header and signature value being created and validated together.

Each JWS Signature value is computed on the JWS Secured Input corresponding to the concatenation of the Encoded JWS Header, a period (\(\cdot\)) character, and the Encoded JWS Payload in the same manner described in the JWS specification. This has the desirable result that each Encoded JWS signature value in the recipients array is identical to the value that would be used for the same parameters in a JWS.

### 4. Example JWS-JS

This section contains an example using the JWS JSON Serialization. This example demonstrates the capability for conveying multiple digital signatures and/or MACs for the same payload.

The Encoded JWS Payload used in this example is the same as used in the examples in Appendix A of JWS (with line breaks for display purposes only):

```
eyjpc3Mi0iJqb2UjLA0KICJ1eHAi0jEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFt
CGxlLmNvbS9pc19yb290Ijpo0cnVlFQ
```

Two digital signatures are used in this example: an RSA SHA-256 signature, for which the header and signature values are the same as in Appendix A.2 of JWS, and an ECDSA P-256 SHA-256 signature, for which the header and signature values are the same as in Appendix A.3 of JWS. The two Decoded JWS Header Segments used are:

```
{"alg":"RS256"}
```

and:

```
{"alg":"ES256"}
```

Since the computations of the JWS Header and JWS Signature values are the same as in Appendix A.2 and Appendix A.3 of JWS, they are not repeated here.

The complete JSON Web Signature JSON Serialization (JWS-JS) for these values is as follows (with line breaks for display purposes only):

```
{"recipients":[
    {
      "header":"eyJhbGciOiJhI0IJSUzI1NiJ9",
      "signature":
        "c4hiUpo9Eetdgtv3hF80EgruB__dzERat0XF9g2VtQgr9PJbu3X0iZj5RZ
        mh7AuHIv48h-QQc_lF5YKt08W2Fp5jujGbs9uJdBF9CUAr71dnZcAcqjb
        KBYN4BAynRFdiuB--f_nZLgrnbyTyw075vRlK5h6xBArLIARNPvksJtqBMH1
        b1L07qeK0GarZRMb_eSN9383LcoL6n_d0--xi12jzDwusC-eOKHESqtFZES
c6bf7I0noQPPyhJ1phCnW6ieY2w9Q0YEuiUT18np6LbgGY9Fs989rVt5AX
        LIHwKwlywVMtVrBp9igcN_10ypG1UPQGe77Rw",
    },
    {
      "header":"eyJhbGciOiJhI0IJSUzI1NiJ9",
      "signature":
        "DteHut1jbEg8L38VAFuAoyKAM6-xx-F4GawxaepmXFCgTjDxw5djxLa8IS
        1SApmWQxfKTUjqPPP-Kg6NU0Q"
    }
],
"payload":
```

5. IANA Considerations

This specification makes no requests of IANA.

6. Security Considerations

The security considerations for this specification are the same as those for the JSON Web Signature (JWS) [JWS] specification.

7. References

7.1. Normative References


7.2. Informative References


Appendix A. Acknowledgements

JSON serializations for secured content were previously explored by Magic Signatures [MagicSignatures] and JSON Simple Sign [JSS].

Appendix B. Open Issues

[[ to be removed by the RFC editor before publication as an RFC ]]

The following items remain to be considered or done in this draft:

- Track changes that occur in the JWS spec.

Appendix C. Document History

[[ to be removed by the RFC editor before publication as an RFC ]]
• Changed to use an array of structures for per-recipient values, rather than a set of parallel arrays.

• Generalized language to refer to Message Authentication Codes (MACs) rather than Hash-based Message Authentication Codes (HMACs).

• Renamed draft-jones-json-web-signature-json-serialization to draft-jones-jose-jws-json-serialization to have "jose" be in the document name so it can be included in the Related Documents list at http://datatracker.ietf.org/wg/jose/. No normative changes.

draft-jones-json-web-signature-json-serialization-02
• Tracked editorial changes made to the JWS spec.

draft-jones-json-web-signature-json-serialization-01
• Corrected the Magic Signatures reference.

draft-jones-json-web-signature-json-serialization-00
• Created the initial version incorporating JOSE working group input and drawing from the JSON Serialization previously proposed in draft-jones-json-web-token-01.

Authors’ Addresses

Michael B. Jones
Microsoft
Email: mbj@microsoft.com
URI: http://self-issued.info/

John Bradley
independent
Email: ve7ith@ve7ith.com

Nat Sakimura
Nomura Research Institute
Email: n-sakimura@nri.co.jp