Abstract

JSON Web Signature (JWS) represents content secured with digital signatures or Message Authentication Codes (MACs) using JavaScript Object Notation (JSON) based data structures. Cryptographic algorithms and identifiers for use with this specification are described in the separate JSON Web Algorithms (JWA) specification and an IANA registry defined by that specification. Related encryption capabilities are described in the separate JSON Web Encryption (JWE) 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 December 22, 2014.

Copyright Notice

Copyright (c) 2014 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.
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 .............................................. 4
   1.1. Notational Conventions .............................. 4
2. Terminology ............................................... 5
3. JSON Web Signature (JWS) Overview ....................... 6
   3.1. Example JWS ......................................... 8
4. JWS Header ................................................ 9
   4.1. Registered Header Parameter Names .................. 9
   4.1.1. "alg" (Algorithm) Header Parameter ............... 10
   4.1.2. "jku" (JWK Set URL) Header Parameter .......... 10
   4.1.3. "jwk" (JSON Web Key) Header Parameter ........... 10
   4.1.4. "kid" (Key ID) Header Parameter ................ 10
   4.1.5. "x5u" (X.509 URL) Header Parameter ............. 11
   4.1.6. "x5c" (X.509 Certificate Chain) Header Parameter . 11
   4.1.7. "x5t" (X.509 Certificate SHA-1 Thumbprint) Header Parameter .................. 11
   4.1.8. "x5t#S256" (X.509 Certificate SHA-256 Thumbprint) Header Parameter .......... 11
   4.1.9. "typ" (Type) Header Parameter ................... 12
   4.1.10. "cty" (Content Type) Header Parameter .......... 12
   4.1.11. "crit" (Critical) Header Parameter ............. 13
   4.2. Public Header Parameter Names ..................... 14
   4.3. Private Header Parameter Names .................... 14
5. Producing and Consuming JWSs .......................... 14
   5.1. Message Signature or MAC Computation ............... 14
   5.2. Message Signature or MAC Validation ............... 15
   5.3. String Comparison Rules ........................... 16
6. Key Identification ...................................... 17
7. Serializations ......................................... 17
   7.1. JWS Compact Serialization ........................... 17
   7.2. JWS JSON Serialization ............................. 18
8. TLS Requirements ........................................ 19
9. IANA Considerations .................................... 20
   9.1. JSON Web Signature and Encryption Header Parameters Registry ......................... 20
   9.1.1. Registration Template ............................ 21
   9.1.2. Initial Registry Contents ....................... 21
   9.2. Media Type Registration ............................ 23
   9.2.1. Registry Contents ............................... 23
10. Security Considerations ........................................ 24
  10.1. Key Entropy .............................................. 24
  10.2. Chosen Plaintext Attacks ................................ 25
  10.3. Timing Attacks ........................................... 25
  10.4. Differences between Digital Signatures and MACs ........ 25
  10.5. SHA-1 Certificate Thumbprints ............................. 25
  10.6. JSON Security Considerations ............................. 26
  10.7. Unicode Comparison Security Considerations ............. 26
11. References ...................................................... 27
  11.1. Normative References ..................................... 27
  11.2. Informative References ................................... 28
Appendix A. JWS Examples ............................................ 29
  A.1. Example JWS using HMAC SHA-256 ........................... 29
       A.1.1. Encoding ............................................. 29
       A.1.2. Validating .......................................... 32
  A.2. Example JWS using RSASSA-PKCS-v1_5 SHA-256 ............... 32
       A.2.1. Encoding ............................................. 32
       A.2.2. Validating .......................................... 35
  A.3. Example JWS using ECDSA P-256 SHA-256 ..................... 35
       A.3.1. Encoding ............................................. 35
       A.3.2. Validating .......................................... 37
  A.4. Example JWS using ECDSA P-521 SHA-512 .................... 37
       A.4.1. Encoding ............................................. 37
       A.4.2. Validating .......................................... 39
  A.5. Example Plaintext JWS ...................................... 40
  A.6. Example JWS Using JWS JSON Serialization .................. 40
       A.6.1. JWS Per-Signature Protected Headers ................ 41
       A.6.2. JWS Per-Signature Unprotected Headers ............... 41
       A.6.3. Complete JWS Header Values .......................... 41
       A.6.4. Complete JWS JSON Serialization Representation .... 42
Appendix B. "x5c" (X.509 Certificate Chain) Example .............. 42
Appendix C. Notes on implementing base64url encoding without padding ........................................... 44
Appendix D. Notes on Key Selection ................................ 45
Appendix E. Negative Test Case for "crit" Header Parameter .... 47
Appendix F. Detached Content ...................................... 48
Appendix G. Acknowledgements .................................... 48
Appendix H. Document History ..................................... 49
Authors’ Addresses ................................................. 57
1. Introduction

JSON Web Signature (JWS) represents content secured with digital signatures or Message Authentication Codes (MACs) using JavaScript Object Notation (JSON) [RFC7159] based data structures. The JWS cryptographic mechanisms provide integrity protection for an arbitrary sequence of octets.

Two closely related serializations for JWS objects are defined. The JWS Compact Serialization is a compact, URL-safe representation intended for space constrained environments such as HTTP Authorization headers and URI query parameters. The JWS JSON Serialization represents JWS objects as JSON objects and enables multiple signatures and/or MACs to be applied to the same content. Both share the same cryptographic underpinnings.

Cryptographic algorithms and identifiers for use with this specification are described in the separate JSON Web Algorithms (JWA) [JWA] specification and an IANA registry defined by that specification. Related encryption capabilities are described in the separate JSON Web Encryption (JWE) [JWE] specification.

Names defined by this specification are short because a core goal is for the resulting representations to be compact.

1.1. 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 Key words for use in RFCs to Indicate Requirement Levels [RFC2119]. If these words are used without being spelled in uppercase then they are to be interpreted with their normal natural language meanings.

BASE64URL(OCTETS) denotes the base64url encoding of OCTETS, per Section 2.

UTF8(STRING) denotes the octets of the UTF-8 [RFC3629] representation of STRING.

ASCII(STRING) denotes the octets of the ASCII [USASCII] representation of STRING.

The concatenation of two values A and B is denoted as A || B.
2. Terminology

JSON Web Signature (JWS)
A data structure representing a digitally signed or MACed message.

JWS Header
JSON object containing the parameters describing the cryptographic operations and parameters employed. The JWS Header members are the union of the members of the JWS Protected Header and the JWS Unprotected Header. The members of the JWS Header are Header Parameters.

JWS Payload
The sequence of octets to be secured -- a.k.a., the message. The payload can contain an arbitrary sequence of octets.

JWS Signature
Digital signature or MAC over the JWS Protected Header and the JWS Payload.

Header Parameter
A name/value pair that is member of the JWS Header.

JWS Protected Header
JSON object that contains the JWS Header Parameters that are integrity protected by the JWS Signature digital signature or MAC operation. For the JWS Compact Serialization, this comprises the entire JWS Header. For the JWS JSON Serialization, this is one component of the JWS Header.

JWS Unprotected Header
JSON object that contains the JWS Header Parameters that are not integrity protected. This can only be present when using the JWS JSON Serialization.

Base64url Encoding
Base64 encoding using the URL- and filename-safe character set defined in Section 5 of RFC 4648 [RFC4648], with all trailing ‘=’ characters omitted (as permitted by Section 3.2) and without the inclusion of any line breaks, white space, or other additional characters. (See Appendix C for notes on implementing base64url encoding without padding.)

JWS Signing Input
The input to the digital signature or MAC computation. Its value is ASCII(BASE64URL(UTF8(JWS Protected Header)) || ‘.’ || BASE64URL(JWS Payload)).
JWS Compact Serialization
A representation of the JWS as a compact, URL-safe string.

JWS JSON Serialization
A representation of the JWS as a JSON object. Unlike the JWS Compact Serialization, the JWS JSON Serialization enables multiple digital signatures and/or MACs to be applied to the same content. This representation is neither optimized for compactness nor URL-safe.

Collision-Resistant Name
A name in a namespace that enables names to be allocated in a manner such that they are highly unlikely to collide with other names. Examples of collision-resistant namespaces include: Domain Names, Object Identifiers (OIDs) as defined in the ITU-T X.660 and X.670 Recommendation series, and Universally Unique IDentifiers (UUIDs) [RFC4122]. When using an administratively delegated namespace, the definer of a name needs to take reasonable precautions to ensure they are in control of the portion of the namespace they use to define the name.

StringOrURI
A JSON string value, with the additional requirement that while arbitrary string values MAY be used, any value containing a ":" character MUST be a URI [RFC3986]. StringOrURI values are compared as case-sensitive strings with no transformations or canonicalizations applied.

3. JSON Web Signature (JWS) Overview

JWS represents digitally signed or MACed content using JSON data structures and base64url encoding. A JWS represents these logical values:

JWS Header
JSON object containing the parameters describing the cryptographic operations and parameters employed. The JWS Header members are the union of the members of the JWS Protected Header and the JWS Unprotected Header, as described below.

JWS Payload
The sequence of octets to be secured -- a.k.a., the message. The payload can contain an arbitrary sequence of octets.
JWS Signature
Digital signature or MAC over the JWS Protected Header and the JWS Payload.

The JWS Header represents the combination of these values:

JWS Protected Header
JSON object that contains the JWS Header Parameters that are integrity protected by the JWS Signature digital signature or MAC operation.

JWS Unprotected Header
JSON object that contains the JWS Header Parameters that are not integrity protected.

This document defines two serializations for JWS objects: a compact, URL-safe serialization called the JWS Compact Serialization and a JSON serialization called the JWS JSON Serialization. In both serializations, the JWS Protected Header, JWS Payload, and JWS Signature are base64url encoded for transmission, since JSON lacks a way to directly represent octet sequences.

In the JWS Compact Serialization, no JWS Unprotected Header is used. In this case, the JWS Header and the JWS Protected Header are the same.

In the JWS Compact Serialization, a JWS object is represented as the combination of these three string values,
BASE64URL(UTF8(JWS Protected Header)),
BASE64URL(JWS Payload), and
BASE64URL(JWS Signature),
concatenated in that order, with the three strings being separated by two period (‘.’) characters.

In the JWS JSON Serialization, one or both of the JWS Protected Header and JWS Unprotected Header MUST be present. In this case, the members of the JWS Header are the combination of the members of the JWS Protected Header and the JWS Unprotected Header values that are present.

In the JWS JSON Serialization, a JWS object is represented as the combination of these four values,
BASE64URL(UTF8(JWS Protected Header)),
JWS Unprotected Header,
BASE64URL(JWS Payload), and
BASE64URL(JWS Signature),
with the three base64url encoding result strings and the JWS Unprotected Header value being represented as members within a JSON
object. The inclusion of some of these values is OPTIONAL. The JWS JSON Serialization can also represent multiple signature and/or MAC values, rather than just one. See Section 7.2 for more information about the JWS JSON Serialization.

3.1. Example JWS

This section provides an example of a JWS. Its computation is described in more detail in Appendix A.1, including specifying the exact octet sequences representing the JSON values used and the key value used.

The following example JWS Protected Header declares that the encoded object is a JSON Web Token (JWT) [JWT] and the JWS Protected Header and the JWS Payload are secured using the HMAC SHA-256 algorithm:

```json
{"typ":"JWT",
 "alg":"HS256"}
```

Encoding this JWS Protected Header as BASE64URL(UTF8(JWS Protected Header)) gives this value:

```
eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9
```

The UTF-8 representation of following JSON object is used as the JWS Payload. (Note that the payload can be any content, and need not be a representation of a JSON object.)

```json
{"iss":"joe",
 "exp":1300819380,
 "http://example.com/is_root":true}
```

Encoding this JWS Payload as BASE64URL(JWS Payload) gives this value (with line breaks for display purposes only):

```
eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFt
cGxlNvbS9pc19yb290Ijp0cnVlfQ
```

Computing the HMAC of the JWS Signing Input ASCII(BASE64URL(UTF8(JWS Protected Header)) || '.' || BASE64URL(JWS Payload)) with the HMAC SHA-256 algorithm using the key specified in Appendix A.1 and base64url encoding the result yields this BASE64URL(JWS Signature) value:

```
dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk
```

Concatenating these values in the order Header.Payload.Signature with period ('.') characters between the parts yields this complete JWS
representation using the JWS Compact Serialization (with line breaks for display purposes only):

eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9 .
eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFt cGxlLmNvbS9pc19yb290Ijp0cnVlfiQ .
dBjftJe24CVP-mB92K27uhbUJJU1plr_wW1gFWFOEjXk

See Appendix A for additional examples.

4. JWS Header

The members of the JSON object(s) representing the JWS Header describe the digital signature or MAC applied to the JWS Protected Header and the JWS Payload and optionally additional properties of the JWS. The Header Parameter names within the JWS Header MUST be unique; recipients MUST either reject JWSs with duplicate Header Parameter names or use a JSON parser that returns only the lexically last duplicate member name, as specified in Section 15.12 (The JSON Object) of ECMAScript 5.1 [ECMAScript].

Implementations are required to understand the specific Header Parameters defined by this specification that are designated as "MUST be understood" and process them in the manner defined in this specification. All other Header Parameters defined by this specification that are not so designated MUST be ignored when not understood. Unless listed as a critical Header Parameter, per Section 4.1.11, all Header Parameters not defined by this specification MUST be ignored when not understood.

There are three classes of Header Parameter names: Registered Header Parameter names, Public Header Parameter names, and Private Header Parameter names.

4.1. Registered Header Parameter Names

The following Header Parameter names are registered in the IANA JSON Web Signature and Encryption Header Parameters registry defined in Section 9.1, with meanings as defined below.

As indicated by the common registry, JWSs and JWEs share a common Header Parameter space; when a parameter is used by both specifications, its usage must be compatible between the specifications.
4.1.1. "alg" (Algorithm) Header Parameter

The "alg" (algorithm) Header Parameter identifies the cryptographic algorithm used to secure the JWS. The signature, MAC, or plaintext value is not valid if the "alg" value does not represent a supported algorithm, or if there is not a key for use with that algorithm associated with the party that digitally signed or MACed the content. "alg" values should either be registered in the IANA JSON Web Signature and Encryption Algorithms registry defined in [JWA] or be a value that contains a Collision-Resistant Name. The "alg" value is a case-sensitive string containing a StringOrURI value. This Header Parameter MUST be present and MUST be understood and processed by implementations.

A list of defined "alg" values for this use can be found in the IANA JSON Web Signature and Encryption Algorithms registry defined in [JWA]; the initial contents of this registry are the values defined in Section 3.1 of the JSON Web Algorithms (JWA) [JWA] specification.

4.1.2. "jku" (JWK Set URL) Header Parameter

The "jku" (JWK Set URL) Header Parameter is a URI [RFC3986] that refers to a resource for a set of JSON-encoded public keys, one of which corresponds to the key used to digitally sign the JWS. The keys MUST be encoded as a JSON Web Key Set (JWK Set) [JWK]. The protocol used to acquire the resource MUST provide integrity protection; an HTTP GET request to retrieve the JWK Set MUST use TLS [RFC2818] [RFC5246]; the identity of the server MUST be validated, as per Section 6 of RFC 6125 [RFC6125]. Use of this Header Parameter is OPTIONAL.

4.1.3. "jwk" (JSON Web Key) Header Parameter

The "jwk" (JSON Web Key) Header Parameter is the public key that corresponds to the key used to digitally sign the JWS. This key is represented as a JSON Web Key [JWK]. Use of this Header Parameter is OPTIONAL.

4.1.4. "kid" (Key ID) Header Parameter

The "kid" (key ID) Header Parameter is a hint indicating which key was used to secure the JWS. This parameter allows originators to explicitly signal a change of key to recipients. The structure of the "kid" value is unspecified. Its value MUST be a string. Use of this Header Parameter is OPTIONAL.

When used with a JWK, the "kid" value is used to match a JWK "kid" parameter value.
4.1.5. "x5u" (X.509 URL) Header Parameter

The "x5u" (X.509 URL) Header Parameter is a URI [RFC3986] that refers to a resource for the X.509 public key certificate or certificate chain [RFC5280] corresponding to the key used to digitally sign the JWS. The identified resource MUST provide a representation of the certificate or certificate chain that conforms to RFC 5280 [RFC5280] in PEM encoded form [RFC1421]. The certificate containing the public key corresponding to the key used to digitally sign the JWS MUST be the first certificate. This MAY be followed by additional certificates, with each subsequent certificate being the one used to certify the previous one. The protocol used to acquire the resource MUST provide integrity protection; an HTTP GET request to retrieve the certificate MUST use TLS [RFC2818] [RFC5246]; the identity of the server MUST be validated, as per Section 6 of RFC 6125 [RFC6125]. Use of this Header Parameter is OPTIONAL.

4.1.6. "x5c" (X.509 Certificate Chain) Header Parameter

The "x5c" (X.509 Certificate Chain) Header Parameter contains the X.509 public key certificate or certificate chain [RFC5280] corresponding to the key used to digitally sign the JWS. The certificate or certificate chain is represented as a JSON array of certificate value strings. Each string in the array is a base64 encoded ([RFC4648] Section 4 -- not base64url encoded) DER [ITU.X690.1994] PKIX certificate value. The certificate containing the public key corresponding to the key used to digitally sign the JWS MUST be the first certificate. This MAY be followed by additional certificates, with each subsequent certificate being the one used to certify the previous one. The recipient MUST validate the certificate chain according to [RFC5280] and reject the signature if any validation failure occurs. Use of this Header Parameter is OPTIONAL.

See Appendix B for an example "x5c" value.

4.1.7. "x5t" (X.509 Certificate SHA-1 Thumbprint) Header Parameter

The "x5t" (X.509 Certificate SHA-1 Thumbprint) Header Parameter is a base64url encoded SHA-1 thumbprint (a.k.a. digest) of the DER encoding of the X.509 certificate [RFC5280] corresponding to the key used to digitally sign the JWS. Use of this Header Parameter is OPTIONAL.

4.1.8. "x5t#S256" (X.509 Certificate SHA-256 Thumbprint) Header Parameter

The "x5t#S256" (X.509 Certificate SHA-256 Thumbprint) Header
Parameter is a base64url encoded SHA-256 thumbprint (a.k.a. digest) of the DER encoding of the X.509 certificate [RFC5280] corresponding to the key used to digitally sign the JWS. Use of this Header Parameter is OPTIONAL.

4.1.9. "typ" (Type) Header Parameter

The "typ" (type) Header Parameter is used by JWS applications to declare the MIME Media Type [IANA.MediaTypes] of this complete JWS object. This is intended for use by the application when more than one kind of object could be present in an application data structure that can contain a JWS object; the application can use this value to disambiguate among the different kinds of objects that might be present. It will typically not be used by applications when the kind of object is already known. This parameter has no effect upon the JWS processing. Use of this Header Parameter is OPTIONAL.

Per [RFC2045], all media type values, subtype values, and parameter names are case-insensitive. However, parameter values are case-sensitive unless otherwise specified for the specific parameter.

To keep messages compact in common situations, it is RECOMMENDED that senders omit an "application/" prefix of a media type value in a "typ" Header Parameter when no other '/' appears in the media type value. A recipient using the media type value MUST treat it as if "application/" were prepended to any "typ" value not containing a '/'. For instance, a "typ" value of "example" SHOULD be used to represent the "application/example" media type; whereas, the media type "application/example;part="1/2"" cannot be shortened to "example;part="1/2"".

The "typ" value "JOSE" can be used by applications to indicate that this object is a JWS or JWE using the JWS Compact Serialization or the JWE Compact Serialization. The "typ" value "JOSE+JSON" can be used by applications to indicate that this object is a JWS or JWE using the JWS JSON Serialization or the JWE JSON Serialization. Other type values can also be used by applications.

4.1.10. "cty" (Content Type) Header Parameter

The "cty" (content type) Header Parameter is used by JWS applications to declare the MIME Media Type [IANA.MediaTypes] of the secured content (the payload). This is intended for use by the application when more than one kind of object could be present in the JWS payload; the application can use this value to disambiguate among the different kinds of objects that might be present. It will typically not be used by applications when the kind of object is already known. This parameter has no effect upon the JWS processing. Use of this
Header Parameter is OPTIONAL.

Per [RFC2045], all media type values, subtype values, and parameter names are case-insensitive. However, parameter values are case-sensitive unless otherwise specified for the specific parameter.

To keep messages compact in common situations, it is RECOMMENDED that senders omit an "application/" prefix of a media type value in a "cty" Header Parameter when no other '/ ' appears in the media type value. A recipient using the media type value MUST treat it as if "application/" were prepended to any "cty" value not containing a '/ '. For instance, a "cty" value of "example" SHOULD be used to represent the "application/example" media type; whereas, the media type "application/example;part="1/2'" cannot be shortened to "example;part="1/2'".

4.1.11. "crit" (Critical) Header Parameter

The "crit" (critical) Header Parameter indicates that extensions to the initial RFC versions of [[ this specification ]] and [JWA] are being used that MUST be understood and processed. Its value is an array listing the Header Parameter names present in the JWS Header that use those extensions. If any of the listed extension Header Parameters are not understood and supported by the receiver, it MUST reject the JWS. Senders MUST NOT include Header Parameter names defined by the initial RFC versions of [[ this specification ]] or [JWA] for use with JWS, duplicate names, or names that do not occur as Header Parameter names within the JWS Header in the "crit" list. Senders MUST NOT use the empty list "[]" as the "crit" value.

Recipients MAY reject the JWS if the critical list contains any Header Parameter names defined by the initial RFC versions of [[ this specification ]] or [JWA] for use with JWS, or any other constraints on its use are violated. This Header Parameter MUST be integrity protected, and therefore MUST occur only within the JWS Protected Header, when used. Use of this Header Parameter is OPTIONAL. This Header Parameter MUST be understood and processed by implementations.

An example use, along with a hypothetical "exp" (expiration-time) field is:

```json
{"alg":"ES256",
 "crit":["exp"],
 "exp":1363284000}
```
4.2. Public Header Parameter Names

Additional Header Parameter names can be defined by those using JWSs. However, in order to prevent collisions, any new Header Parameter name should either be registered in the IANA JSON Web Signature and Encryption Header Parameters registry defined in Section 9.1 or be a Public Name: a value that contains a Collision-Resistant Name. In each case, the definer of the name or value needs to take reasonable precautions to make sure they are in control of the part of the namespace they use to define the Header Parameter name.

New Header Parameters should be introduced sparingly, as they can result in non-interoperable JWSs.

4.3. Private Header Parameter Names

A producer and consumer of a JWS may agree to use Header Parameter names that are Private Names: names that are not Registered Header Parameter names Section 4.1 or Public Header Parameter names Section 4.2. Unlike Public Header Parameter names, Private Header Parameter names are subject to collision and should be used with caution.

5. Producing and Consuming JWSs

5.1. Message Signature or MAC Computation

To create a JWS, one MUST perform these steps. The order of the steps is not significant in cases where there are no dependencies between the inputs and outputs of the steps.

1. Create the content to be used as the JWS Payload.
2. Compute the encoded payload value BASE64URL(JWS Payload).
3. Create the JSON object(s) containing the desired set of Header Parameters, which together comprise the JWS Header: the JWS Protected Header, and if the JWS JSON Serialization is being used, the JWS Unprotected Header.
4. Compute the encoded header value BASE64URL(UTF8(JWS Protected Header)). If the JWS Protected Header is not present (which can only happen when using the JWS JSON Serialization and no "protected" member is present), let this value be the empty string.
5. Compute the JWS Signature in the manner defined for the particular algorithm being used over the JWS Signing Input ASCII(BASE64URL(UTF8(JWS Protected Header))) || "." || BASE64URL(JWS Payload)). The "alg" (algorithm) Header Parameter MUST be present in the JWS Header, with the algorithm value accurately representing the algorithm used to construct the JWS.
Signature.

6. Compute the encoded signature value BASE64URL(JWS Signature).

7. These three encoded values are used in both the JWS Compact
   Serialization and the JWS JSON Serialization representations.

8. If the JWS JSON Serialization is being used, repeat this process
   (steps 3-7) for each digital signature or MAC operation being
   performed.

9. Create the desired serialized output. The JWS Compact
   Serialization of this result is BASE64URL(UTF8(JWS Protected
   Header)) || '.' || BASE64URL(JWS Payload) || '.' || BASE64URL(JWS
   Signature). The JWS JSON Serialization is described in
   Section 7.2.

5.2. Message Signature or MAC Validation

When validating a JWS, the following steps MUST be taken. The order
of the steps is not significant in cases where there are no
dependencies between the inputs and outputs of the steps. If any of
the listed steps fails, then the signature or MAC cannot be
validated.

It is an application decision which signatures, MACs, or plaintext
values must successfully validate for the JWS to be accepted. In
some cases, all must successfully validate or the JWS will be
rejected. In other cases, only a specific signature, MAC, or
plaintext value needs to be successfully validated. However, in all
cases, at least one signature, MAC, or plaintext value MUST
successfully validate or the JWS MUST be rejected.

1. Parse the JWS representation to extract the serialized values
   for the components of the JWS -- when using the JWS Compact
   Serialization, the base64url encoded representations of the JWS
   Protected Header, the JWS Payload, and the JWS Signature, and
   when using the JWS JSON Serialization, also the unencoded JWS
   Unprotected Header value. When using the JWS Compact
   Serialization, the JWS Protected Header, the JWS Payload, and
   the JWS Signature are represented as base64url encoded values in
   that order, separated by two period ('.') characters. The JWS
   JSON Serialization is described in Section 7.2.

2. The encoded representation of the JWS Protected Header MUST be
   successfully base64url decoded following the restriction that no
   padding characters have been used.

3. The resulting octet sequence MUST be a UTF-8 encoded
   representation of a completely valid JSON object conforming to
   [RFC7159], which is the JWS Protected Header.

4. If using the JWS Compact Serialization, let the JWS Header be
   the JWS Protected Header; otherwise, when using the JWS JSON
   Serialization, let the JWS Header be the union of the members of
the corresponding JWS Protected Header and JWS Unprotected
Header, all of which must be completely valid JSON objects.
5. The resulting JWS Header MUST NOT contain duplicate Header
Parameter names. When using the JWS JSON Serialization, this
restriction includes that the same Header Parameter name also
MUST NOT occur in distinct JSON object values that together
comprise the JWS Header.
6. Verify that the implementation understands and can process all
fields that it is required to support, whether required by this
specification, by the algorithm being used, or by the "crit"
Header Parameter value, and that the values of those parameters
are also understood and supported.
7. The encoded representation of the JWS Payload MUST be
successfully base64url decoded following the restriction that no
padding characters have been used.
8. The encoded representation of the JWS Signature MUST be
successfully base64url decoded following the restriction that no
padding characters have been used.
9. The JWS Signature MUST be successfully validated against the JWS
Signing Input ASCII(BASE64URL(UTF8(JWS Protected Header)) || 
| | BASE64URL(JWS Payload)) in the manner defined for the
algorithm being used, which MUST be accurately represented by
the value of the "alg" (algorithm) Header Parameter, which MUST
be present.
10. If the JWS JSON Serialization is being used, repeat this process
(steps 4-9) for each digital signature or MAC value contained in
the representation.

5.3. String Comparison Rules

Processing a JWS inevitably requires comparing known strings to
members and values in a JSON object. For example, in checking what
the algorithm is, the Unicode string "alg" will be checked against
the member names in the JWS Header to see if there is a matching
Header Parameter name. The same process is then used to determine if
the value of the "alg" Header Parameter represents a supported
algorithm.

Since the only string comparison operations that are performed are
equality and inequality, the same rules can be used for comparing
both member names and member values against known strings. The JSON
rules for doing member name comparison are described in Section 8.3
of [RFC7159].

Also, see the JSON security considerations in Section 10.6 and the
Unicode security considerations in Section 10.7.
6. Key Identification

It is necessary for the recipient of a JWS to be able to determine the key that was employed for the digital signature or MAC operation. The key employed can be identified using the Header Parameter methods described in Section 4.1 or can be identified using methods that are outside the scope of this specification. Specifically, the Header Parameters "jku", "jwk", "kid", "x5u", "x5c", "x5t", and "x5t#S256" can be used to identify the key used. These Header Parameters MUST be integrity protected if the information that they convey is to be utilized in a trust decision.

The sender SHOULD include sufficient information in the Header Parameters to identify the key used, unless the application uses another means or convention to determine the key used. Validation of the signature or MAC fails when the algorithm used requires a key (which is true of all algorithms except for "none") and the key used cannot be determined.

The means of exchanging any shared symmetric keys used is outside the scope of this specification.

Also, see Appendix D for notes on possible key selection algorithms.

7. Serializations

JWS objects use one of two serializations, the JWS Compact Serialization or the JWS JSON Serialization. Applications using this specification need to specify what serialization and serialization features are used for that application. For instance, applications might specify that only the JWS JSON Serialization is used, that only JWS JSON Serialization support for a single signature or MAC value is used, or that support for multiple signatures and/or MAC values is used. JWS implementations only need to implement the features needed for the applications they are designed to support.

7.1. JWS Compact Serialization

The JWS Compact Serialization represents digitally signed or MACed content as a compact URL-safe string. This string is BASE64URL(UTF8(JWS Protected Header)) || '.' || BASE64URL(JWS Payload) || '.' || BASE64URL(JWS Signature). Only one signature/MAC is supported by the JWS Compact Serialization and it provides no syntax to represent a JWS Unprotected Header value.
7.2. JWS JSON Serialization

The JWS JSON Serialization represents digitally signed or MACed content as a JSON object. Content using the JWS JSON Serialization can be secured with more than one digital signature and/or MAC operation. This representation is neither optimized for compactness nor URL-safe.

The following members are defined for use in top-level JSON objects used for the JWS JSON Serialization:

payload
The "payload" member MUST be present and contain the value BASE64URL(JWS Payload).

signatures
The "signatures" member value MUST be an array of JSON objects. Each object represents a signature or MAC over the JWS Payload and the JWS Protected Header.

The following members are defined for use in the JSON objects that are elements of the "signatures" array:

protected
The "protected" member MUST be present and contain the value BASE64URL(UTF8(JWS Protected Header)) when the JWS Protected Header value is non-empty; otherwise, it MUST be absent. These Header Parameter values are integrity protected.

header
The "header" member MUST be present and contain the value JWS Unprotected Header when the JWS Unprotected Header value is non-empty; otherwise, it MUST be absent. This value is represented as an unencoded JSON object, rather than as a string. These Header Parameter values are not integrity protected.

signature
The "signature" member MUST be present and contain the value BASE64URL(JWS Signature).

At least one of the "protected" and "header" members MUST be present for each signature/MAC computation so that an "alg" Header Parameter value is conveyed.

Additional members can be present in both the JSON objects defined above; if not understood by implementations encountering them, they MUST be ignored.

The Header Parameter values used when creating or validating individual signature or MAC values are the union of the two sets of Header Parameter values that may be present: (1) the JWS Protected Header represented in the "protected" member of the signature/MAC's array element, and (2) the JWS Unprotected Header in the "header"
Each JWS Signature value is computed using the parameters of the corresponding JWS Header value in the same manner as for the JWS Compact Serialization. This has the desirable property that each JWS Signature value represented in the "signatures" array is identical to the value that would have been computed for the same parameter in the JWS Compact Serialization, provided that the JWS Protected Header value for that signature/MAC computation (which represents the integrity-protected Header Parameter values) matches that used in the JWS Compact Serialization.

In summary, the syntax of a JWS using the JWS JSON Serialization is as follows:

```json
{
  "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>"}
  ]
}
```

See Appendix A.6 for an example of computing a JWS using the JWS JSON Serialization.

8. TLS Requirements

Implementations MUST support TLS. Which version(s) ought to be implemented will vary over time, and depend on the widespread deployment and known security vulnerabilities at the time of implementation. At the time of this writing, TLS version 1.2 [RFC5246] is the most recent version.

To protect against information disclosure and tampering, confidentiality protection MUST be applied using TLS with a ciphersuite that provides confidentiality and integrity protection.

Whenever TLS is used, the identity of the service provider encoded in the TLS server certificate MUST be verified using the procedures described in Section 6 of RFC 6125 [RFC6125].

---

9. IANA Considerations

The following registration procedure is used for all the registries established by this specification.

Values are registered with a Specification Required [RFC5226] after a two-week review period on the [TBD]@ietf.org mailing list, on the advice of one or more Designated Experts. However, to allow for the allocation of values prior to publication, the Designated Expert(s) may approve registration once they are satisfied that such a specification will be published.

Registration requests must be sent to the [TBD]@ietf.org mailing list for review and comment, with an appropriate subject (e.g., "Request for access token type: example"). [Note to the RFC Editor: The name of the mailing list should be determined in consultation with the IESG and IANA. Suggested name: jose-reg-review.]

Within the review period, the Designated Expert(s) will either approve or deny the registration request, communicating this decision to the review list and IANA. Denials should include an explanation and, if applicable, suggestions as to how to make the request successful. Registration requests that are undetermined for a period longer than 21 days can be brought to the IESG’s attention (using the iesg@iesg.org mailing list) for resolution.

Criteria that should be applied by the Designated Expert(s) includes determining whether the proposed registration duplicates existing functionality, determining whether it is likely to be of general applicability or whether it is useful only for a single application, and whether the registration makes sense.

IANA must only accept registry updates from the Designated Expert(s) and should direct all requests for registration to the review mailing list.

It is suggested that multiple Designated Experts be appointed who are able to represent the perspectives of different applications using this specification, in order to enable broadly-informed review of registration decisions. In cases where a registration decision could be perceived as creating a conflict of interest for a particular Expert, that Expert should defer to the judgment of the other Expert(s).

9.1. JSON Web Signature and Encryption Header Parameters Registry

This specification establishes the IANA JSON Web Signature and Encryption Header Parameters registry for JWS and JWE Header
Parameter names. The registry records the Header Parameter name and a reference to the specification that defines it. The same Header Parameter name can be registered multiple times, provided that the parameter usage is compatible between the specifications. Different registrations of the same Header Parameter name will typically use different Header Parameter Usage Location(s) values.

9.1.1. Registration Template

Header Parameter Name:
The name requested (e.g., "example"). Because a core goal of this specification is for the resulting representations to be compact, it is RECOMMENDED that the name be short -- not to exceed 8 characters without a compelling reason to do so. This name is case-sensitive. Names may not match other registered names in a case-insensitive manner unless the Designated Expert(s) state that there is a compelling reason to allow an exception in this particular case.

Header Parameter Description:
Brief description of the Header Parameter (e.g., "Example description").

Header Parameter Usage Location(s):
The Header Parameter usage locations, which should be one or more of the values "JWS" or "JWE".

Change Controller:
For Standards Track RFCs, state "IESG". For others, give the name of the responsible party. Other details (e.g., postal address, email address, home page URI) may also be included.

Specification Document(s):
Reference to the document(s) that specify the parameter, preferably including URI(s) that can be used to retrieve copies of the document(s). An indication of the relevant sections may also be included but is not required.

9.1.2. Initial Registry Contents

This specification registers the Header Parameter names defined in Section 4.1 in this registry.

- Header Parameter Name: "alg"
  - Header Parameter Description: Algorithm
  - Header Parameter Usage Location(s): JWS
  - Change Controller: IESG
  - Specification Document(s): Section 4.1.1 of [[ this document ]]

- Header Parameter Name: "jku"
o Header Parameter Description: JWK Set URL
o Header Parameter Usage Location(s): JWS
o Change Controller: IESG
o Specification Document(s): Section 4.1.2 of [[ this document ]]

o Header Parameter Name: "jwk"
o Header Parameter Description: JSON Web Key
o Header Parameter Usage Location(s): JWS
o Change Controller: IESG
o Specification document(s): Section 4.1.3 of [[ this document ]]

o Header Parameter Name: "kid"
o Header Parameter Description: Key ID
o Header Parameter Usage Location(s): JWS
o Change Controller: IESG
o Specification Document(s): Section 4.1.4 of [[ this document ]]

o Header Parameter Name: "x5u"
o Header Parameter Description: X.509 URL
o Header Parameter Usage Location(s): JWS
o Change Controller: IESG
o Specification Document(s): Section 4.1.5 of [[ this document ]]

o Header Parameter Name: "x5c"
o Header Parameter Description: X.509 Certificate Chain
o Header Parameter Usage Location(s): JWS
o Change Controller: IESG
o Specification Document(s): Section 4.1.6 of [[ this document ]]

o Header Parameter Name: "x5t"
o Header Parameter Description: X.509 Certificate SHA-1 Thumbprint
o Header Parameter Usage Location(s): JWS
o Change Controller: IESG
o Specification Document(s): Section 4.1.7 of [[ this document ]]

o Header Parameter Name: "x5t#S256"
o Header Parameter Description: X.509 Certificate SHA-256 Thumbprint
o Header Parameter Usage Location(s): JWS
o Change Controller: IESG
o Specification Document(s): Section 4.1.8 of [[ this document ]]

o Header Parameter Name: "typ"
o Header Parameter Description: Type
o Header Parameter Usage Location(s): JWS
o Change Controller: IESG
o Specification Document(s): Section 4.1.9 of [[ this document ]]
9.2. Media Type Registration

9.2.1. Registry Contents

This specification registers the "application/jose" Media Type [RFC2046] in the MIME Media Types registry [IANA.MediaTypes], which can be used to indicate that the content is a JWS or JWE object using the JWS Compact Serialization or the JWE Compact Serialization and the "application/jose+json" Media Type in the MIME Media Types registry, which can be used to indicate that the content is a JWS or JWE object using the JWS JSON Serialization or the JWE JSON Serialization.

- Type name: application
- Subtype name: jose
- Required parameters: n/a
- Optional parameters: n/a
- Encoding considerations: 8bit; application/jose values are encoded as a series of base64url encoded values (some of which may be the empty string) separated by period ('.') characters.
- Security considerations: See the Security Considerations section of [[ this document ]]
- Interoperability considerations: n/a
- Published specification: [[ this document ]]
- Applications that use this media type: OpenID Connect, Mozilla Persona, Salesforce, Google, Android, Windows Azure, Xbox One, and numerous others that use JWTs
- Additional information: Magic number(s): n/a, File extension(s): n/a, Macintosh file type code(s): n/a
- Person & email address to contact for further information: Michael B. Jones, mbj@microsoft.com
- Intended usage: COMMON
- Restrictions on usage: none
- Author: Michael B. Jones, mbj@microsoft.com
10. Security Considerations

All of the security issues faced by any cryptographic application must be faced by a JWS/JWE/JWK agent. Among these issues are protecting the user’s asymmetric private and symmetric secret keys, preventing various attacks, and helping avoid mistakes such as inadvertently encrypting a message to the wrong recipient. The entire list of security considerations is beyond the scope of this document, but some significant concerns are listed here.

All the security considerations in XML DSIG 2.0 [W3C.NOTE-xmldsig-core2-20130411], also apply to this specification, other than those that are XML specific. Likewise, many of the best practices documented in XML Signature Best Practices [W3C.NOTE-xmldsig-bestpractices-20130411] also apply to this specification, other than those that are XML specific.

10.1. Key Entropy

Keys are only as strong as the amount of entropy used to generate them. A minimum of 128 bits of entropy should be used for all keys, and depending upon the application context, more may be required. In particular, it may be difficult to generate sufficiently random values in some browsers and application environments.
10.2. Chosen Plaintext Attacks

Creators of JWSs should not allow third parties to insert arbitrary content into the message without adding entropy not controlled by the third party.

10.3. Timing Attacks

When cryptographic algorithms are implemented in such a way that successful operations take a different amount of time than unsuccessful operations, attackers may be able to use the time difference to obtain information about the keys employed. Therefore, such timing differences must be avoided.

10.4. Differences between Digital Signatures and MACs

While MACs and digital signatures can both be used for integrity checking, there are some significant differences between the security properties that each of them provides. These need to be taken into consideration when designing protocols and selecting the algorithms to be used in protocols.

Both signatures and MACs provide for integrity checking -- verifying that the message has not been modified since the integrity value was computed. However, MACs provide for origination identification only under specific circumstances. It can normally be assumed that a private key used for a signature is only in the hands of a single entity (although perhaps a distributed entity, in the case of replicated servers); however, a MAC key needs to be in the hands of all the entities that use it for integrity computation and checking. This means that origination can only be determined if a MAC key is known only to two entities and the receiver knows that it did not create the message. MAC validation cannot be used to prove origination to a third party.

10.5. SHA-1 Certificate Thumbprints

A SHA-1 hash is used when computing "x5t" (X.509 Certificate SHA-1 Thumbprint) values, for compatibility reasons. Should an effective means of producing SHA-1 hash collisions be developed, and should an attacker wish to interfere with the use of a known certificate on a given system, this could be accomplished by creating another certificate whose SHA-1 hash value is the same and adding it to the certificate store used by the intended victim. A prerequisite to this attack succeeding is the attacker having write access to the intended victim’s certificate store.

Alternatively, the "x5t#S256" (X.509 Certificate SHA-256 Thumbprint)
Internet-Draft          JSON Web Signature (JWS)               June 2014

Header Parameter could be used instead of "x5t". However, at the
time of this writing, no development platform is known to support
SHA-256 certificate thumbprints.

10.6. JSON Security Considerations

Strict JSON [RFC7159] validation is a security requirement. If
malformed JSON is received, then the intent of the sender is
impossible to reliably discern. Ambiguous and potentially
exploitable situations could arise if the JSON parser used does not
reject malformed JSON syntax. In particular, any JSON inputs not
conforming to the JSON-text syntax defined in RFC 7159 input MUST be
rejected in their entirety.

Section 4 of the JSON Data Interchange Format specification [RFC7159]
states "The names within an object SHOULD be unique", whereas this
specification states that "Header Parameter names within this object
MUST be unique; recipients MUST either reject JWSs with duplicate
Header Parameter names or use a JSON parser that returns only the
lexically last duplicate member name, as specified in Section 15.12
(The JSON Object) of ECMAScript 5.1 [ECMAScript]". Thus, this
specification requires that the Section 4 "SHOULD" be treated as a
"MUST" by senders and that it be either treated as a "MUST" or in the
manner specified in ECMAScript 5.1 by receivers. Ambiguous and
potentially exploitable situations could arise if the JSON parser
used does not enforce the uniqueness of member names or returns an
unpredictable value for duplicate member names.

Some JSON parsers might not reject input that contains extra
significant characters after a valid input. For instance, the input
"{"tag":"value"}ABCD" contains a valid JSON-text object followed by
the extra characters "ABCD". Such input MUST be rejected in its
entirety.

10.7. Unicode Comparison Security Considerations

Header Parameter names and algorithm names are Unicode strings. For
security reasons, the representations of these names must be compared
verbatim after performing any escape processing (as per Section 8.3
of [RFC7159]). This means, for instance, that these JSON strings
must compare as being equal ("sig", "\u0073ig"), whereas these must
all compare as being not equal to the first set or to each other
("SIG", "Sig", "si\u0047").

JSON strings can contain characters outside the Unicode Basic
Multilingual Plane. For instance, the G clef character (U+1D11E) may
be represented in a JSON string as "\uD834\uDD1E". Ideally, JWS
implementations SHOULD ensure that characters outside the Basic
Multilingual Plane are preserved and compared correctly; alternatively, if this is not possible due to these characters exercising limitations present in the underlying JSON implementation, then input containing them MUST be rejected.

11. References

11.1. Normative References


[IANA.MediaTypes]  Internet Assigned Numbers Authority (IANA), "MIME Media Types", 2005.


[JWK]  Jones, M., "JSON Web Key (JWK)", draft-ietf-jose-json-web-key (work in progress), June 2014.


11.2. Informative References


Appendix A.  JWS Examples

This section provides several examples of JWSs. While the first three examples all represent JSON Web Tokens (JWTs) [JWT], the payload can be any octet sequence, as shown in Appendix A.4.

A.1. Example JWS using HMAC SHA-256

A.1.1. Encoding

The following example JWS Protected Header declares that the data structure is a JSON Web Token (JWT) [JWT] and the JWS Signing Input is secured using the HMAC SHA-256 algorithm.

{"typ":"JWT",
 "alg":"HS256"}

To remove potential ambiguities in the representation of the JSON object above, the actual octet sequence representing UTF8(JWS Protected Header) used in this example is also included below. (Note that ambiguities can arise due to differing platform representations of line breaks (CRLF versus LF), differing spacing at the beginning
and ends of lines, whether the last line has a terminating line break or not, and other causes. In the representation used in this example, the first line has no leading or trailing spaces, a CRLF line break (13, 10) occurs between the first and second lines, the second line has one leading space (32) and no trailing spaces, and the last line does not have a terminating line break.) The octets representing UTF8(JWS Protected Header) in this example (using JSON array notation) are:

[123, 34, 116, 121, 112, 34, 58, 34, 74, 87, 84, 34, 44, 13, 10, 32, 34, 97, 108, 103, 34, 58, 34, 72, 83, 50, 53, 54, 34, 125]  

Encoding this JWS Protected Header as BASE64URL(UTF8(JWS Protected Header)) gives this value:

eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9

The JWS Payload used in this example is the octets of the UTF-8 representation of the JSON object below. (Note that the payload can be any base64url encoded octet sequence, and need not be a base64url encoded JSON object.)

{"iss":"joe",  
"exp":1300819380,  
"http://example.com/is_root":true}

The following octet sequence, which is the UTF-8 representation used in this example for the JSON object above, is the JWS Payload:


Encoding this JWS Protected Header as BASE64URL(UTF8(JWS Protected Header)) gives this value (with line breaks for display purposes only):

eyJpc3MiOiIjQjgb2U1LA0KICJjleHAI0jEzMDA4MTzkQDAsDQogImh0dHA6Ly9leGFFt  
cGxILmNvbS9pc19yb290Ijp0cnVlfoFQ

Combining these as BASE64URL(UTF8(JWS Protected Header)) || '.' || BASE64URL(JWS Payload) gives this string (with line breaks for display purposes only):

The resulting JWS Signing Input value, which is the ASCII representation of above string, is the following octet sequence (using JSON array notation):

```
```

HMACs are generated using keys. This example uses the symmetric key represented in JSON Web Key [JWK] format below (with line breaks for display purposes only):

```
{"kty":"oct",
 "k":"AyM1SysPpbyDfgZld3umj1qzKObwVMkoqQ-EstJQlr_T-lqS0gZH75
 aKtMN3Yj0iPS4hcgUuTwjAzr1Z9CAow"
}
```

Running the HMAC SHA-256 algorithm on the JWS Signing Input with this key yields this JWS Signature octet sequence:

```
```

Encoding this JWS Signature as BASE64URL(JWS Signature) gives this value:

```
dBjftJeZ4CVP-mB92K27uhbUJJUlplr_wW1gFWFOEjXk
```

Concatenating these values in the order Header.Payload.Signature with period (’.’) characters between the parts yields this complete JWS representation using the JWS Compact Serialization (with line breaks for display purposes only):

```
eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9
 .
eyJpc3MiOiJqb2UiLA0KICJ1eHAiOjEzMDA4MTkcOA0l6OdGQcm6b2Z0aW9iZASq
 cGxlMmNvbS9pct9yb290Ij00cnV1fQ
```

A.1.2. Validating

Since the "alg" Header Parameter is "HS256", we validate the HMAC SHA-256 value contained in the JWS Signature.

To validate the HMAC value, we repeat the previous process of using the correct key and the JWS Signing Input (which is the initial substring of the JWS Compact Serialization representation up until but not including the second period character) as input to the HMAC SHA-256 function and then taking the output and determining if it matches the JWS Signature (which is base64url decoded from the value encoded in the JWS representation). If it matches exactly, the HMAC has been validated.

A.2. Example JWS using RSASSA-PKCS-v1_5 SHA-256

A.2.1. Encoding

The JWS Protected Header in this example is different from the previous example in two ways: First, because a different algorithm is being used, the "alg" value is different. Second, for illustration purposes only, the optional "typ" parameter is not used. (This difference is not related to the algorithm employed.) The JWS Protected Header used is:

{"alg":"RS256"}

The octets representing UTF8(JWS Protected Header) in this example (using JSON array notation) are:

[123, 34, 97, 108, 103, 34, 58, 34, 82, 83, 50, 53, 54, 34, 125]

Encoding this JWS Protected Header as BASE64URL=UTF8(JWS Protected Header)) gives this value:

eyJhbGciOiJSUzI1NiJ9

eyJpc3MiOiJqb2UiLCJhbGciOiJIUzI1NiJ9

The JWS Payload used in this example, which follows, is the same as in the previous example. Since the BASE64URL(JWS Payload) value will therefore be the same, its computation is not repeated here.
{"iss": "joe",
"exp": 1300819380,
"http://example.com/is_root": true}

Combining these as BASE64URL(UTF8(JWS Protected Header)) || '.' || BASE64URL(JWS Payload) gives this string (with line breaks for display purposes only):

eyJhbGciOiJSUzI1NiJ9.
eyJpc3MiOiJqb2UiLCJpZCI6IjEiLCJhbGciOiJSUzI1NiJ9

The resulting JWS Signing Input value, which is the ASCII representation of above string, is the following octet sequence:


This example uses the RSA key represented in JSON Web Key [JWK] format below (with line breaks for display purposes only):

{"kty": "RSA",
"n": "ofgWCuLjybRlzo0tZWJjNiuSfb4p4fAkdxHnHQP-Vaw-4qPCJrcS2mJPMFzPlr08m4d4Q1L-yrFt-7Fd21ZS-pCgNMsD1W_YpRPEwOVg6g326990r2j247soMZOwGzjb_7QmGOLl-BSf63kpsahSXVds5z5rexMdbBYUsLA9e-KXXbDQOS-UTO77WBEa2R2capHg665xsmtDvMTBQY4uDZLvxbuq3CQoZkXh9kG4LT6rI5IhJlH7aghyxXfVuUK-DMNnouF8NACo9_hiaGNj9q2ethFkMLa91kxz2PAdCTW9gb54h4FRWyuXpoQ",
"e": "AQAB",
"d": "Eq5xpGnNCivDf1JsRQBhxlh6Rk6U1w2JHD50LpxYwFPEaP88vLNO97Ijla7_GQ5sLMqyvTeXz9S5E-7Yw6p2XNcOaJe46sui395IW_GO-pWJi100BkTGo6EnbKVRUCgu-GjBVaYLU6f319kJfFNS3EQoVbdxzubU3Mkqzjk439XOM_V51gfrPLR19jYanrC4D4qtdGcopV_02HZHzQ1BjudU2QvX4eNhNYtCBr6XClQUShbljuU01zdYoFaFQ7T5Tw8bGUL_x_Jt3ccPDVZFD9pIuhLhBOneufuBiB4cS9812SR_RQyGWSwJnczT0QU91pDhOVRuOopznQ"}

The RSA private key is then passed to the RSA signing function, which also takes the hash type, SHA-256, and the JWS Signing Input as inputs. The result of the digital signature is an octet sequence, which represents a big endian integer. In this example, it is:
Encoding the signature as BASE64URL(JWS Signature) produces this value (with line breaks for display purposes only):

cC4hiUPo9Eetdgtv3hF80EGruhB__dzERat0XF92Vqgr9PJu3XiZj5RZmh7AAuHIm4Bh-0Qc_lF5YKt_0W2Fp5jujGbd9uJdbBF9CUAR7t1dnZcAcQjkbKBYNX4BAynRFdiuB--f_n2LgrnbyTyWz075vR45h62XBarLIARNFvKs7tQB8H1b8L07qe7K0Gar2Rnm_e5N9383Lc0L6n6_0O--x1i2zjDwusC-e0kHWEsqtFZESc68f17no6Pqv
hJjphCnWh61eY12w9QOYEuiUpUTI8np6LbgGY9Fs98qrVt5AXLIhWkWylVmtVrBp0lgcN_IoypG1UPQGe77Rw

Concatenating these values in the order Header.Payload.Signature with period (‘.’) characters between the parts yields this complete JWS representation using the JWS Compact Serialization (with line breaks for display purposes only):

eyJhbGciOiJSUzI1NiJ9

eyJpc3MiOlJqbp2UIA0KICJjeHAIoEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ

cC4hiUPo9Eetdgtv3hF80EGruhB__dzERat0XF92Vqgr9PJu3XiZj5RZmh7AAuHIm4Bh-0Qc_lF5YKt_0W2Fp5jujGbd9uJdbBF9CUAR7t1dnZcAcQjkbKBYNX4BAynRFdiuB--f_n2LgrnbyTyWz075vR45h62XBarLIARNFvKs7tQB8H1b8L07qe7K0Gar2Rnm_e5N9383Lc0L6n6_0O--x1i2zjDwusC-e0kHWEsqtFZESc68f17no6Pqv
hJjphCnWh61eY12w9QOYEuiUpUTI8np6LbgGY9Fs98qrVt5AXLIhWkWylVmtVrBp0lgcN_IoypG1UPQGe77Rw
A.2.2. Validating

Since the "alg" Header Parameter is "RS256", we validate the RSASSA-PKCS-v1_5 SHA-256 digital signature contained in the JWS Signature.

Validating the JWS Signature is a bit different from the previous example. We pass the public key (n, e), the JWS Signature (which is base64url decoded from the value encoded in the JWS representation), and the JWS Signing Input (which is the initial substring of the JWS Compact Serialization representation up until but not including the second period character) to an RSASSA-PKCS-v1_5 signature verifier that has been configured to use the SHA-256 hash function.

A.3. Example JWS using ECDSA P-256 SHA-256

A.3.1. Encoding

The JWS Protected Header for this example differs from the previous example because a different algorithm is being used. The JWS Protected Header used is:

{"alg":"ES256"}

The octets representing UTF8(JWS Protected Header) in this example (using JSON array notation) are:

[123, 34, 97, 108, 103, 34, 58, 34, 69, 83, 50, 53, 54, 34, 125]

Encoding this JWS Protected Header as BASE64URL(UTF8(JWS Protected Header)) gives this value:

eyJhbGciOiJFUzI1NiJ9

The JWS Payload used in this example, which follows, is the same as in the previous examples. Since the BASE64URL(JWS Payload) value will therefore be the same, its computation is not repeated here.

{"iss":"joe",
 "exp":1300819380,
 "http://example.com/is_root":true}

Combining these as BASE64URL(UTF8(JWS Protected Header)) || '.' || BASE64URL(JWS Payload) gives this string (with line breaks for display purposes only):

eyJhbGciOiJFUzI1NiI6eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFt
The resulting JWS Signing Input value, which is the ASCII representation of above string, is the following octet sequence:

```
```

This example uses the elliptic curve key represented in JSON Web Key [JWK] format below:

```
{"kty":"EC",
 "crv":"P-256",
 "x":"f83OJ3D2xF1Bq8vub9tLe1gHMzV76e8Tu9uPHvRVEU",
 "y":"x_FEzRu9m36HLN_tue659LnpXW6pcYstikYjKIWI5a0",
 "d":"jpsQnnGqMl-YYIffH1136cspYG6-0iYf7kE9-E96K"
}
```

The ECDSA private part d is then passed to an ECDSA signing function, which also takes the curve type, P-256, the hash type, SHA-256, and the JWS Signing Input as inputs. The result of the digital signature is the EC point (R, S), where R and S are unsigned integers. In this example, the R and S values, given as octet sequences representing big endian integers are:

<table>
<thead>
<tr>
<th>Result Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>[197, 10, 7, 211, 140, 60, 112, 229, 216, 241, 45, 175, 8, 74, 84, 128, 166, 101, 144, 197, 242, 147, 80, 154, 143, 63, 127, 138, 131, 163, 84, 213]</td>
</tr>
</tbody>
</table>

The JWS Signature is the value R || S. Encoding the signature as BASE64URL(JWS Signature) produces this value (with line breaks for display purposes only):

```
DtEhU3ljbEg8L38VWAfUAQyKAM6-Xx-F4GawxaepmXFCgfTjDxw5djxLa8IS1SA
```
Concatenating these values in the order Header.Payload.Signature with period (\'\.') characters between the parts yields this complete JWS representation using the JWS Compact Serialization (with line breaks for display purposes only):

```json
eyJhbGciOiJFUzI1NiJ9.
eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFt
 cGx1LmNvbS9pc19yb290Ijp0cnVlfQ.
DtEhU3ljbEg8L38VWAfUAqOyKAM6-Xx-F4GawxaepmXFCgfTjDxw5djxLa8IS1SA
pmWQxfKTUJqPP3-Kg6NU1Q
```

### A.3.2. Validating

Since the "alg" Header Parameter is "ES256", we validate the ECDSA P-256 SHA-256 digital signature contained in the JWS Signature.

Validating the JWS Signature is a bit different from the previous examples. We need to split the 64 member octet sequence of the JWS Signature (which is base64url decoded from the value encoded in the JWS representation) into two 32 octet sequences, the first representing R and the second S. We then pass the public key (x, y), the signature (R, S), and the JWS Signing Input (which is the initial substring of the JWS Compact Serialization representation up until but not including the second period character) to an ECDSA signature verifier that has been configured to use the P-256 curve with the SHA-256 hash function.

### A.4. Example JWS using ECDSA P-521 SHA-512

#### A.4.1. Encoding

The JWS Protected Header for this example differs from the previous example because different ECDSA curves and hash functions are used. The JWS Protected Header used is:

```json
{"alg":"ES512"}
```

The octets representing UTF8(JWS Protected Header) in this example (using JSON array notation) are:

```
[123, 34, 97, 108, 103, 34, 58, 34, 69, 83, 53, 49, 50, 34, 125]
```

Encoding this JWS Protected Header as BASE64URL(UTF8(JWS Protected Header)) gives this value:
eyJhbGciOiJFUzUxMiJ9

The JWS Payload used in this example, is the ASCII string "Payload". The representation of this string is the octet sequence:

[80, 97, 121, 108, 111, 97, 100]

Encoding this JWS Payload as BASE64URL(JWS Payload) gives this value:

UGF5bG9hZA

Combining these as BASE64URL(UTF8(JWS Protected Header)) || '.' || BASE64URL(JWS Payload) gives this string (with line breaks for display purposes only):

   eyJhbGciOiJFUzUxMiJ9.UGF5bG9hZA

The resulting JWS Signing Input value, which is the ASCII representation of above string, is the following octet sequence:


This example uses the elliptic curve key represented in JSON Web Key [JWK] format below (with line breaks for display purposes only):

{"kty":"EC",
 "crv":"P-521",
 "x":"AekpBQ8ST8a8VcfVOTN1353vSrDCLLJXmPk06wTjxrrjcBpXp5EOnYG_NjJ260vLFV1jSfS9tsz4qUxcWceqwQGk",
 "y":"ADSmRA43Z1DSNhx_RvcLi187cdL0716jQyyBXMoxVg_l2Th-x3S1WdhjDly79ajL4Kkd0AZMaZmh9ubmf63e3kyMj2",
 "d":"AY5pb7A0UFIb3RELSD64fTLOSY_jazdF7fLYyuTw810fRhwG6Y6rUrPA xerEzgdRhajnu0ferB0d53vM9mEl5j2C"
}

The ECDSA private part d is then passed to an ECDSA signing function, which also takes the curve type, P-521, the hash type, SHA-512, and the JWS Signing Input as inputs. The result of the digital signature is the EC point (R, S), where R and S are unsigned integers. In this example, the R and S values, given as octet sequences representing big endian integers are:
The JWS Signature is the value R || S. Encoding the signature as BASE64URL(JWS Signature) produces this value (with line breaks for display purposes only):

```
AdwMgeerwtHoh-l192l60hp9wAHZ2VJbLfd_UxMi70cwnZOYaR1bKRW0c-mZZq
wqT2SI-KGDKB34X0aw_7XdtAG8GaSwFKdCAPZgoXD2YBZCPE3xKpRwcdO08Kp
EHwJjyqOgzDO7iKwU8vcnwNrmxYbSW9ERBlkOxoLzeO_Jn
```

Concatenating these values in the order Header.Payload.Signature with period ('.') characters between the parts yields this complete JWS representation using the JWS Compact Serialization (with line breaks for display purposes only):

```
eyJhbGciOiJFUzUxM0Yi
. UGF5bG9hZA
. AdwMgeerwtHoh-1192160hp9wAHZ2VJbLfd_UxMi70cwnZOAyR1bKRW0c-mZZq
wqT2SI-KGDKB34X0aw_7XdtAG8GaSwFKdCAPZgoXD2YBZCPE3xKpRwcdO08Kp
EHwJjyqOgzDO7iKwU8vcnwNrmxYbSW9ERBlkOxoLzeO_Jn
```

A.4.2. Validating

Since the "alg" Header Parameter is "ES512", we validate the ECDSA P-521 SHA-512 digital signature contained in the JWS Signature.

Validating this JWS Signature is very similar to the previous example. We need to split the 132 member octet sequence of the JWS Signature into two 66 octet sequences, the first representing R and the second S. We then pass the public key (x, y), the signature (R, S), and the JWS Header to the ECDSA verification function.
S), and the JWS Signing Input to an ECDSA signature verifier that has been configured to use the P-521 curve with the SHA-512 hash function.

A.5. Example Plaintext JWS

The following example JWS Protected Header declares that the encoded object is a Plaintext JWS:

```json
{"alg":"none"}
```

Encoding this JWS Protected Header as BASE64URL(UTF8(JWS Protected Header)) gives this value:

```
eyJhbGciOiJub25lIn0
```

The JWS Payload used in this example, which follows, is the same as in the previous examples. Since the BASE64URL(JWS Payload) value will therefore be the same, its computation is not repeated here.

```json
{"iss":"joe",
 "exp":1300819380,
  "http://example.com/is_root":true}
```

The JWS Signature is the empty octet string and BASE64URL(JWS Signature) is the empty string.

Concatenating these parts in the order Header.Payload.Signature with period (\'.\') characters between the parts yields this complete JWS (with line breaks for display purposes only):

```
eyJhbGciOiJub25lIn0.
eyJpc3MiOiJqb2UiLA0KICJleHAijEZMDEASMTkzODAsDQogImh0dHA6Ly91eGtccGxILmNvbS9pc19yb290Ijp0cnVlfQ.
```

A.6. Example JWS Using JWS JSON Serialization

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 JWS Payload used in this example is the same as that used in the examples in Appendix A.2 and Appendix A.3 (with line breaks for display purposes only):

```
eyJpc3MiOiJqb2UiLA0KICJleHAijEZMDEASMTkzODAsDQogImh0dHA6Ly91eGFt
cGxILmNvbS9pc19yb290Ijp0cnVlfQ
```

Two digital signatures are used in this example: the first using RSASSA-PKCS-v1_5 SHA-256 and the second using ECDSA P-256 SHA-256. For the first, the JWS Protected Header and key are the same as in Appendix A.2, resulting in the same JWS Signature value; therefore, its computation is not repeated here. For the second, the JWS Protected Header and key are the same as in Appendix A.3, resulting in the same JWS Signature value; therefore, its computation is not repeated here.

A.6.1. JWS Per-Signature Protected Headers

The JWS Protected Header value used for the first signature is:

{"alg":"RS256"}

Encoding this JWS Protected Header as BASE64URL(UTF8(JWS Protected Header)) gives this value:

eyJhbGciOiJSUzI1NiJ9

The JWS Protected Header value used for the second signature is:

{"alg":"ES256"}

Encoding this JWS Protected Header as BASE64URL(UTF8(JWS Protected Header)) gives this value:

eyJhbGciOiJFUzI1NiJ9

A.6.2. JWS Per-Signature Unprotected Headers

Key ID values are supplied for both keys using per-signature Header Parameters. The two values used to represent these Key IDs are:

{"kid":"2010-12-29"}

and

{"kid":"e9bc097a-ce51-4036-9562-d2ade882db0d"}

A.6.3. Complete JWS Header Values

Combining the protected and unprotected header values supplied, the JWS Header values used for the first and second signatures respectively are:
A.6.4. Complete JWS JSON Serialization Representation

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

```
{"payload":
 "eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ",

"signatures":
[{
  "protected": "eyJhbGciOiJSUzI1NiJ9",
  "header":
   {"kid": "2010-12-29"},
  "signature":
   "cC4hiUPoj9Eetdgtv3hF80EGrhuB__dzERat0XF9g2VtQgr9PJbu3X0i2j5RZ
   mh7AAuHIm4Bh-0Qc_lF5YKt_08W2Fp5jujGbds9uJdbF9CUAr7tldnZcAcQjbKBYNX4BAynRFdiuB--f_nZlgrnbyTyWz075vRK5h6xBArlLIARNPvksJtQBMH1l
   b1L07Qe7K0GarZrmB_eSN9383LcOLn6_d0--xil2jzDwusC-e0kHWEsqtFZES
c6BfI7noOgyhJihpCnvWh6IeY12w9QOYEUipUTI8np6LbgG1hF9Fs98rqVt5AX
   L1hWkWwylVmtVrBp0igcN_iopgL1UPQGe77Rw"},
{
  "protected": "eyJhbGciOiJFUzI1NiJ9",
  "header":
   {"kid": "e9bc097a-ce51-4036-9562-d2ade882db0d"},
  "signature":
   "DtEhU3ljbEg8l38VWAFUAqOyKAM6-Xx-F4GawxaepmXFCgfTjDxw5djhLa8IS
   1SApmWQxfKTUJqPP3-Kg6NU1Q"}
]
```

Appendix B. "x5c" (X.509 Certificate Chain) Example

The JSON array below is an example of a certificate chain that could be used as the value of an "x5c" (X.509 Certificate Chain) Header Parameter, per Section 4.1.6. Note that since these strings contain base64 encoded (not base64url encoded) values, they are allowed to contain white space and line breaks.

```
["MIIE3CCA8agAwIBAgICAwEwDQYJKBZIhvMAAqQFBo4YzELMAkGA1UEBhMCVM
   xITAfBgNVBAoTGFRoZSBHbyBEYWRkeSBHcm91cCwgSW5jLjExMC8GA1UECwMoR2
   8gKGFzZhg2Qxhc3MgM1BDXJ0aW2pY2F0aW9uIEFlgdHvcn10eTaFw0NjExMT
   YwMTU0MzdaFw0yNjExMTywMTU0MzdaMIHdMQswCQYDVQQGEwJUVzEQMA4GA1UE
```
Appendix C. Notes on implementing base64url encoding without padding

This appendix describes how to implement base64url encoding and decoding functions without padding based upon standard base64 encoding and decoding functions that do use padding.

To be concrete, example C# code implementing these functions is shown below. Similar code could be used in other languages.
As per the example code above, the number of '=' padding characters that needs to be added to the end of a base64url encoded string without padding to turn it into one with padding is a deterministic function of the length of the encoded string. Specifically, if the length mod 4 is 0, no padding is added; if the length mod 4 is 2, two '=' padding characters are added; if the length mod 4 is 3, one '=' padding character is added; if the length mod 4 is 1, the input is malformed.

An example correspondence between unencoded and encoded values follows. The octet sequence below encodes into the string below, which when decoded, reproduces the octet sequence.
3 236 255 224 193
A-z_4ME

Appendix D. Notes on Key Selection

This appendix describes a set of possible algorithms for selecting the key to be used to validate the digital signature or MAC of a JWS object or for selecting the key to be used to decrypt a JWE object. This guidance describes a family of possible algorithms, rather than a single algorithm, because in different contexts, not all the
The steps below are described for illustration purposes only; specific applications can and are likely to use different algorithms or perform some of the steps in different orders. Specific applications will frequently have a much simpler method of determining the keys to use, as there may be one or two key selection methods that are profiled for the application’s use. This appendix supplements the normative information on key location in Section 6.

These algorithms include the following steps. Note that the steps can be performed in any order and do not need to be treated as distinct. For example, keys can be tried as soon as they are found, rather than collecting all the keys before trying any.

1. Collect the set of potentially applicable keys. Sources of keys may include:

* Keys supplied by the application protocol being used.

* Keys referenced by the "jku" (JWK Set URL) Header Parameter.

* The key provided by the "jwk" (JSON Web Key) Header Parameter.

* The key referenced by the "x5u" (X.509 URL) Header Parameter.

* The key provided by the "x5c" (X.509 Certificate Chain) Header Parameter.

* Other applicable keys available to the application.

The order for collecting and trying keys from different key sources is typically application dependent. For example, frequently all keys from a one set of locations, such as local caches, will be tried before collecting and trying keys from other locations.

2. Filter the set of collected keys. For instance, some applications will use only keys referenced by "kid" (key ID) or "x5t" (X.509 certificate SHA-1 thumbprint) parameters. If the application uses the "alg" (algorithm), "use" (public key use), or "key_ops" (key operations) parameters, keys with keys with inappropriate values of those parameters would be excluded. Additionally, keys might be filtered to include or exclude keys with certain other member values in an application specific manner. For some applications, no filtering will be applied.
3. Order the set of collected keys. For instance, keys referenced by "kid" (Key ID) or "x5t" (X.509 Certificate SHA-1 Thumbprint) parameters might be tried before keys with neither of these values. Likewise, keys with certain member values might be ordered before keys with other member values. For some applications, no ordering will be applied.

4. Make trust decisions about the keys. Signatures made with keys not meeting the application’s trust criteria would not be accepted. Such criteria might include, but is not limited to the source of the key, whether the TLS certificate validates for keys retrieved from URLs, whether a key in an X.509 certificate is backed by a valid certificate chain, and other information known by the application.

5. Attempt signature or MAC validation for a JWS object or decryption of a JWE object with some or all of the collected and possibly filtered and/or ordered keys. A limit on the number of keys to be tried might be applied. This process will normally terminate following a successful validation or decryption.

Note that it is reasonable for some applications to perform signature or MAC validation prior to making a trust decision about a key, since keys for which the validation fails need no trust decision.

Appendix E. Negative Test Case for "crit" Header Parameter

Conforming implementations must reject input containing critical extensions that are not understood or cannot be processed. The following JWS must be rejected by all implementations, because it uses an extension Header Parameter name "http://example.invalid/UNDEFINED" that they do not understand. Any other similar input, in which the use of the value "http://example.invalid/UNDEFINED" is substituted for any other Header Parameter name not understood by the implementation, must also be rejected.

The JWS Protected Header value for this JWS is:

```
{"alg":"none",
 "crit":{"http://example.invalid/UNDEFINED":true
 ```
Appendix F. Detached Content

In some contexts, it is useful integrity protect content that is not itself contained in a JWS object. One way to do this is create a JWS object in the normal fashion using a representation of the content as the payload, but then delete the payload representation from the JWS, and send this modified object to the recipient, rather than the JWS. When using the JWS Compact Serialization, the deletion is accomplished by replacing the second field (which contains BASE64URL(JWS Payload)) value with the empty string; when using the JWS JSON Serialization, the deletion is accomplished by deleting the "payload" member. This method assumes that the recipient can reconstruct the exact payload used in the JWS. To use the modified object, the recipient reconstructs the JWS by re-inserting the payload representation into the modified object, and uses the resulting JWS in the usual manner. Note that this method needs no support from JWS libraries, as applications can use this method by modifying the inputs and outputs of standard JWS libraries.

Appendix G. Acknowledgements

Solutions for signing JSON content were previously explored by Magic Signatures [MagicSignatures], JSON Simple Sign [JSS], and Canvas Applications [CanvasApp], all of which influenced this draft.

Thanks to Axel Nennker for his early implementation and feedback on the JWS and JWE specifications.

This specification is the work of the JOSE Working Group, which includes dozens of active and dedicated participants. In particular, the following individuals contributed ideas, feedback, and wording that influenced this specification:

Jim Schaad and Karen O’Donoghue chaired the JOSE working group and Sean Turner, Stephen Farrell, and Kathleen Moriarty served as Security area directors during the creation of this specification.

Appendix H. Document History

-28

o Revised the introduction to the Security Considerations section. Also introduced additional subsection headings for security considerations items and also moved a security consideration item here from the JWA draft.

o Added text about when applications typically would and would not use "typ" and "cty" header parameters.

-27

o Added the "x5t#S256" (X.509 Certificate SHA-256 Thumbprint) header parameter.

o Stated that any JSON inputs not conforming to the JSON-text syntax defined in RFC 7159 input MUST be rejected in their entirety.

o Simplified the TLS requirements.

-26

o Referenced Section 6 of RFC 6125 for TLS server certificate identity validation.

o Described potential sources of ambiguity in representing the JSON objects used in the examples. The octets of the actual UTF-8 representations of the JSON objects used in the examples are included to remove these ambiguities.

o Added a small amount of additional explanatory text to the signature validation examples to aid implementers.

o Noted that octet sequences are depicted using JSON array notation.

o Updated references, including to W3C specifications.

-25
No changes were made, other than to the version number and date.

-24

-23

-22

-21

-20

-19
- Reordered the key selection parameters.
- Updated the mandatory-to-implement (MTI) language to say that applications using this specification need to specify what serialization and serialization features are used for that application, addressing issue #119.
- Changes to address editorial and minor issues #25, #89, #97, #110, #114, #115, #116, #117, #120, and #184.
- Added and used Header Parameter Description registry field.
- Refined the "typ" and "cty" definitions to always be MIME Media Types, with the omission of "application/" prefixes recommended for brevity, addressing issue #50.
- Updated the mandatory-to-implement (MTI) language to say that general-purpose implementations must implement the single signature/MAC value case for both serializations whereas special-purpose implementations can implement just one serialization if that meets the needs of the use cases the implementation is designed for, addressing issue #119.
- Explicitly named all the logical components of a JWS and defined the processing rules and serializations in terms of those components, addressing issues #60, #61, and #62.
- Replaced verbose repetitive phases such as "base64url encode the octets of the UTF-8 representation of X" with mathematical notation such as "BASE64URL(UTF8(X))".
- Terms used in multiple documents are now defined in one place and incorporated by reference. Some lightly used or obvious terms were also removed. This addresses issue #58.
- Changes to address editorial and minor issues #50, #98, #99, #102, #104, #106, #107, #111, and #112.
- Clarified that it is an application decision which signatures, MACs, or plaintext values must successfully validate for the JWS
to be accepted, addressing issue #35.

- Corrected editorial error in "ES512" example.

- Changes to address editorial and minor issues #34, #96, #100, #101, #104, #105, and #106.

- Stated that the "signature" parameter is to be omitted in the JWS JSON Serialization when its value would be empty (which is only the case for a Plaintext JWS).

- Made all header parameter values be per-signature/MAC, addressing issue #24.

- Clarified that the "typ" and "cty" header parameters are used in an application-specific manner and have no effect upon the JWS processing.

- Replaced the MIME types "application/jws+json" and "application/jws" with "application/jose+json" and "application/jose".

- Stated that recipients MUST either reject JWSs with duplicate Header Parameter Names or use a JSON parser that returns only the lexically last duplicate member name.

- Added a Serializations section with parallel treatment of the JWS Compact Serialization and the JWS JSON Serialization and also moved the former Implementation Considerations content there.

- Added Key Identification section.

- For the JWS JSON Serialization, enable header parameter values to be specified in any of three parameters: the "protected" member that is integrity protected and shared among all recipients, the "unprotected" member that is not integrity protected and shared among all recipients, and the "header" member that is not integrity protected and specific to a particular recipient. (This does not affect the JWS Compact Serialization, in which all header parameter values are in a single integrity protected JWE Header
value.)

- Removed suggested compact serialization for multiple digital signatures and/or MACs.
- Changed the MIME type name "application/jws-js" to "application/jws+json", addressing issue #22.
- Tightened the description of the "crit" (critical) header parameter.
- Added a negative test case for the "crit" header parameter

- Added an appendix suggesting a possible compact serialization for JWSs with multiple digital signatures and/or MACs.

- Added JWS JSON Serialization, as specified by draft-jones-jose-jws-json-serialization-04.
- Registered "application/jws-js" MIME type and "JWS-JS" typ header parameter value.
- Defined that the default action for header parameters that are not understood is to ignore them unless specifically designated as "MUST be understood" or included in the new "crit" (critical) header parameter list. This addressed issue #6.
- Changed term "JWS Secured Input" to "JWS Signing Input".
- Changed from using the term "byte" to "octet" when referring to 8 bit values.
- Changed member name from "recipients" to "signatures" in the JWS JSON Serialization.
- Added complete values using the JWS Compact Serialization for all examples.

- Applied editorial improvements suggested by Jeff Hodges and Hannes Tschofenig. Many of these simplified the terminology used.
o Clarified statements of the form "This header parameter is OPTIONAL" to "Use of this header parameter is OPTIONAL".

o Added a Header Parameter Usage Location(s) field to the IANA JSON Web Signature and Encryption Header Parameters registry.

o Added seriesInfo information to Internet Draft references.

-07

o Updated references.

-06

o Changed "x5c" (X.509 Certificate Chain) representation from being a single string to being an array of strings, each containing a single base64 encoded DER certificate value, representing elements of the certificate chain.

o Applied changes made by the RFC Editor to RFC 6749’s registry language to this specification.

-05

o Added statement that "StringOrURI values are compared as case-sensitive strings with no transformations or canonicalizations applied".

o Indented artwork elements to better distinguish them from the body text.

-04

o Completed JSON Security Considerations section, including considerations about rejecting input with duplicate member names.

o Completed security considerations on the use of a SHA-1 hash when computing "x5t" (x.509 certificate thumbprint) values.

o Refer to the registries as the primary sources of defined values and then secondarily reference the sections defining the initial contents of the registries.

o Normatively reference XML DSIG 2.0 for its security considerations.

o Added this language to Registration Templates: "This name is case sensitive. Names that match other registered names in a case
insensitive manner SHOULD NOT be accepted."

- Reference draft-jones-jose-jws-json-serialization instead of
draft-jones-json-web-signature-json-serialization.

- Described additional open issues.

- Applied editorial suggestions.

-03

- Added the "cty" (content type) header parameter for declaring type
information about the secured content, as opposed to the "typ"
(type) header parameter, which declares type information about
this object.

- Added "Collision Resistant Namespace" to the terminology section.

- Reference ITU.X690.1994 for DER encoding.

- Added an example JWS using ECDSA P-521 SHA-512. This has
particular illustrative value because of the use of the 521 bit
integers in the key and signature values. This is also an example
in which the payload is not a base64url encoded JSON object.

- Added an example "x5c" value.

- No longer say "the UTF-8 representation of the JWS Secured Input
(which is the same as the ASCII representation)". Just call it
"the ASCII representation of the JWS Secured Input".

- Added Registration Template sections for defined registries.

- Added Registry Contents sections to populate registry values.

- Changed name of the JSON Web Signature and Encryption "typ" Values
registry to be the JSON Web Signature and Encryption Type Values
registry, since it is used for more than just values of the "typ"
parameter.

- Moved registries JSON Web Signature and Encryption Header
Parameters and JSON Web Signature and Encryption Type Values to
the JWS specification.

- Numerous editorial improvements.

-02
o Clarified that it is an error when a "kid" value is included and no matching key is found.

o Removed assumption that "kid" (key ID) can only refer to an asymmetric key.

o Clarified that JWSs with duplicate Header Parameter Names MUST be rejected.

o Clarified the relationship between "typ" header parameter values and MIME types.

o Registered application/jws MIME type and "JWS" typ header parameter value.

o Simplified JWK terminology to get replace the "JWK Key Object" and "JWK Container Object" terms with simply "JSON Web Key (JWK)" and "JSON Web Key Set (JWK Set)" and to eliminate potential confusion between single keys and sets of keys. As part of this change, the Header Parameter Name for a public key value was changed from "jpk" (JSON Public Key) to "jwk" (JSON Web Key).

o Added suggestion on defining additional header parameters such as "x5t#S256" in the future for certificate thumbprints using hash algorithms other than SHA-1.

o Specify RFC 2818 server identity validation, rather than RFC 6125 (paralleling the same decision in the OAuth specs).

o Generalized language to refer to Message Authentication Codes (MACs) rather than Hash-based Message Authentication Codes (HMACs) unless in a context specific to HMAC algorithms.

o Reformatted to give each header parameter its own section heading.

-01

o Moved definition of Plaintext JWSs (using "alg":"none") here from the JWT specification since this functionality is likely to be useful in more contexts that just for JWTs.

o Added "jpk" and "x5c" header parameters for including JWK public keys and X.509 certificate chains directly in the header.

o Clarified that this specification is defining the JWS Compact Serialization. Referenced the new JWS-JS spec, which defines the JWS JSON Serialization.
o Added text "New header parameters should be introduced sparingly since an implementation that does not understand a parameter MUST reject the JWS".

o Clarified that the order of the creation and validation steps is not significant in cases where there are no dependencies between the inputs and outputs of the steps.

o Changed "no canonicalization is performed" to "no canonicalization need be performed".

o Corrected the Magic Signatures reference.

o Made other editorial improvements suggested by JOSE working group participants.

-00

o Created the initial IETF draft based upon draft-jones-json-web-signature-04 with no normative changes.

o Changed terminology to no longer call both digital signatures and HMACs "signatures".

Authors' Addresses

Michael B. Jones
Microsoft

Email: mbj@microsoft.com
URI: http://self-issued.info/

John Bradley
Ping Identity

Email: ve7jtb@ve7jtb.com
URI: http://www.thread-safe.com/

Nat Sakimura
Nomura Research Institute

Email: n-sakimura@nri.co.jp
URI: http://nat.sakimura.org/