JSON Web Encryption (JWE)
draft-ietf-jose-json-web-encryption-20

Abstract

JSON Web Encryption (JWE) represents encrypted content 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 IANA registries defined by that specification. Related digital signature and MAC capabilities are described in the separate JSON Web Signature (JWS) 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 July 24, 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. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction
   1.1. Notational Conventions
2. Terminology
3. JSON Web Encryption (JWE) Overview
   3.1. Example JWE
4. JWE Header
   4.1. Registered Header Parameter Names
       4.1.1. "alg" (Algorithm) Header Parameter
       4.1.2. "enc" (Encryption Algorithm) Header Parameter
       4.1.3. "zip" (Compression Algorithm) Header Parameter
4.1.3. "zip" (Compression Algorithm) Header Parameter
4.1.4. "jku" (JWK Set URL) Header Parameter
4.1.5. "jwk" (JSON Web Key) Header Parameter
4.1.6. "kid" (Key ID) Header Parameter
4.1.7. "x5u" (X.509 URL) Header Parameter
4.1.8. "x5c" (X.509 Certificate Chain) Header Parameter
4.1.9. "x5t" (X.509 Certificate SHA-1 Thumbprint) Header Parameter
4.1.10. "typ" (Type) Header Parameter
4.1.11. "cty" (Content Type) Header Parameter
4.1.12. "crit" (Critical) Header Parameter

4.2. Public Header Parameter Names
4.3. Private Header Parameter Names

5. Producing and Consuming JWEs
5.1. Message Encryption
5.2. Message Decryption
5.3. String Comparison Rules

6. Key Identification

7. Serializations
7.1. JWE Compact Serialization
7.2. JWE JSON Serialization

8. TLS Requirements

9. Distinguishing between JWS and JWE Objects

10. IANA Considerations
10.1. JSON Web Signature and Encryption Header Parameters Registration
10.1.1. Registry Contents

11. Security Considerations
12. References
12.1. Normative References
12.2. Informative References

Appendix A. JWE Examples
A.1. Example JWE using RSAES OAEP and AES GCM
A.1.1. JWE Header
A.1.2. Content Encryption Key (CEK)
A.1.3. Key Encryption
A.1.4. Initialization Vector
A.1.5. Additional Authenticated Data
A.1.6. Content Encryption
A.1.7. Complete Representation
A.1.8. Validation

A.2. Example JWE using RSAES-PKCS1-V1_5 and AES_128_CBC_HMAC_SHA_256
A.2.1. JWE Header
A.2.2. Content Encryption Key (CEK)
A.2.3. Key Encryption
A.2.4. Initialization Vector
A.2.5. Additional Authenticated Data
A.2.6. Content Encryption
A.2.7. Complete Representation
A.2.8. Validation

A.3. Example JWE using AES Key Wrap and AES_128_CBC_HMAC_SHA_256
A.3.1. JWE Header
A.3.2. Content Encryption Key (CEK)
A.3.3. Key Encryption
A.3.4. Initialization Vector
A.3.5. Additional Authenticated Data
A.3.6. Content Encryption
A.3.7. Complete Representation
A.3.8. Validation

A.4. Example JWE using JWE JSON Serialization
A.4.1. JWE Per-Recipient Unprotected Headers
A.4.2. JWE Protected Header
A.4.3. JWE Unprotected Header
A.4.4. Complete JWE Header Values
A.4.5. Additional Authenticated Data
A.4.6. Content Encryption
A.4.7. Complete JWE JSON Serialization Representation

Appendix B. Example AES_128_CBC_HMAC_SHA_256 Computation
B.1. Extract MAC_KEY and ENC_KEY from Key
B.2. Encrypt Plaintext to Create Ciphertext
1. Introduction

JSON Web Encryption (JWE) represents encrypted content using JavaScript Object Notation (JSON) [I-D.ietf-json-rfc4627bis] based data structures. The JWE cryptographic mechanisms encrypt and provide integrity protection for an arbitrary sequence of octets.

Two closely related serializations for JWE objects are defined. The JWE Compact Serialization is a compact, URL-safe representation intended for space constrained environments such as HTTP Authorization headers and URI query parameters. The JWE JSON Serialization represents JWE objects as JSON objects and enables the same content to be encrypted to multiple parties. 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 IANA registries defined by that specification. Related digital signature and MAC capabilities are described in the separate JSON Web Signature (JWS) [JWS] 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", "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

These terms defined by the JSON Web Signature (JWS) [JWS] specification are incorporated into this specification: "JSON Web Signature (JWS)", "Base64url Encoding", "Collision-Resistant Name", and "StringOrURI".

These terms are defined for use by this specification:

JSON Web Encryption (JWE)
A data structure representing an encrypted and integrity protected message.

Authenticated Encryption with Associated Data (AEAD)
An AEAD algorithm is one that encrypts the Plaintext, allows Additional Authenticated Data to be specified, and provides an integrated content integrity check over the Ciphertext and Additional Authenticated Data. AEAD algorithms accept two inputs, the Plaintext and the Additional Authenticity Data value, and
produce two outputs, the Ciphertext and the Authentication Tag value. AES Galois/Counter Mode (GCM) is one such algorithm.

Plaintext
The sequence of octets to be encrypted -- a.k.a., the message. The plaintext can contain an arbitrary sequence of octets.

Ciphertext
An encrypted representation of the Plaintext.

Additional Authenticated Data (AAD)
An input to an AEAD operation that is integrity protected but not encrypted.

Authentication Tag
An output of an AEAD operation that ensures the integrity of the Ciphertext and the Additional Authenticated Data. Note that some algorithms may not use an Authentication Tag, in which case this value is the empty octet sequence.

Content Encryption Key (CEK)
A symmetric key for the AEAD algorithm used to encrypt the Plaintext for the recipient to produce the Ciphertext and the Authentication Tag.

JWE Header
JSON object containing the parameters describing the cryptographic operations and parameters employed. The JWE Header members are the union of the members of the JWE Protected Header, the JWE Shared Unprotected Header, and the JWE Per-Recipient Unprotected Header. The members of the JWE Header are Header Parameters.

JWE Encrypted Key
Encrypted Content Encryption Key (CEK) value. Note that for some algorithms, the JWE Encrypted Key value is specified as being the empty octet sequence.

JWE Initialization Vector
Initialization Vector value used when encrypting the plaintext. Note that some algorithms may not use an Initialization Vector, in which case this value is the empty octet sequence.

JWE AAD
Additional value to be integrity protected by the authenticated encryption operation. This can only be present when using the JWE JSON Serialization.

JWE Ciphertext
Ciphertext value resulting from authenticated encryption of the plaintext with additional associated data.

JWE Authentication Tag
Authentication Tag value resulting from authenticated encryption of the plaintext with additional associated data.

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

JWE Protected Header
JSON object that contains the JWE Header Parameters that are integrity protected by the authenticated encryption operation. These parameters apply to all recipients of the JWE. For the JWE Compact Serialization, this comprises the entire JWE Header. For the JWE JSON Serialization, this is one component of the JWE Header.

JWE Shared Unprotected Header
JSON object that contains the JWE Header Parameters that apply to all recipients of the JWE that are not integrity protected. This can only be present when using the JWE JSON Serialization.

JWE Per-Recipient Unprotected Header
JSON object that contains JWE Header Parameters that apply to a single recipient of the JWE. This value is not integrity protected. This can only be present when using the JWE JSON Serialization.

JWE Compact Serialization
A representation of the JWE as a compact, URL-safe string.

JWE JSON Serialization
A representation of the JWE as a JSON object. The JWE JSON Serialization enables the same content to be encrypted to multiple parties. This representation is neither optimized for compactness nor URL-safe.

Key Management Mode
A method of determining the Content Encryption Key (CEK) value to use. Each algorithm used for determining the CEK value uses a specific Key Management Mode. Key Management Modes employed by this specification are Key Encryption, Key Wrapping, Direct Key Agreement, Key Agreement with Key Wrapping, and Direct Encryption.

Key Encryption
A Key Management Mode in which the Content Encryption Key (CEK) value is
3. JSON Web Encryption (JWE) Overview

JWE represents encrypted content using JSON data structures and base64url encoding. A JWE represents these logical values:

- **JWE Header**
  JSON object containing the parameters describing the cryptographic operations and parameters employed. The JWE Header members are the union of the members of the JWE Protected Header, the JWE Shared Unprotected Header, and the JWE Per-Recipient Unprotected Header, as described below.

- **JWE Encrypted Key**
  Encrypted Content Encryption Key (CEK) value.

- **JWE Initialization Vector**
  Initialization Vector value used when encrypting the plaintext.

- **JWE AAD**
  Additional value to be integrity protected by the authenticated encryption operation.

- **JWE Ciphertext**
  Ciphertext value resulting from authenticated encryption of the plaintext with additional associated data.

- **JWE Authentication Tag**
  Authentication Tag value resulting from authenticated encryption of the plaintext with additional associated data.

The JWE Header represents the combination of these logical values:

- **JWE Protected Header**
  JSON object that contains the JWE Header Parameters that are integrity protected by the authenticated encryption operation. These parameters apply to all recipients of the JWE.

- **JWE Shared Unprotected Header**
  JSON object that contains the JWE Header Parameters that apply to all recipients of the JWE that are not integrity protected.

- **JWE Per-Recipient Unprotected Header**
  JSON object that contains JWE Header Parameters that apply to a single recipient of the JWE. This value is not integrity protected.

This document defines two serializations for JWE objects: a compact, URL-safe serialization called the JWE Compact Serialization and a JSON serialization called the JWE JSON Serialization. In both serializations, the JWE Protected Header, JWE Encrypted Key, JWE Initialization Vector, JWE Ciphertext, and JWE Authentication Tag are base64url encoded for transmission, since JSON lacks a way to directly represent octet sequences. When present, the JWE AAD is also base64url encoded for transmission.

In the JWE Compact Serialization, no JWE Shared Unprotected Header or JWE Per-Recipient Unprotected Header are used. In this case, the JWE Header and the JWE Protected Header are the same.

In the JWE Compact Serialization, a JWE object is represented as the combination of these five string values,
BASE64URL(UTF8(JWE Protected Header)),
BASE64URL(JWE Encrypted Key),
BASE64URL(JWE Initialization Vector),
BASE64URL(JWE Ciphertext), and
BASE64URL(JWE Authentication Tag),
concatenated in that order, with the five strings being separated by four period ('.') characters.

In the JWE JSON Serialization, one or more of the JWE Protected Header, JWE Shared Unprotected Header, and JWE Per-Recipient Unprotected Header MUST be present. In this case, the members of the JWE Header are the combination of the members of the JWE Protected Header, JWE Shared Unprotected Header, and JWE Per-Recipient Unprotected Header values that are present.

In the JWE JSON Serialization, a JWE object is represented as the combination of these eight values,

   BASE64URL(UTF8(JWE Protected Header)),
   JWE Shared Unprotected Header,
   JWE Per-Recipient Unprotected Header,
   BASE64URL(JWE Encrypted Key),
   BASE64URL(JWE Initialization Vector),
   BASE64URL(JWE Ciphertext),
   BASE64URL(JWE Authentication Tag), and
   BASE64URL(JWE AAD),

with the six base64url encoding result strings and the two unprotected JSON object values being represented as members within a JSON object. The inclusion of some of these values is OPTIONAL. The JWE JSON Serialization can also encrypt the plaintext to multiple recipients. See Section 7.2 for more information about the JWE JSON Serialization.

JWE utilizes authenticated encryption to ensure the confidentiality and integrity of the Plaintext and the integrity of the JWE Protected Header and the JWE AAD.

### 3.1. Example JWE

This example encrypts the plaintext "The true sign of intelligence is not knowledge but imagination." to the recipient using RSAES OAEP for key encryption and AES GCM for content encryption.

The following example JWE Protected Header declares that:

- the Content Encryption Key is encrypted to the recipient using the RSAES OAEP algorithm to produce the JWE Encrypted Key and
- the Plaintext is encrypted using the AES GCM algorithm with a 256 bit key to produce the Ciphertext.

```json
{"alg":"RSA-OAEP", "enc":"A256GCM"}
```

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

```text
eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkEyNTZHQ00ifQ
```

```text
eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkEyNTZHQ00ifQ
```
The remaining steps to finish creating this JWE are:

- Generate a random Content Encryption Key (CEK).
- Encrypt the CEK with the recipient's public key using the RSAES OAEP algorithm to produce the JWE Encrypted Key.
- Base64url encode the JWE Encrypted Key.
- Generate a random JWE Initialization Vector.
- Base64url encode the JWE Initialization Vector.
- Let the Additional Authenticated Data encryption parameter be ASCII(BASE64URL(UTF8(JWE Protected Header))).
- Encrypt the Plaintext with AES GCM using the CEK as the encryption key, the JWE Initialization Vector, and the Additional Authenticated Data value, requesting a 128 bit Authentication Tag output.
- Base64url encode the Ciphertext.
- Base64url encode the Authentication Tag.
- Assemble the final representation: The Compact Serialization of this result is the string BASE64URL(UTF8(JWE Protected Header)) || '.' || BASE64URL(JWE Encrypted Key) || '.' || BASE64URL(JWE Initialization Vector) || '.' || BASE64URL(JWE Ciphertext) || '.' || BASE64URL(JWE Authentication Tag).

The final result in this example (with line breaks for display purposes only) is:

eyJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkEyNTZHQ00ifQ.
OKOawDo13gRp2ojahV7LFpZcgv776DVZktyKOMTYUmRoTCJvJRgckCL9kiMT03JGe
ipsEdy3mx_etlLbW5rFr05kLczSr4qKaq7YN7e9wQRb3nfa6c9d-StrImEYFDb
Sw04uVuxIpe5zm1gNXXKDKa14B8S4rzvRltdYwam_1dp5xZAyPqdb766dIkLaV
mqgfwX7XwR7v23221-vDxRfQnzO_tETKzpyLzfiwyQeyPGBLI056Y7e0bdv0je8
1860pamavovo35ugoRdByaBcoh9QcylyQr66oc6vFXRcZ_ZT2La5WCWTIy3br6P1
6u1kflcpIMfIj71GdXXHzg.
48V1_ALb6US94U3b.
5eym8rW_c8SuK8ltJ3rpYIz0eDQz7TALvtu6UG9oMo4vpzs9tX_EFShtS81B7j6ji
SdiwkIr3ajqw2aBtQqD_A.
XFB0MYUZodetZdvTlFvSkQ

See Appendix A.1 for the complete details of computing this JWE. See other parts of Appendix A for additional examples.

4. JWE Header

The members of the JSON object(s) representing the JWE Header describe the encryption applied to the Plaintext and optionally additional properties of the JWE. The Header Parameter names within the JWE Header MUST be unique; recipients MUST either reject JWEs 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.

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 4.1.12, 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
The following Header Parameter names are registered in the IANA JSON Web Signature and Encryption Header Parameters registry defined in [JWS], 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

This parameter has the same meaning, syntax, and processing rules as the alg Header Parameter defined in Section 4.1.1 of [JWS], except that the Header Parameter identifies the cryptographic algorithm used to encrypt or determine the value of the Content Encryption Key (CEK). The encrypted content is not usable if the alg value does not represent a supported algorithm, or if the recipient does not have a key that can be used with that algorithm.

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 4.1 of the JSON Web Algorithms (JWA) [JWA] specification.

### 4.1.2. "enc" (Encryption Algorithm) Header Parameter

The enc (encryption algorithm) Header Parameter identifies the content encryption algorithm used to encrypt the Plaintext to produce the Ciphertext. This algorithm MUST be an AEAD algorithm with a specified key length. The recipient MUST reject the JWE if the enc value does not represent a supported algorithm. enc 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 enc 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 enc 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 5.1 of the JSON Web Algorithms (JWA) [JWA] specification.

### 4.1.3. "zip" (Compression Algorithm) Header Parameter

The zip (compression algorithm) applied to the Plaintext before encryption, if any. The zip value defined by this specification is:

- DEF - Compression with the DEFLATE [RFC1951] algorithm

Other values MAY be used. Compression algorithm values can be registered in the IANA JSON Web Encryption Compression Algorithm registry defined in [JWA]. The zip value is a case-sensitive string. If no zip parameter is present, no compression is applied to the Plaintext before encryption. This Header Parameter MUST be integrity protected, and therefore MUST occur only within the JWE Protected Header, when used. Use of this Header Parameter is OPTIONAL. This Header Parameter MUST be understood and processed by implementations.

### 4.1.4. "jku" (JWK Set URL) Header Parameter

This parameter has the same meaning, syntax, and processing rules as the jku Header Parameter defined in Section 4.1.2 of [JWS], except that the JWK Set resource contains the public key to which the JWE was encrypted; this can be used to determine the private key needed to decrypt the JWE.
4.1.5. "jwk" (JSON Web Key) Header Parameter

This parameter has the same meaning, syntax, and processing rules as the jwk Header Parameter defined in Section 4.1.3 of [JWS], except that the key is the public key to which the JWE was encrypted; this can be used to determine the private key needed to decrypt the JWE.

4.1.6. "kid" (Key ID) Header Parameter

This parameter has the same meaning, syntax, and processing rules as the kid Header Parameter defined in Section 4.1.4 of [JWS], except that the key hint references the public key to which the JWE was encrypted; this can be used to determine the private key needed to decrypt the JWE. This parameter allows originators to explicitly signal a change of key to JWE recipients.

4.1.7. "x5u" (X.509 URL) Header Parameter

This parameter has the same meaning, syntax, and processing rules as the x5u Header Parameter defined in Section 4.1.5 of [JWS], except that the X.509 public key certificate or certificate chain [RFC5280] contains the public key to which the JWE was encrypted; this can be used to determine the private key needed to decrypt the JWE.

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

This parameter has the same meaning, syntax, and processing rules as the x5c Header Parameter defined in Section 4.1.6 of [JWS], except that the X.509 public key certificate or certificate chain [RFC5280] contains the public key to which the JWE was encrypted; this can be used to determine the private key needed to decrypt the JWE.

See Appendix B of [JWS] for an example x5c value.

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

This parameter has the same meaning, syntax, and processing rules as the x5t Header Parameter defined in Section 4.1.7 of [JWS], except that certificate referenced by the thumbprint contains the public key to which the JWE was encrypted; this can be used to determine the private key needed to decrypt the JWE.

4.1.10. "typ" (Type) Header Parameter

This parameter has the same meaning, syntax, and processing rules as the typ Header Parameter defined in Section 4.1.8 of [JWS], except that the type is of this complete JWE object.

4.1.11. "cty" (Content Type) Header Parameter

This parameter has the same meaning, syntax, and processing rules as the cty Header Parameter defined in Section 4.1.9 of [JWS], except that the type is of the secured content (the payload).
4.1.12. "crit" (Critical) Header Parameter

This parameter has the same meaning, syntax, and processing rules as the crit Header Parameter defined in Section 4.1.10 of [JWS], except that JWE Header Parameters are being referred to, rather than JWS Header Parameters.

4.2. Public Header Parameter Names

Additional Header Parameter names can be defined by those using JWEs. 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 [JWS] 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 JWEs.

4.3. Private Header Parameter Names

A producer and consumer of a JWE 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 JWEs

5.1. Message Encryption

The message encryption process is as follows. The order of the steps is not significant in cases where there are no dependencies between the inputs and outputs of the steps.

1. Determine the Key Management Mode employed by the algorithm used to determine the Content Encryption Key (CEK) value. (This is the algorithm recorded in the alg (algorithm) Header Parameter of the resulting JWE.)
2. When Key Wrapping, Key Encryption, or Key Agreement with Key Wrapping are employed, generate a random Content Encryption Key (CEK) value. See RFC 4086 [RFC4086] for considerations on generating random values. The CEK MUST have a length equal to that required for the content encryption algorithm.
3. When Direct Key Agreement or Key Agreement with Key Wrapping are employed, use the key agreement algorithm to compute the value of the agreed upon key. When Direct Key Agreement is employed, let the Content Encryption Key (CEK) be the agreed upon key. When Key Agreement with Key Wrapping is employed, the agreed upon key will be used to wrap the CEK.
4. When Key Wrapping, Key Encryption, or Key Agreement with Key Wrapping are employed, encrypt the CEK to the recipient and let the result be the JWE Encrypted Key.
5. When Direct Key Agreement or Direct Encryption are employed, let the JWE Encrypted Key be the empty octet sequence.
6. When Direct Encryption is employed, let the Content Encryption Key (CEK) be the shared symmetric key.
7. Compute the encoded key value BASE64URL(JWE Encrypted Key).
8. If the JWE JSON Serialization is being used, repeat this process (steps 1-7) for
9. Generate a random JWE Initialization Vector of the correct size for the content encryption algorithm (if required for the algorithm); otherwise, let the JWE Initialization Vector be the empty octet sequence.

10. Compute the encoded initialization vector value BASE64URL(JWE Initialization Vector).

11. If a zip parameter was included, compress the Plaintext using the specified compression algorithm.

12. Serialize the (compressed) Plaintext into an octet sequence M.

13. Create the JSON object(s) containing the desired set of Header Parameters, which together comprise the JWE Header: the JWE Protected Header, and if the JWE JSON Serialization is being used, the JWE Shared Unprotected Header and the JWE Per-Recipient Unprotected Header.

14. Compute the Encoded Protected Header value BASE64URLUTF8(JWE Protected Header). If the JWE Protected Header is not present (which can only happen when using the JWE JSON Serialization and no protected member is present), let this value be the empty string.

15. Let the Additional Authenticated Data encryption parameter be ASCII(Encoded Protected Header). However if a JWE AAD value is present (which can only be the case when using the JWE JSON Serialization), instead let the Additional Authenticated Data encryption parameter be ASCII(Encoded Protected Header || '.' || BASE64URL(JWE AAD)).

16. Encrypt M using the CEK, the JWE Initialization Vector, and the Additional Authenticated Data value using the specified content encryption algorithm to create the JWE Ciphertext value and the JWE Authentication Tag (which is the Authentication Tag output from the encryption operation).

17. Compute the encoded ciphertext value BASE64URL(JWE Ciphertext).

18. Compute the encoded authentication tag value BASE64URL(JWE Authentication Tag).

19. The five encoded values are used in both the JWE Compact Serialization and the JWE JSON Serialization representations.

20. If a JWE AAD value is present, compute the encoded AAD value BASE64URL(JWE AAD).

21. Create the desired serialized output. The Compact Serialization of this result is the string BASE64URLUTF8(JWE Protected Header) || '.' || BASE64URL(JWE Encrypted Key) || '.' || BASE64URL(JWE Initialization Vector) || '.' || BASE64URL(JWE Ciphertext) || '.' || BASE64URL(JWE Authentication Tag). The JWE JSON Serialization is described in Section 7.2.

5.2. Message Decryption

The message decryption process is the reverse of the encryption process. 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 these steps fails, the encrypted content cannot be validated.

It is an application decision which recipients' encrypted content must successfully validate for the JWE to be accepted. In some cases, encrypted content for all recipients must successfully validate or the JWE will be rejected. In other cases, only the encrypted content for a single recipient needs to be successfully validated. However, in all cases, the encrypted content for at least one recipient MUST successfully validate or the JWE MUST be rejected.

1. Parse the JWE representation to extract the serialized values for the components of the JWE - when using the JWE Compact Serialization, the base64url encoded representations of the JWE Protected Header, the JWE Encrypted Key, the JWE Initialization Vector, the JWE Ciphertext, and the JWE Authentication Tag, and when using the JWE JSON Serialization, also the base64url encoded representation of the JWE AAD and the unencoded JWE Shared Unprotected Header and JWE Per-Recipient Unprotected Header values. When using the JWE Compact Serialization, the JWE Protected Header, the JWE Encrypted Key, the JWE Initialization Vector, the JWE Ciphertext, and the JWE Authentication Tag are represented as base64url encoded values in that order, separated by four period ('.') characters. The JWE JSON Serialization is described in Section 7.2.

2. The encoded representations of the JWE Protected Header, the JWE Encrypted Key, the JWE Initialization Vector, the JWE Ciphertext, the JWE Authentication Tag, and the JWE AAD MUST be successfully base64url decoded following the
3. The octet sequence resulting from decoding the encoded JWE Protected Header MUST be a UTF-8 encoded representation of a completely valid JSON object conforming to [I-D.ietf-json-rfc4627bis], which is the JWE Protected Header.
4. If using the JWE Compact Serialization, let the JWE Header be the JWE Protected Header; otherwise, when using the JWE JSON Serialization, let the JWE Header be the union of the members of the JWE Protected Header, the JWE Shared Unprotected Header and the corresponding JWE Per-Recipient Unprotected Header, all of which must be completely valid JSON objects.
5. The resulting JWE Header MUST NOT contain duplicate Header Parameter names. When using the JWE JSON Serialization, this restriction includes that the same Header Parameter name also MUST NOT occur in distinct JSON object values that together comprise the JWE 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 algorithms being used, or by the crit Header Parameter value, and that the values of those parameters are also understood and supported.
7. Determine the Key Management Mode employed by the algorithm specified by the alg (algorithm) Header Parameter.
8. Verify that the JWE uses a key known to the recipient.
9. When Direct Key Agreement or Key Agreement with Key Wrapping are employed, use the key agreement algorithm to compute the value of the agreed upon key. When Direct Key Agreement is employed, let the Content Encryption Key (CEK) be the agreed upon key. When Key Agreement with Key Wrapping is employed, the agreed upon key will be used to decrypt the JWE Encrypted Key.
10. When Key Wrapping, Key Encryption, or Key Agreement with Key Wrapping are employed, decrypt the JWE Encrypted Key to produce the Content Encryption Key (CEK). The CEK MUST have a length equal to that required for the content encryption algorithm. Note that when there are multiple recipients, each recipient will only be able decrypt any JWE Encrypted Key values that were encrypted to a key in that recipient's possession. It is therefore normal to only be able to decrypt one of the per-recipient JWE Encrypted Key values to obtain the CEK value. To mitigate the attacks described in RFC 3218 [RFC3218], the recipient MUST NOT distinguish between format, padding, and length errors of encrypted keys. It is strongly recommended, in the event of receiving an improperly formatted key, that the receiver substitute a randomly generated CEK and proceed to the next step, to mitigate timing attacks.
11. When Direct Key Agreement or Direct Encryption are employed, verify that the JWE Encrypted Key value is empty octet sequence.
12. When Direct Encryption is employed, let the Content Encryption Key (CEK) be the shared symmetric key.
13. If the JWE JSON Serialization is being used, repeat this process (steps 4-12) for each recipient contained in the representation until the CEK value has been determined.
14. Compute the Encoded Protected Header value BASE64URL(UTF8(JWE Protected Header)). If the JWE Protected Header is not present (which can only happen when using the JWE JSON Serialization and no protected member is present), let this value be the empty string.
15. Let the Additional Authenticated Data encryption parameter be ASCII(Encoded Protected Header). However if a JWE AAD value is present (which can only be the case when using the JWE JSON Serialization), instead let the Additional Authenticated Data encryption parameter be ASCII(Encoded Protected Header || \''\' || BASE64URL(JWE AAD)).
16. Decrypt the JWE Ciphertext using the CEK, the JWE Initialization Vector, the Additional Authenticated Data value, and the JWE Authentication Tag (which is the Authentication Tag input to the calculation) using the specified content encryption algorithm, returning the decrypted plaintext and validating the JWE Authentication Tag in the manner specified for the algorithm, rejecting the input without emitting any decrypted output if the JWE Authentication Tag is incorrect.
17. If a zip parameter was included, uncompress the decrypted plaintext using the specified compression algorithm.
18. If all the previous steps succeeded, output the resulting Plaintext.
The string comparison rules for this specification are the same as those defined in Section 5.3 of [JWS].

6. Key Identification

The key identification methods for this specification are the same as those defined in Section 6 of [JWS], except that the key being identified is the public key to which the JWE was encrypted.

7. Serializations

JWE objects use one of two serializations, the JWE Compact Serialization or the JWE 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 JWE JSON Serialization is used, that only JWE JSON Serialization support for a single recipient is used, or that support for multiple recipients is used. JWE implementations only need to implement the features needed for the applications they are designed to support.

7.1. JWE Compact Serialization

The JWE Compact Serialization represents encrypted content as a compact URL-safe string. This string is BASE64URL(UTF8(JWE Protected Header)) || '.' || BASE64URL(JWE Encrypted Key) || '.' || BASE64URL(JWE Initialization Vector) || '.' || BASE64URL(JWE Ciphertext) || '.' || BASE64URL(JWE Authentication Tag). Only one recipient is supported by the JWE Compact Serialization and it provides no syntax to represent JWE Shared Unprotected Header, JWE Per-Recipient Unprotected Header, or JWE AAD values.

7.2. JWE JSON Serialization

The JWE JSON Serialization represents encrypted content as a JSON object. Content using the JWE JSON Serialization can be encrypted to more than one recipient. 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 JWE JSON Serialization:

- `protected`: The value BASE64URL(UTF8(JWE Protected Header)), if non-empty, is stored in the `protected` member.
- `unprotected`: The value BASE64URL(UTF8(JWE Shared Unprotected Header)), if non-empty, is stored in the `unprotected` member. If present, a JWE Shared Unprotected Header value is represented as an unencoded JSON object, rather than as a string.
- `iv`: The value BASE64URL(JWE Initialization Vector), if non-empty, is stored in the `iv` member.
- `aad`: A JWE AAD value can be included to supply a base64url encoded value to be integrity protected but not encrypted. (Note that this can also be achieved when using either serialization by including the AAD value as a protected Header Parameter value, but at the cost of the value being double base64url encoded.) If a JWE AAD value is present, the value BASE64URL(JWE AAD)) is stored in the `aad` member.
- `ciphertext`: The value BASE64URL(JWE Ciphertext) is stored in the `ciphertext` member.
The value BASE64URL(JWE Authentication Tag), if non-empty, is stored in the tag member.

recipients
A JSON array in the recipients member is used to hold values that are specific to a particular recipient, with one array element per recipient represented. These array elements are JSON objects, as specified below.

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

- header
  Each JWE Per-Recipient Unprotected Header value, if non-empty, is stored in the header member. If present, a JWE Per-Recipient Unprotected Header value is represented as an unencoded JSON object, rather than as a string.

- encrypted_key
  Each value BASE64URL(JWE Encrypted Key), if non-empty, is stored in the encrypted_key member.

Of these members of the two JSON objects defined above, only the ciphertext and recipients members MUST be present. The recipients array MUST always be present, even if the array elements contain only the empty JSON object {} (which can happen when all Header Parameter values are shared between all recipients and when no encrypted key is used, such as when doing Direct Encryption).

The iv, tag, and encrypted_key members MUST be present when corresponding JWE Initialization Vector, JWE Authentication Tag, and JWE Encrypted Key values are non-empty. The recipients member MUST be present when any header or encrypted_key members are needed for recipients. At least one of the header, protected, and unprotected members MUST be present so that alg and enc Header Parameter values are conveyed for each recipient computation.

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

Some Header Parameters, including the alg parameter, can be shared among all recipient computations. Header Parameters in the JWE Protected Header and JWE Shared Unprotected Header values are shared among all recipients.

Not all Header Parameters are integrity protected. The shared Header Parameters in the JWE Protected Header value member are integrity protected, and are base64url encoded for transmission. The per-recipient Header Parameters in the JWE Per-Recipient Unprotected Header values and the shared Header Parameters in the JWE Shared Unprotected Header value are not integrity protected. These JSON objects containing Header Parameters that are not integrity protected are not base64url encoded.

The Header Parameter values used when creating or validating per-recipient Ciphertext and Authentication Tag values are the union of the three sets of Header Parameter values that may be present: (1) the JWE Protected Header values represented in the protected member, (2) the JWE Shared Unprotected Header values represented in the unprotected member, and (3) the JWE Per-Recipient Unprotected Header values represented in the header member of the recipient's array element. The union of these sets of Header Parameters comprises the JWE Header. The Header Parameter names in the three locations MUST be disjoint.

The contents of the JWE Encrypted Key, JWE Initialization Vector, JWE Ciphertext, and JWE Authentication Tag values are exactly as defined in the rest of this specification. They are interpreted and validated in the same manner, with each corresponding JWE Encrypted Key, JWE Initialization Vector, JWE Ciphertext, JWE Authentication Tag, and set of Header Parameter values being created and validated together. The JWE Header values used are the union of the Header Parameters in the JWE Protected Header, JWE Shared Unprotected Header, and corresponding JWE Per-Recipient Unprotected Header values, as described earlier.

Each JWE Encrypted Key value is computed using the parameters of the corresponding JWE Header value in the same manner as for the JWE Compact Serialization. This has the desirable property that each JWE Encrypted Key value in the recipients array is identical to the value that would have been computed for the same parameter in the JWE Compact
the value that would have been computed for the same parameter in the JWE Compact Serialization.

Likewise, the JWE Ciphertext and JWE Authentication Tag values match those produced for the JWE Compact Serialization, provided that the JWE Protected Header value (which represents the integrity-protected Header Parameter values) matches that used in the JWE Compact Serialization.

All recipients use the same JWE Protected Header, JWE Initialization Vector, JWE Ciphertext, and JWE Authentication Tag values, when present, resulting in potentially significant space savings if the message is large. Therefore, all Header Parameters that specify the treatment of the Plaintext value MUST be the same for all recipients. This primarily means that the **enc** (encryption algorithm) Header Parameter value in the JWE Header for each recipient and any parameters of that algorithm MUST be the same.

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

```json
{"protected":"<integrity-protected shared header contents>",  
"unprotected":<non-integrity-protected shared header contents>,  
"recipients":[
  {"header":<per-recipient unprotected header 1 contents>,  
   "encrypted_key":"<encrypted key 1 contents>"},
  ...
  {"header":<per-recipient unprotected header N contents>,  
   "encrypted_key":"<encrypted key N contents>"},
  "aad":"<additional authenticated data contents>"},  
  "iv":"<initialization vector contents>"},  
  "ciphertext":"<ciphertext contents>",  
  "tag":"<authentication tag contents>"}
```

See Appendix A.4 for an example of computing a JWE using the JWE JSON Serialization.

---

8. TLS Requirements

The TLS requirements for this specification are the same as those defined in Section 8 of [JWS].

---

9. Distinguishing between JWS and JWE Objects

There are several ways of distinguishing whether an object is a JWS or JWE object. All these methods will yield the same result for all legal input values; they may yield different results for malformed inputs.

- If the object is using the JWS Compact Serialization or the JWE Compact Serialization, the number of base64url encoded segments separated by period (\.') characters differs for JWSs and JWEs. JWSs have three segments separated by two period (\.') characters. JWEs have five segments separated by four period (\.') characters.
- If the object is using the JWS JSON Serialization or the JWE JSON Serialization, the members used will be different. JWSs have a `signatures` member and JWEs do not. JWEs have a `recipients` member and JWSs do not.
- A JWS Header can be distinguished from a JWE header by examining the **alg** (algorithm) Header Parameter value. If the value represents a digital signature or MAC algorithm, or is the value **none**, it is for a JWS; if it represents a Key Encryption, Key Wrapping, Direct Key Agreement, Key Agreement with Key Wrapping, or Direct Encryption algorithm, it is for a JWE. (Extracting the **alg** value to examine is straightforward when using the JWS Compact Serialization or the JWE Compact Serialization and may be more difficult when using the JWS JSON Serialization or the JWE JSON Serialization.)
- A JWS Header can also be distinguished from a JWE header by determining whether an **enc** (encryption algorithm) member exists. If the **enc** member exists, it is a JWE; otherwise, it is a JWS.
10. IANA Considerations

10.1. JSON Web Signature and Encryption Header Parameters Registration

This specification registers the Header Parameter names defined in Section 4.1 in the IANA JSON Web Signature and Encryption Header Parameters registry defined in [JWS].

10.1.1. Registry Contents

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

- Header Parameter Name: **enc**  
  Header Parameter Description: Encryption Algorithm  
  Header Parameter Usage Location(s): JWE  
  Change Controller: IESG  
  Specification Document(s): Section 4.1.2 of [[this document]]

- Header Parameter Name: **zip**  
  Header Parameter Description: Compression Algorithm  
  Header Parameter Usage Location(s): JWE  
  Change Controller: IESG  
  Specification Document(s): Section 4.1.3 of [[this document]]

- Header Parameter Name: **jku**  
  Header Parameter Description: JWK Set URL  
  Header Parameter Usage Location(s): JWE  
  Change Controller: IESG  
  Specification Document(s): Section 4.1.4 of [[this document]]

- Header Parameter Name: **jwk**  
  Header Parameter Description: JSON Web Key  
  Header Parameter Usage Location(s): JWE  
  Change Controller: IESG  
  Specification Document(s): Section 4.1.5 of [[this document]]

- Header Parameter Name: **kid**  
  Header Parameter Description: Key ID  
  Header Parameter Usage Location(s): JWE  
  Change Controller: IESG  
  Specification Document(s): Section 4.1.6 of [[this document]]

- Header Parameter Name: **x5u**  
  Header Parameter Description: X.509 URL  
  Header Parameter Usage Location(s): JWE  
  Change Controller: IESG  
  Specification Document(s): Section 4.1.7 of [[this document]]

- Header Parameter Name: **x5c**  
  Header Parameter Description: X.509 Certificate Chain  
  Header Parameter Usage Location(s): JWE  
  Change Controller: IESG  
  Specification Document(s): Section 4.1.8 of [[this document]]

- Header Parameter Name: **x5t**
11. 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 private and symmetric keys, preventing various attacks, and helping the user avoid mistakes such as inadvertently encrypting a message for the wrong recipient. The entire list of security considerations is beyond the scope of this document.

All the security considerations in the JWS specification also apply to this specification. Likewise, all the security considerations in XML Encryption 1.1 [W3C.CR-xmenc-core1-20120313] also apply, other than those that are XML specific.

When decrypting, particular care must be taken not to allow the JWE recipient to be used as an oracle for decrypting messages. RFC 3218 should be consulted for specific countermeasures to attacks on RSAES-PKCS1-V1_5. An attacker might modify the contents of the alg parameter from RSA-OAEP to RSA1_5 in order to generate a formatting error that can be detected and used to recover the CEK even if RSAES OAEP was used to encrypt the CEK. It is therefore particularly important to report all formatting errors to the CEK, Additional Authenticated Data, or ciphertext as a single error when the encrypted content is rejected.

Additionally, this type of attack can be prevented by the use of "key tainting". This method restricts the use of a key to a limited set of algorithms -- usually one. This means, for instance, that if the key is marked as being for RSA-OAEP only, any attempt to decrypt a message using the RSA1_5 algorithm with that key would fail immediately due to invalid use of the key.

12. References
12.2. Informative References


Appendix A. JWE Examples

This section provides examples of JWE computations.

A.1. Example JWE using RSAES OAEP and AES GCM

This example encrypts the plaintext "The true sign of intelligence is not knowledge but imagination." to the recipient using RSAES OAEP for key encryption and AES GCM for content encryption. The representation of this plaintext is:


A.1.1. JWE Header

The following example JWE Protected Header declares that:

- the Content Encryption Key is encrypted to the recipient using the RSAES OAEP algorithm to produce the JWE Encrypted Key and
- the Plaintext is encrypted using the AES GCM algorithm with a 256 bit key to produce the Ciphertext.

{"alg":"RSA-OAEP","enc":"A256GCM"}

Encoding this JWE Protected Header as BASE64URL(UTF8(JWE Protected Header)) gives this value:
A.1.2. Content Encryption Key (CEK)

Generate a 256 bit random Content Encryption Key (CEK). In this example, the value is:

\[\begin{array}{c}
177, 161, 244, 128, 84, 143, 225, 115, 63, 180, 3, 255, 107, 154, 212, 246, 138, 7, 110, 91, 112, 46, 34, 105, 47, 130, 203, 46, 122, 234, 64, 252
\end{array}\]

A.1.3. Key Encryption

Encrypt the CEK with the recipient's public key using the RSAES OAEP algorithm to produce the JWE Encrypted Key. This example uses the RSA key represented in JSON Web Key (JWK) format below (with line breaks for display purposes only):

```
{"kty":"RSA",
 "n":"oahUTowW0KusKNUoR6H4wkf4oBUxHTxRvgb48E-BVvxkeDNjbC4he8rUWcJoZm2s2h7M76imEvHvRU5djINXtgllr1X4DFqciIIdgjT9LeWvD8M2Krfs3Pstk_ZkoFn1iakGygtwpZ3uesH-PFABNIUypOIN15dsQRkgr0vEhxN9V121sa0b0nSzeayzk17ZuwxrroExvv6kc5twXq4h-QCHLoIn8-mtU2wfsRaMStpsm6S6xrgxnxwbwoj6f63stuEQueGC-FCMfraq36C9knDFGzkKsnA7LZK2djYgyd3JR_MB_4NUjW_Tq0TvHYBxev0JArm-LSStowjzyg-_bq6GW",
 "e":"AQAAB",
 "d":"kJldHj6BDks_ApCSTYOt6cCNN1tKioyPzMrXHeI-ykJF7-koPdxY4-WY5NWV5KnTaeeEX51j82375xhWHMHyxfYecP79fpoR_M9gVbn9Hhr2anTpT9D3b62ypW3Ds2BnTrvYui1wWRgBKREYY46qAZIrA2xAwnm2X7uGR1hghkqDP0vq13kbsCzlXYfcs6_LehBwtxH1yh8R1py40p24mo0AgbxVw3xrT_v1t3uVe4W03k0oZlpuf-KTV21Ptgm-dArXTeE-id-40Jr0h-K-VFs3VSnVTiznSxfrj8I8LM6G_Uv8YAu7VILSB310W085-4qE3DzgrTjgyQ"
}
```

The resulting JWE Encrypted Key value is:

\[\begin{array}{c}
\end{array}\]

Encoding this JWE Encrypted Key as BASE64URL (JWE Encrypted Key) gives this value (with line breaks for display purposes only):

```
OKOawDo13gRp2ojaHV7LFpZcgV7T6DVZKTyKOMTUYmKoTCVJRgckCL9k1mMT03JGepsEd3ymx_etLbbwSwSrFr05KlZscSr4QKaQ7YNe79jwQRb23nfa6c9d-Stn1m6yFDhSv04uVuxIp5Zms1gNxKXKK2DaIAQ88S4rzVRltdYwam_1dp5xZAYpQdb76KdIuVAmgfwX7WXrvZx2321-VdXrFqNzTo_tETKzqVLzfiwQyeyPQLnI056Y37he0bdv0jje8186oppamavo35UgoRdbjYAcboh9Qcfy1Qr66oc6FwXRcZ_ZT2LawVCWbTY3bGPI6UKlfCpIMfIjf7iGdXKHZg
```
A.1.4. Initialization Vector

Generate a random 96 bit JWE Initialization Vector. In this example, the value is:

[227, 197, 117, 252, 2, 219, 233, 68, 180, 225, 77, 219]

Encoding this JWE Initialization Vector as BASE64URL(JWE Initialization Vector) gives this value:

48V1_ALb6US04U3b

A.1.5. Additional Authenticated Data

Let the Additional Authenticated Data encryption parameter be ASCII(BASE64URL(UTF8(JWE Protected Header))). This value is:

[101, 121, 74, 104, 98, 71, 99, 105, 79, 105, 74, 83, 85, 48, 69, 116, 84, 48, 70, 70, 85, 67, 73, 115, 73, 109, 86, 117, 89, 121, 73, 54, 73, 107, 69, 121, 78, 84, 90, 72, 81, 48, 48, 105, 102, 81]

A.1.6. Content Encryption

Encrypt the Plaintext with AES GCM using the CEK as the encryption key, the JWE Initialization Vector, and the Additional Authenticated Data value above, requesting a 128 bit Authentication Tag output. The resulting Ciphertext is:


The resulting Authentication Tag value is:

[92, 80, 104, 49, 133, 25, 161, 215, 173, 101, 219, 211, 136, 91, 210, 145]

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

5eym8TW_c8SuK0ltJ3rpYIzOeDQz7TALvtu6UG9oMo4vpzs9tX_EFSbS81B7j6sdiwkIr3ajwQzaBtQD_A

Encoding this JWE Authentication Tag as BASE64URL(JWE Authentication Tag) gives this value:

XFB0MYUZodetZdvTFvSkQ

A.1.7. Complete Representation

Assemble the final representation: The Compact Serialization of this result is the string BASE64URL(UTF8(JWE Protected Header)) || '.' || BASE64URL(JWE Encrypted Key) || '.' || BASE64URL(JWE Initialization Vector) || '.' || BASE64URL(JWE Ciphertext) || '.' || BASE64URL(JWE Authentication Tag).

The final result in this example (with line breaks for display purposes only) is:
A.1.8. Validation

This example illustrates the process of creating a JWE with RSAES OAEP for key encryption and AES GCM for content encryption. These results can be used to validate JWE decryption implementations for these algorithms. Note that since the RSAES OAEP computation includes random values, the encryption results above will not be completely reproducible. However, since the AES GCM computation is deterministic, the JWE Encrypted Ciphertext values will be the same for all encryptions performed using these inputs.

A.2. Example JWE using RSAES-PKCS1-V1_5 and AES_128_CBC_HMAC_SHA_256

This example encrypts the plaintext "Live long and prosper." to the recipient using RSAES-PKCS1-V1_5 for key encryption and AES_128_CBC_HMAC_SHA_256 for content encryption. The representation of this plaintext is:


A.2.1. JWE Header

The following example JWE Protected Header declares that:

- the Content Encryption Key is encrypted to the recipient using the RSAES-PKCS1-V1_5 algorithm to produce the JWE Encrypted Key and
- the Plaintext is encrypted using the AES_128_CBC_HMAC_SHA_256 algorithm to produce the Ciphertext.

```
{"alg":"RSA1_5","enc":"A128CBC-HS256"}
```

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

```
eyJhbGciOiJSU0ExXzUiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2In0
```

A.2.2. Content Encryption Key (CEK)

Generate a 256 bit random Content Encryption Key (CEK). In this example, the key value is:

[4, 211, 31, 197, 84, 157, 252, 254, 11, 100, 157, 250, 63, 170, 106, 206, 107, 124, 212, 45, 111, 107, 9, 219, 200, 177, 0, 240, 143, 156, 44, 207]
A.2.3. Key Encryption

Encrypt the CEK with the recipient's public key using the RSAES-PKCS1-V1_5 algorithm to produce the JWE Encrypted Key. This example uses the RSA key represented in JSON Web Key [JWK] format below (with line breaks for display purposes only):

```
{"kty": "RSA",
 "n": "XchDaQebHnP1gvyDQAT4saGEUtSy09MLo0WFsueri23b0dqWp4Dy1W1Uzewbg8Hod5pcM9H95G0Rv3JXb0iRROSBigeC5jyJ1hGzHhYxXs8uDPrecbAfYxkTeQkhs1ANGRUnzdTQ65qTrsLaT6BYyvVRdh8xS8EYZYe4_c4gs_7sv1JQ4H9_NxsiOlLuAek7-3UXERGyWv75IDrGA84-1A_-CT4eT1XHBIY2ErV77LrJJaynV3Cpkv4LkJrTTAm11YquhrHhZLuFRJLqHP2kgWFLU7-VTdl1VBc2tejC21aLMepk1BzBZl0kQ80aDFWLN-aEaw3vRw",
 "e": "AQAB",
 "d": "VFCWqXr8nvZNyaaJLXdnNPXZKRwCjkuUQ22eq9QqTBMWhpMrzWprR85xq10PThhJ6MUDbZ35wky9b8eEO0pwN8SxX1h10FRBr0NqDIKWkOu5aZb-rynq8cxjDTLQZ6F7s7jSjR1K1op-YkAuHCh9gsEofQqYrPhzSA-QgajZGBP_0ZaVdHfydv7WUBUKunFMScbfLjA0YjRqFIVw8vRY5zWEEceuJnNTO_CVSj-VvXL05ZVfcUAVLWh4dpf1SrZt34YLSrRbS127re6GUwq9Ch-KyvjT1SkHgUWVRCgycy7uVGRSDwxsypDrNinPA4jlhoNdzizK2zF2CWo"
}
```

The resulting JWE Encrypted Key value is:


Encoding this JWE Encrypted Key as BASE64URL(JWE Encrypted Key) gives this value (with line breaks for display purposes only):

```
UghIOguC7IuEvf_NPVaX5MoLomvvc1Gyql1KOK1nN94HPOl5GRhWhv7Zx0-kFM11Nnb8LE9hXH59_i8J0PH52ZyNfgy2xGdULU7sHNF6gp2vPLgNz_delKxGH7PcHALUzoOegE1-8E66jX2E4zyKj-xyzZII1RzeC5h1Rirb6Y5CL-pko3YkvkysZ1FNPcexRU7dve1WPxqbb2YWk8ZkA2rMWW1ng80tvz1V7e1prCbuPhcCdZ6XDP0_F8rkXds2vE4X-nco1BMhAYYHIi29N0mck1RaA6-D-ljQTP-cFPgwCp6X-nZZd9oHBv-B3oWh2TboqScqZM4Rgp_A
```

A.2.4. Initialization Vector

Generate a random 128 bit JWE Initialization Vector. In this example, the value is:


Encoding this JWE Initialization Vector as BASE64URL(JWE Initialization Vector) gives this value:

```
Axy8DctGalsGlipb3RoZQ
```
A.2.5. Additional Authenticated Data

Let the Additional Authenticated Data encryption parameter be ASCII(BASE64URL(UTF8(JWE Protected Header))). This value is:


A.2.6. Content Encryption

Encrypt the Plaintext with AES_128_CBC_HMAC_SHA_256 using the CEK as the encryption key, the JWE Initialization Vector, and the Additional Authenticated Data value above. The resulting Ciphertext is:


The resulting Authentication Tag value is:

\[\text{Authentication Tag} = \{246, 17, 244, 190, 4, 95, 98, 3, 231, 0, 115, 157, 242, 203, 100, 191\}\]

Encoding this JWE Ciphertext as BASE64URL(JWE Ciphertext) gives this value:

KDlTtXchhZTGufMYm0YG4HffxPSUrfmqCHXaI9wOGY

Encoding this JWE Authentication Tag as BASE64URL(JWE Authentication Tag) gives this value:

9hH0vgRfYgPnAH0d8stkvw

A.2.7. Complete Representation

Assemble the final representation: The Compact Serialization of this result is the string BASE64URL(UTF8(JWE Protected Header)) || '.' || BASE64URL(JWE Encrypted Key) || '.' || BASE64URL(JWE Initialization Vector) || '.' || BASE64URL(JWE Ciphertext) || '.' || BASE64URL(JWE Authentication Tag).

The final result in this example (with line breaks for display purposes only) is:

eyJhbGciOiJSU0ExXzUiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2In0.
UGhIOguC7IuEvf_NPVaXsGm0LOmBwScn16UYq1IKOK1nN94nHP0ltGRhWw7Zx0-kFm1nJn8LE9XSHH59_8J0PH5ZZYzNf6y2xGdULU7sHNF6Gp2vPLgNZ__deLkxGHZ7PcHALUzo0egeEI-8E66jX2E4zyJKx-YxzZIIrTc51Rirb6Y5C1_p-k03YvkkysZIFNPccxRU7qe1YPoqbb2Yw8kZqa2rMWI5ng80tvz1V7e1prCbuPhcCdZ6XDP0_F8rKdxe2vE4X-nc0IM8hAYHhi29NX0mciK2a0-D-1jQTP-cFPgwCp6X-nZz90HBv-
B30Wh2TbqmScqXMR4gp_A.
Axy8BctDaGl6bGljb3RoZQ.
KDlTtXchhZTGufMYm0YG4HffxPSUrfmqCHXaI9wOGY.
9hH0vgRfYgPnAH0d8stkvw

A.2.8. Validation

Appendix A.3

Appendix B
This example illustrates the process of creating a JWE with RSAES-PKCS1-V1_5 for key encryption and AES_CBC_HMAC_SHA2 for content encryption. These results can be used to validate JWE decryption implementations for these algorithms. Note that since the RSAES-PKCS1-V1_5 computation includes random values, the encryption results above will not be completely reproducible. However, since the AES CBC computation is deterministic, the JWE Encrypted Ciphertext values will be the same for all encryptions performed using these inputs.

A.3. Example JWE using AES Key Wrap and AES_128_CBC_HMAC_SHA_256

This example encrypts the plaintext "Live long and prosper." to the recipient using AES Key Wrap for key encryption and AES GCM for content encryption. The representation of this plaintext is:


A.3.1. JWE Header

The following example JWE Protected Header declares that:

- the Content Encryption Key is encrypted to the recipient using the AES Key Wrap algorithm with a 128 bit key to produce the JWE Encrypted Key and
- the Plaintext is encrypted using the AES_128_CBC_HMAC_SHA_256 algorithm to produce the Ciphertext.

{"alg":"A128KW","enc":"A128CBC-HS256"}

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

eyJhbGciOiJBMTI4S1ciLCJlbmMiOiJBMTI4Q0JDLUhTMjU2In0

A.3.2. Content Encryption Key (CEK)

Generate a 256 bit random Content Encryption Key (CEK). In this example, the value is:

[4, 211, 31, 197, 84, 157, 252, 254, 11, 100, 157, 250, 63, 170, 106, 206, 107, 124, 212, 45, 111, 107, 9, 219, 200, 177, 0, 240, 143, 156, 44, 207]

A.3.3. Key Encryption

Encrypt the CEK with the shared symmetric key using the AES Key Wrap algorithm to produce the JWE Encrypted Key. This example uses the symmetric key represented in JSON Web Key [JWK] format below:

{"kty":"oct","k":"GawgguyFyGrWKav7AX4VKuG"}

The resulting JWE Encrypted Key value is:

Encoding this JWE Encrypted Key as BASE64URL(JWE Encrypted Key) gives this value:

6KB707dM9YTIGHtLVtgWQ8mKwbo3W3of9locizkDTHzBC2IlrT1oOQ

A.3.4. Initialization Vector

Generate a random 128 bit JWE Initialization Vector. In this example, the value is:


Encoding this JWE Initialization Vector as BASE64URL(JWE Initialization Vector) gives this value:

AxY8DctDaGlsbGljb3RoQZ

A.3.5. Additional Authenticated Data

Let the Additional Authenticated Data encryption parameter be ASCII(BASE64URL=UTF8(JWE Protected Header)). This value is:


A.3.6. Content Encryption

Encrypt the Plaintext with AES_128_CBC_HMAC_SHA_256 using the CEK as the encryption key, the JWE Initialization Vector, and the Additional Authenticated Data value above. The steps for doing this using the values from this example are detailed in Appendix B. The resulting Ciphertext is:


The resulting Authentication Tag value is:

[83, 73, 191, 98, 104, 205, 211, 128, 201, 189, 199, 133, 32, 38, 194, 85]

Encoding this JWE Ciphertext as BASE64URL(JWE Ciphertext) gives this value:

KDlTtXchhZTGufMYmOYG5S4HffxPSUrfmqCHXaI9wOGY

Encoding this JWE Authentication Tag as BASE64URL(JWE Authentication Tag) gives this value:

U0m_YmjN04DJvceFICdCVQ

A.3.7. Complete Representation

Assemble the final representation: The Compact Serialization of this result is the string
The Compact Serialization of this result is the string

BASE64URL(UTF8(JWE Protected Header)) || '.' || BASE64URL(JWE Encrypted Key) || '.' ||
BASE64URL(JWE Initialization Vector) || '.' || BASE64URL(JWE Ciphertext) || '.' ||
BASE64URL(JWE Authentication Tag).

The final result in this example (with line breaks for display purposes only) is:

eyJhbGciOiJBMTI4S1ciLCJlbmMiOiJBMTI4Q0JDLUhTMjU2In0.
6KB707dM9YTtgHLtvgQW8mKwboJW3of9locizkDTH2BC2IlrT1oQ.
Axy8DCtDaGlsbGljb3RoZQ.
KDIThXchhZTGufMYmOYGSAHffxPSUrfmqCHXaI9wOGY.
U0m_YmjN04DJveFICbCVQ

A.3.8. Validation

This example illustrates the process of creating a JWE with AES Key Wrap for key encryption
and AES GCM for content encryption. These results can be used to validate JWE decryption
implementations for these algorithms. Also, since both the AES Key Wrap and AES GCM
computations are deterministic, the resulting JWE value will be the same for all encryptions
performed using these inputs. Since the computation is reproducible, these results can also
be used to validate JWE encryption implementations for these algorithms.

A.4. Example JWE using JWE JSON Serialization

This section contains an example using the JWE JSON Serialization. This example
demonstrates the capability for encrypting the same plaintext to multiple recipients.

Two recipients are present in this example. The algorithm and key used for the first recipient
are the same as that used in Appendix A.2. The algorithm and key used for the second
recipient are the same as that used in Appendix A.3. The resulting JWE Encrypted Key
values are therefore the same; those computations are not repeated here.

The Plaintext, the Content Encryption Key (CEK), Initialization Vector, and JWE Protected
Header are shared by all recipients (which must be the case, since the Ciphertext and
Authentication Tag are also shared).

A.4.1. JWE Per-Recipient Unprotected Headers

The first recipient uses the RSAES-PKCS1-V1_5 algorithm to encrypt the Content Encryption
Key (CEK). The second uses AES Key Wrap to encrypt the CEK. Key ID values are supplied for
both keys. The two per-recipient header values used to represent these algorithms and Key
IDs are:

{"alg":"RSA1_5","kid":"2011-04-29"}

and

{"alg":"A128KW","kid":"7"}

A.4.2. JWE Protected Header

The Plaintext is encrypted using the AES_128_CBC_HMAC_SHA_256 algorithm to produce
the common JWE Ciphertext and JWE Authentication Tag values. The JWE Protected Header
value representing this is:
Encoding this JWE Protected Header as BASE64URL(UTF8(JWE Protected Header)) gives this value:

eyJlbmMiOiJBMTI4Q0JDLUhTMjU2In0

A.4.3. JWE Unprotected Header

This JWE uses the jku Header Parameter to reference a JWK Set. This is represented in the following JWE Unprotected Header value as:

{"jku":"https://server.example.com/keys.jwks"}

A.4.4. Complete JWE Header Values

Combining the per-recipient, protected, and unprotected header values supplied, the JWE Header values used for the first and second recipient respectively are:

{"alg":"RSA1_5",
 "kid":"2011-04-29",
 "enc":"A128CBC-HS256",
 "jku":"https://server.example.com/keys.jwks"}

and

{"alg":"A128KW",
 "kid":"7",
 "enc":"A128CBC-HS256",
 "jku":"https://server.example.com/keys.jwks"}

A.4.5. Additional Authenticated Data

Let the Additional Authenticated Data encryption parameter be ASCII(BASE64URL(UTF8(JWE Protected Header))). This value is:


A.4.6. Content Encryption

Encrypt the Plaintext with AES_128_CBC_HMAC_SHA_256 using the CEK as the encryption key, the JWE Initialization Vector, and the Additional Authenticated Data value above. The steps for doing this using the values from Appendix A.3 are detailed in Appendix B. The resulting Ciphertext is:

The resulting Authentication Tag value is:

[51, 63, 149, 60, 252, 148, 225, 25, 92, 185, 139, 245, 35, 2, 47, 207]

Encoding this JWE Ciphertext as BASE64URL(JWE Ciphertext) gives this value:

KDlTtXchhZTGuM6Y6S4HffxPSUrfmqCHXaI9wOGY

Encoding this JWE Authentication Tag as BASE64URL(JWE Authentication Tag) gives this value:

Mz-VPPyU4R1cuYv1IwIvzw

A.4.7. Complete JWE JSON Serialization Representation

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

```json
{"protected":
  "eyJlbmMiOiJBMTI4Q0JDLUhTMjU2In0",
  "unprotected":
  {
    "jku": "https://server.example.com/keys.jwks",
    "recipients": [
      {
        "alg": "RSA1_5",
        "encrypted_key": "UGhIOguC7IuEvf_NPVaXSMoLoMWVc1GqlIKOK1nN94nHPo1tGRhWWhw7ZXo-
                        kFmlNIN89ShS59_i8J0PH5ZZYnFgy2xGdULU7sHNF66p2vPLgNZ__dELKx
                        GHZ7pCIALUzo0eoGI-8E66jX2E4zyJKx-YzzZlYrZ5h1Rirb6Y5C1_p-ko3
                        YvkvysZlFNPccxR7u7ve1WPxqb2Yw8kZqa2rMWIS6n80tvz1V7elprCbuPh
                        cCd2Z6XDPO_F8rkXds2V4E-X-nCOI8hAYHHi29NX0mckI1RaD0-D-ljQP-cFPG
                        wCp6X-nZZd90HBv-B30wh2TbqmScqXM4Rg_A"},
      {
        "alg": "A128KW",
        "encrypted_key": "6KB707dM9YTIgHtLvtgWboJW3of9locizkDTHzBC2llT1oOQ"},
    ]
  },
  "iv": "AxY8DCTdAglsbGljb3RoZQ",
  "ciphertext": "KDlTtXchhZTGuM6Y6S4HffxPSUrfmqCHXaI9wOGY",
  "tag": "Mz-VPPyU4R1cuYv1IwIvzw"
}
```

Appendix B. Example AES_128_CBC_HMAC_SHA_256 Computation

This example shows the steps in the AES_128_CBC_HMAC_SHA_256 authenticated encryption computation using the values from the example in Appendix A.3. As described where this algorithm is defined in Sections 4.8 and 4.8.3 of JWA, the AES_CBC_HMAC_SHA2 family of algorithms are implemented using Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode with PKCS #5 padding to perform the encryption and an HMAC SHA-2 function to perform the integrity calculation - in this case, HMAC SHA-256.

B.1. Extract MAC_KEY and ENC_KEY from Key

The 256 bit AES_128_CBC_HMAC_SHA_256 key K used in this example is:
Use the first 128 bits of this key as the HMAC SHA-256 key MAC_KEY, which is:

[4, 211, 31, 197, 84, 157, 252, 254, 11, 100, 157, 250, 63, 170, 106, 206, 107, 124, 212, 45, 111, 107, 9, 219, 200, 177, 0, 240, 143, 156, 44, 207]

Use the last 128 bits of this key as the AES CBC key ENC_KEY, which is:

[107, 124, 212, 45, 111, 107, 9, 219, 200, 177, 0, 240, 143, 156, 44, 207]

Note that the MAC key comes before the encryption key in the input key K; this is in the opposite order of the algorithm names in the identifiers "AES_128_CBC_HMAC_SHA_256" and A128CBC-HS256.

B.2. Encrypt Plaintext to Create Ciphertext

Encrypt the Plaintext with AES in Cipher Block Chaining (CBC) mode using PKCS #5 padding using the ENC_KEY above. The Plaintext in this example is:


The encryption result is as follows, which is the Ciphertext output:


B.3. 64 Bit Big Endian Representation of AAD Length

The Additional Authenticated Data (AAD) in this example is:


This AAD is 51 bytes long, which is 408 bits long. The octet string AL, which is the number of bits in AAD expressed as a big endian 64 bit unsigned integer is:

[0, 0, 0, 0, 0, 0, 1, 152]

B.4. Initialization Vector Value

The Initialization Vector value used in this example is:


B.5. Create Input to HMAC Computation

Concatenate the AAD, the Initialization Vector, the Ciphertext, and the AL value. The result of this concatenation is:

B.6. Compute HMAC Value

Compute the HMAC SHA-256 of the concatenated value above. This result M is:

\[83, 73, 191, 98, 104, 205, 211, 128, 201, 189, 199, 133, 32, 38, 194, 85, 9, 84, 229, 201, 219, 135, 44, 252, 145, 102, 179, 140, 105, 86, 229, 116\]

B.7. Truncate HMAC Value to Create Authentication Tag

Use the first half (128 bits) of the HMAC output M as the Authentication Tag output T. This truncated value is:

\[83, 73, 191, 98, 104, 205, 211, 128, 201, 189, 199, 133, 32, 38, 194, 85\]

Appendix C. Acknowledgements

Solutions for encrypting JSON content were also explored by JSON Simple Encryption [JSE] and JavaScript Message Security Format [I-D.rescorla-jsms], both of which significantly influenced this draft. This draft attempts to explicitly reuse as many of the relevant concepts from XML Encryption 1.1 [W3C.CR-xmenc-core1-20120313] and RFC 5652 [RFC5652] as possible, while utilizing simple, compact JSON-based data structures.

Special thanks are due to John Bradley and Nat Sakimura for the discussions that helped inform the content of this specification and to Eric Rescorla and Joe Hildebrand for allowing the reuse of text from [I-D.rescorla-jsms] in this document.

Thanks to Axel Nennker, Emmanuel Raviart, Brian Campbell, and Edmund Jay for validating the examples in this specification.

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 and Stephen Farrell served as Security area directors during the creation of this specification.

Appendix D. Document History

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

-20

- Made terminology definitions more consistent, addressing issue #165.
- Restructured the JSON Serialization section to call out the parameters used in hanging lists, addressing issue #178.
- Replaced references to RFC 4627 with draft-ietf-json/rfc4627bis, addressing issue #90.

-19

- Reordered the key selection parameters.
-17

-16

-15

-14

-13

-12
-11

- Changed terminology from "block encryption" to "content encryption".
- Added Key Identification section.
- Removed the Encrypted Key value from the AAD computation since it is already effectively integrity protected by the encryption process. The AAD value now only contains the representation of the JWE Encrypted Header.
- For the JWE 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 JWE Compact Serialization, in which all Header Parameter values are in a single integrity protected JWE Header value.)
- Shortened the names authentication_tag to tag and initialization_vector to iv in the JWE JSON Serialization, addressing issue #20.
- Removed apv (agreement PartyVInfo) since it is no longer used.
- Removed suggested compact serialization for multiple recipients.
- Changed the MIME type name application/jwe-js to application/jwe+json, addressing issue #22.
- Tightened the description of the crit (critical) header parameter.

-10

- Changed the JWE processing rules for multiple recipients so that a single AAD value contains the header parameters and encrypted key values for all the recipients, enabling AES GCM to be safely used for multiple recipients.
- Added an appendix suggesting a possible compact serialization for JWEs with multiple recipients.

-09

- Added JWE JSON Serialization, as specified by draft-jones-jose-jwe-json-serialization-04.
- Registered application/jwe-js MIME type and JWE-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.
- Corrected x5c description. This addressed issue #12.
- Changed from using the term "byte" to "octet" when referring to 8 bit values.
- Added Key Management Mode definitions to terminology section and used the defined terms to provide clearer key management instructions. This addressed issue #5.
- Added text about preventing the recipient from behaving as an oracle during decryption, especially when using RSAES-PKCS1-V1_5.
- Changed from using the term "Integrity Value" to "Authentication Tag".
- Changed member name from integrity_value to authentication_tag in the JWE JSON Serialization.
- Removed Initialization Vector from the AAD value since it is already integrity protected by all of the authenticated encryption algorithms specified in the JWA specification.
- Replaced A128CBC+HS256 and A256CBC+HS512 with A128CBC-HS256 and A256CBC-HS512. The new algorithms perform the same cryptographic computations as [I-D.mcgrew-aead-aes-cbc-hmac-sha2], but with the Initialization Vector and Authentication Tag values remaining separate from the Ciphertext value in the output representation. Also deleted the header parameters epu (encryption PartyUInfo) and epv (encryption PartyVInfo), since they are no longer used.

-08

- Replaced uses of the term "AEAD" with "Authenticated Encryption", since the term AEAD in the RFC 5116 sense implied the use of a particular data...
representation, rather than just referring to the class of algorithms that perform authenticated encryption with associated data.

- Applied editorial improvements suggested by Jeff Hodges and Hannes Tschofenig. Many of these simplified the terminology used.
- Clarified statements of the form "This header parameter is OPTIONAL" to "Use of this header parameter is OPTIONAL".
- Added a Header Parameter Usage Location(s) field to the IANA JSON Web Signature and Encryption Header Parameters registry.
- Added seriesInfo information to Internet Draft references.
- Added a data length prefix to PartyUInfo and PartyVInfo values.
- Updated values for example AES CBC calculations.
- Made several local editorial changes to clean up loose ends left over from the decision to only support block encryption methods providing integrity. One of these changes was to explicitly state that the enc (encryption method) algorithm must be an Authenticated Encryption algorithm with a specified key length.

- Removed the int and kdf parameters and defined the new composite Authenticated Encryption algorithms A128CBC+HS256 and A256CBC+HS512 to replace the former uses of AES CBC, which required the use of separate integrity and key derivation functions.
- Included additional values in the Concat KDF calculation -- the desired output size and the algorithm value, and optionally PartyUInfo and PartyVInfo values. Added the optional header parameters apu (agreement PartyUInfo), apv (agreement PartyVInfo), epu (encryption PartyUInfo), and epv (encryption PartyVInfo). Updated the KDF examples accordingly.
- Promoted Initialization Vector from being a header parameter to being a top-level JWE element. This saves approximately 16 bytes in the compact serialization, which is a significant savings for some use cases. Promoting the Initialization Vector out of the header also avoids repeating this shared value in the JSON serialization.
- 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.
- Added an AES Key Wrap example.
- Reordered the encryption steps so CMK creation is first, when required.
- Correct statements in examples about which algorithms produce reproducible results.

- Support both direct encryption using a shared or agreed upon symmetric key, and the use of a shared or agreed upon symmetric key to key wrap the CMK.
- Added statement that "StringOrURI values are compared as case-sensitive strings with no transformations or canonicalizations applied".
- Updated open issues.
- Indented artwork elements to better distinguish them from the body text.

- Refer to the registries as the primary sources of defined values and then secondarily reference the sections defining the initial contents of the registries.
- Described additional open issues.
- Applied editorial suggestions.

- Added the kdf (key derivation function) header parameter to provide crypto agility for key derivation. The default KDF remains the Concat KDF with the SHA-256 digest function.
-02

-01

-00
Authors' Addresses

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

Eric Rescorla
RTFM, Inc.
Email: ekr@rtfm.com

Joe Hildebrand
Cisco Systems, Inc.
Email: jhildebr@cisco.com