Table of Contents

原文链接：https://tools.ietf.org/rfc/rfc7519.txt 翻译：qunfanyi.com

1. Introduction

[en]JSON Web Token (JWT) is a compact claims representation format intended for space constrained environments such as HTTP Authorization headers and URI query parameters.
[zh_CN]JSON Web令牌（JWT）是一种用于空间受限环境（如HTTP授权标头和URI查询参数）的紧凑声明声明格式。

[en]JWTs encode claims to be transmitted as a JSON [RFC7159] object that is used as the payload of a JSON Web Signature (JWS) [JWS] structure or as the plaintext of a JSON Web Encryption (JWE) [JWE] structure, enabling the claims to be digitally signed or integrity protected with a Message Authentication Code (MAC) and/or encrypted.
[zh_CN]JWT将声明作为JSON[RFC7159]对象进行编码，该对象用作JSON Web签名（JWS）[JWS]结构的有效负载或JSON Web加密（JWE）[JWE]结构的明文，从而能够对声明进行数字签名或使用消息身份验证保护完整性代码（MAC）和/或加密。

[en]JWTs are always represented using the JWS Compact Serialization or the JWE Compact Serialization.
[zh_CN]JWTS总是使用JWS紧凑序列化或JWE紧凑序列化来表示。

[en]The suggested pronunciation of JWT is the same as the English word "jot".
[zh_CN]JWT的建议发音与英语单词“JOT”相同。

1.1. Notational Conventions

[en]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].
[zh_CN]本文档中的关键词“必须”、“必须不要”、“要求”、“必须”、“不应该”、“应该”、“不应该”、“推荐”、“不推荐”、“MAY”和“可选”应解释为“RFC中使用的关键词以指示需求级别”[RFC2119]。

[en]The interpretation should only be applied when the terms appear in all capital letters.
[zh_CN]只有在所有大写字母中出现术语时才解释。

2. Terminology

[en]The terms "JSON Web Signature (JWS)", "Base64url Encoding", "Header Parameter", "JOSE Header", "JWS Compact Serialization", "JWS Payload", "JWS Signature", and "Unsecured JWS" are defined by the JWS specification [JWS].
[zh_CN]术语“JSON Web签名（JWS）”、“Base64url编码”、“头参数”、“JOSE头”、“JWS紧凑序列化”、“JWS有效载荷”、“JWS签名”和“不安全JWS”由JWS规范[JWS]定义。

[en]The terms "JSON Web Encryption (JWE)", "Content Encryption Key (CEK)", "JWE Compact Serialization", "JWE Encrypted Key", and "JWE Initialization Vector" are defined by the JWE specification [JWE].
[zh_CN]术语“JSON Web加密（JWE）”、“内容加密密钥（CEK）”、“JWE压缩序列化”、“JWE加密密钥”和“JWE初始化向量”由JWE规范[JWE]定义。

[en]The terms "Ciphertext", "Digital Signature", "Message Authentication Code (MAC)", and "Plaintext" are defined by the "Internet Security Glossary, Version 2" [RFC4949].
[zh_CN]术语“密文”、“数字签名”、“消息认证码(MAC)”和“明文”由“互联网安全术语表，版本2”[RFC4949]定义。

[en]Jones, et al.
[zh_CN]琼斯等。

[en]Standards Track [Page 4] RFC 7519 JSON Web Token (JWT) May 2015 These terms are defined by this specification: JSON Web Token (JWT) A string representing a set of claims as a JSON object that is encoded in a JWS or JWE, enabling the claims to be digitally signed or MACed and/or encrypted.
[zh_CN]标准跟踪[第4页]RFC 7519 JSON Web Token(JWT)2015年5月这些术语由本规范定义：JSON Web Token(JWT)表示一组声明的字符串，作为JSON对象，编码在JWS或JWE中，使声明能够被数字签名、MACed和/或加密。

[en]JWT Claims Set A JSON object that contains the claims conveyed by the JWT.
[zh_CN]JWT声明设置JSON对象，该对象包含JWT传递的声明。

[en]Claim A piece of information asserted about a subject.
[zh_CN]声称有关某一主题的信息。

[en]A claim is represented as a name/value pair consisting of a Claim Name and a Claim Value.
[zh_CN]索赔被表示为由索赔名称和索赔值组成的名称/值对。

[en]Claim Name The name portion of a claim representation.
[zh_CN]索赔名称索赔声明的名称部分。

[en]A Claim Name is always a string.
[zh_CN]声明名称总是字符串。

[en]Claim Value The value portion of a claim representation.
[zh_CN]索赔价值索赔声明的价值部分。

[en]A Claim Value can be any JSON value.
[zh_CN]索赔值可以是任何JSON值。

[en]Nested JWT A JWT in which nested signing and/or encryption are employed.
[zh_CN]嵌套JWT JWT，其中采用嵌套签名和/或加密。

[en]In Nested JWTs, a JWT is used as the payload or plaintext value of an enclosing JWS or JWE structure, respectively.
[zh_CN]在嵌套的JWTS中，JWT分别用作封闭JWS或JWE结构的有效载荷或明文值。

[en]Unsecured JWT A JWT whose claims are not integrity protected or encrypted.
[zh_CN]不安全的JWT JWT，其声明没有完整性保护或加密。

[en]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.
[zh_CN]抗冲突名称：名称空间中的一个名称，它允许以某种方式分配名称，使得名称极不可能与其他名称冲突。

[en]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].
[zh_CN]抗冲突名称空间的示例包括：域名、ITU-T X.660和X.670建议系列中定义的对象标识符(OID)和通用唯一标识(UUID)[RFC4122]。

[en]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.
[zh_CN]当使用管理上委托的名称空间时，名称的定义者需要采取合理的预防措施，以确保他们能够控制用于定义名称的名称空间的部分。

[en]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].
[zh_CN]StringOrURI JSON字符串值，还有一个附加要求，即尽管可以使用任意的字符串值，但是任何包含“:”字符的值都必须是URI[RFC3986]。

[en]StringOrURI values are compared as case-sensitive strings with no transformations or canonicalizations applied.
[zh_CN]将Strugururi值作为不带转换或规范的情况敏感字符串进行比较。

[en]Jones, et al.
[zh_CN]琼斯等。

[en]Standards Track [Page 5] RFC 7519 JSON Web Token (JWT) May 2015 NumericDate A JSON numeric value representing the number of seconds from 1970-01-01T00:00:00Z UTC until the specified UTC date/time, ignoring leap seconds.
[zh_CN]标准跟踪[第5页]RFC 7519 JSON Web令牌(JWT)2015年5月NumericDate一个JSON数值，表示从UTC 1970-01-01T00:00:00Z到指定UTC日期/时间的秒数，忽略闰秒。

[en]This is equivalent to the IEEE Std 1003.1, 2013 Edition [POSIX.1] definition "Seconds Since the Epoch", in which each day is accounted for by exactly 86400 seconds, other than that non-integer values can be represented.
[zh_CN]这等同于IEEE Std 1003.1，2013版[POSIX.1]定义的“自纪元以来的第二天”，其中，除了可以表示非整数值之外，每天精确地占86400秒。

[en]See RFC 3339 [RFC3339] for details regarding date/times in general and UTC in particular.
[zh_CN]参见RFC 3339 [RFC33 39]，详细说明日期/时间，特别是UTC。

3. JSON Web Token (JWT) Overview

[en]JWTs represent a set of claims as a JSON object that is encoded in a JWS and/or JWE structure.
[zh_CN]JWTs表示一组声明，称为JSON对象，该对象在JWS和/或JWE结构中编码。

[en]This JSON object is the JWT Claims Set.
[zh_CN]这个JSON对象是JWT声明集。

[en]As per Section 4 of RFC 7159 [RFC7159], the JSON object consists of zero or more name/value pairs (or members), where the names are strings and the values are arbitrary JSON values.
[zh_CN]根据RFC 7159[RFC7159]的第4节，JSON对象由零个或多个名称/值对（或成员）组成，其中名称是字符串，值是任意JSON值。

[en]These members are the claims represented by the JWT.
[zh_CN]这些成员是JWT所代表的权利要求。

[en]This JSON object MAY contain whitespace and/or line breaks before or after any JSON values or structural characters, in accordance with Section 2 of RFC 7159 [RFC7159].
[zh_CN]根据RFC 7159 [RFC7159]的第2节，这个JSON对象可以在任何JSON值或结构字符之前或之后包含空格和/或断线。

[en]The member names within the JWT Claims Set are referred to as Claim Names.
[zh_CN]JWT声明集中的成员名称为索赔名。

[en]The corresponding values are referred to as Claim Values.
[zh_CN]相应的值被称为索赔值。

[en]The contents of the JOSE Header describe the cryptographic operations applied to the JWT Claims Set.
[zh_CN]若泽报头的内容描述了应用于JWT声明集的加密操作。

[en]If the JOSE Header is for a JWS, the JWT is represented as a JWS and the claims are digitally signed or MACed, with the JWT Claims Set being the JWS Payload.
[zh_CN]如果JOSE头是针对JWS的，那么JWT表示为JWS，并且声明是数字签名或MAC化的，JWT声明集是JWS有效载荷。

[en]If the JOSE Header is for a JWE, the JWT is represented as a JWE and the claims are encrypted, with the JWT Claims Set being the plaintext encrypted by the JWE.
[zh_CN]如果JOSE头是针对JWE的，则JWT表示为JWE，并且声明被加密，其中JWT声明集是由JWE加密的明文。

[en]A JWT may be enclosed in another JWE or JWS structure to create a Nested JWT, enabling nested signing and encryption to be performed.
[zh_CN]JWT可以封装在另一个JWE或JWS结构中以创建嵌套JWT，从而能够执行嵌套签名和加密。

[en]A JWT is represented as a sequence of URL-safe parts separated by period ('.') characters.
[zh_CN]JWT被表示为URL安全部分的序列，该部分由周期（'.'）字符分隔。

[en]Each part contains a base64url-encoded value.
[zh_CN]每个部分包含一个Base64 URL编码值。

[en]The number of parts in the JWT is dependent upon the representation of the resulting JWS using the JWS Compact Serialization or JWE using the JWE Compact Serialization.
[zh_CN]JWT中的部件数量取决于使用JWS紧凑序列化的结果JWS或使用JWE紧凑序列化的JWE的表示。

[en]Jones, et al.
[zh_CN]琼斯等。

3.1. Example JWT

[en]The following example JOSE Header declares that the encoded object is a JWT, and the JWT is a JWS that is MACed using the HMAC SHA-256 algorithm: {"typ":"JWT", "alg":"HS256"} To remove potential ambiguities in the representation of the JSON object above, the octet sequence for the actual UTF-8 representation used in this example for the JOSE Header above is also included below.
[zh_CN]下面的示例JOSE Header声明已编码的对象是JWT，并且JWT是使用HMAC SHA-256算法进行MAC化的JWS：{“typ”“JWT”“alg”“HS256”}以消除上述JSON对象表示中的潜在歧义，实际的UTF-8repr的八位序列上面的若泽标题中使用的ESPORT也包括在下面。

en, differing spacing at the beginning and ends of lines, whether the last line has a terminating line break or not, and other causes.
[zh_CN]（请注意，由于线路中断的不同平台表示（CRLF与LF）、线路开始和结束处的不同间隔、最后一行是否具有终止线路中断以及其他原因，可能产生模糊性。

[en]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 the UTF-8 representation of the JOSE 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] Base64url encoding the octets of the UTF-8 representation of the JOSE Header yields this encoded JOSE Header value: eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9 The following is an example of a JWT Claims Set: {"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 JWT Claims Set above, is the JWS Payload: [123, 34, 105, 115, 115, 34, 58, 34, 106, 111, 101, 34, 44, 13, 10, 32, 34, 101, 120, 112, 34, 58, 49, 51, 48, 48, 56, 49, 57, 51, 56, 48, 44, 13, 10, 32, 34, 104, 116, 116, 112, 58, 47, 47, 101, 120, 97, 109, 112, 108, 101, 46, 99, 111, 109, 47, 105, 115, 95, 114, 111, 111, 116, 34, 58, 116, 114, 117, 101, 125] Jones, et al.
[zh_CN]在本示例中使用的表示中，第一行没有前导或后导空间，在第一和第二行之间出现CRLF断线(13，10)，第二行具有一个前导空间(32)和没有后导空间，最后一行没有终止断线。)在这个示例中，表示JOSE报头的UTF-8表示的s（使用JSON数组符号）是：[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]Base64url，编码第th个UTF-8表示的八位字节e JOSE Header产生这个编码的JOSE Header值：eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9以下是JWT声明集的示例：{"iss":"joe","exp":1300819380","http://example.com/is_root":true}以下八位组序列，它是在本示例中使用的UTF-8表示，例如以上所设置的JWT索赔是JWS有效载荷：[123、34、105、115、115、34、58、34、106、111、101、34、44、13、10、32、34、101、120、112、112、34、112、58、49、120、112、112、49、51、51、51、51、51、51、48、48、48、48、57、51、56、56、48、44、13、10、32、34、104、116、116、116、116、112、58、47、101、101、120、97、109、112、108、46、99、109、47、105、115, 95, 114，111, 111, 116，34, 58, 116，114, 117, 101，125，琼斯等。

[en]Standards Track [Page 7] RFC 7519 JSON Web Token (JWT) May 2015 Base64url encoding the JWS Payload yields this encoded JWS Payload (with line breaks for display purposes only): eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly 9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ Computing the MAC of the encoded JOSE Header and encoded JWS Payload with the HMAC SHA-256 algorithm and base64url encoding the HMAC value in the manner specified in [JWS] yields this encoded JWS Signature: dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk Concatenating these encoded parts in this order with period ('.') characters between the parts yields this complete JWT (with line breaks for display purposes only): eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9 .
[zh_CN]标准跟踪[第7页]RFC 7519 JSON Web令牌(JWT)2015年5月Base64url编码JWS Payload产生此编码的JWS Payload(仅用于显示目的的换行)：eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQog Imh0dHA6Ly9leGFtcGxlLmNvbS9pc190Ijp0cnVlfQ计算e的MAC用HMAC SHA-256算法编码的JOSE Header和编码的

JWS Payload以及以[JWS]中指定的方式对HMAC值进行编码的base64url产生这个编码的JWS签名：dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk，按照这个顺序将这些编码部分与周期('.')字符连接部件之间的rs产生这个完整的JWT（仅用于显示目的的换行）： eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9。

[en]eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFt
cGxlLmNvbS9pc19yb290Ijp0cnVlfQ .
[zh_CN]EYJPC3MIOIJQB2UIA00KICJLYHOIZEJMAD44MTKZODASDQOGIMIMH0DHA6LY9LYFFT
CGXLLMNVBS9BPC19YB290IJP0CNVLFQ。

[en]dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk This computation is illustrated in more detail in Appendix A.1 of [JWS].
[zh_CN]这一计算在[JWS]的附录A.1中更详细地说明。

[en]See Appendix A.1 for an example of an encrypted JWT.
[zh_CN]有关加密JWT的示例，请参见附录A.1。

4. JWT Claims

[en]The JWT Claims Set represents a JSON object whose members are the claims conveyed by the JWT.
[zh_CN]JWT Read SET表示JSON对象，其成员是JWT传递的声明。

[en]The Claim Names within a JWT Claims Set MUST be unique; JWT parsers MUST either reject JWTs with duplicate Claim 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].
[zh_CN]JWT声明集中的声明名必须是唯一的；JWT解析器必须拒绝使用重复的声明名的JWTs，或者使用只返回词汇上最后一个重复成员名的JSON解析器，如ECMAScript 5.1 [ECMAScript]的第15.12节（“JSON对象”）中指定的。

[en]The set of claims that a JWT must contain to be considered valid is context dependent and is outside the scope of this specification.
[zh_CN]JWT必须包含的一组声明被认为是有效的，这与上下文有关，超出了本规范的范围。

[en]Specific applications of JWTs will require implementations to understand and process some claims in particular ways.
[zh_CN]JWTS的具体应用将需要实现以特定方式理解和处理某些索赔。

[en]However, in the absence of such requirements, all claims that are not understood by implementations MUST be ignored.
[zh_CN]然而，在没有这样的要求的情况下，所有不被实现理解的请求都必须被忽略。

[en]There are three classes of JWT Claim Names: Registered Claim Names, Public Claim Names, and Private Claim Names.
[zh_CN]JWT索赔名称有三类：注册索赔名称、公共索赔名称和私人索赔名称。

[en]Jones, et al.
[zh_CN]琼斯等。

4.1. Registered Claim Names

[en]The following Claim Names are registered in the IANA "JSON Web Token Claims" registry established by Section 10.1.
[zh_CN]下列索赔名称在IANA“JSON Web令牌索赔”注册处注册，由第10.1节建立。

[en]None of the claims defined below are intended to be mandatory to use or implement in all cases, but rather they provide a starting point for a set of useful, interoperable claims.
[zh_CN]下列定义中的任何一项都不是强制性地在所有情况下使用或实施，而是为一套有用的互操作性索赔提供起点。

[en]Applications using JWTs should define which specific claims they use and when they are required or optional.
[zh_CN]使用JWTS的应用程序应该定义它们使用哪些特定的声明以及何时需要或可选。

[en]All the names are short because a core goal of JWTs is for the representation to be compact.
[zh_CN]所有的名字都是短的，因为JWTS的核心目标是表示简洁。

4.1.1. "iss" (Issuer) Claim

[en]The "iss" (issuer) claim identifies the principal that issued the JWT.
[zh_CN]“ISS”（颁发者）声明标识了发布JWT的主体。

[en]The processing of this claim is generally application specific.
[zh_CN]该索赔的处理一般是特定于应用的。

[en]The "iss" value is a case-sensitive string containing a StringOrURI value.
[zh_CN]“ISS”值是一个包含String Rururi值的大小写敏感字符串。

[en]Use of this claim is OPTIONAL.
[zh_CN]使用此索赔是可选的。

4.1.2. "sub" (Subject) Claim

[en]The "sub" (subject) claim identifies the principal that is the subject of the JWT.
[zh_CN]“子”（主语）权利要求是指JWT的主体。

[en]The claims in a JWT are normally statements about the subject.
[zh_CN]JWT中的权利要求通常是关于主体的陈述。

[en]The subject value MUST either be scoped to be locally unique in the context of the issuer or be globally unique.
[zh_CN]主题值必须在发行者的上下文中被限定为局部唯一的，或者是全局唯一的。

[en]The processing of this claim is generally application specific.
[zh_CN]该索赔的处理一般是特定于应用的。

[en]The "sub" value is a case-sensitive string containing a StringOrURI value.
[zh_CN]“子”值是一个包含String Rururi值的大小写敏感字符串。

[en]Use of this claim is OPTIONAL.
[zh_CN]使用此索赔是可选的。

4.1.3. "aud" (Audience) Claim

[en]The "aud" (audience) claim identifies the recipients that the JWT is intended for.
[zh_CN]“AUD”（观众）声明标识JWT想要的收件人。

[en]Each principal intended to process the JWT MUST identify itself with a value in the audience claim.
[zh_CN]每个想要处理JWT的主体都必须在观众要求中确定自己的价值。

[en]If the principal processing the claim does not identify itself with a value in the "aud" claim when this claim is present, then the JWT MUST be rejected.
[zh_CN]如果当存在索赔时，主处理索赔没有用“aud”索赔中的值标识自己，则必须拒绝JWT。

[en]In the general case, the "aud" value is an array of case- sensitive strings, each containing a StringOrURI value.
[zh_CN]在一般情况下，“AUD”值是一个区分大小写字符串的数组，每个字符串包含一个StRigururi值。

[en]In the special case when the JWT has one audience, the "aud" value MAY be a single case-sensitive string containing a StringOrURI value.
[zh_CN]在JWT只有一个受众的特殊情况下，“aud”值可能是包含StringOrURI值的单个区分大小写的字符串。

[en]The interpretation of audience values is generally application specific.
[zh_CN]受众价值的解释通常是特定于应用的。

[en]Use of this claim is OPTIONAL.
[zh_CN]使用此索赔是可选的。

4.1.4. "exp" (Expiration Time) Claim

[en]The "exp" (expiration time) claim identifies the expiration time on or after which the JWT MUST NOT be accepted for processing.
[zh_CN]“EXP”（到期时间）要求标识JWT在处理之后或之后不能接受的到期时间。

[en]The processing of the "exp" claim requires that the current date/time MUST be before the expiration date/time listed in the "exp" claim.
[zh_CN]“EXP”索赔的处理要求当前日期/时间必须在“EXP”索赔中列出的有效日期/时间之前。

[en]Jones, et al.
[zh_CN]琼斯等。

[en]Standards Track [Page 9] RFC 7519 JSON Web Token (JWT) May 2015 Implementers MAY provide for some small leeway, usually no more than a few minutes, to account for clock skew.
[zh_CN]标准跟踪[第9页]RFC 7519 JSON Web Token(JWT)2015年5月实现程序可能提供一些小的回旋余地，通常不超过几分钟，以解决时钟偏移。

[en]Its value MUST be a number containing a NumericDate value.
[zh_CN]它的值必须是包含数值日期值的数字。

[en]Use of this claim is OPTIONAL.
[zh_CN]使用此索赔是可选的。

4.1.5. "nbf" (Not Before) Claim

[en]The "nbf" (not before) claim identifies the time before which the JWT MUST NOT be accepted for processing.
[zh_CN]“NBF”（以前没有）要求识别JWT在处理之前不被接受的时间。

[en]The processing of the "nbf" claim requires that the current date/time MUST be after or equal to the not-before date/time listed in the "nbf" claim.
[zh_CN]“nbf”索赔的处理要求当前日期/时间必须在“nbf”索赔中列出的日期/时间之后或相等。

[en]Implementers MAY provide for some small leeway, usually no more than a few minutes, to account for clock skew.
[zh_CN]实施者可以提供一些小的余地，通常不超过几分钟，以解释时钟偏移。

[en]Its value MUST be a number containing a NumericDate value.
[zh_CN]它的值必须是包含数值日期值的数字。

[en]Use of this claim is OPTIONAL.
[zh_CN]使用此索赔是可选的。

4.1.6. "iat" (Issued At) Claim

[en]The "iat" (issued at) claim identifies the time at which the JWT was issued.
[zh_CN]“IAT”（发出）要求确定JWT发出的时间。

[en]This claim can be used to determine the age of the JWT.
[zh_CN]这种说法可以用来确定JWT的年龄。

[en]Its value MUST be a number containing a NumericDate value.
[zh_CN]它的值必须是包含数值日期值的数字。

[en]Use of this claim is OPTIONAL.
[zh_CN]使用此索赔是可选的。

4.1.7. "jti" (JWT ID) Claim

[en]The "jti" (JWT ID) claim provides a unique identifier for the JWT.
[zh_CN]“JTI”（JWT ID）声明为JWT提供了唯一的标识符。

[en]The identifier value MUST be assigned in a manner that ensures that there is a negligible probability that the same value will be accidentally assigned to a different data object; if the application uses multiple issuers, collisions MUST be prevented among values produced by different issuers as well.
[zh_CN]标识符值必须以能够确保将相同的值意外地分配给不同的数据对象的可能性可以忽略不计的方式分配；如果应用程序使用多个发行者，则必须防止不同发行者产生的值之间的冲突，就像我们这样陆上通信线。

[en]The "jti" claim can be used to prevent the JWT from being replayed.
[zh_CN]“JTI”声明可以用来防止JWT被重放。

[en]The "jti" value is a case- sensitive string.
[zh_CN]“JTI”值是一个区分大小写的字符串。

[en]Use of this claim is OPTIONAL.
[zh_CN]使用此索赔是可选的。

4.2. Public Claim Names

[en]Claim Names can be defined at will by those using JWTs.
[zh_CN]使用JWTS的人可以随意定义索赔名称。

[en]However, in order to prevent collisions, any new Claim Name should either be registered in the IANA "JSON Web Token Claims" registry established by Section 10.1 or be a Public Name: a value that contains a Collision-Resistant Name.
[zh_CN]然而，为了防止冲突，任何新的索赔名称都应该注册在由第10.1节建立的IANA“JSON Web令牌索赔”注册表中，或者为公共名称：包含抗碰撞名称的值。

[en]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 Claim Name.
[zh_CN]在每种情况下，名称或值的定义者都需要采取合理的预防措施，以确保它们能够控制用于定义Claim Name的名称空间的一部分。

4.3. Private Claim Names

[en]A producer and consumer of a JWT MAY agree to use Claim Names that are Private Names: names that are not Registered Claim Names (Section 4.1) or Public Claim Names (Section 4.2).
[zh_CN]JWT的生产者和消费者可能同意使用作为私有名称的索赔名称：不是注册索赔名称（第4.1节）或公共索赔名称（第4.2节）的名称。

[en]Unlike Public Jones, et al.
[zh_CN]不像公众琼斯等。

[en]Standards Track [Page 10] RFC 7519 JSON Web Token (JWT) May 2015 Claim Names, Private Claim Names are subject to collision and should be used with caution.
[zh_CN]标准轨道[第10页] RFC 7519 JSON Web令牌（JWT）2015年5月索赔名称，私人索赔名称受到碰撞，并应谨慎使用。

5. JOSE Header

[en]For a JWT object, the members of the JSON object represented by the JOSE Header describe the cryptographic operations applied to the JWT and optionally, additional properties of the JWT.
[zh_CN]对于JWT对象，由JOSE Header表示的JSON对象的成员描述应用于JWT的加密操作以及可选的JWT的附加属性。

[en]Depending upon whether the JWT is a JWS or JWE, the corresponding rules for the JOSE Header values apply.
[zh_CN]根据JWT是否是JWS或JWE，应用若泽头值的相应规则。

[en]This specification further specifies the use of the following Header Parameters in both the cases where the JWT is a JWS and where it is a JWE.
[zh_CN]此规范进一步指定在JWT是JWS和JWE两种情况下使用以下Header Parameters。

5.1. "typ" (Type) Header Parameter

[en]The "typ" (type) Header Parameter defined by [JWS] and [JWE] is used by JWT applications to declare the media type [IANA.MediaTypes] of this complete JWT.
[zh_CN]JWT应用程序使用[JWS]和[JWE]定义的“typ”（type）Header Parameter来声明这个完整的JWT的媒体类型[IANA.MediaTypes]。

[en]This is intended for use by the JWT application when values that are not JWTs could also be present in an application data structure that can contain a JWT object; the application can use this value to disambiguate among the different kinds of objects that might be present.
[zh_CN]当非JWT的值也可以出现在可以包含JWT对象的应用程序数据结构中时，JWT应用程序将使用这个值；应用程序可以使用这个值来消除可能存在的不同类型的对象之间的歧义。

[en]It will typically not be used by applications when it is already known that the object is a JWT.
[zh_CN]当它已经知道对象是JWT时，它通常不会被应用程序使用。

[en]This parameter is ignored by JWT implementations; any processing of this parameter is performed by the JWT application.
[zh_CN]JWT实现忽略了此参数；该参数的任何处理都由JWT应用程序执行。

[en]If present, it is RECOMMENDED that its value be "JWT" to indicate that this object is a JWT.
[zh_CN]如果存在，建议其值为“JWT”，以指示该对象是JWT。

[en]While media type names are not case sensitive, it is RECOMMENDED that "JWT" always be spelled using uppercase characters for compatibility with legacy implementations.
[zh_CN]虽然媒体类型名称不区分大小写，但为了与遗留实现兼容，始终使用大写字母拼写“JWT”是RECOMMENDED。

[en]Use of this Header Parameter is OPTIONAL.
[zh_CN]此头参数的使用是可选的。

5.2. "cty" (Content Type) Header Parameter

[en]The "cty" (content type) Header Parameter defined by [JWS] and [JWE] is used by this specification to convey structural information about the JWT.
[zh_CN]本规范使用[JWS]和[JWE]定义的“cty”（内容类型）Header Parameter来传递关于JWT的结构信息。

[en]In the normal case in which nested signing or encryption operations are not employed, the use of this Header Parameter is NOT RECOMMENDED.
[zh_CN]在不采用嵌套签名或加密操作的正常情况下，不建议使用此Header参数。

[en]In the case that nested signing or encryption is employed, this Header Parameter MUST be present; in this case, the value MUST be "JWT", to indicate that a Nested JWT is carried in this JWT.
[zh_CN]在采用嵌套签名或加密的情况下，必须存在该报头参数；在这种情况下，值必须是“JWT”，以指示在该JWT中携带嵌套JWT。

[en]While media type names are not case sensitive, it is RECOMMENDED that "JWT" always be spelled using uppercase characters for compatibility with legacy implementations.
[zh_CN]虽然媒体类型名称不区分大小写，但为了与遗留实现兼容，始终使用大写字母拼写“JWT”是RECOMMENDED。

[en]See Appendix A.2 for an example of a Nested JWT.
[zh_CN]关于嵌套JWT的一个例子，参见附录A.2。

[en]Jones, et al.
[zh_CN]琼斯等。

5.3. Replicating Claims as Header Parameters

[en]In some applications using encrypted JWTs, it is useful to have an unencrypted representation of some claims.
[zh_CN]在一些使用加密JWTS的应用中，有一些请求的未加密表示是有用的。

[en]This might be used, for instance, in application processing rules to determine whether and how to process the JWT before it is decrypted.
[zh_CN]例如，这可以在应用程序处理规则中使用，以确定是否以及如何在对JWT进行解密之前对其进行处理。

[en]This specification allows claims present in the JWT Claims Set to be replicated as Header Parameters in a JWT that is a JWE, as needed by the application.
[zh_CN]根据应用程序的需要，此规范允许在JWT索赔集中出现的索赔作为JWE的JWT中的Header参数进行复制。

[en]If such replicated claims are present, the application receiving them SHOULD verify that their values are identical, unless the application defines other specific processing rules for these claims.
[zh_CN]如果存在这种复制的索赔，则接收它们的应用程序应验证其值是否相同，除非应用程序为这些索赔定义了其他特定的处理规则。

[en]It is the responsibility of the application to ensure that only claims that are safe to be transmitted in an unencrypted manner are replicated as Header Parameter values in the JWT.
[zh_CN]应用程序的职责是确保仅将安全地以未加密方式传输的声明复制为JWT中的Header Parameter值。

[en]Section 10.4.1 of this specification registers the "iss" (issuer), "sub" (subject), and "aud" (audience) Header Parameter names for the purpose of providing unencrypted replicas of these claims in encrypted JWTs for applications that need them.
[zh_CN]本规范的第10.4.1节注册“iss”（发行者）、“sub”（主题）和“aud”（观众）报头参数名称，以便为需要它们的应用程序在加密的JWT中提供这些声明的未加密副本。

[en]Other specifications MAY similarly register other names that are registered Claim Names as Header Parameter names, as needed.
[zh_CN]根据需要，其他规范也可以将注册请求名称的其他名称作为头参数名注册。

6. Unsecured JWTs

[en]To support use cases in which the JWT content is secured by a means other than a signature and/or encryption contained within the JWT (such as a signature on a data structure containing the JWT), JWTs MAY also be created without a signature or encryption.
[zh_CN]为了支持JWT内容由JWT中包含的签名和/或加密以外的方法（例如，在包含JWT的数据结构上的签名）来确保的JWT内容的使用情况，JWTS也可以在没有签名或加密的情况下被创建。

[en]An Unsecured JWT is a JWS using the "alg" Header Parameter value "none" and with the empty string for its JWS Signature value, as defined in the JWA specification [JWA]; it is an Unsecured JWS with the JWT Claims Set as its JWS Payload.
[zh_CN]不安全JWT是使用“alg”Header Parameter值“none”的JWS，其JWS签名值使用空字符串，如JWA规范[JWA]中所定义；它是一个不安全JWS，JWT声明集作为其JWS有效负载。

6.1. Example Unsecured JWT

[en]The following example JOSE Header declares that the encoded object is an Unsecured JWT: {"alg":"none"} Base64url encoding the octets of the UTF-8 representation of the JOSE Header yields this encoded JOSE Header value: eyJhbGciOiJub25lIn0 Jones, et al.
[zh_CN]下面的示例JOSE Header声明所编码的对象是一个不安全的JWT：{"alg":"none"}Base64url对JOSE Header的UTF-8表示的八位元组进行编码，得到这个已编码的JOSE Header值：eyJhbGciOiJub25lIn0 Jones等。

[en]Standards Track [Page 12] RFC 7519 JSON Web Token (JWT) May 2015 The following is an example of a JWT Claims Set: {"iss":"joe", "exp":1300819380, "http://example.com/is_root":true} Base64url encoding the octets of the UTF-8 representation of the JWT Claims Set yields this encoded JWS Payload (with line breaks for display purposes only): eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFt
cGxlLmNvbS9pc19yb290Ijp0cnVlfQ The encoded JWS Signature is the empty string.
[zh_CN]标准跟踪[第12页]RFC 7519 JSON Web令牌（JWT）2015年5月以下是JWT声明集的一个示例：
{"iss":"joe","exp":1300819380,"http://example.com/is_root":true}Base64url编码JWT声明集的UTF-8表示的八位字节，从而产生这个编码的JWS Payload（具有仅用于显示目的的换行：
eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFt
cGxlLmNvbS9pc19yb290Ijp0cnVlfQ编码JWS签名是空字符串。

[en]Concatenating these encoded parts in this order with period ('.') characters between the parts yields this complete JWT (with line breaks for display purposes only): eyJhbGciOiJub25lIn0 .
[zh_CN]以这种顺序将这些编码部分与部分之间的句点（“.”）字符连接产生完整的JWT（仅用于显示目的的换行符）：
eyJhbGciOiJub25lIn0。

[en]eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogImh0dHA6Ly9leGFt
cGxlLmNvbS9pc19yb290Ijp0cnVlfQ .
[zh_CN]EYJPC3MIOIJQB2UIA00KICJLYHOIZEJMAD44MTKZODASDQOGIMIMH0DHA6LY9LYFFT
CGXLLMNVBS9BPC19YB290IJP0CNVLFQ。

7. Creating and Validating JWTs

7.1. Creating a JWT

[en]To create a JWT, the following steps are performed.
[zh_CN]要创建JWT，执行以下步骤。

[en]The order of the steps is not significant in cases where there are no dependencies between the inputs and outputs of the steps.
[zh_CN]在步骤的输入和输出之间不存在依赖关系的情况下，步骤的顺序并不重要。

[en]1.
[zh_CN]1。

[en]Create a JWT Claims Set containing the desired claims.
[zh_CN]创建包含期望索赔的JWT索赔集。

[en]Note that whitespace is explicitly allowed in the representation and no canonicalization need be performed before encoding.
[zh_CN]注意，在表示中明确允许空白，并且在编码之前不需要执行规范化。

[en]2.
[zh_CN]2。

[en]Let the Message be the octets of the UTF-8 representation of the JWT Claims Set.
[zh_CN]让消息成为JWT声明集的UTF-8表示的八位字节。

[en]3.
[zh_CN]三。

[en]Create a JOSE Header containing the desired set of Header Parameters.
[zh_CN]创建包含所需的头参数集的若泽标题。

[en]The JWT MUST conform to either the [JWS] or [JWE] specification.
[zh_CN]JWT必须符合[JWS]或[JWE]规范。

[en]Note that whitespace is explicitly allowed in the representation and no canonicalization need be performed before encoding.
[zh_CN]注意，在表示中明确允许空白，并且在编码之前不需要执行规范化。

[en]Jones, et al.
[zh_CN]琼斯等。

[en]Standards Track [Page 13] RFC 7519 JSON Web Token (JWT) May 2015 4.
[zh_CN]标准轨道[页面13] RFC 7519 JSON Web令牌（JWT）2015年5月4。

[en]Depending upon whether the JWT is a JWS or JWE, there are two cases: *If the JWT is a JWS, create a JWS using the Message as the JWS Payload; all steps specified in [JWS] for creating a JWS MUST be followed.*
*[zh_CN]*根据*JWT*是*JWS*还是*JWE*，有两种情况：如果JWT是JWS，则使用Message作为JWS有效负载创建JWS；必须遵循[JWS]中为创建JWS指定的所有步骤。

[en] *Else, if the JWT is a JWE, create a JWE using the Message as the plaintext for the JWE; all steps specified in [JWE] for creating a JWE MUST be followed.*
*[zh_CN]*否则，如果JWT是JWE，则使用Message作为JWE的明文创建一个JWE；必须遵循[JWE]中为创建JWE指定的所有步骤。

[en]5.
[zh_CN]5。

[en]If a nested signing or encryption operation will be performed, let the Message be the JWS or JWE, and return to Step 3, using a "cty" (content type) value of "JWT" in the new JOSE Header created in that step.
[zh_CN]如果将执行嵌套签名或加密操作，则让Message为JWS或JWE，并使用该步骤中创建的新JOSE Header中的“cty”（内容类型）值“JWT”返回步骤3。

[en]6.
[zh_CN]6。

[en]Otherwise, let the resulting JWT be the JWS or JWE.
[zh_CN]否则，使所得JWT为JWS或JWE。

7.2. Validating a JWT

[en]When validating a JWT, the following steps are performed.
[zh_CN]在验证JWT时，执行以下步骤。

[en]The order of the steps is not significant in cases where there are no dependencies between the inputs and outputs of the steps.
[zh_CN]在步骤的输入和输出之间不存在依赖关系的情况下，步骤的顺序并不重要。

[en]If any of the listed steps fail, then the JWT MUST be rejected -- that is, treated by the application as an invalid input.
[zh_CN]如果列出的任何步骤失败，则必须拒绝JWT，也就是说，应用程序作为无效输入进行处理。

[en]1.
[zh_CN]1。

[en]Verify that the JWT contains at least one period ('.') character.
[zh_CN]验证JWT包含至少一个周期（'.'）字符。

[en]2.
[zh_CN]2。

[en]Let the Encoded JOSE Header be the portion of the JWT before the first period ('.') character.
[zh_CN]让编码的若泽头在第一个周期（'.'）字符之前是JWT的一部分。

[en]3.
[zh_CN]三。

[en]Base64url decode the Encoded JOSE Header following the restriction that no line breaks, whitespace, or other additional characters have been used.
[zh_CN]Base64url对Encoded JOSE Header进行解码，遵守没有使用分行、空白或其他附加字符的限制。

[en]4.
[zh_CN]4。

[en]Verify that the resulting octet sequence is a UTF-8-encoded representation of a completely valid JSON object conforming to RFC 7159 [RFC7159]; let the JOSE Header be this JSON object.
[zh_CN]验证所得到的八位字节序列是符合RFC7159[RFC7159]的完全有效的JSON对象的UTF-8编码表示；让JOSE Header是这个JSON对象。

[en]5.
[zh_CN]5。

[en]Verify that the resulting JOSE Header includes only parameters and values whose syntax and semantics are both understood and supported or that are specified as being ignored when not understood.
[zh_CN]验证所得到的JOSE Header仅包括语法和语义都可理解和支持的参数和值，或者当不理解时指定为忽略的参数和值。

[en]6.
[zh_CN]6。

[en]Determine whether the JWT is a JWS or a JWE using any of the methods described in Section 9 of [JWE].
[zh_CN]使用JWE的第9节中描述的任何方法来确定JWT是否是JWS或JWE。

[en]Jones, et al.
[zh_CN]琼斯等。

[en]Standards Track [Page 14] RFC 7519 JSON Web Token (JWT) May 2015 7.
[zh_CN]标准轨道[页面14] RFC 7519 JSON Web令牌（JWT）2015年5月7。

[en]Depending upon whether the JWT is a JWS or JWE, there are two cases: *If the JWT is a JWS, follow the steps specified in [JWS] for validating a JWS.*
*[zh_CN]*根据*JWT*是*JWS*还是*JWE*，有两种情况：如果JWT是JWS，请遵循[JWS]中指定的步骤来验证JWS。

[en]Let the Message be the result of base64url decoding the JWS Payload.
[zh_CN]让消息是Base64 URL解码JWS有效载荷的结果。

[en]* Else, if the JWT is a JWE, follow the steps specified in [JWE] for validating a JWE.
[zh_CN]否则，如果JWT是JWE，按照JWE中指定的步骤来验证JWE。

[en]Let the Message be the resulting plaintext.
[zh_CN]让消息成为最终的明文。

[en]8.
[zh_CN]8。

[en]If the JOSE Header contains a "cty" (content type) value of "JWT", then the Message is a JWT that was the subject of nested signing or encryption operations.
[zh_CN]如果JOSE头包含“JWT”的“cty”（内容类型）值，则消息是嵌套签名或加密操作的主题。

[en]In this case, return to Step 1, using the Message as the JWT.
[zh_CN]在这种情况下，返回到步骤1，使用该消息作为JWT。

[en]9.
[zh_CN]9。

[en]Otherwise, base64url decode the Message following the restriction that no line breaks, whitespace, or other additional characters have been used.
[zh_CN]否则，base64url在没有使用分行、空白或其他附加字符的限制下对Message进行解码。

[en]10.
[zh_CN]10。

[en]Verify that the resulting octet sequence is a UTF-8-encoded representation of a completely valid JSON object conforming to RFC 7159 [RFC7159]; let the JWT Claims Set be this JSON object.
[zh_CN]验证所得到的八位字节序列是符合RFC7159[RFC7159]的完全有效的JSON对象的UTF-8编码表示；让JWT声明集是这个JSON对象。

[en]Finally, note that it is an application decision which algorithms may be used in a given context.
[zh_CN]最后，请注意，它是一种应用决策，算法可以在给定的上下文中使用。

[en]Even if a JWT can be successfully validated, unless the algorithms used in the JWT are acceptable to the application, it SHOULD reject the JWT.
[zh_CN]即使JWT可以成功验证，除非JWT中使用的算法被应用程序接受，否则它应该拒绝JWT。

7.3. String Comparison Rules

[en]Processing a JWT inevitably requires comparing known strings to members and values in JSON objects.
[zh_CN]处理JWT不可避免地需要将已知字符串与JSON对象中的成员和值进行比较。

[en]For example, in checking what the algorithm is, the Unicode [UNICODE] string encoding "alg" will be checked against the member names in the JOSE Header to see if there is a matching Header Parameter name.
[zh_CN]例如，在检查算法是什么时，将根据JOSE Header中的成员名称检查编码“alg”的Unicode[UNICODE]字符串，以查看是否有匹配的Header Parameter名称。

[en]The JSON rules for doing member name comparison are described in Section 8.3 of RFC 7159 [RFC7159].
[zh_CN]在RFC 7159 [RFC7159]的第8.3节中描述了用于执行成员名称比较的JSON规则。

[en]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.
[zh_CN]因为执行的唯一字符串比较操作是相等和不等式，所以可以使用相同的规则来比较成员名和成员值与已知字符串。

[en]These comparison rules MUST be used for all JSON string comparisons except in cases where the definition of the member explicitly calls out that a different comparison rule is to be used for that member value.
[zh_CN]这些比较规则必须用于所有JSON字符串比较，除非成员的定义显式地调用将对该成员值使用不同的比较规则。

[en]In this specification, only the "typ" and "cty" member values do not use these comparison rules.
[zh_CN]在本规范中，只有“TYP”和“CTY”成员值不使用这些比较规则。

[en]Jones, et al.
[zh_CN]琼斯等。

[en]Standards Track [Page 15] RFC 7519 JSON Web Token (JWT) May 2015 Some applications may include case-insensitive information in a case- sensitive value, such as including a DNS name as part of the "iss" (issuer) claim value.
[zh_CN]标准跟踪[第15页]RFC 7519 JSON Web令牌(JWT)2015年5月一些应用程序可能在区分大小写的值中包括不区分大小写的信息，例如将DNS名称作为“iss”(发行者)索赔值的一部分包含。

[en]In those cases, the application may need to define a convention for the canonical case to use for representing the case-insensitive portions, such as lowercasing them, if more than one party might need to produce the same value so that they can be compared.
[zh_CN]在这些情况下，如果多方可能需要产生相同的值以便能够进行比较，则应用程序可能需要定义用于表示不区分大小写的部分的规范用例的约定，例如将其小写。

8. Implementation Requirements

[en]This section defines which algorithms and features of this specification are mandatory to implement.
[zh_CN]本节定义了该规范的哪些算法和特征是强制实现的。

[en]Applications using this specification can impose additional requirements upon implementations that they use.
[zh_CN]使用此规范的应用程序可以对它们使用的实现施加额外的要求。

[en]For instance, one application might require support for encrypted JWTs and Nested JWTs, while another might require support for signing JWTs with the Elliptic Curve Digital Signature Algorithm (ECDSA) using the P-256 curve and the SHA-256 hash algorithm ("ES256").
[zh_CN]例如，一个应用程序可能需要支持加密JWT和嵌套JWT，而另一个应用程序可能需要支持使用P-256曲线和SHA-256散列算法(“ES256”)使用椭圆曲线数字签名算法(ECDSA)对JWT进行签名。

[en]Of the signature and MAC algorithms specified in JSON Web Algorithms [JWA], only HMAC SHA-256 ("HS256") and "none" MUST be implemented by conforming JWT implementations.
[zh_CN]在JSON Web算法[JWA]中指定的签名和MAC算法中，只有HMAC SHA-256(“HS256”)和“none”必须通过符合JWT实现来实现。

[en]It is RECOMMENDED that implementations also support RSASSA-PKCS1-v1_5 with the SHA-256 hash algorithm ("RS256") and ECDSA using the P-256 curve and the SHA-256 hash algorithm ("ES256").
[zh_CN]建议使用SHA-256散列算法(“RS256”)以及使用P-256曲线和SHA-256散列算法(“ES256”)的ECDSA，实现也支持RSASSA-PKCS1-v1_5。

[en]Support for other algorithms and key sizes is OPTIONAL.
[zh_CN]其他算法和密钥大小的支持是可选的。

[en]Support for encrypted JWTs is OPTIONAL.
[zh_CN]对加密JWT的支持是可选的。

[en]If an implementation provides encryption capabilities, of the encryption algorithms specified in [JWA], only RSAES-PKCS1-v1_5 with 2048-bit keys ("RSA1_5"), AES Key Wrap with 128- and 256-bit keys ("A128KW" and "A256KW"), and the composite authenticated encryption algorithm using AES-CBC and HMAC SHA-2 ("A128CBC-HS256" and "A256CBC-HS512") MUST be implemented by conforming implementations.
[zh_CN]如果一个实现提供了[JWA]中指定的加密算法的加密能力，则只有RSAES-PKCS1-v1_5具有2048位的密钥(“RSA1_5”)，AES密钥包装具有128位和256位的密钥(“A128KW”和“A256KW”)，以及使用AES-CBC和HMAC S的复合认证加密算法。HA-2（“A128CBC-HS256”和“A256CBC-HS512”）必须通过一致的实现来实现。

[en]It is RECOMMENDED that implementations also support using Elliptic Curve Diffie-Hellman Ephemeral Static (ECDH-ES) to agree upon a key used to wrap the Content Encryption Key ("ECDH-ES+A128KW" and "ECDH-ES+A256KW") and AES in Galois/Counter Mode (GCM) with 128- and 256-bit keys ("A128GCM" and "A256GCM").
[zh_CN]建议实现还支持使用椭圆曲线.ie-Hellman临时静态(ECDH-ES)来商定用于将内容加密密钥(“ECDH-ES+A128KW”和“ECDH-ES+A256KW”)和AES封装为Galois/.模式(GCM)的128位和256位密钥(“A128GCM”和“A256KW”)的密钥。GCM“。

[en]Support for other algorithms and key sizes is OPTIONAL.
[zh_CN]其他算法和密钥大小的支持是可选的。

[en]Support for Nested JWTs is OPTIONAL.
[zh_CN]对嵌套JWT的支持是可选的。

[en]Jones, et al.
[zh_CN]琼斯等。

9. URI for Declaring that Content is a JWT

[en]This specification registers the URN "urn:ietf:params:oauth:token-type:jwt" for use by applications that declare content types using URIs (rather than, for instance, media types) to indicate that the content referred to is a JWT.
[zh_CN]本规范注册URN“urn:ietf:params:oauth:token-type:jwt”，供使用URI（而不是，例如，媒体类型）声明内容类型的应用程序使用，以指示引用的内容是JWT。

10. IANA Considerations

10.1. JSON Web Token Claims Registry

[en]This section establishes the IANA "JSON Web Token Claims" registry for JWT Claim Names.
[zh_CN]本节建立了IANA“JSON Web令牌声明”JWT请求名称注册表。

[en]The registry records the Claim Name and a reference to the specification that defines it.
[zh_CN]注册表记录索赔名称和对定义它的规范的引用。

[en]This section registers the Claim Names defined in Section 4.1.
[zh_CN]本节登记在第4.1节中定义的索赔名称。

[en]Values are registered on a Specification Required [RFC5226] basis after a three-week review period on the jwt-reg-review@ietf.org mailing list, on the advice of one or more Designated Experts.
[zh_CN]根据一个或多个指定专家的建议，在jwt-reg-.@ietf.org邮件列表上经过三周的审查期后，以规范要求[RFC5226]为基础注册值。

[en]However, to allow for the allocation of values prior to publication, the Designated Experts may approve registration once they are satisfied that such a specification will be published.
[zh_CN]然而，为了允许在发布之前分配值，一旦指定专家确信将公布这样的规范，他们就可以批准注册。

[en]Registration requests sent to the mailing list for review should use an appropriate subject (e.g., "Request to register claim: example").
[zh_CN]发送到邮件列表以供审查的注册请求应当使用适当的主题（例如，“请求注册索赔：示例”）。

[en]Within the review period, the Designated Experts will either approve or deny the registration request, communicating this decision to the review list and IANA.
[zh_CN]在审查期内，指定专家将批准或拒绝登记请求，将该决定传达给审查清单和IANA。

[en]Denials should include an explanation and, if applicable, suggestions as to how to make the request successful.
[zh_CN]拒绝应该包括一个解释，如果适用的话，关于如何使请求成功的建议。

[en]Registration requests that are undetermined for a period longer than 21 days can be brought to the IESG's attention (using the iesg@ietf.org mailing list) for resolution.
[zh_CN]未确定超过21天的注册请求可以提请IESG注意（使用iesg@ietf.org邮件列表）进行解决。

[en]Criteria that should be applied by the Designated Experts includes determining whether the proposed registration duplicates existing functionality, whether it is likely to be of general applicability or whether it is useful only for a single application, and whether the registration description is clear.
[zh_CN]应由指定专家应用的标准包括确定提议的注册是否重复现有功能、它是否可能具有普遍适用性或它是否仅对单个应用程序有用，以及注册描述是否为清楚。

[en]IANA must only accept registry updates from the Designated Experts and should direct all requests for registration to the review mailing list.
[zh_CN]IANA必须只接受指定专家的注册表更新，并应将所有注册请求导向审阅邮件列表。

[en]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.
[zh_CN]建议任命多名指定专家，他们能够使用本说明书代表不同应用的观点，以便能够广泛地审查登记决定。

[en]In cases where a registration decision could Jones, et al.
[zh_CN]在注册决定可以琼斯等的情况下。

[en]Standards Track [Page 17] RFC 7519 JSON Web Token (JWT) May 2015 be perceived as creating a conflict of interest for a particular Expert, that Expert should defer to the judgment of the other Experts.
[zh_CN]标准跟踪[第17页]RFC 7519 JSON Web令牌(JWT)2015年5月被看作为特定专家造成利益冲突，该专家应服从

其他专家的判断。

10.1.1. Registration Template

[en]Claim Name: The name requested (e.g., "iss").
[zh_CN]索赔名称：要求的名称（例如“ISS”）。

[en]Because a core goal of this specification is for the resulting representations to be compact, it is RECOMMENDED that the name be short -- that is, not to exceed 8 characters without a compelling reason to do so.
[zh_CN]因为本规范的核心目标是使结果表示紧凑，所以建议名称要短——也就是说，如果没有强制的理由，不要超过8个字符。

[en]This name is case sensitive.
[zh_CN]这个名称是区分大小写的。

[en]Names may not match other registered names in a case-insensitive manner unless the Designated Experts state that there is a compelling reason to allow an exception.
[zh_CN]除非指定专家声明有令人信服的理由允许异常，否则名称可能不会以区分大小写的方式匹配其他注册名称。

[en]Claim Description: Brief description of the claim (e.g., "Issuer").
[zh_CN]索赔描述：索赔的简要描述（如“发行人”）。

[en]Change Controller: For Standards Track RFCs, list the "IESG".
[zh_CN]更改控制器：对于标准轨道RFC，列出“IESG”。

[en]For others, give the name of the responsible party.
[zh_CN]对于其他人，给出责任方的名称。

[en]Other details (e.g., postal address, email address, home page URI) may also be included.
[zh_CN]还可以包括其他细节（例如，邮政地址、电子邮件地址、主页URI）。

[en]Specification Document(s): Reference to the document or documents that specify the parameter, preferably including URIs that can be used to retrieve copies of the documents.
[zh_CN]规范文档：引用指定参数的文档或文档，最好包括可用于检索文档副本的URI。

[en]An indication of the relevant sections may also be included but is not required.
[zh_CN]也可以包括相关部分的指示，但不需要。

10.1.2. Initial Registry Contents

[en]o Claim Name: "iss" o Claim Description: Issuer o Change Controller: IESG o Specification Document(s): Section 4.1.1 of RFC 7519 o Claim Name: "sub" o Claim Description: Subject o Change Controller: IESG o Specification Document(s): Section 4.1.2 of RFC 7519 o Claim Name: "aud" o Claim Description: Audience o Change Controller: IESG o Specification Document(s): Section 4.1.3 of RFC 7519 Jones, et al.
[zh_CN]o索赔名称：“iss”o索赔说明：发出者o变更控制器：IESG o规范文件：RFC 7519o索赔名称第4.1.1节：“sub”o索赔说明：Sub.o索赔说明：Subject o变更控制器：IESG o规范文件：RFC 7519o索赔名称：“aud”o索赔说明第4.1.2节：观众O改变控制器：IEESG O规范文档（S）：RFC 7519琼斯等人的4.1.3节。

10.2. Sub-Namespace Registration of

10.2.1. Registry Contents

[en]This section registers the value "token-type:jwt" in the IANA "OAuth URI" registry established by "An IETF URN Sub-Namespace for OAuth" [RFC6755], which can be used to indicate that the content is a JWT.
[zh_CN]本节在“用于OAuth的IETF URN子名称空间”[RFC6755]建立的IANA“OAuth URI”注册表中注册值“token-type:jwt”，该值可用于指示内容是JWT。

[en]o URN: urn:ietf:params:oauth:token-type:jwt o Common Name: JSON Web Token (JWT) Token Type o Change Controller: IESG o Specification Document(s): RFC 7519 Jones, et al.
[zh_CN]URN：URN:IETF:PARAM:OAuth:令牌类型：JWT O通用名称：JSON Web令牌（JWT）令牌类型O更改控制器：IESG O规范文档（S）：RFC 7519琼斯等。

10.3. Media Type Registration

10.3.1. Registry Contents

[en]This section registers the "application/jwt" media type [RFC2046] in the "Media Types" registry [IANA.MediaTypes] in the manner described in RFC 6838 [RFC6838], which can be used to indicate that the content is a JWT.
[zh_CN]本节以RFC6838[RFC6838]中描述的方式在“媒体类型”注册表[IANA.MediaTypes]中注册“application/jwt”媒体类型[RFC2046]，这可以用于指示内容是JWT。

[en]o Type name: application o Subtype name: jwt o Required parameters: n/a o Optional parameters: n/a o Encoding considerations: 8bit; JWT values are encoded as a series of base64url-encoded values (some of which may be the empty string) separated by period ('.') characters.
[zh_CN]o类型名称：应用程序o子类型名称：jwt o必需参数：n/o可选参数：n/a o编码注意事项：8bit；JWT值被编码为一系列base64url编码的值（其中一些值可能是空字符串），由句点（'.'）字符分隔。

[en]o Security considerations: See the Security Considerations section of RFC 7519 o Interoperability considerations: n/a o Published specification: RFC 7519 o Applications that use this media type: OpenID Connect, Mozilla Persona, Salesforce, Google, Android, Windows Azure, Amazon Web Services, and numerous others o Fragment identifier considerations: n/a o Additional information: Magic number(s): n/a File extension(s): n/a Macintosh file type code(s): n/a o Person & email address to contact for further information: Michael B.
[zh_CN]o安全注意事项：参见RFC 7519o互操作性注意事项：n/o发布规范：RFC 7519o使用这种媒体类型的应用程序：OpenID连接、Mozilla Persona、Salesforce、Google、Android、Windows Azure、Amazon Web服务和nu片断标识符注意事项：n/a o附加信息：魔术数字：n/a文件扩展名：n/a Macintosh文件类型代码：n/a o个人和电子邮件地址以联系进一步的信息：Michael B。

[en]Jones, mbj@microsoft.com o Intended usage: COMMON o Restrictions on usage: none o Author: Michael B.
[zh_CN]琼斯，Mbj@微软公司打算使用：通用O限制使用：没有O作者：Michael B.

[en]Jones, mbj@microsoft.com o Change controller: IESG o Provisional registration?
[zh_CN]琼斯，MJJ@微软公司更改控制器：IESG临时注册?

10.4. Header Parameter Names Registration

[en]This section registers specific Claim Names defined in Section 4.1 in the IANA "JSON Web Signature and Encryption Header Parameters" registry established by [JWS] for use by claims replicated as Header Parameters in JWEs, per Section 5.3.
[zh_CN]本节在[JWS]建立的IANA“JSON Web签名和加密报头参数”注册表中注册第4.1节中定义的特定索赔名称，以供按5.3节复制为JWE中的报头参数的索赔使用。

[en]Jones, et al.
[zh_CN]琼斯等。

10.4.1. Registry Contents

11. Security Considerations

[en]All of the security issues that are pertinent to any cryptographic application must be addressed by JWT/JWS/JWE/JWK agents.
[zh_CN]所有与任何密码应用相关的安全问题都必须由JWT/JWS/JWE/JWK代理来解决。

[en]Among these issues are protecting the user's asymmetric private and symmetric secret keys and employing countermeasures to various attacks.
[zh_CN]这些问题包括保护用户的非对称私钥和对称密钥，并采取各种攻击对策。

[en]All the security considerations in the JWS specification also apply to JWT, as do the JWE security considerations when encryption is employed.
[zh_CN]JWS规范中的所有安全性注意事项也适用于JWT，在使用加密时JWE安全性注意事项也适用于JWT。

[en]In particular, Sections 10.12 ("JSON Security Considerations") and 10.13 ("Unicode Comparison Security Considerations") of [JWS] apply equally to the JWT Claims Set in the same manner that they do to the JOSE Header.
[zh_CN]特别是，[JWS]的第10.12节（“JSON安全考虑”）和10.13节（“Unicode比较安全考虑”）以与JOSE头部相同的方式同样地应用于JWT声明集。

11.1. Trust Decisions

[en]The contents of a JWT cannot be relied upon in a trust decision unless its contents have been cryptographically secured and bound to the context necessary for the trust decision.
[zh_CN]JWT的内容不能在信任决策中得到依赖，除非其内容已被加密地保护并绑定到信任决策所需的上下文。

[en]In particular, the key(s) used to sign and/or encrypt the JWT will typically need to verifiably be under the control of the party identified as the issuer of the JWT.
[zh_CN]特别地，用于对JWT进行签名和/或加密的密钥通常需要在被识别为JWT发行者的一方的控制下进行可验证地操作。

11.2. Signing and Encryption Order

[en]While syntactically the signing and encryption operations for Nested JWTs may be applied in any order, if both signing and encryption are necessary, normally producers should sign the message and then Jones, et al.
[zh_CN]虽然从语法上讲，嵌套JWT的签名和加密操作可以按任何顺序应用，但是如果需要签名和加密，通常生产者应该对消息进行签名，然后是Jones等。

[en]Standards Track [Page 21] RFC 7519 JSON Web Token (JWT) May 2015 encrypt the result (thus encrypting the signature).
[zh_CN]标准轨道[页面21] RFC 7519 JSON Web令牌（JWT）2015年5月加密结果（从而加密签名）。

[en]This prevents attacks in which the signature is stripped, leaving just an encrypted message, as well as providing privacy for the signer.
[zh_CN]这防止了签名被剥离的攻击，只留下加密的消息，并为签名者提供隐私。

[en]Furthermore, signatures over encrypted text are not considered valid in many jurisdictions.
[zh_CN]此外，加密文本上的签名在许多司法管辖区中不被认为是有效的。

[en]Note that potential concerns about security issues related to the order of signing and encryption operations are already addressed by the underlying JWS and JWE specifications; in particular, because JWE only supports the use of authenticated encryption algorithms, cryptographic concerns about the potential need to sign after encryption that apply in many contexts do not apply to this specification.
[zh_CN]注意，基础JWS和JWE规范已经解决了与签名和加密操作的顺序相关的安全问题；特别是，因为JWE只支持使用经过身份验证的加密算法，所以关于在许多上下文中应用加密后的潜在需要不适用于本规范。

12. Privacy Considerations

[en]A JWT may contain privacy-sensitive information.
[zh_CN]JWT可以包含隐私敏感信息。

[en]When this is the case, measures MUST be taken to prevent disclosure of this information to unintended parties.
[zh_CN]在这种情况下，必须采取措施防止将这些信息泄露给非意愿方。

[en]One way to achieve this is to use an encrypted JWT and authenticate the recipient.
[zh_CN]实现这一点的一种方法是使用加密JWT并验证收件人。

[en]Another way is to ensure that JWTs containing unencrypted privacy-sensitive information are only transmitted using protocols utilizing encryption that support endpoint authentication, such as Transport Layer Security (TLS).
[zh_CN]另一种方法是确保包含未加密的隐私敏感信息的JWT仅使用使用支持端点身份验证的加密协议（如传输层安全性（TLS））进行传输。

[en]Omitting privacy-sensitive information from a JWT is the simplest way of minimizing privacy issues.
[zh_CN]从JWT中省略隐私敏感信息是最小化隐私问题的最简单方式。

13. References

13.1. Normative References

[en][ECMAScript] Ecma International, "ECMAScript Language Specification, 5.1 Edition", ECMA Standard 262, June 2011, <http://www.ecma-international.org/ecma-262/5.1/ ECMA-262.pdf>.
[zh_CN][ECMAScript]Ecma国际，“ECMAScript语言规范，5.1版”，ECMA标准262，2011年6月，http://www.ecma-..org/ecma-262/5.1/ECMA-262.pdf。

[en][IANA.MediaTypes] IANA, "Media Types", http://www.iana.org/assignments/media-types.
[zh_CN][IANA，MediaType] IANA，“媒体类型”，<http://www- iaa. orj/赋值/媒体类型>。

[en][JWA] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, http://www.rfc-editor.org/info/rfc7518.
[zh_CN][jWa]琼斯，M.，“JSON Web算法（JWA）”，RFC 7518，DOI 101748 7/RFC75 18，2015年5月，<http://www. RFC-Edgor.org/Fiel/RFC718>。

[en][JWE] Jones, M.
[zh_CN]琼斯，M.

[en]and J.
[zh_CN]J.

[en]Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015, http://www.rfc-editor.org/info/rfc7516.
[zh_CN]希尔德布兰德，“JSON Web加密（JWE）”，RFC 7516，DOI 101748 7/RFC75 16，2015年5月，http://www. RFC-Edgor.org/Fiel/RFC716>。

[en]Jones, et al.
[zh_CN]琼斯等。

[en]Standards Track [Page 22] RFC 7519 JSON Web Token (JWT) May 2015 [JWS] Jones, M., Bradley, J., and N.
[zh_CN]标准轨道[页面22] RFC 7519 JSON Web令牌（JWT）2015年5月[JWS]琼斯，M.，布拉德利，J.和N。

[en]Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC, May 2015, http://www.rfc-editor.org/info/rfc7515.
[zh_CN]Sakimura，“JSON Web签名（JWS）”，RFC 7515，DOI 101748 7/RFC，2015年5月，http://www. RFC-Edgor.org/Fiel/RFC715>。

[en][RFC20] Cerf, V., "ASCII format for Network Interchange", STD 80, RFC 20, DOI 10.17487/RFC0020, October 1969, http://www.rfc-editor.org/info/rfc20.
[zh_CN][RFC20]Cerf，V.，“用于网络交换的ASCII格式”，STD 80，RFC 20，DOI 10.17487/RFC0020，1969年10月，http://www.rfc-..org/info/rfc20。

[en][RFC2046] Freed, N.
[zh_CN][FRC2046]释放，N.

[en]and N.
[zh_CN]N.

[en]Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, http://www.rfc-editor.org/info/rfc2046.
[zh_CN]Borenstein，“多用途因特网邮件扩展（MIME）第二部分：媒体类型”，RFC 2046，DOI 10.17487/RFC2046，1996年11月，http://www.rfc-..org/info/rfc2046。

[en][RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, http://www.rfc-editor.org/info/rfc2119.
[zh_CN][RFC2119]Bradner，S.，“RFC中使用的关键词指示需求水平”，BCP 14，RFC 2119，DOI 10.17487/RFC2119，1997年3月，http://www.rfc-..org/info/rfc2119。

[en][RFC3986] Berners-Lee, T., Fielding, R., and L.
[zh_CN][RCFC986] Berners Lee，T.，菲尔丁，R，L。

[en]Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, http://www.rfc-editor.org/info/rfc3986.
[zh_CN]Mas.，“统一资源标识符（URI）：通用语法”，STD 66，RFC 3986，DOI 10.17487/RFC3986，2005年1月，http://www.rfc-..org/info/rfc3986。

[en][RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, http://www.rfc-editor.org/info/rfc4949.
[zh_CN][RFC4949]Shirey，R.，“互联网安全词汇表，版本2”，FYI 36，RFC 4949，DOI 10.17487/RFC4949，2007年8月，http://www.rfc-..org/info/rfc4949。

[en][RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, http://www.rfc-editor.org/info/rfc7159.
[zh_CN][RFC7159]Bray，T，Ed.，“JavaScript对象符号（JSON）数据交换格式”，RFC7159，DOI 10.17487/RFC7159，2014年3月，http://www.rfc-..org/info/rfc7159。

[en][UNICODE] The Unicode Consortium, "The Unicode Standard", http://www.unicode.org/versions/latest/.
[zh_CN][Unicode] Unicode联盟，“Unicode标准”，<http://www. unicode .org /版本/最新/>。

13.2. Informative References