

互联网工程任务组 (IETF)
征求意见稿 7517
类别：标准跟踪
ISSN: 2070-1721

M. Jones
微软
2015 年 5 月

JSON Web 密钥 (JWK)

摘要

JSON Web 密钥 (JWK) 是用来表示密码密钥的一种 JavaScript 对象符号 (JSON) 数据结构。本规范还定义了用来表示成组 JWK 的一种 JWK 集 JSON 数据结构。至于与本规范配套使用的密码算法和标识符，将在“JSON Web 算法 (JWA)”规范和由该规范建立的 IANA 注册表中单独描述。

目录

1. 介绍
 - 1.1 表述约定
2. 词语
3. JWK 示例
4. JSON Web 密钥 (JWK) 的格式
 - 4.1 “kty” (密钥类型) 参数
 - 4.2 “use” (公钥用途) 参数
 - 4.3 “key_ops” (密钥操作) 参数
 - 4.4 “alg” (算法) 参数
 - 4.5 “kid” (密钥 ID) 参数
 - 4.6 “x5u” (X.509 URL) 参数
 - 4.7 “x5c” (X.509 证书链) 参数
 - 4.8 “x5t” (X.509 证书 SHA-1 指纹) 参数
 - 4.9 “x5t#S256” (X.509 证书 SHA-256 指纹) 参数
5. JWK 集的格式
 - 5.1 “keys” 参数
6. 字符串比较规则
7. 被加密 JWK 和被加密 JWK 集的格式
8. JANA 方面的考虑
 - 8.1 JSON Web 密钥参数注册表
 - 8.1.1 注册模板
 - 8.1.2 注册表初始内容
 - 8.2 JSON 密钥用途注册表
 - 8.2.1 注册模板
 - 8.2.2 初始注册表目录
 - 8.3 JSON Web 密钥操作注册表
 - 8.3.1 注册模板
 - 8.3.2 注册表初始内容
 - 8.4 JSON Web 密钥集参数注册表
 - 8.4.1 注册模板
 - 8.4.2 注册表初始内容
 - 8.5 媒介类型注册
 - 8.5.1 注册表内容
9. 安全考虑
 - 9.1 密钥的来源和可信度
 - 9.2 防止非公钥信息泄露
 - 9.3 RSA 私钥的表示形式与盲化
 - 9.4 密钥熵与随机值
10. 参考文献
 - 10.1 标准性文献
 - 10.2 资料性文献

附录 A JSON Web 密钥集示例

A.1 公钥示例

A.2 私钥示例

A.3 对称密钥示例

附录 B “x5c” 用途 (X.509 证书链) 参数示例

附录 C 被加密 RSA 私钥示例

C.1 明文 RSA 私钥

C.2 JOSE 标头

C.3 内容加密密钥 (CEK)

C.4 密钥派生

C.5 密钥加密

C.6 初始化向量

C.7 附加认证数据

C.8 内容加密

C.9 完整表示形式