Clave Web JSON (JSON Web Key, JWK)

Una Clave Web JSON (JWK) es un formato basado en JSON utilizado para representar claves criptográficas. Cuando múltiples JWK deben agruparse, se organizan en un Conjunto de Claves Web JSON (JWKS).

- ¿Qué es una Clave Web JSON (JWK)?

¿Qué es una Clave Web JSON (JWK)?

Una Clave Web JSON (JWK) es un formato basado en JSON utilizado para representar claves criptográficas. Se utiliza ampliamente en el contexto de JSON Web Signature (JWS) y Cifrado Web JSON (JSON Web Encryption, JWE) para validar la integridad y confidencialidad de JSON Web Tokens (JWT) . También se usa en OpenID Connect (OIDC) para la gestión de identidad y acceso (access management).

Por ejemplo, una clave pública ECDSA codificada en PEM:

```
-----BEGIN PUBLIC KEY-----
MHYwEAYHKoZIzj0CAQYFK4EEACIDYgAEF/xQdbOho2Jw0hgmNPD0VAEPAgkQrfD4
f1Qx3y49cUm646fMBX9DYx+43HzXm6VdX77uFymz90aO4dBunpTdUzLFRAiT7+In
gzZGDrIE+FG6CcqQuRP65r65SUzDOmP5
-----END PUBLIC KEY-----
```

...puede representarse como un JWK:

```
{
  "kty": "EC",
  "crv": "P-384",
  "x": "F_xQdbOho2Jw0hgmNPD0VAEPAgkQrfD4f1Qx3y49cUm646fMBX9DYx-43HzXm6Vd",
  "y": "X77uFymz90aO4dBunpTdUzLFRAiT7-IngzZGDrIE-FG6CcqQuRP65r65SUzDOmP5"
}
```

¿Cómo funciona un JWK?

Dado que el JWK es un formato basado en JSON, puede contener metadatos ricos sobre la clave en comparación con formatos tradicionales como PEM. Aquí hay algunos atributos comunes en un JWK:

- `kty` (Key Type): La familia de algoritmos criptográficos utilizada con la clave. Los valores comunes incluyen `RSA`, `EC` y `oct`. `EC` ha sido marcado como “Recomendado+” en RFC 7518 .

- `use` (Public Key Use): El uso previsto de la clave pública. Los valores comunes incluyen `sig` (firma) y `enc`(encriptación).
- `key_ops` (Key Operations): Las operaciones de clave admitidas por la clave. Los valores comunes incluyen `sign`, `verify`, `encrypt` y `decrypt`.
- `alg` (Algorithm): El algoritmo previsto para su uso con la clave. Dependiendo del tipo de clave, el algoritmo puede variar. Por ejemplo, se puede usar `RS256` con una clave RSA, mientras que `ES256` se puede usar con una clave EC.
- `kid` (Key ID): Un identificador único para la clave. Puede usarse para identificar una clave específica en un conjunto de claves.

Excepto `kty`, todos los demás atributos son opcionales y pueden usarse para proporcionar contexto adicional sobre la clave. Según el valor de `kty`, otros atributos pueden ser necesarios u opcionales. En el ejemplo anterior, el JWK representa una clave ECDSA (`kty: "EC"`) con una curva P-384 (`crv: "P-384"`). Los atributos `x` e `y`contienen las coordenadas de la clave pública.

Aquí hay otro ejemplo no normativo de un JWK de clave pública RSA:

```
{
  "kty": "RSA",
  "use": "sig",
  "alg": "RS256",
  "n": "0vx7agoebGcQSuuPiLJXZpt...-TmV4HCA1T8jXg3fE2VbA",
  "e": "AQAB",
  "kid": "2011-04-29-1234"
}
```

Para obtener información detallada sobre los atributos de JWK y sus significados, consulte RFC 7517 .

Conjunto de Claves Web JSON (JWKS)

Cuando múltiples JWK deben agruparse, se organizan en un Conjunto de Claves Web JSON (JWKS). Un JWKS es un objeto JSON que contiene un array de JWK. Es comúnmente utilizado en la respuesta del endpoint `jwks_uri` en Descubrimiento de OpenID Connect (OpenID Connect Discovery) para proporcionar las claves públicas para la validación de signing-key de JWT.

Aquí hay un ejemplo no normativo de un JWKS que contiene dos JWK:

```
{
  "keys": [
    {
      "kty": "RSA",
      "use": "sig",
      "alg": "RS256",
      "n": "0vx7agoebGcQSuuPiLJXZpt...-TmV4HCA1T8jXg3fE2VbA",
      "e": "AQAB",
      "kid": "2011-04-29-1234"
    },
    {
      "kty": "EC",
      "crv": "P-384",
      "x": "F_xQdbOho2Jw0hgmNPD0VAEPAgkQrfD4f1Qx3y49cUm646fMBX9DYx-43HzXm6Vd",
      "y": "X77uFymz90aO4dBunpTdUzLFRAiT7-IngzZGDrIE-FG6CcqQuRP65r65SUzDOmP5"
    }
  ]
}
```


En este ejemplo, el JWKS contiene dos JWK: una clave RSA y una clave EC. El atributo `keys` es un array de JWK, cada uno representando una clave diferente.