Cifrado Web JSON (JSON Web Encryption, JWE)

JSON Web Encryption (JWE) es una forma estándar de cifrar y descifrar datos en formato JSON. Se utiliza a menudo para proteger información sensible en los Tokens Web JSON (JWTs) en tránsito.

¿Qué es JSON Web Encryption (JWE)?

Como se define en el **RFC 7516**, JSON Web Encryption (JWE) es un mecanismo para cifrar y descifrar datos en formato JSON. Agrega una capa de confidencialidad a los datos, y es particularmente útil al transmitir información sensible a través de una red no confiable.

JWE se utiliza a menudo junto con Tokens Web JSON (JWTs) para proteger los datos de carga útil. Por ejemplo, un Token de ID (ID token) o un Token de acceso (Access token) pueden cifrarse utilizando JWE para asegurar que los datos estén protegidos durante la transmisión.

¿Cómo funciona JWE?

JWE tiene dos formatos de serialización: compacto y JSON. Cada formato tiene su propia manera de representar los datos cifrados.

Serialización compacta

En la serialización compacta, el JWE se representa como una cadena con cinco partes codificadas en Base64URL separadas por puntos (`.`). Las cinco partes son:

```
{{header}}.{{encrypted-key}}.{{iv}}.{{ciphertext}}.{{tag}}
```

Cada parte tiene un propósito específico:

- `header`: Contiene metadatos sobre el algoritmo de cifrado y la gestión de claves.
- `encrypted-key`: La clave de cifrado de contenido encriptada (CEK) utilizada para cifrar la carga útil.
- `iv`: El vector de inicialización utilizado en el proceso de cifrado.
- `ciphertext`: Los datos de carga útil cifrados.
- `tag`: La etiqueta de autenticación utilizada para verificar la integridad de los datos cifrados.

Serialización JSON

La serialización JSON es más extensa y proporciona una forma estructurada de representar el JWE. El JWE se representa como un objeto JSON con las siguientes propiedades:

```
{
 "protected": "{{protected-header}}",
 "unprotected": "{{unprotected-header}}",
 "header": "{{header}}",
 "encrypted_key": "{{encrypted-key}}",
 "iv": "{{iv}}",
 "ciphertext": "{{ciphertext}}",
 "tag": "{{tag}}",
 "aad": "{{additional-authenticated-data}}"
}
```

- `protected`: Contiene la cabecera protegida codificada en Base64URL.
- `unprotected`: Contiene la cabecera desprotegida compartida de JWE.
- `header`: Contiene la cabecera desprotegida por destinatario de JWE.
- `encrypted_key`: Contiene la clave de cifrado de contenido encriptada (CEK) codificada en Base64URL.
- `iv`: Contiene el vector de inicialización codificado en Base64URL.
- `ciphertext`: Contiene el texto cifrado codificado en Base64URL (carga útil cifrada).
- `tag`: Contiene la etiqueta de autenticación codificada en Base64URL.
- `aad`: Contiene los datos adicionales autenticados codificados en Base64URL.

El cliente debería poder descifrar el JWE utilizando la clave y el algoritmo apropiados. Se puede utilizar una clave precomunicada o una clave derivada de un protocolo de acuerdo de claves para descifrar el JWE.

Por ejemplo, un Token de ID (ID token) puede cifrarse utilizando JWE, y el cliente puede descifrarlo utilizando la clave apropiada obtenida del endpoint `jwks_uri` del proveedor de OpenID.