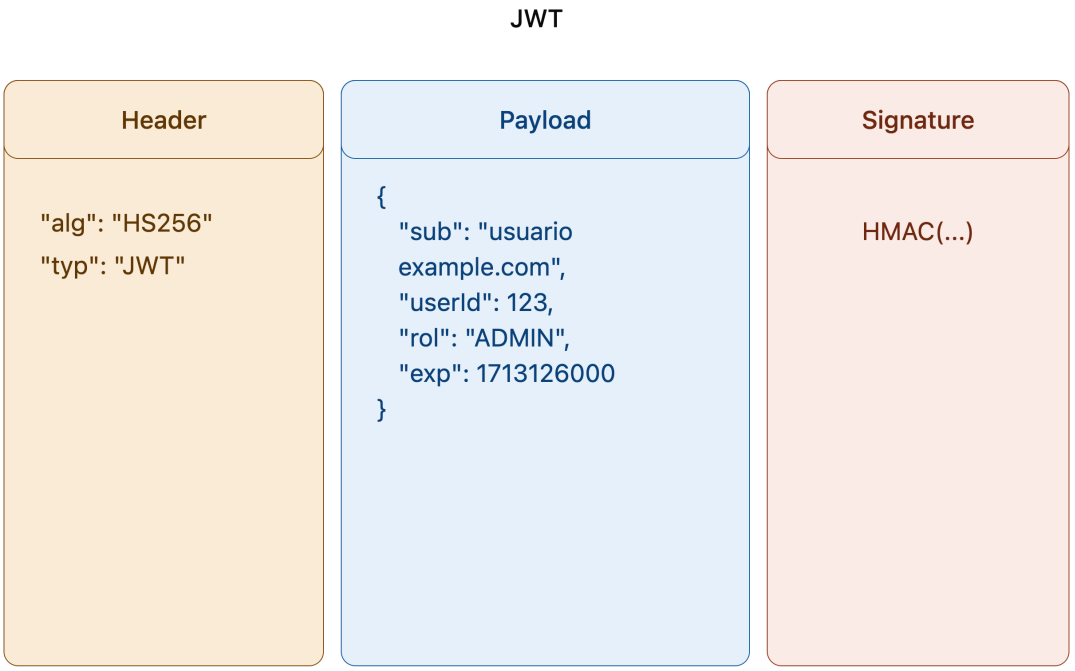
JWT

Json Web Token



Un **JWT** tiene **3 partes**, siempre separadas por puntos:

```
xxxxx.yyyyy.zzzzz
```

1️⃣ Header (encabezado)

Contiene la **información técnica** del token.

Ejemplo:

```
{
  "alg": "HS256",
  "typ": "JWT"
```

```
}
```

- `alg`: algoritmo usado para firmar (HS256, RS256...)
- `typ`: tipo (siempre JWT)

2️⃣ Payload (claims)

Son los **datos** que viajan dentro del token.

Ejemplo:

```
{
  "sub": "usuario@example.com",
  "userId": 123,
  "rol": "ADMIN",
  "exp": 1713126000
  "iat": 1232321132
}
```

Incluye:

- Claims estándar (`sub`, `iat`, `exp`, etc.)
- Claims personalizados (`userId`, `rolId`, etc.)

⚠️ No va cifrado, solo codificado en Base64 → **cualquiera puede verlo**.

3️⃣ Signature (firma)

Garantiza que:

- el token no fue modificado
- proviene de quien tiene la clave secreta

Se genera :

openssl rand -base64 32

Sin esta firma el backend no confía en el token.

Parte	Qué contiene	Para qué sirve
Header	Algoritmo + tipo	Define cómo validar la firma
Payload	Datos del usuario (claims)	Información que se quiere transmitir
Signature	Firma del header + payload	Verifica autenticidad e integridad