WDD330

Ribeka Nanjo

W0 Reading (L 08)

● What is Jason web Token(JWT)?

- an open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object.

Compact: it can be sent through an URL, Post parameter, or inside an HTTP header.

Self-contained: the payload contains all the required information about the user, to avoid querying the database more than once.

● When to use Jason web Token

➢ Used as an access token to prevent unwanted access to a protected resource; login process, single-sign-on.

● Structure

➢ Header: JWT の署名検証を行うのに必要な情報を格納する

```
E.g. {
        "alg": "HS256",
        "typ": "JWT"
        }
```

➢ Payload: やりとりに必要な属性情報

- **Reserved claims** – predefined claims, which are not mandatory, but RECOMMENDED.
- **Public claims** - should be defined in the IANA JSON Web Token Registry or be defined as a URI that contains a collision resistant namespace.
- **Private claims** - the custom claims created to share information between parties that agree on using them.

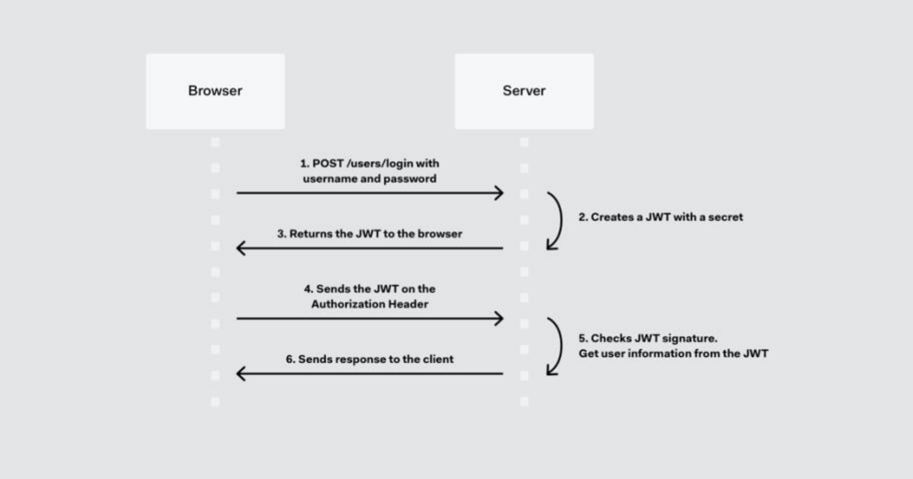
➢ Signature:エンコード済みヘッダー、ピリオド、ペイロードを連結したもの

- E.g. HMAC SHA256 algorithm

```
HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
    secret)
```

- Don’t store sensitive session data in browser storage due to lack of security.

- How Jason web Tokens work?


Browser
Server
1. POST /users/login with username and password
2. Creates a JWT with a secret
3. Returns the JWT to the browser
4. Sends the JWT on the Authorization Header
5. Checks JWT signature. Get user information from the JWT
6. Sends response to the client