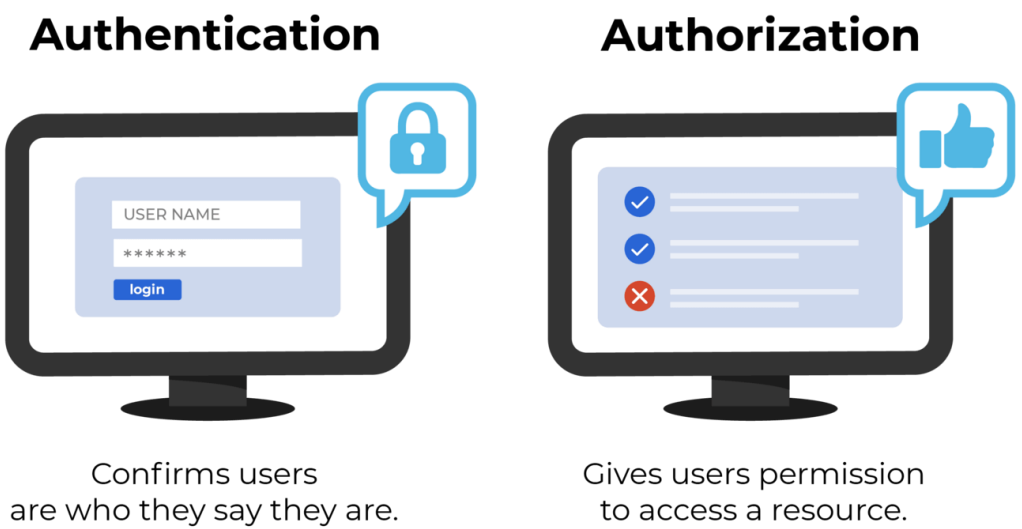
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Istruzione e del Merito
Italiadomani
ITS Tecnologie dell'Informazione e della Comunicazione

Autenticazione e Autorizzazioni in API RESTful
Introduzione a JSON Web Token (JWT)



Intervento realizzato da ITS Tecnologie dell'Informazione e della Comunicazione
okta

JWT

- **JWT** è uno standard per la creazione di **token sicuri e autoverificabili** utilizzati per l'autenticazione e autorizzazione.
- Strutturato in tre parti:

1.Header
2.Payload
3.Signature

- È usato principalmente per la trasmissione sicura di informazioni tra parti.

JWT

Un JWT è una stringa composta da tre parti separate da punti (.):

- **Header**: Informa il tipo di token e l'algoritmo di firma utilizzato.
- **Payload**: Contiene le informazioni (claims).
- **Signature**: Verifica l'integrità del token

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikpva
G4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKx
wRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) secret base64 encoded
```

Il **Header** è composto da due campi:

- alg: L'algoritmo di hashing utilizzato (es. HS256, RS256).
- typ: Indica che si tratta di un token JWT

Il Payload del JWT

- Il **Payload** contiene le informazioni dell'utente o altri dati utili (claims).
- I claim possono essere:
  - **Registered claims**: Claim predefiniti (es. iss, exp).
  - **Public claims**: Claim definiti da standard pubblici.
  - **Private claims**: Claim personalizzati

La Signature del JWT

La **Signature** serve a verificare che il token non sia stato modificato.

È generata combinando:

- Base64Url di Header
- Base64Url di Payload
- Una chiave segreta

Come funziona il JWT?

- **Login dell'utente**: L'utente invia le proprie credenziali.
- **Creazione del token**: Se le credenziali sono valide, viene generato un JWT e restituito al client.
- **Uso del token**: Il client invia il JWT in ogni richiesta (nell'header Authorization: Bearer <token>).
- **Validazione del token**: Il server verifica il token in base alla firma.

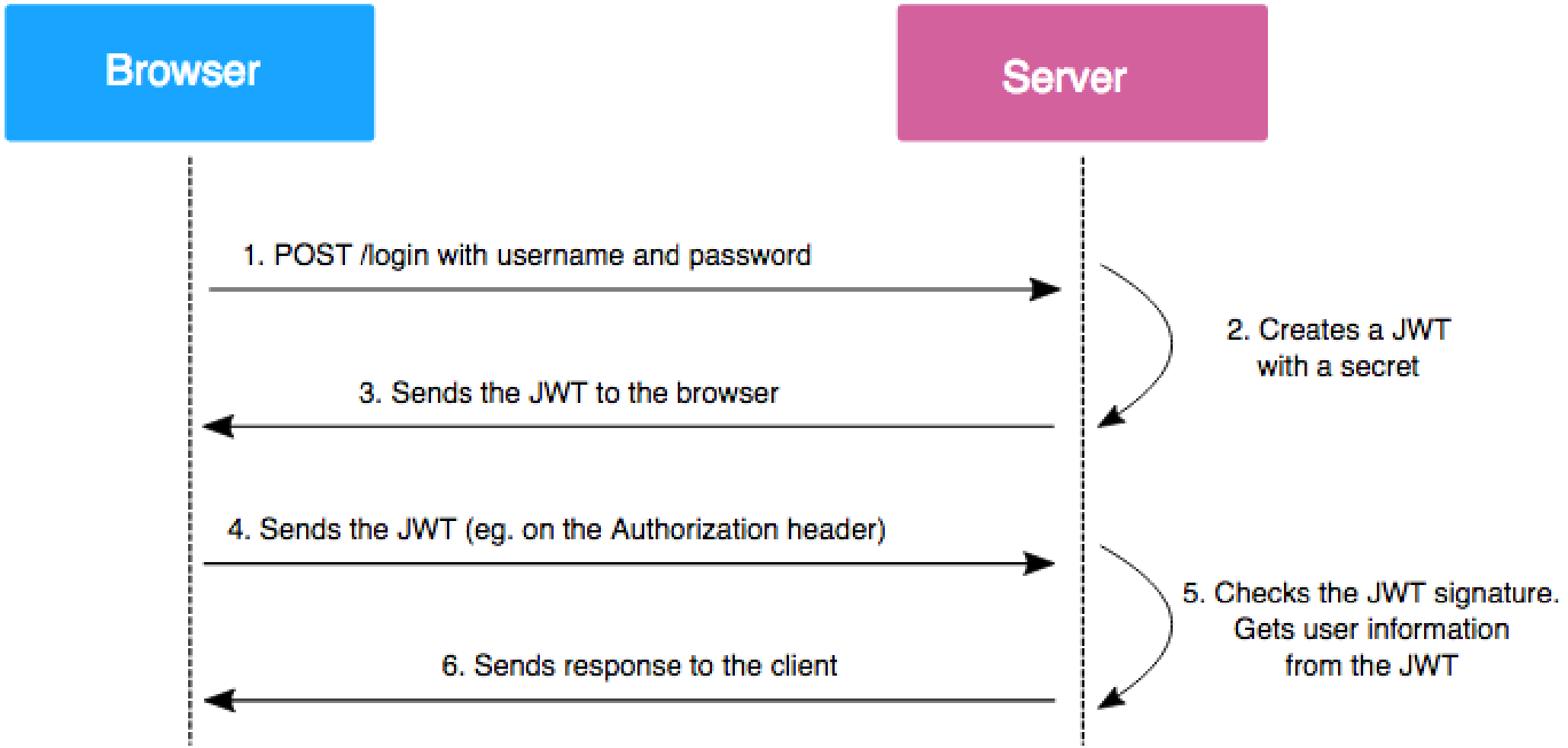
Vantaggi del JWT?

- **Autocontenuto**: Tutte le informazioni necessarie sono nel token.
- **Sicuro**: Firmato per garantirne l'integrità.
- **Scalabile**: Non è necessario mantenere lo stato sul server (stateless).
- **Flessibile**: Può essere utilizzato per l'autenticazione e l'autorizzazione.

Svantaggi del JWT?

- **Non revocabile**: Una volta emesso, non può essere revocato fino alla scadenza.
- **Dimensione**: Più grande rispetto ad altri token, come i session ID.
- **Attenzione alla sicurezza**: Un JWT mal gestito può essere vulnerabile.

Cofinanziato dall'Unione europea



Intervento realizzato da ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE