

Ciclo di Vita JWT Token - Autenticazione UniprBooks

1. STRUTTURA/CONFIGURAZIONE TOKEN JWT

Header . Payload . Signature

Algoritmo: HS256
Scadenza: 8 ore (28800s)
Secret: env(JWT_SECRET)
Libreria: firebase/php-jwt

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

```
PAYLOAD
{
  "sub": 123,
  "email": "user@example.it",
  "iat": 1737450000,
  "exp": 1737478800
}
```

```
SIGNATURE
HMACSHA256 (
  base64(header) + "." +
  base64(payload),
  JWT_SECRET
)
```

2. GENERAZIONE (dopo login)

Login Success

JWTService.generateToken()
userId + email + expiry

Token JWT

Salva

Frontend
(localStorage)

3. UTILIZZO (richieste protette)

Frontend

Header HTTP

Authorization: Bearer

Backend API

4. VALIDAZIONE (backend)

Estrai token
dall'header

Verifica
Signature

OK

Verifica
Expiry (exp)

Accesso
Autorizzato

FAIL

```
{status: "error",
message: "Unauthorized"}
```

EXPIRED

6. TIMELINE TOKEN

t=0
Login
iat

Token Valido (0-8h)

t=8h
Scadenza
exp

Token Scaduto → Richiede nuovo login