# AUTENTIFICARE - JSON Web Tokens (JWT)

JWT reprezinta un mod de a transmite in mod sigur informatiile intre partile componente sub forma unui obiect JSON. Informatiile pot fi verificate cu ajutorul semnaturi digitale, pe baza unor perechi de id-uri(keys). Astfel, putem fi siguri ca utilizatorul care detine cheia privata este cel de la care dorim sa primim informatiile

JWT este folositor in momentul in care dorim sa oferim anumite drepturi utilizatorului de a accesa anumite servicii si resurse care ii sunt permise folosind un token.

Folosing private/public keys putem sa fim siguri ca utilizatorii care transmit informatia sunt autentici.

Un token este format din :

* Header (x)
* Payload (y)
* Signature (z)

avand forma xxxxx.yyyyyy.zzzzz

In header se afla tipul de token (JWT) si algoritmul de semnare folosit.

De ex:

{

"alg": "HS256",

"typ": "JWT"

}

In payload se afla cererile, acestea reprezentand datele pe care un JWT le stocheaza. De ex:

{

"sub": "1234567890",

"name": "John Doe",

"admin": true

}

Signature:

HMACSHA256(

base64UrlEncode(header) + "." +

base64UrlEncode(payload),

secret)

Acesta este folosit pentru a verifica faptul ca mesajul nu a fost schimbat.

Atunci cand utilizatorul se logheaza, se va returna un token

- indicat de utilizat in legatura cu HTML and HTTP

- folosirea XML cu XML Digital Signature fara a avea probleme de securitate este destul de dificila in comparatie cu simplitatea oferita de JSON

- JSON parsers are common in most programming languages because they map directly to objects.

- XML nu are document-to-object mapping, de care avem nevoie avand in vedere faptul ca folosim MongoDB