Călușeru Veronica-Ștefania,
An IV-IS,Grup 2.1

TEMA 1-DATC

JSON Web Token (JWT) este un standard deschis care definește un mod compact și autonom pentru transmiterea sigură a informațiilor între părți ca obiect JSON. Aceste informații pot fi verificate și de încredere deoarece sunt semnate digital. JWT-urile pot fi semnate folosind un secret (cu algoritmul HMAC) sau o pereche de chei publice / private utilizând RSA sau ECDSA .JWT consta in trei părți separate prin punct :Antet ,Încărcătura utilă și Semnătura (exp: **xxxxx.yyyyy.zzzzz**). **Antetul** constă de obicei din două părți: tipul de jeton, care este JWT, și algoritmul de ștergere folosit, cum ar fi HMAC SHA256 sau RSA.
Încărcătura utilă conține declarații despre o entitate(utilizatorul) și despre date suplimentare.
Semnătură folosim antetul codificat si sarcina utilă codificată(Base64Url).
Jason Web Token este folosit pentru :

- **Autorizație** : Acesta este cel mai frecvent scenariu pentru utilizarea JWT. Odată ce utilizatorul este conectat, fiecare solicitare ulterioară va include JWT, permițând utilizatorului să acceseze rute, servicii și resurse care sunt permise cu respectivul jeton.
- **Schimbul de informații** : JSON Web Token reprezintă o modalitate bună de transmitere sigură a informațiilor între părți, deoarece folosește chei private/publice.

OpenID este un protocol deschis și protocol de autentificare descentralizat .
Promovat de Fundația **OpenID** non-profit , permite utilizatorilor să fie autentificați de site-urile care cooperează (cunoscute sub numele de părți de bază sau RP) folosind un serviciu terță parte, eliminând necesitatea ca webmasterii să furnizeze propriile sisteme de conectare și permițând utilizatorilor să se conecteze la mai multe site-uri care nu au legătură, fără a trebui să aibă o identitate și o parolă separate pentru fiecare.
OAuth - cea mai importantă caracteristică a **OAuth** este token-ul de acces care oferă o metodă de lungă durată de a face cereri suplimentare.
Comparatie: spre deosebire de **OpenID**, **OAuth** nu se încheie cu autentificarea, ci oferă un token de acces pentru a obține acces la resurse suplimentare furnizate de același serviciu terță parte. **Diferența crucială** este că în cazul de utilizare a *autentificării* OpenID , răspunsul furnizorului de identitate este o afirmație de identitate,iar în cazul de *autorizare* OAuth , furnizorul de identitate este, de asemenea, un furnizor de API , iar răspunsul furnizorului de identitate este un atribut de acces care poate acorda aplicației acces permanent la unele dintre API-urile furnizorului de identitate, în numele utilizatorului.