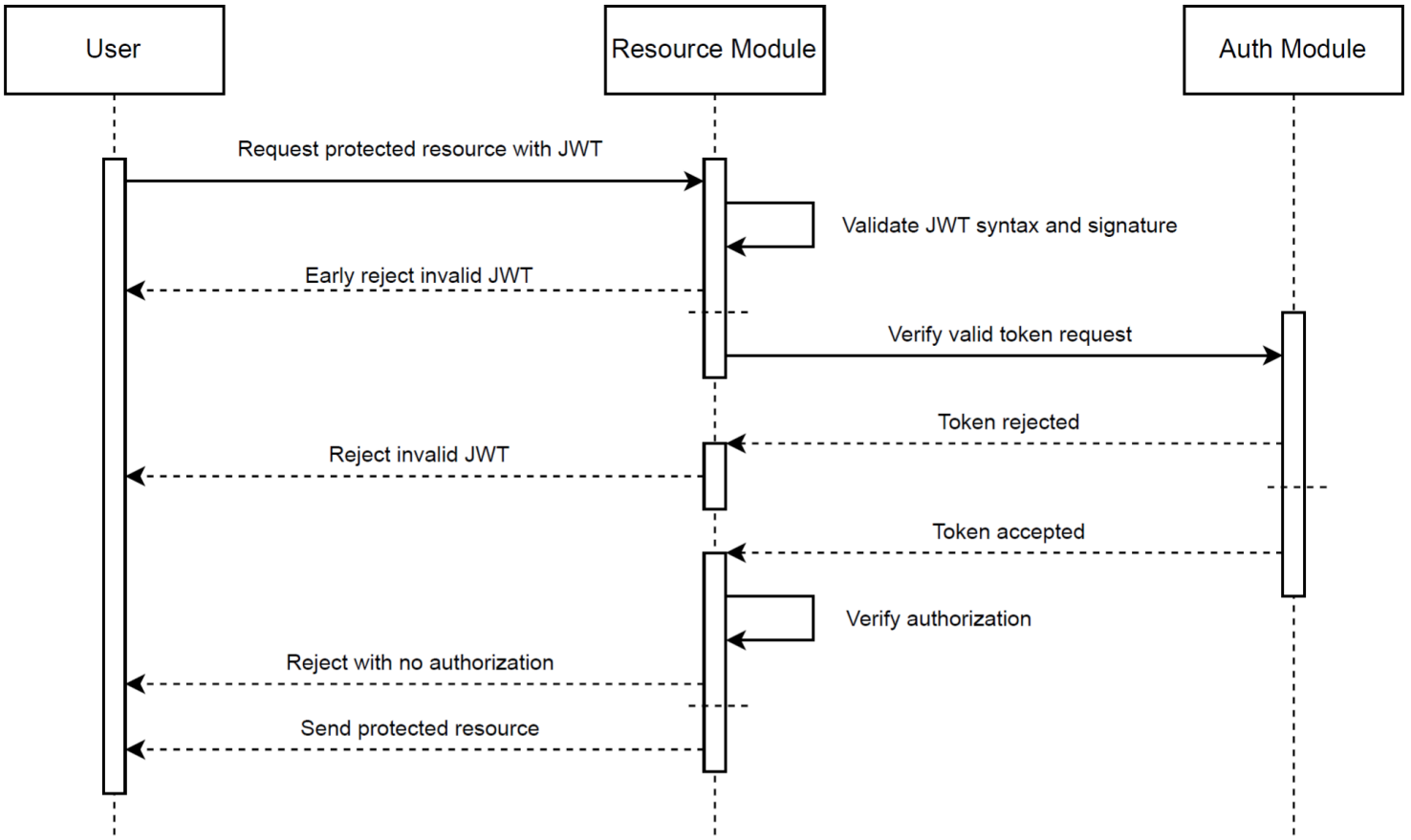
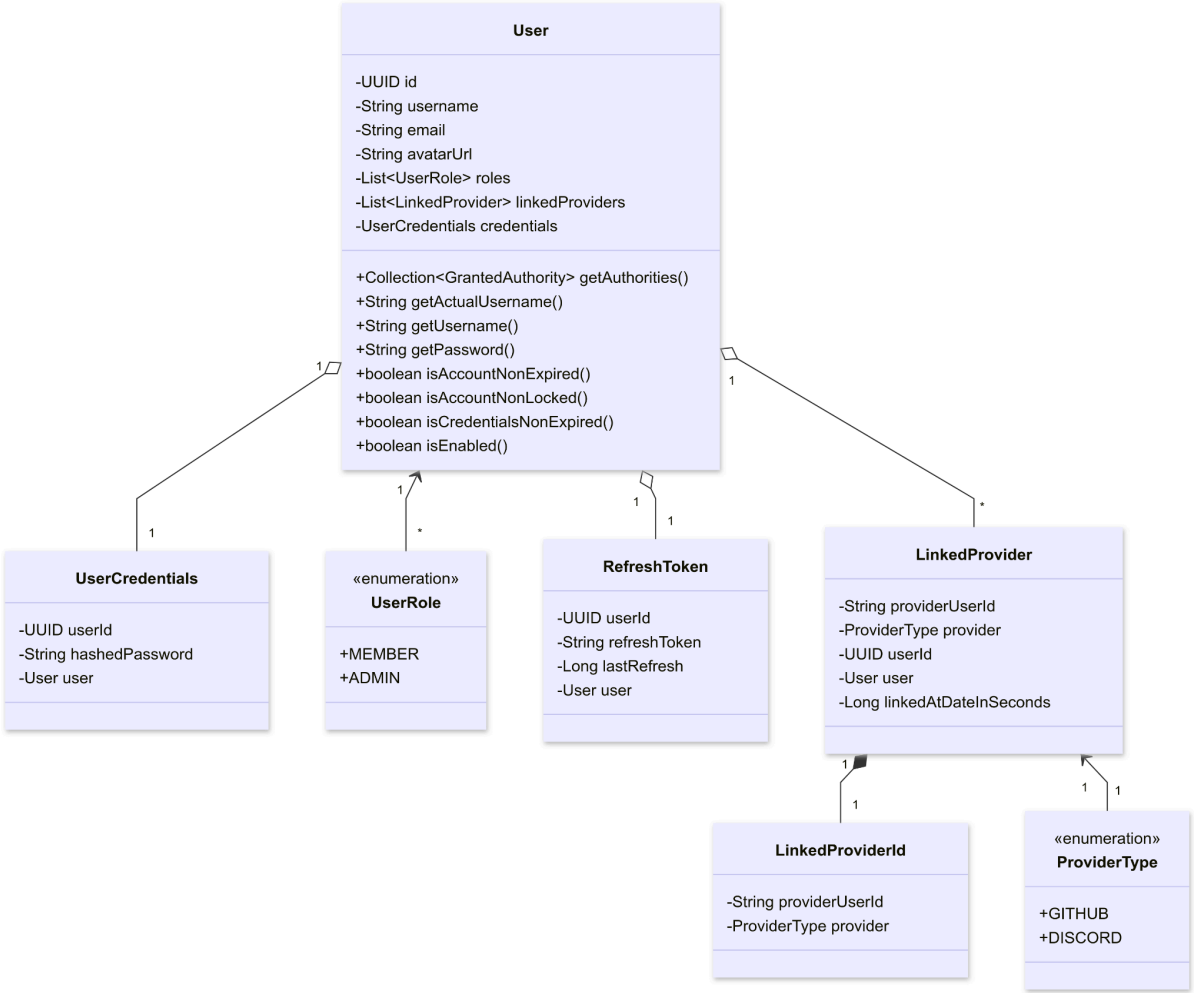
Diagramă de interacțiune pentru accesarea resurselor



1. User-ul trimite un request către o resursă protejată a aplicației (să zicem zborurile).
2. Request-ul este recepționat de modulul de resurse (care se ocupă și de zboruri) și încearcă să valideze sintaxa tokenului și semnătura acestuia. În caz că token-ul este formatat greșit ca sintaxa sau nu este generat de aplicația noastră (signatura nu corespunde) este refuzat devreme.
3. Altfel, dacă request-ul trece de validarea inițială, el este trimis mai departe către modulul de autentificare, care dă verdictul final.
4. Token-ul a expirat fie a fost invalidat de generarea unui alt token, trimitem un răspuns negativ către modulul de resurse, care la rândul lui respinge accesarea resursei.
5. Token-ul a fost acceptat și transmitem modului de resurse această informație (printr-un status code 200).
6. Presupunând că token-ul a fost acceptat (s-a executat pasul 5), serverul de resurse o să verifice dacă utilizatorul are permisiunea necesară de a accesa resursa. Dacă nu are acces, modulul de resurse respinge cererea de accesare, altfel, trimite resursa protejată către utilizator.

Diagrama claselor implicate în autentificare și validarea utilizatorilor



Un User poate deține maxim un UserCredentials, un RefreshToken și mai mulți LinkedProviders.

Un User are unul sau mai multe roluri (marcate prin UserRole).

Un LinkedProvider conține un id (folosit pentru maparea entității în baza de date) și are un tip, marcat prin ProviderType.

Toate câmpurile sunt private, dar totodată ele au și Getter și Setter, care nu au mai fost specificate în diagramă. Funcțiile specifice User-ului sunt necesare pentru a putea fi integrat în Spring Security.

Diagrame individuale,
Ghinea Dragoș-Dumitru