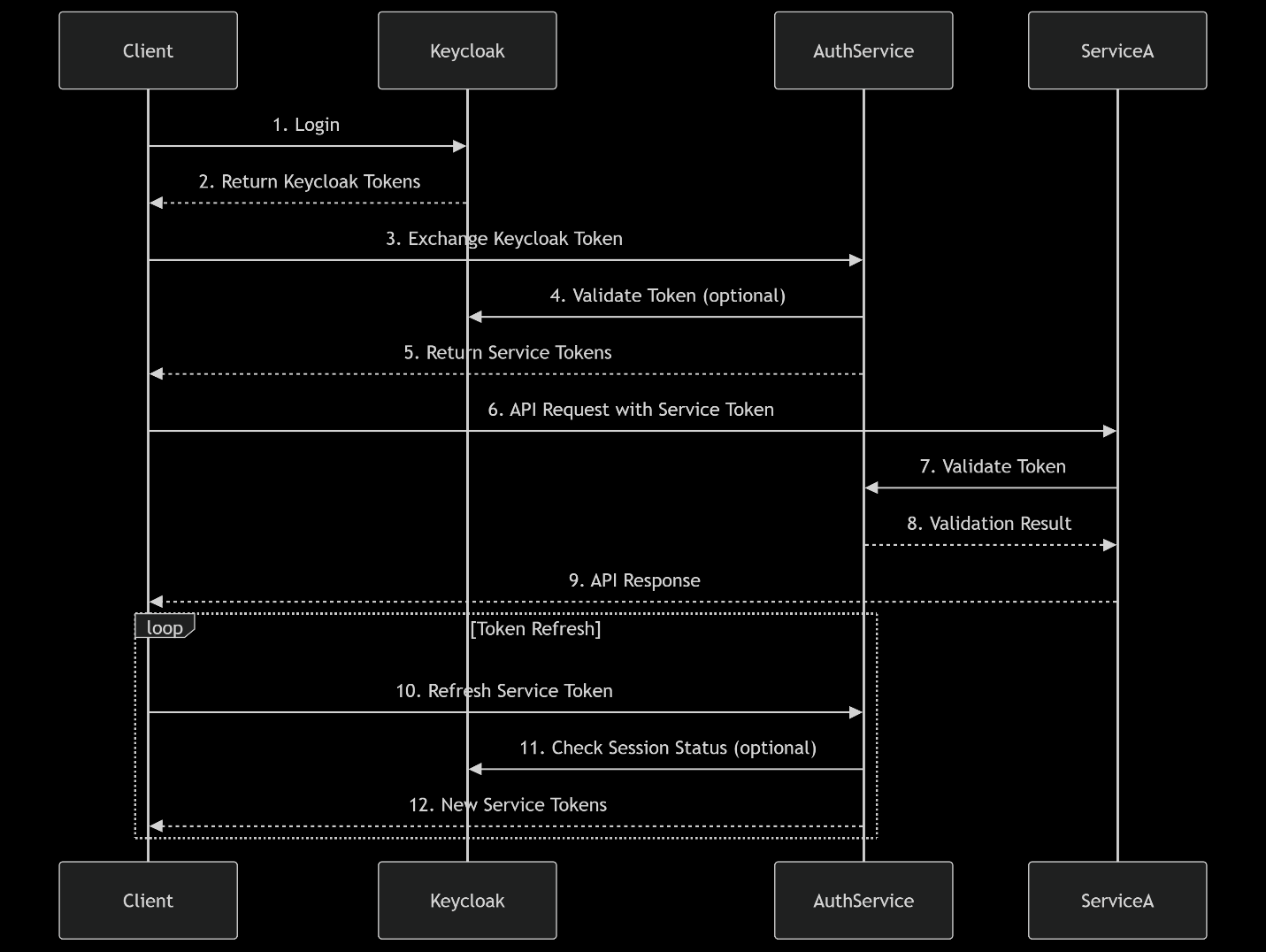
Authentication With Keycloak

  
**Authentication Flow Overview:**

* Client(Angular App) will redirect to Keycloak to complete the login process.
* Keycloak will return its token to the ui, they will be stored in the sessions as keycloak\_access\_token, and keycloak\_refresh\_token.
* Keycloak token will then be sent to our AuthService to exchange tokens. Our AuthService will validate the keycloak token from keycloak. Then it will generate tokens for our applications using our roles, permissions, scopes.
* Our AuthService will return these tokens to the UI and it will be stored in the session storage or local storage. These token will be added to all requests requesting resources from our services.
* Optional step: We can verify the signing key from our Auth Service, or just depend on the access\_token directly.
* When our AuthService access\_token expires, we will request another access\_token using our refresh token.
* Optional step: refresh the keycloak tokens as well.

PoC for this approach:

* Backend services are done and running.
* Working on the angular app at the moment.
* Estimate: 4 hours