

# SPRC 2022-2023 - Tema 1 - Aplicație Client/Server pentru autorizare OAuth folosind RPC

Responsabili: George-Mircea Grosu și Silvia-Elena Nistor

Titular curs: Florin Pop

## 1 Obiectivele temei

În cadrul temei veți dezvolta o aplicație de tip client/server folosind conceptul de Remote Procedure Call (RPC) pentru simularea unui sistem de autorizare de tip OAuth (Vezi fig. [1]).

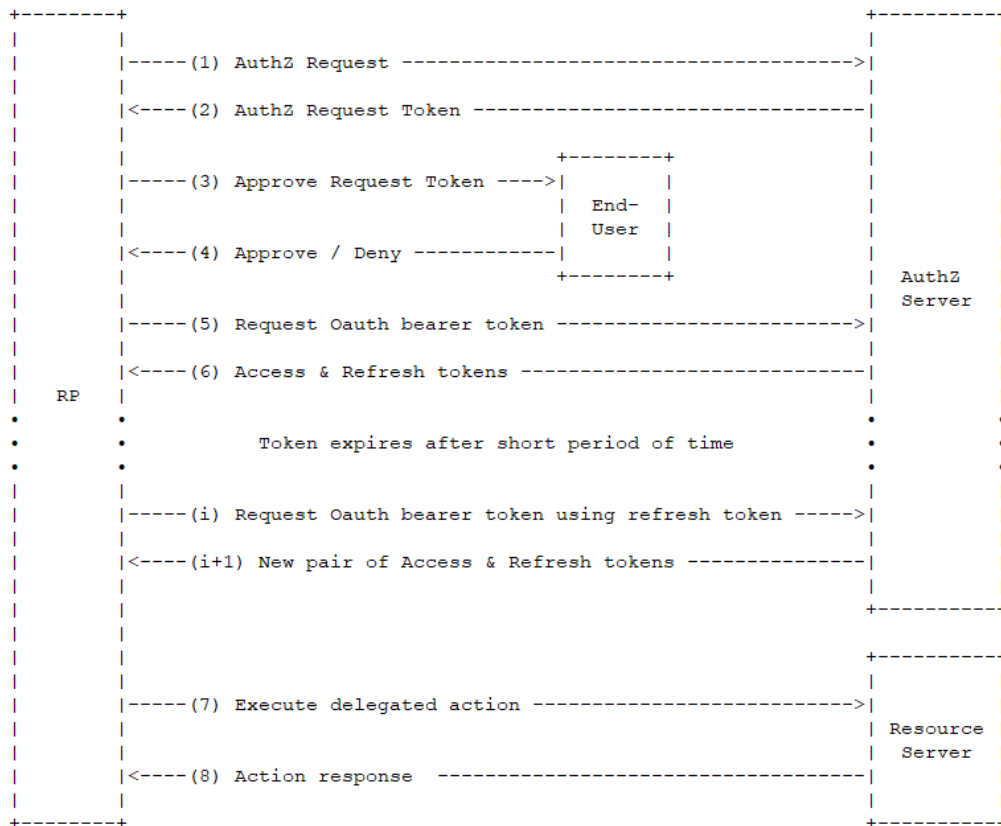


Figura 1: Prezentare generală a arhitecturii propuse.

Obiectivele principale ale acestei teme de laborator sunt:

- realizarea unei aplicații de tip client/server bazată pe RPC cu cereri/răspunsuri multiple prin care se pot autoriza operații de tip RIMDX (Read, Insert, Modify, Delete, Execute) pe un sistem de fișiere;
- utilizarea corectă a modelului de autorizare prin OAuth;
- scrierea de specificații pentru o aplicație simplă de autorizare și administrare a resurselor;
- utilizarea de structuri de date pentru aplicații ce folosesc protocolul RPC.

Cunoștințele necesare rezolvării acestei teme de laborator sunt următoarele:

- programare în C/C++, structuri, funcții, lucrul cu fișiere binare/text;
- noțiuni privind folosirea utilitarului RPCGEN și a compilatorului gcc.

## 2 Descrierea soluției cerute

Pentru această temă ne propunem implementarea unei soluții de tip client/server pentru autorizarea accesului la resurse localizate pe un server de fișiere. Aplicația client/server va fi implementată peste protocolul RPC.

În soluția propusă, clientul reprezintă o aplicație terță, folosită de utilizatorul final, pentru gestionarea fișierelor de pe server. Astfel, clientul este responsabil pentru autorizarea operațiilor delegate de utilizator.

Server-ul are trei funcții: autorizarea clienților, gestionarea resurselor și componenta de aprobare a jetoanelor de autorizare din partea utilizatorului final. În acest sens, server-ul oferă clienților jetoane de acces (tokens) care autorizează operațiile efectuate asupra fișierelor de pe server.

### Exemplu

Un student intenționează să folosească pentru redactarea lucrării de licență, un utilitar online pentru editarea documentelor în LaTeX. Studentul are încărcate toate resursele necesare în mediul de stocare Cloud pus la dispoziție de facultate. Pentru a nu își expune credențialele către utilitarul online, studentul alege să ofere permisiuni de gestionare a fișierelor din Cloud-ul facultății prin intermediul standardului OAuth. Astfel, utilitarul primește un jeton de acces pe care îl atașează operațiilor de editare și salvare a documentelor LaTeX direct în mediul de stocare Cloud al facultății.

### 2.1 Server

#### 2.1.1 Server autorizare

Serverul gestionează în memorie o bază de date în care sunt stocate:

- identificatorii utilizatorilor – încărcăți la pornirea server-ului dintr-un fișier primit ca parametru;

```
1 5 // numarul de utilizatori cunoscuti de server
2 oD0prOgBqAsXBW8 // identificatorul unui utilizator
3 OVotQBYz418Ozkz
4 DQygMQ9F65QzYs7
5 bm5N4D4X2n66nK3
6 Xg6YuaDVv7i1kEk
```

Listing 1: Fișier intrare cu identificatorii utilizatorilor.

- seturile de permisiuni ale utilizatorilor;
- informațiile despre jetoanele de acces autorizate pentru aplicațiile terțe.

Baza de date este populată și administrată pe parcursul execuției server-ului și a interacțiunii cu utilizatorii finali.

Această componentă a server-ului expune un set minimal de proceduri pentru implementarea modelului de autorizare OAuth:

- **Request Authorization**

1. Primește de la client ID-ul asociat utilizatorului.
2. Verifică existența utilizatorului în baza de date.
  - Dacă există, întoarce un jeton pentru autorizarea cererii de acces la resurse.
  - Altfel, întoarce eroarea `USER_NOT_FOUND`.

- **Request Access Token**

1. Primește de la client: ID-ul utilizatorului și jetonul pentru autorizarea cererii de acces (aprobat de utilizator).
2. Verifică dacă jetonul este valid, și:
  - (a) asociază în baza de date utilizatorul cu noul token de acces (întotdeauna va exista un singur token de acces activ pentru un utilizator);
  - (b) întoarce un jeton de acces la resurse, un jeton pentru regenerarea celui de acces și o perioadă de valabilitate a acestora.
3. Jetonul este considerat invalid dacă nu a fost aprobat de utilizator → întoarce eroarea `REQUEST_DENIED`.

### 2.1.2 Server resurse

Serverul validează operațiile primite de la o aplicație terță, delegate de utilizator, în vederea gestionării resurselor de pe server. Resursele disponibile pe server vor fi încărcate dintr-un fișier text.

```

1 6          // numarul de utilizatori cunoscuti de server
2 Files      // numele resursei
3 UserData
4 SystemData
5 SystemSettings
6 Applications
7 Preferences

```

Listing 2: Fișier intrare cu identificatorii utilizatorilor.

Pentru această componentă este necesară implementarea unei proceduri **Validate Delegated Action**.

1. Primește de la client: tipul operației, resursa accesată și jetonul de acces.
2. Verifică dacă jetonul de acces este valid, caz în care:
  - (a) verifică dacă jetonul de acces este asociat id-ului de utilizator, iar dacă nu este, întoarce eroarea `PERMISSION_DENIED`.
  - (b) verifică valabilitatea jetonului și dacă a expirat, atunci întoarce eroarea `TOKEN_EXPIRED`.
  - (c) verifică dacă resursa există, iar în caz contrar întoarce eroarea `RESOURCE_NOT_FOUND`;
  - (d) verifică dacă operația este permisă prin jetonul de acces, iar în caz contrar întoarce eroarea `OPERATION_NOT_PERMITTED`;
  - (e) întoarce valoarea `PERMISSION_GRANTED`;

### 2.1.3 Utilizatorul final

Pentru respectarea modelului client-server, se consideră că interacțiunea cu utilizatorul este realizată printr-o procedură expusă tot de server, **Approve Request Token**.

1. Primește jetonul pentru autorizarea cererii de acces și îi atașează setul de permisiuni pentru fiecare resursă disponibilă pe server.
2. Apoi marchează jetonul ca fiind semnat.
3. Dacă utilizatorul nu aprobă cererea de accesare a datelor, atunci întoarce jetonul neschimbat.

Răspunsurile utilizatorilor vor fi încărcate dintr-un fișier CSV la pornirea server-ului. Acestea vor fi servite clienților în ordine FIFO.

```
1 <resursa>,<permisiune resursa>,<resursa>,<permisiune resursa>,...
2
3 Files ,RM, Applications ,R, User Data ,R
4 Files ,RMD, Applications ,RX, User Data ,RI
5 Files ,RMD, Applications ,RMDX, System Data ,R, Preferences ,RM
6 *,- // utilizatorul nu aproba permisiunile
7 // pe nicio resursa
8 Files ,RM, Applications ,R, UserData ,RIM
```

Listing 3: Fișier intrare pentru aprobările utilizatorilor.

## 2.2 Client

Clientul citește la pornire un fișier CSV și execută în ordine FIFO toate operațiile descrise. În timpul execuției, acesta trebuie să se asigure că respectă și utilizează modelul OAuth pentru autorizarea operațiilor.

În fișier vor exista două tipuri de operații: pentru generarea jetonului de acces și pentru operarea fișierelor de pe server.

```
1 <ID utilizator>,<actiune>,<resursa>
2 <ID utilizator> ,REQUEST, <reimprospatare automata>
3
4 oD0prOgBqAsXBW8, REQUEST, 0
5 oD0prOgBqAsXBW8, MODIFY, Files
6 OVotQBYz418Ozkz, REQUEST, 1
7 OVotQBYz418Ozkz, EXECUTE, Applications
8 OVotQBYz418Ozkz, DELETE, Files
9 oD0prOgBqAsXBW8, INSERT, UserData
10 OVotQBYz418Ozkz, READ, SystemSettings
```

Listing 4: Fișier intrare pentru client.

### 2.2.1 Model de execuție a programului Client

```

1  ===== Fisier clienti =====
2  2
3  Client 1
4  Client 2
5  =====
6
7  ===== Fisier resurse =====
8  6
9  Files
10 UserData
11 SystemData
12 SystemSettings
13 Applications
14 Preferences
15 =====
16
17 ===== Fisier aprobari =====
18
19 Files ,RM, Applications ,R, UserData ,R           // Client 1
20 Files ,RIMD, Applications ,RX, UserData ,RI       // Client 2
21                                                    // 1st request
22 Files ,RIMD, UserData ,RIMD, SystemData ,R, Preferences ,R // Client 2
23                                                    // 2nd request
24 *,—                                              // Client 1
25                                                    // 2nd request
26 Files ,RM, Applications ,R, UserData ,RIM         // Client 1
27                                                    // 3rd request
28 =====
29
30 ===== Fisier operatii =====
31                                                    // Raspuns primit
32 Client 1,REQUEST,1                               // <req. code> -> <acc. token>,
33                                                    // <ref. token>
34 Client 1,MODIFY, Files                           // PERMISSION_GRANTED
35 Client 2,EXECUTE, Applications                    // PERMISSION_DENIED
36 Client 2,REQUEST,0                               // <req. code> -> <acc. token>
37 Client 2,EXECUTE, Applications                    // PERMISSION_GRANTED
38 Client 2,DELETE, Files                           // PERMISSION_GRANTED
39 Client 1,READ, Applications                       // PERMISSION_GRANTED
40 Client 2,READ, SystemSettings                     // TOKEN_EXPIRED
41 Client 2,REQUEST,0                               // <req. code> -> <acc. token>
42 Client 1,INSERT, UserData                         // OPERATION_NOT_PERMITTED
43 Client 1,READ, Files                             // PERMISSION_GRANTED
44 Client 1,REQUEST,0                               // REQUEST_DENIED
45 Client 1,REQUEST,0                               // <req. code> -> <acc. token>
46 Client 1,INSERT, UserData                         // PERMISSION_GRANTED
47 Client 2,EXECUTE, Malware                         // RESOURCE_NOT_FOUND
48 Client 3,REQUEST,0                               // USER_NOT_FOUND
49 =====

```

Listing 5: Exemplu date intrare și comportament așteptat.

```

1 Valabilitate jetoane = 2 operatii
2
3 ===== Iesire client =====
4
5 1 leintC -> e1Cntl i,nCl tlie
6 PERMISSION_GRANTED
7 PERMISSION_DENIED
8 <req. code> -> <acc. token>
9 PERMISSION_GRANTED
10 PERMISSION_GRANTED
11 PERMISSION_GRANTED
12 TOKEN_EXPIRED
13 <req. code> -> <acc. token>
14 OPERATION_NOT_PERMITTED
15 PERMISSION_GRANTED
16 REQUEST_DENIED
17 <req. code> -> <acc. token>
18 PERMISSION_GRANTED
19 RESOURCE_NOT_FOUND
20 USER_NOT_FOUND
21
22
23 ===== Iesire server =====
24
25 BEGIN Client 1 AUTHZ
26   RequestToken = 1 leintC
27   AccessToken = e1Cntl i
28   RefreshToken = nCl tlie
29 PERMIT (MODIFY,Files,e1Cntl i,1) // (actiune,resursa,jeton acces,
30                                     // operatii ramase)
31 DENY (EXECUTE,Applications,,0)
32 BEGIN Client 2 AUTHZ
33   RequestToken = 1 n2ieCt
34   AccessToken = ielC 2tn
35 PERMIT (EXECUTE,Applications,ielC 2tn,1)
36 PERMIT (DELETE,Files,ielC 2tn,0)
37 PERMIT (READ,Applications,e1Cntl i,0)
38 DENY (READ,SystemSettings,,0)
39 BEGIN Client 2 AUTHZ
40   RequestToken = tieC2n 1
41   AccessToken = Ct2i eln
42 BEGIN Client 1 AUTHZ REFRESH
43   AccessToken = ne1tlCi // foloseste jetonul pentru
44                               // reinnoire
45   RefreshToken = enltiC1
46 DENY (INSERT,UserData,ne1tlCi,1)
47 PERMIT (READ,Files,ne1tlCi,0)
48 BEGIN Client 1 AUTHZ
49   RequestToken = nt leiC1
50 BEGIN Client 1 AUTHZ
51   RequestToken = iCn 1tle
52   AccessToken = lCtlien
53   RefreshToken = nlleit C
54 PERMIT (INSERT,UserData,lCtlien ,1)
55 DENY (EXECUTE,Malware,Ct2i eln,1)
56 BEGIN Client 3 AUTHZ
57 =====

```

Listing 6: Model date ieşire client şi server.

```
1 ./server <fisier clienti> <fisier resurse> <fisier aprobari> \  
2 <valabilitate jetoane>  
3  
4 ./client <fisier operatii>
```

Listing 7: Model comenzi rulare client și server.

### 3 Constrângeri pentru implementare

- ID-ul utilizatorilor este un *șir de caractere, alfa-numeric, cu lungime fixă de 15 caractere*.
- Semnarea jetonului pentru autorizarea cererii de acces este simbolică și nu există restricții privind modul de implementare.
- Valabilitatea unui jeton de acces este măsurată în operații autorizate cu acesta. Valoarea este primită ca parametru la rularea server-ului.
- Numele resurselor va fi format din caractere alfa-numerice și nu va conține spații.
- La generarea jetonului de acces folosind jetonul de reînnoire nu se mai cere aprobarea utilizatorului.
- Pentru generarea jetoanelor se folosește funcția X și se respectă următoarea dependență:
  - $f(\text{ID utilizator}) = \text{jeton pentru autorizarea cererii de acces}$
  - $f(\text{jeton pentru autorizarea cererii de acces}) = \text{jeton de acces}$
  - $f(\text{jeton de acces}) = \text{jeton de refresh}$
- Dacă clientul a optat pentru reînnoirea automată a acestuia, jetonul de acces va fi reînnoit înainte de a executa operația (operație care ar fi eșuat din cauza expirării jetonului).
- Dacă clientul nu a optat pentru reînnoire automată, atunci jetonul de reînnoire nu va fi generat.
- Tema se va implementa în C/C++.

### 4 Cerințele pentru realizarea aplicației

Pentru realizarea aplicației OAuth RPC trebuie să efectuați următoarele sarcini:

- 30 de puncte - definirea interfeței care expune tipurile de date și metodele aplicației;
- 10 puncte - descrierea specificațiilor de funcționare (prin comentarii în interfață) pentru toate tipurile de date și funcțiile definite în interfață;
- 40 de puncte - implementarea aplicației server
  - 5 puncte - gestionarea bazei de date cu informațiile utilizatorilor și ale clienților;
  - 15 puncte - procesul de autorizare a clienților (fără reînnoire);
  - 10 puncte - procesul de reînnoire a jetoanelor de acces;
  - 5 puncte - procesul de verificare a operațiilor executate de clienți;
  - 5 puncte - procesul utilizatorului final de aprobare a cererii de autorizare.
- 20 de puncte - implementarea aplicației client
  - 10 puncte - procesul de autorizare (obținerea jetoanelor de acces, fără reînnoire);
  - 5 puncte - procesul de reînnoire a jetoanelor de acces;
  - 5 puncte - execută operațiile descrise în fișier.

## 5 Flux de execuție

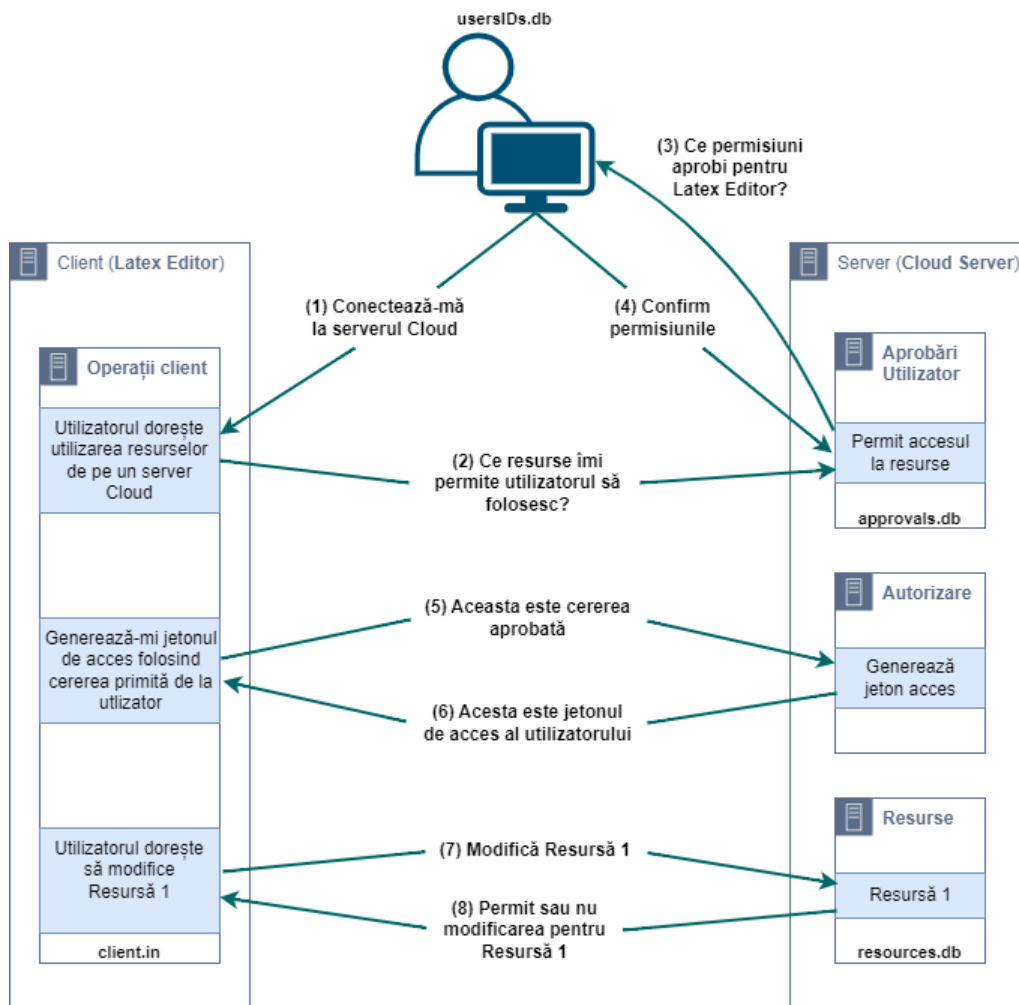


Figura 2: Prezentare vizuală a fluxului de execuție.