Sprawozdanie

Platformy programowo-sprzętowe IBM

#### Dariusz Tomaszewski (235565)

#### Bartosz Rodziewicz (226105)

# Sekcja teoretyczna

## Źródła uprawnień oraz ich hierarchia

1. All object access - nadanie użytkownikowi prawa do wszystkich obiektów w systemie
2. Prywatne/jawnie określone uprawnienia danego użytkownika do danego obiektu
3. Public authority - uprawnienia publiczne, które obowiązują każdego użytkownika, który nie ma specjalnie określonych uprawnień
4. Authorization list
5. Uprawnienia głównej grupy
6. Adopted authority

## Predefiniowane klasy użytkowników

* QSECOFR (Security Officer) - ma uprawnienia do wszystkiego
* QPGMR (Programmer)
* QSYSOPR (System operator) - uprawnienia związane z kontrolą zadań w systemie oraz operacjami save/restore całego systemu
* QUSER (User)
* QDFTOWN (User (Default Owner))
* QSRV (Programmer)
* QSRVBAS (Programmer)

## Poziomy uprawnień

* USE - Użytkownicy/grupy, którzy nie mają specjalnych uprawnień do tego obiektu mogą czytać jego zawartość
* CHANGE - Użytkownicy/grupy, którzy nie mają specjalnych uprawnień do tego obiektu mogą zmieniać zawartość obiektu
* ALL - Użytkownicy/grupy, którzy nie mają specjalnych uprawnień do tego obiektu mają pełne uprawnienia do niego wraz z operacjami na obiekcie, zarządzaniem obiektem oraz uprawnieniami istnienia obiektu (object operational, object management, and object existence authorities)
* EXCLUDE - Użytkownicy/grupy, którzy nie mają specjalnych uprawnień do tego obiektu nie mają do danego obiektu żadnych uprawnień

## Adopted Authrority

Adopted Authority są używane do tymczasowego nadawania uprawnień do obiektów, których użytkownik normalnie by nie miał.

Gdy uruchamiany jest program utworzony za pomocą USRPRF(\*OWNER), dostęp do obiektów jest uzyskiwany z uprawnieniami użytkownika uruchamiającego program plus uprawnienia właściciela programu.

Uprawnienia obowiązują tak długo jak program, który je pierwotnie przyjął, znajduje się jeszcze na stosie.

Przyjmowane są zarówno uprawnienia do obiektów, jak i uprawnienia specjalne.

Przyjmowane są tylko jawne uprawnienia właściciela programu.

## Public authority

Uprawnienia publiczne - poziom uprawnień do danego obiektu, który otrzymuje każdy użytkownik, który nie ma jawnie podanych uprawnień do danego obiektu.

## Własność i przejmowanie

Każdy obiekt posiada jednego właściciela i jest on przypisany do obiektu w momencie jego tworzenia. Początkowo właściciel ma pełnie praw do obiektu.

Prawo własności może być przekazane innemu użytkownikowi.

Właściciel może mieć zabrane uprawnienia do obiektu, jednak w każdej chwili może je sobie przywrócić.

Nie ma możliwości usunięcia użytkownika, który posiada prawo własności do jakiegoś obiektu.

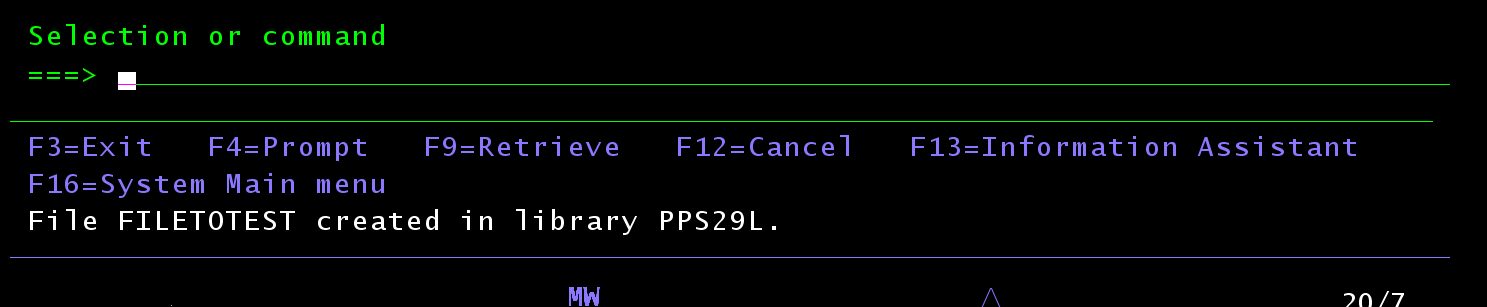
W razie uszkodzenia użytkownika mającego prawo do jakiś obiektów, właścicielem tych obiektów staje się QDTFOWN.

# 

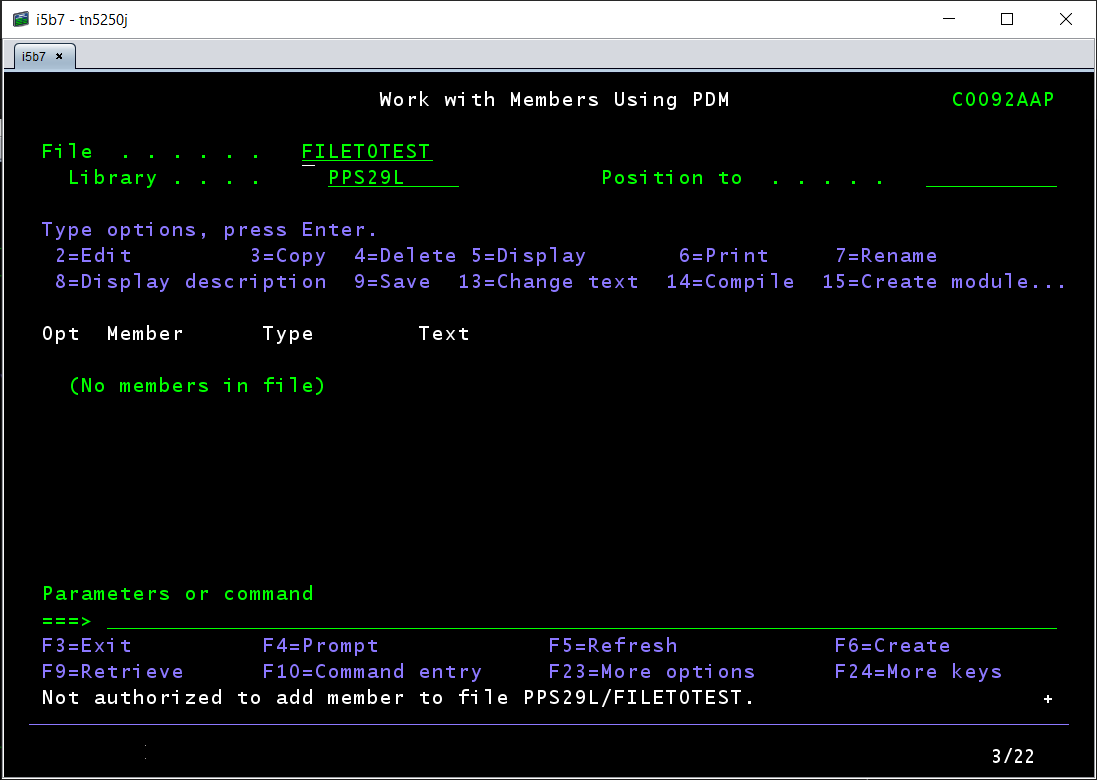
# Sekcja praktyczna

## Należy stworzyć obiekt (np. bibliotekę, Source Physical File w bibliotece)

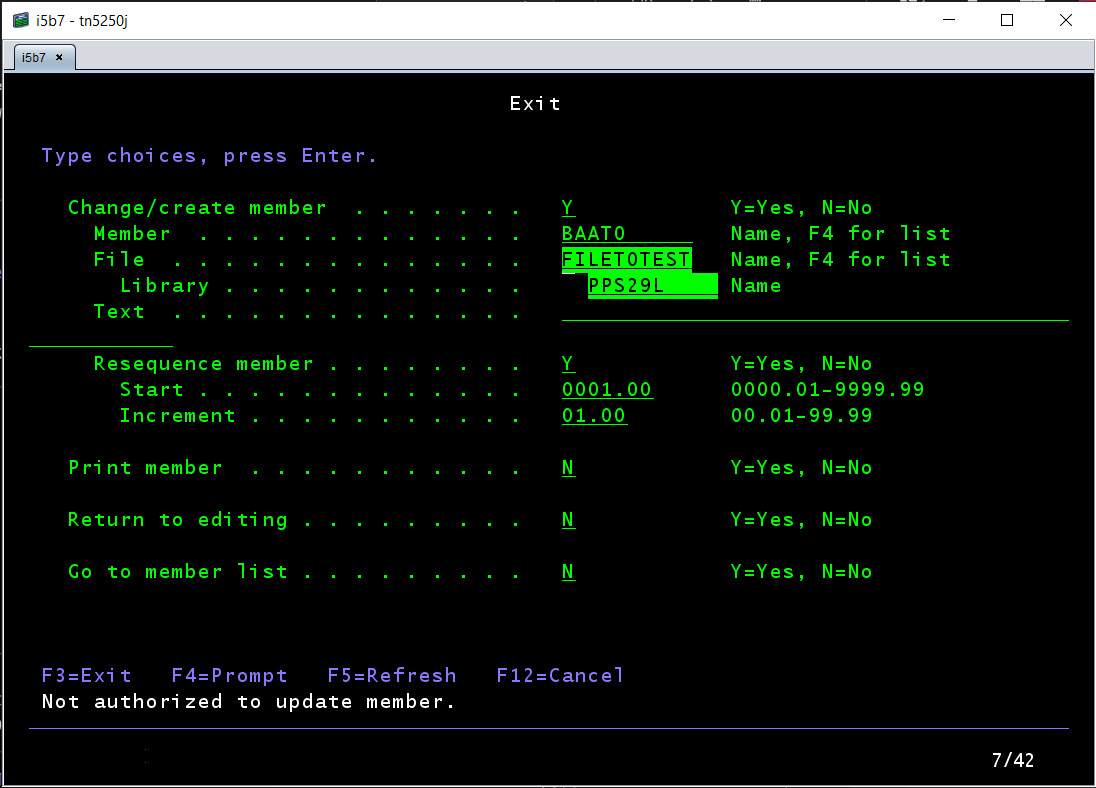
Plik został stworzony za pomocą komendy CRTSRCPF w bibliotece PPS29L.



Domyślnie inny użytkownik nie ma praw do dodawania nowych memberów.



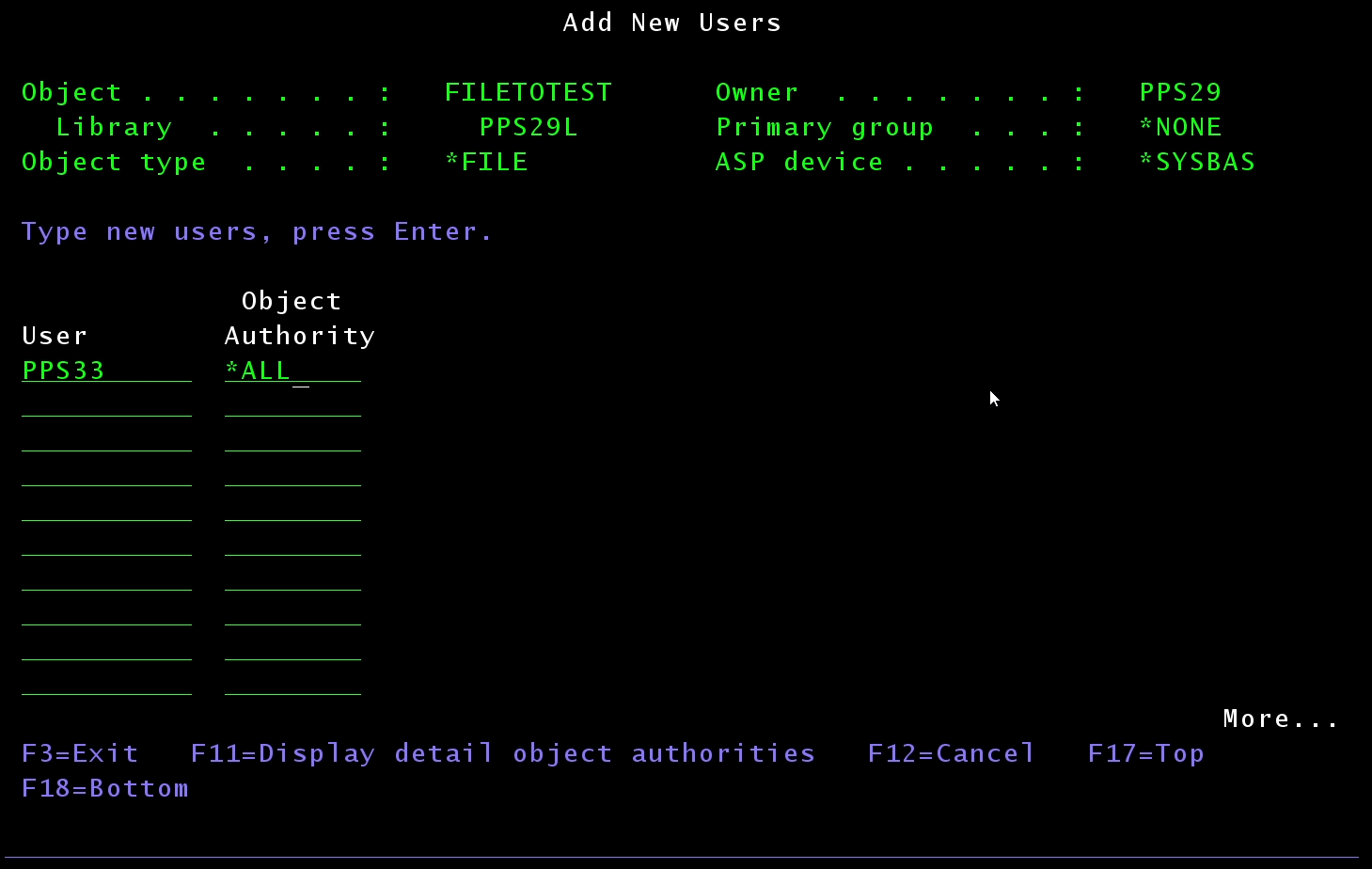
Po stworzeniu membera, domyślnie inny użytkownik nie ma również prawa edycji membera.

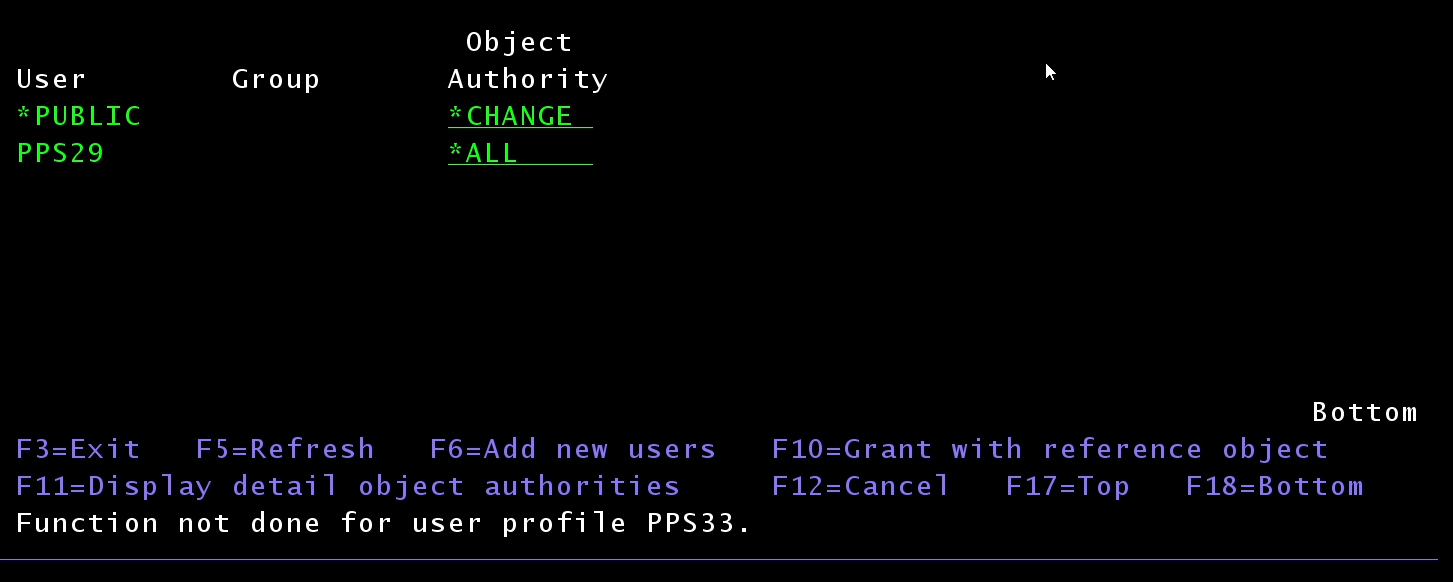


## 

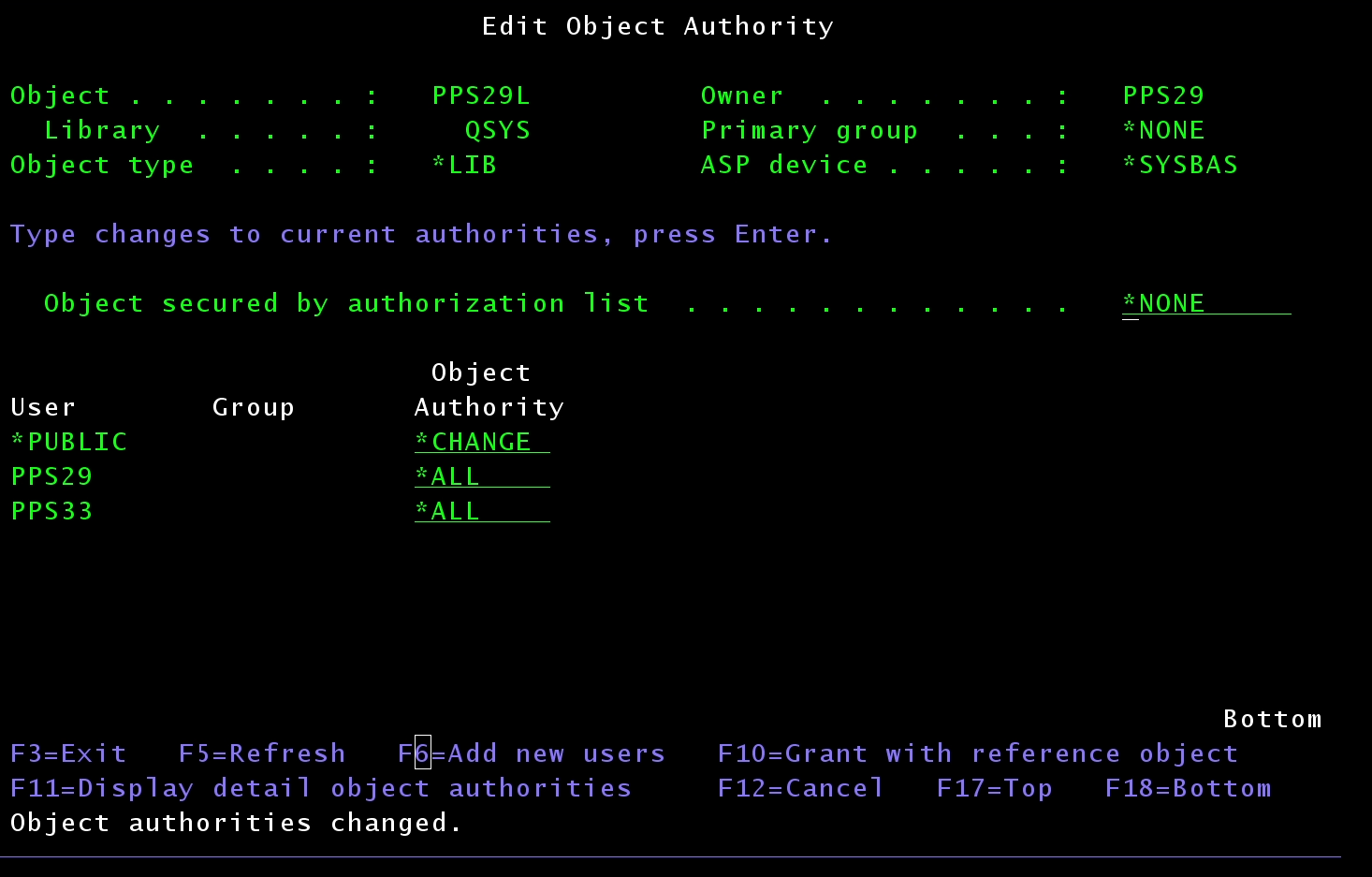
## Nadać uprawnienia bezpośrednie, pokazać działanie.

Tutaj nie wiemy czemu, ale próba nadania uprawnień komendą EDTOBJAUT ciągle skutkowała niepowodzeniem (EDTOBJAUT -> F3 Add new user), co pokazaliśmy na poniższych zrzutach.

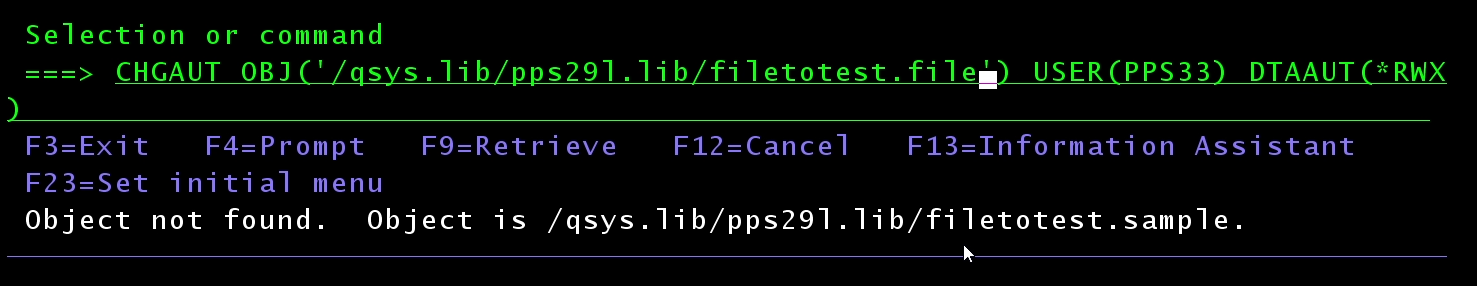


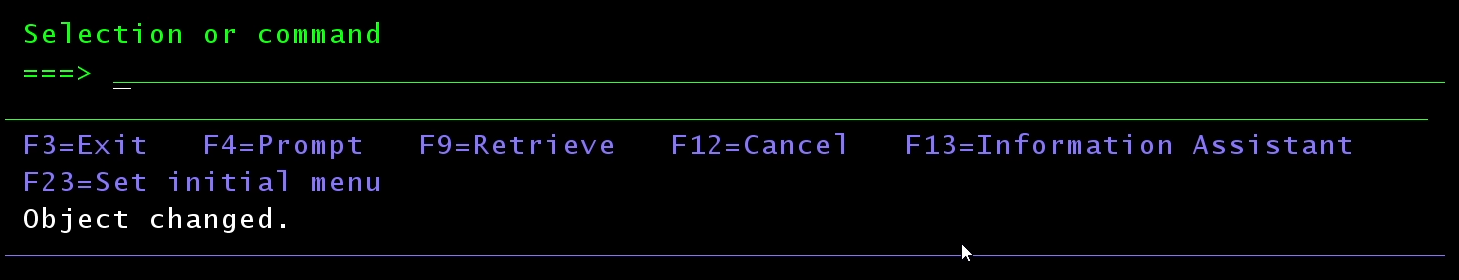


Po analizie dokumentacji stwierdziliśmy, że może to być spowodowane niedostatecznymi uprawnieniami dla użytkownika z poziomu biblioteki. Korzystając z EDTOBJAUT nadaliśmy pełne prawa użytkownikowi do biblioteki.

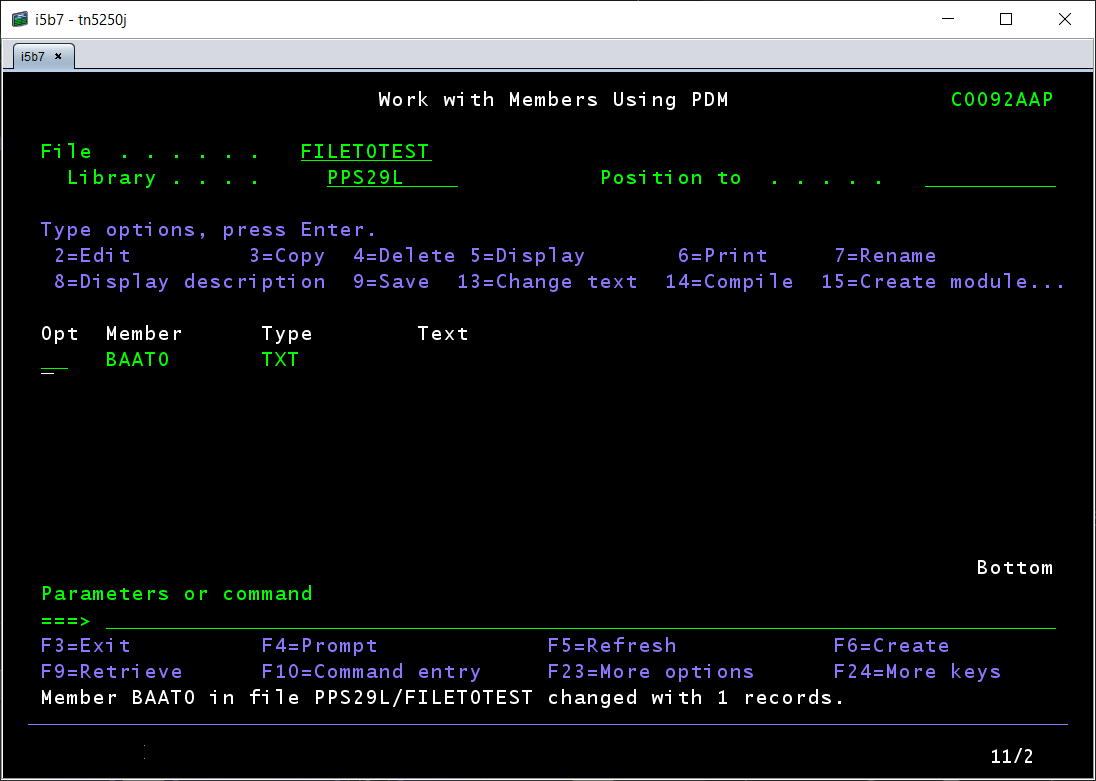
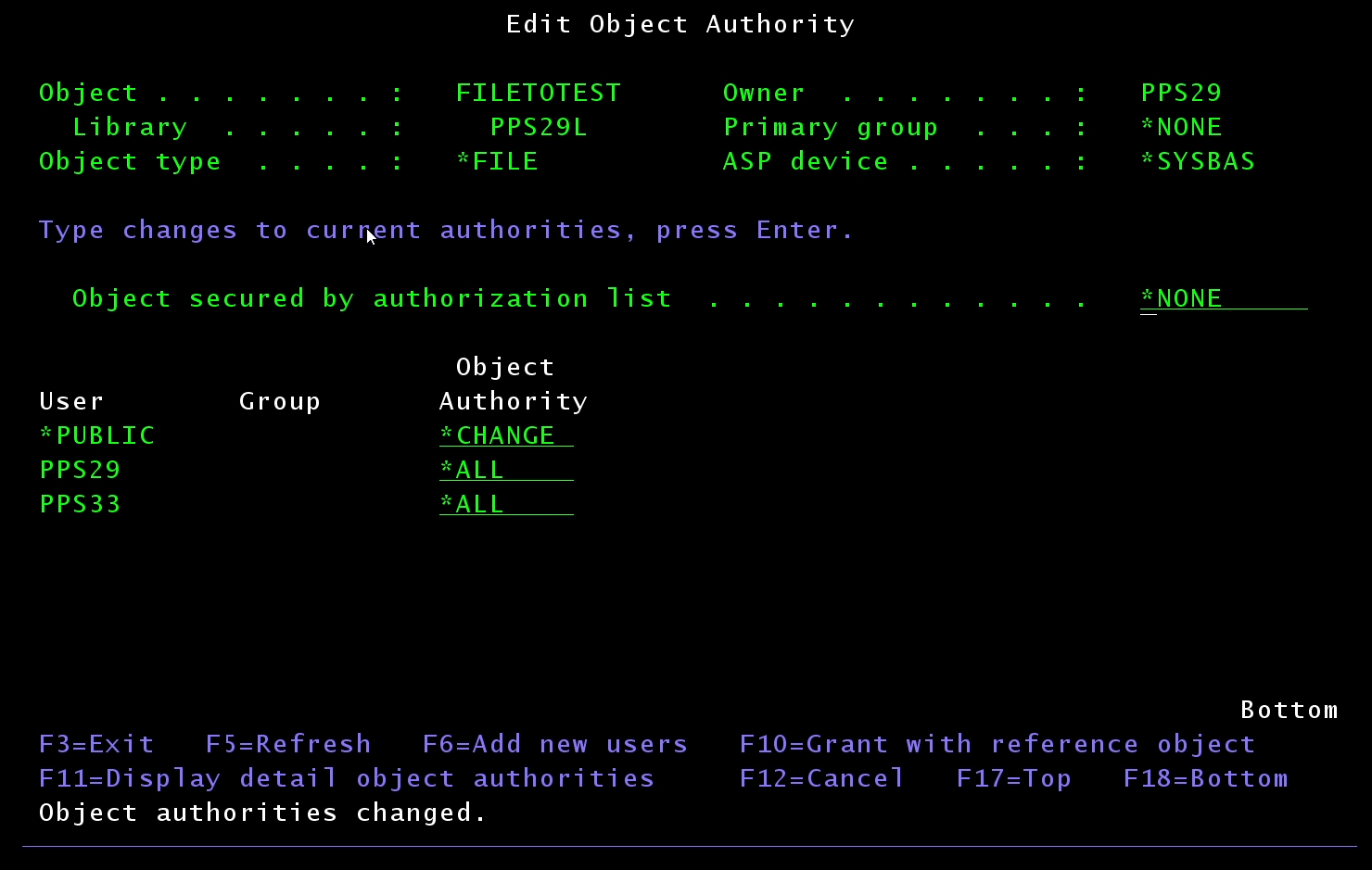


W dalszym ciągu nie rozwiązało to również problemów z nadaniem uprawnień dla obiektu. Dopiero użycie komendy CHGAUT przedstawionej poniżej zadziałało i użytkownik PPS33 dostał wpis uprawnień w pliku FILETOTEST.



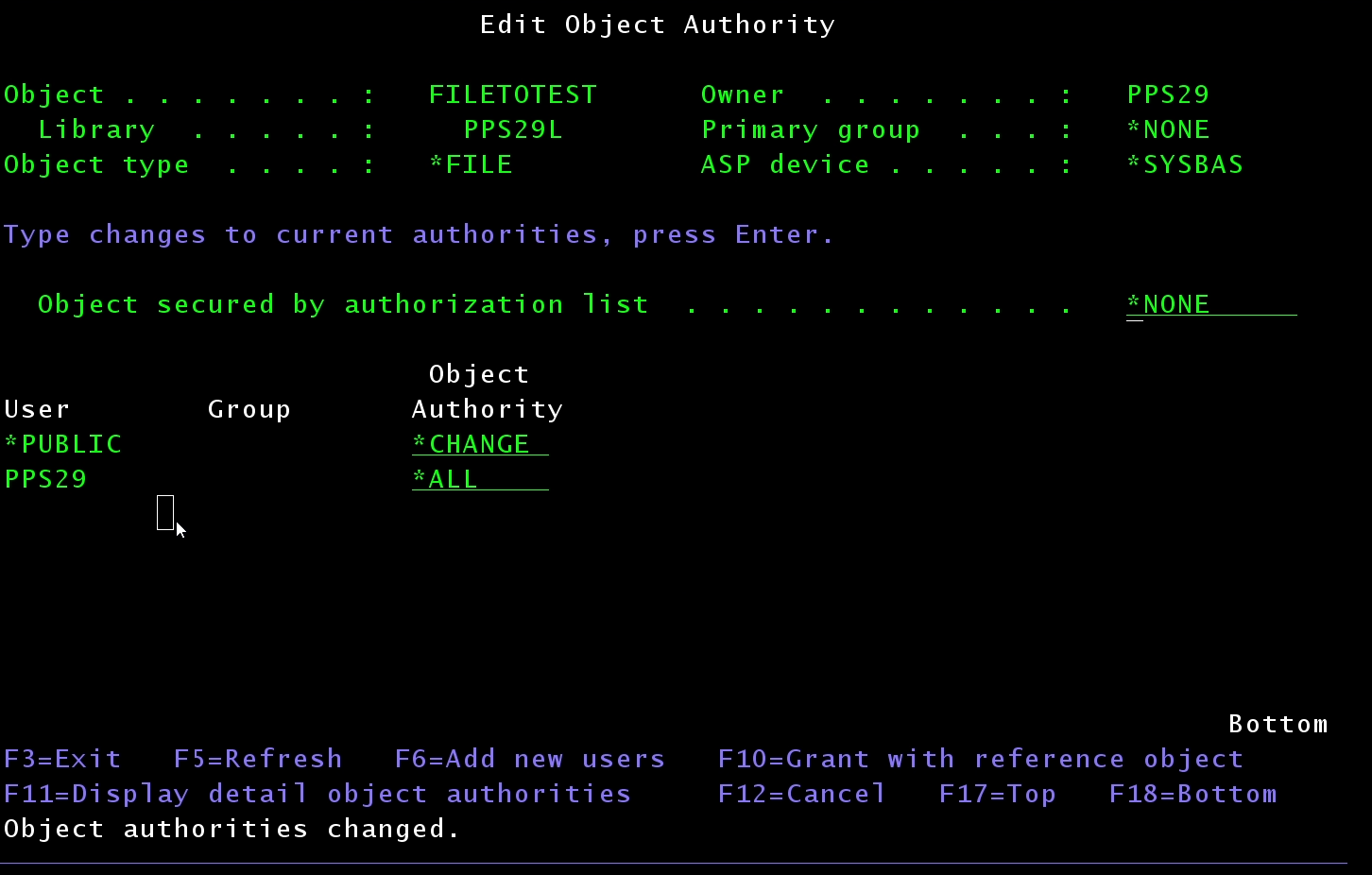


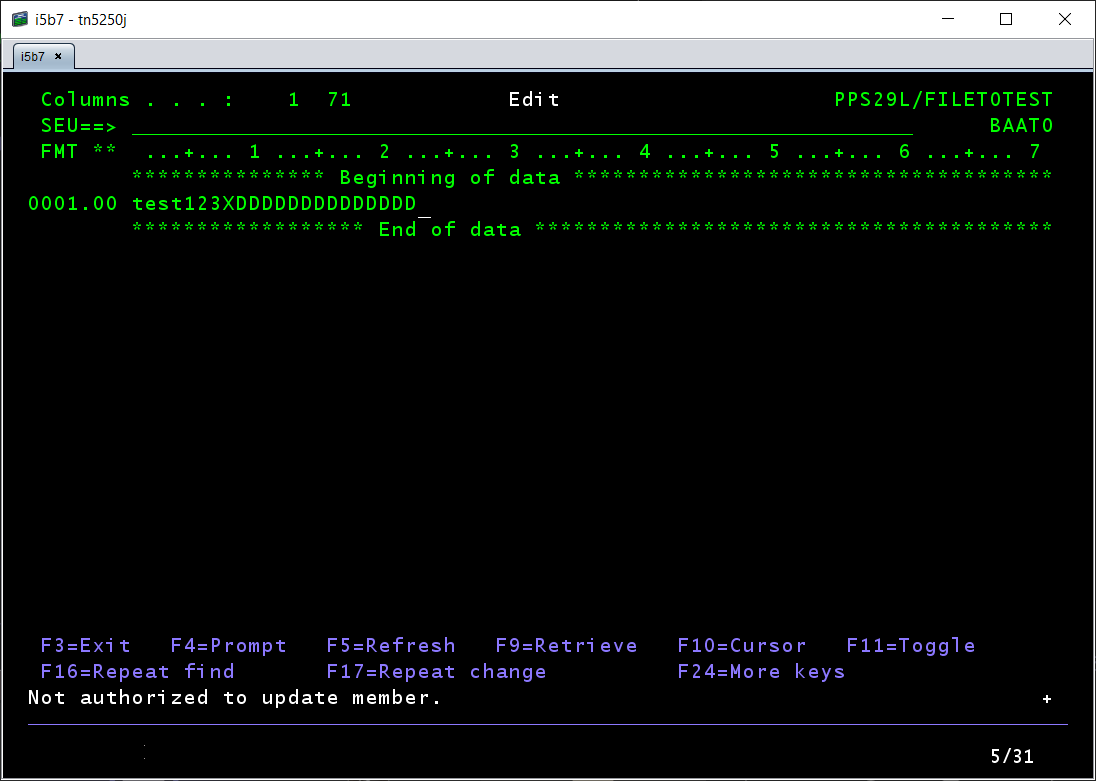
Wpis, który powyższa komenda dała dał użytkownikowi PPS33 uprawnienia na poziomie \*CHANGE. Nie wystarczyły one jednak do edycji obiektu, dopiero zmiana tych uprawnień na uprawnienia pełne pozwoliła wykonać edycję. Tym razem ta zmiana przebiegła bez problemu.



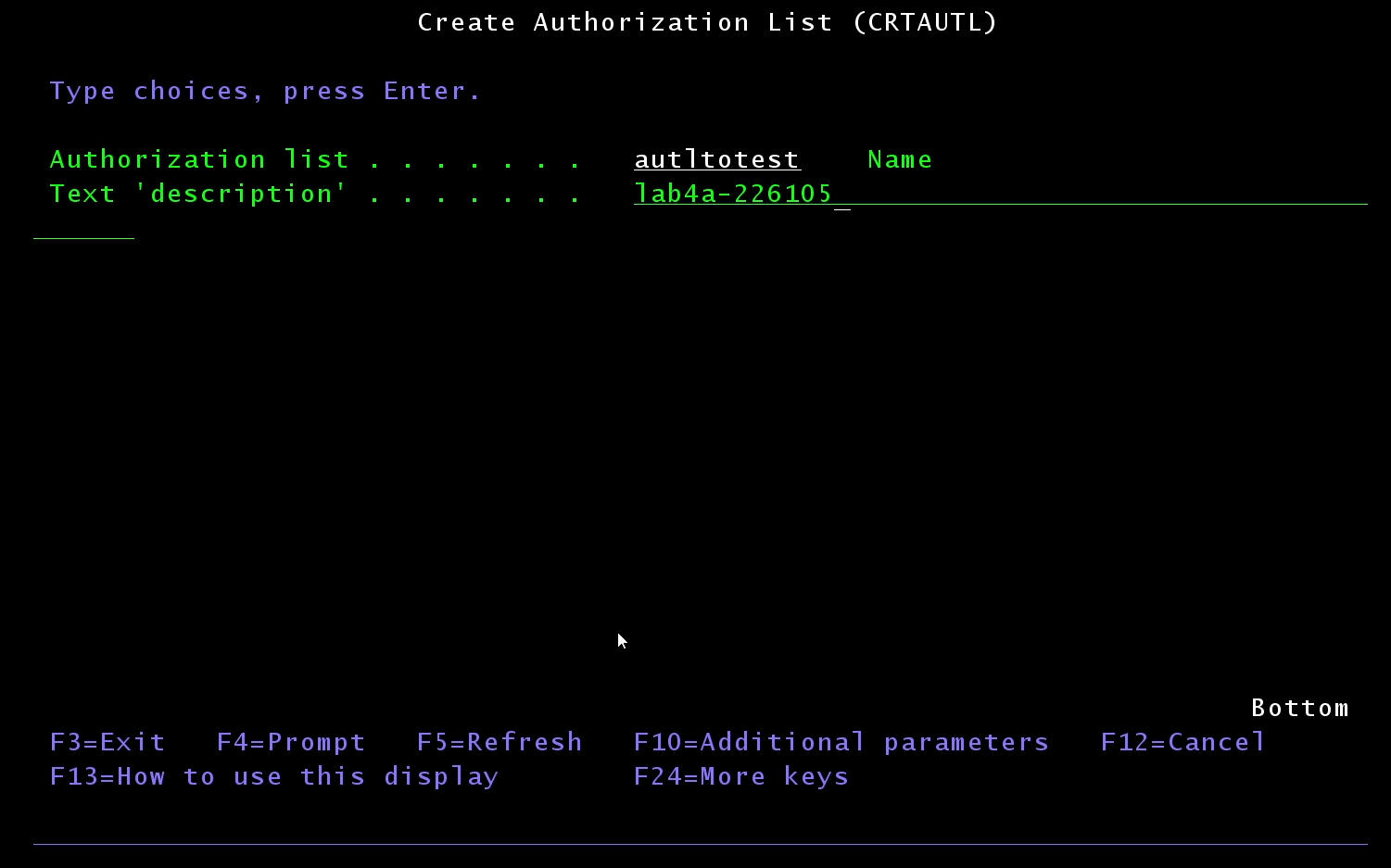
## Stworzyć listę autoryzacji

Przed stworzeniem listy autoryzacji cofnięte zostały nadane ręcznie uprawnienia oraz sprawdzone zostało, że użytkownik stracił prawa do edycji.



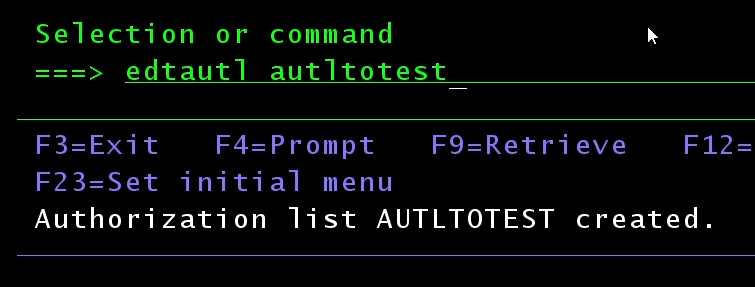


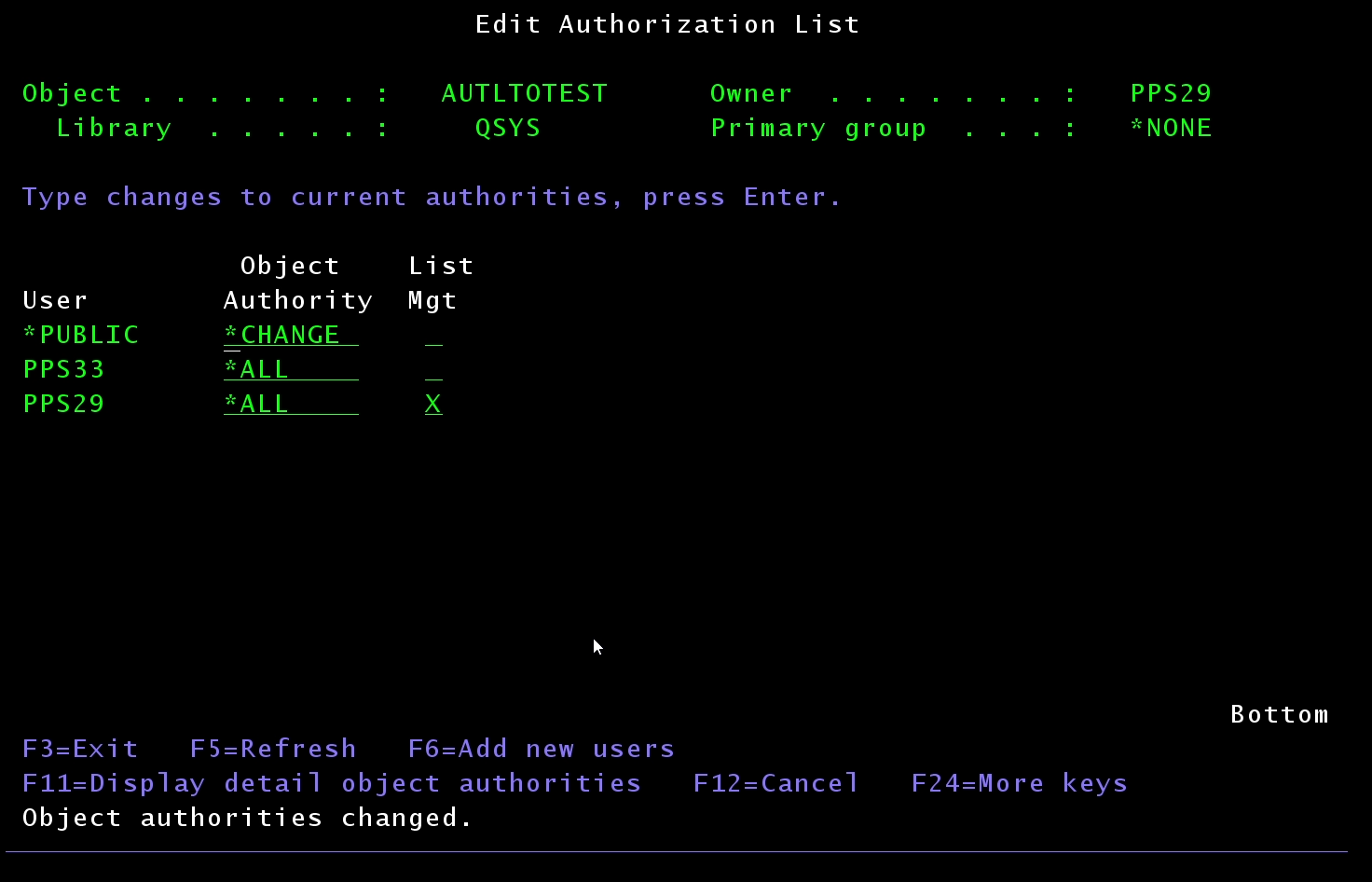
Lista autoryzacji została stworzona poleceniem CRTAUTL.



## Nadać uprawnienia przez listę autoryzacji

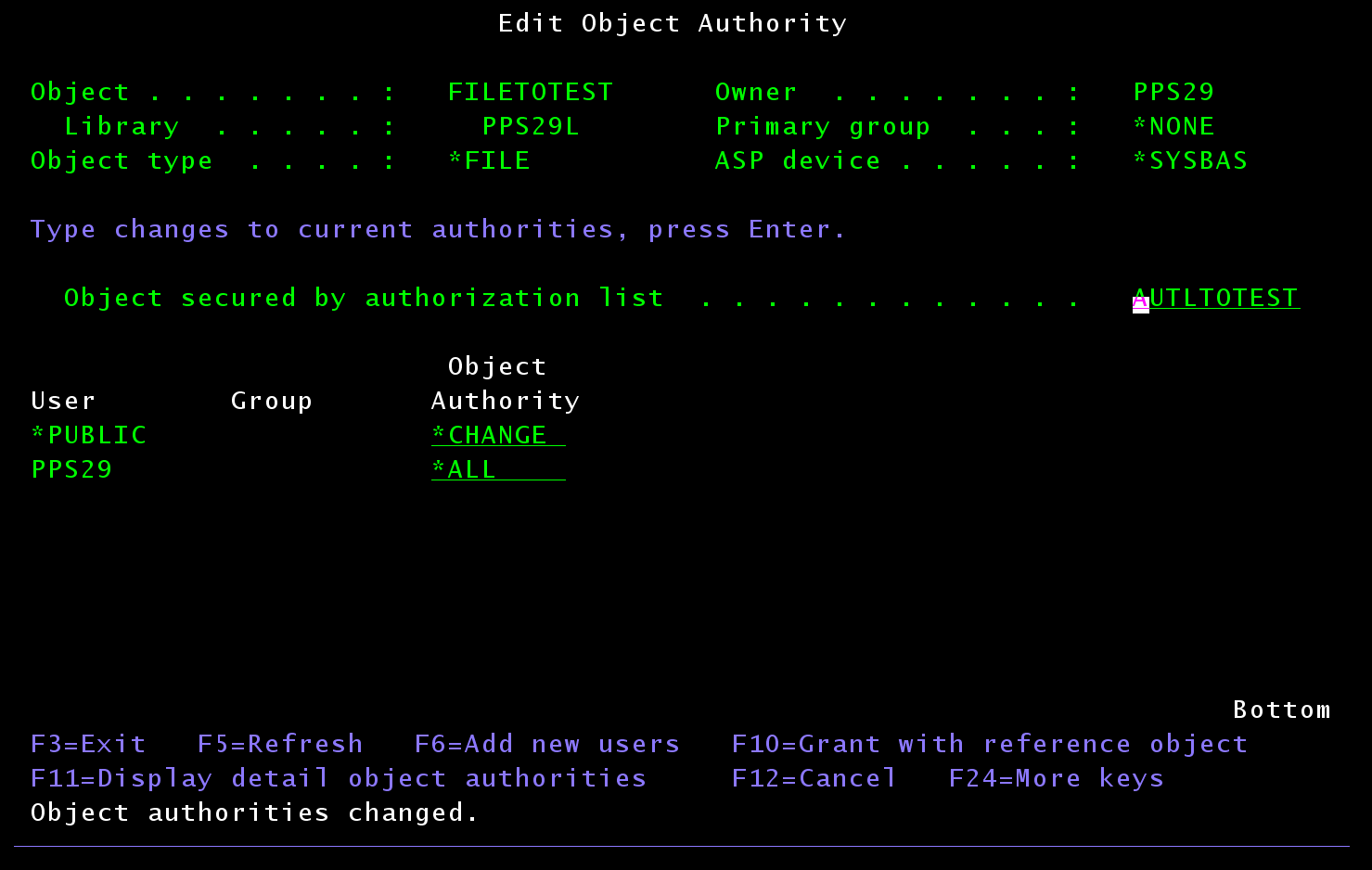
Tutaj zamieniona została przez nas kolejność i najpierw przypisaliśmy do listy użytkownika, a dopiero później powiązaliśmy listę z plikiem. Nie zmienia to jednak efektu tego zadania. Użytkownik został do listy przypisany za pomocą komendy EDTAUTL.





## Skojarzyć listę z pktu 3 z obiektem (1), pokazać działanie.

Dodanie listy do obiektu przebiegło bez większych komplikacji, zostało to wykonane komendą EDTOBJAUT.



Po powiązaniu listy z plikiem sprawdzone zostało, że użytkownik znowu ma prawa do edycji obiektu.

