INF4420: Éléments de Sécurité Informatique

Corrigé des exercices : Autorisation, Contrôle d'accès

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices Autorisation, Contrôle d'accès

- Exercice 1 : Expression de la politique d'autorisation d'une agence bancaire

- Objectif :
  - Savoir identifier les rôles et les ressources dans une politique d'autorisation
  - Savoir appliquer les modèles DAC, RBAC et ABAC
  - Comprendre les différences entre DAC, RBAC et ABAC

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices Autorisation, Contrôle d'accès

- Exercice 1 : Expression de la politique d'autorisation d'une agence bancaire

- Vous venez d'être embauché comme administrateur de la sécurité dans un grand groupe bancaire
- Votre première mission consiste à redéfinir la politique d'autorisation des agences bancaires du groupe
- Pour réaliser cette mission, vous décidez de commencer par recenser les types d'usager (rôles) ainsi que les types de ressource présents dans les agences bancaires

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices Autorisation, Contrôle d'accès

- Question 1 : Quels sont les différents types d'usagers que vous avez identifiés ?

Exercices Autorisation, Contrôle d'accès

- Réponse (possible) question 1 :
  - Responsable_agence
  - Conseiller_financier
  - Conseiller_immobilier
  - Service_clientele
  - Client

Exercices Autorisation, Contrôle d'accès

- Question 2 : Quels sont les différents types de ressource que vous avez identifiés ?

Exercices Autorisation, Contrôle d'accès

- Réponse (possible) question 2 :

- Ressources logiques (données)
  - Profil_client
  - Compte_client
  - Carte_client
  - Prêt (hypothèque)
  - Historique_operation
  - Historique_credit

- Ressources physiques
  - Ordinateur
  - Imprimante
  - Coffre
  - Armoire
  - Porte
  - DAB
  - Etc.

Exercices Autorisation, Contrôle d'accès

- Votre mission concerne la définition de la politique de contrôle d'accès aux données logiques

- Vous décidez de faire une visite à une agence de la banque
  - Vous collectez les informations suivantes :
    - L'agence a 10 employés : 1 directeur, 3 conseillers, 1 conseiller immobilier et 5 service_clientèle
    - L'agence a 50 clients ayant chacun un profil
    - En moyenne, chaque client a 3 comptes, un prêt hypothécaire et 1 carte
    - Un historique d'opération est associé à chaque compte
    - Un historique de crédit est associé à chaque carte

Exercices Autorisation, Contrôle d'accès

- Question 3 : quelle serait, en moyenne, la taille de la matrice de contrôle d'accès si vous utilisiez le modèle DAC ?
  1. 5 * 6
  2. 60 * 60
  3. 12 * 500
  4. 60 * 500

Exercices Autorisation, Contrôle d'accès

- Réponse question 3 : 60 * 500
  - 60 lignes : 10 employés + 50 clients
  - 500 colonnes : 10 objets * 50 clients

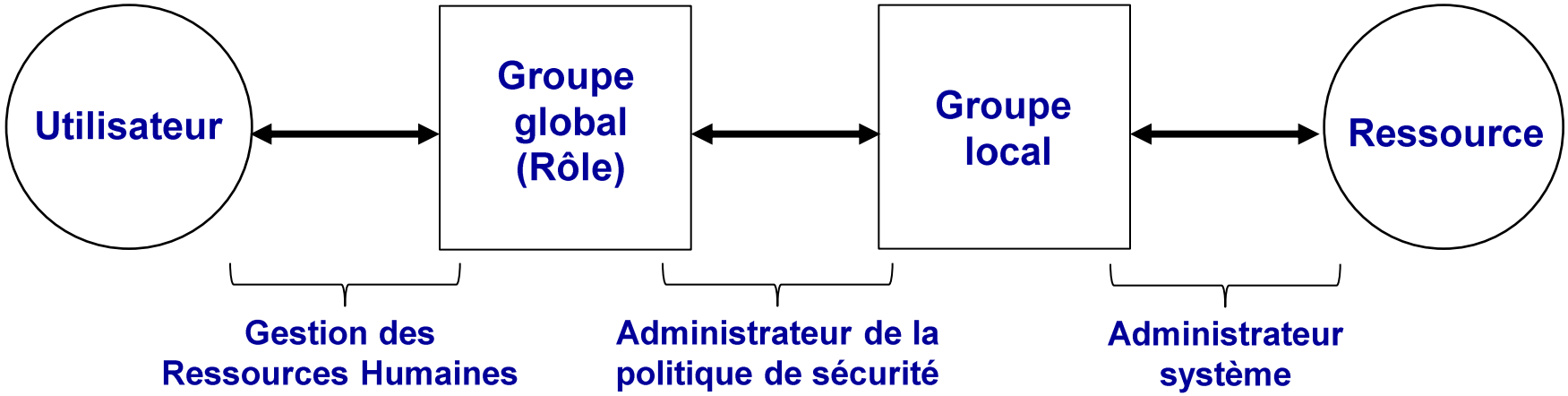
- Votre conclusion est que la matrice de contrôle d'accès est trop grande pour être gérable avec le modèle DAC

- Vous décidez d'étudier si le modèle RBAC (Role Based Access Control) convient

- Comme la banque est sous Windows, vous optez pour l'implémentation AGLP (Access – Global – Local – Permissions) de RBAC

Exercices Autorisation, Contrôle d'accès

- AGLP (Rappel)



- Après discussion avec la RH, vous décidez d'associer chaque type d'usager que vous avez identifié à un groupe global (rôle)
- Après discussion avec le sys admin, vous décidez d'associer chaque type de ressource que vous avez identifié à un groupe local

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices Autorisation, Contrôle d'accès

- Vous apprenez que le conseiller_financier peut jouer occasionnellement le rôle de service_clientèle

- Vous apprenez également que le responsable_agence peut jouer occasionnellement les rôles de conseiller_financier et de conseiller_immobilier

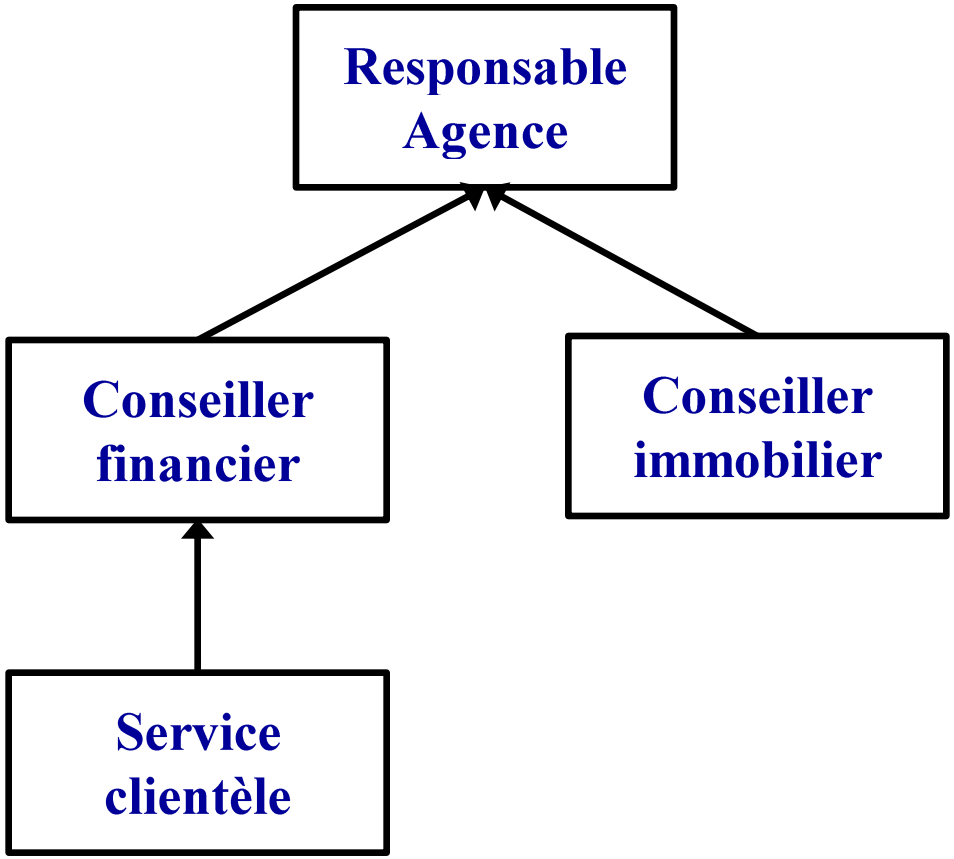
- Question 4 : Proposez une organisation hiérarchique des rôles correspondant à cette organisation

Exercices Autorisation, Contrôle d'accès

- Réponse question 4 :

Exercices Autorisation, Contrôle d'accès

- Réponse question 4 :



POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices Autorisation, Contrôle d'accès

- Vous apprenez qu'aucun usager ne devrait pouvoir cumuler les permissions de conseiller immobilier et de conseiller financier (contrainte 1)

- Question 5 : Quelle anomalie cela crée-t-il dans votre modélisation ?

Exercices Autorisation, Contrôle d'accès

- Réponse question 5 : Comme le responsable d'agence hérite des rôles de conseiller financier et de conseiller immobilier, il cumule les permissions de ces rôles. Ce qui viole la contrainte 1

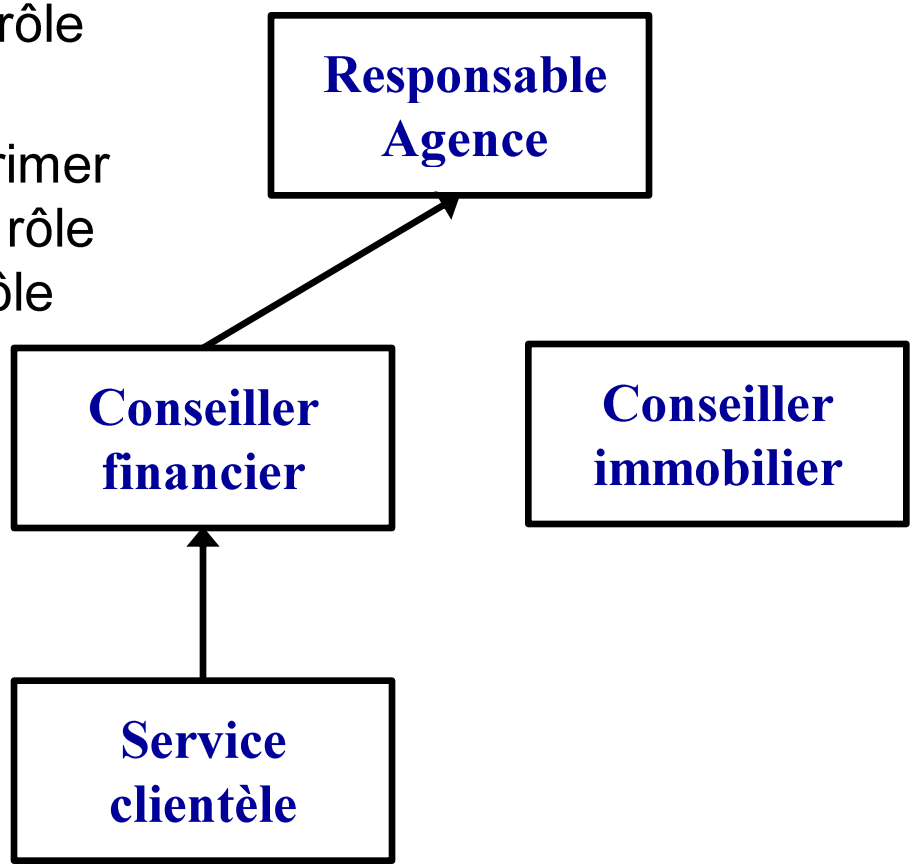
POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices Autorisation, Contrôle d'accès

- Question 6 : Comment proposez-vous de résoudre le problème ?

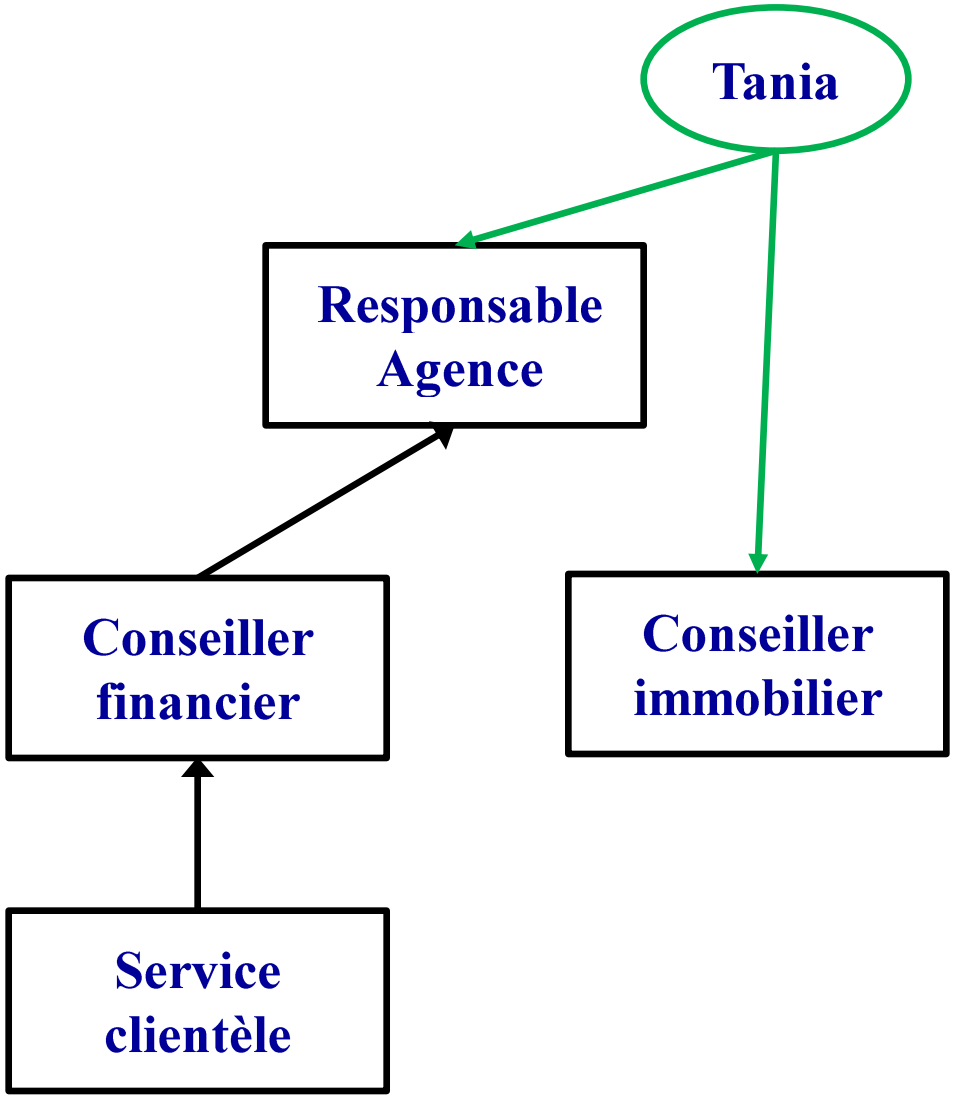
Exercices Autorisation, Contrôle d'accès

- Réponse question 6 :
  - Il faut modifier la hiérarchie de rôle pour éliminer le conflit
    - Par exemple, on peut supprimer le lien hiérarchique entre le rôle conseiller immobilier et le rôle responsable d'agence



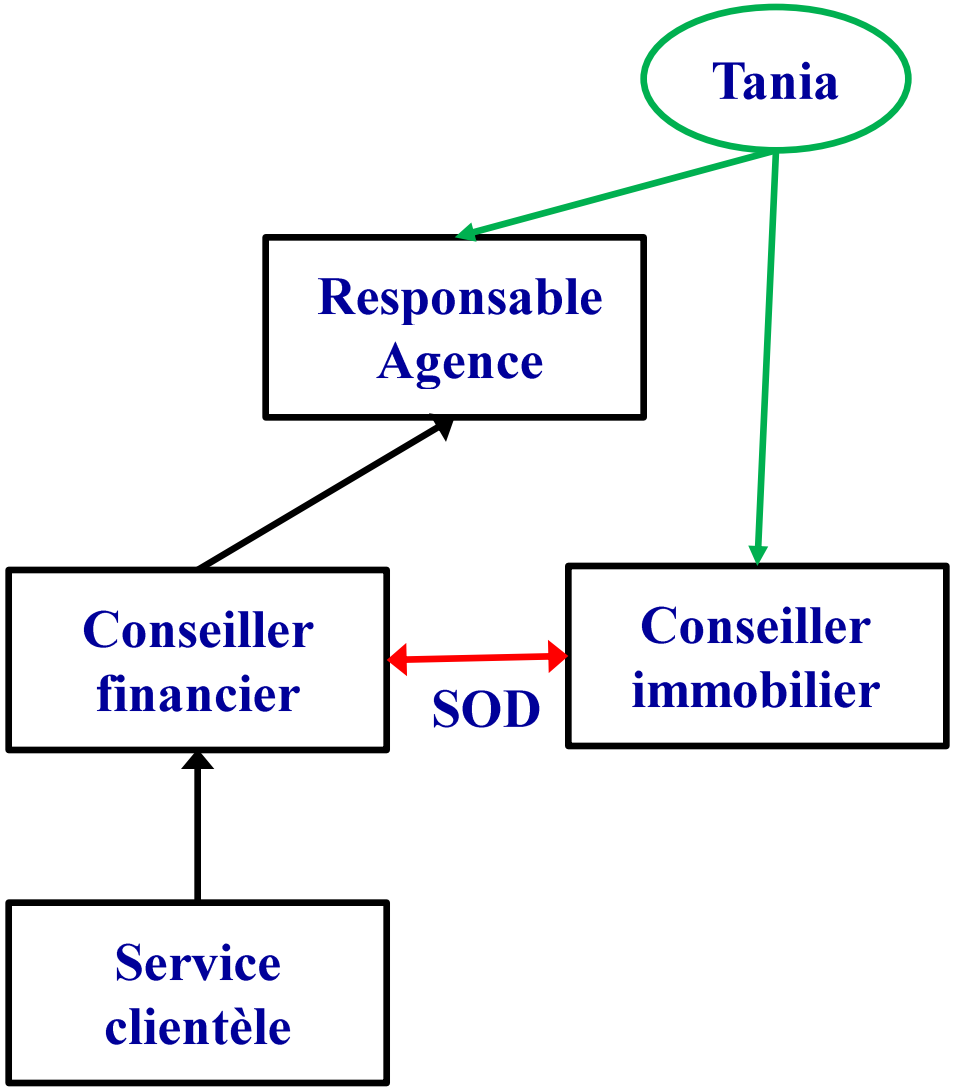
Exercices Autorisation, Contrôle d'accès

- Réponse question 6 :
  - Supposons que Tania soit la responsable d'agence et que Tania soit *explicitement* affectée aux deux rôles :
    - Responsable d'agence
    - Conseiller immobilier



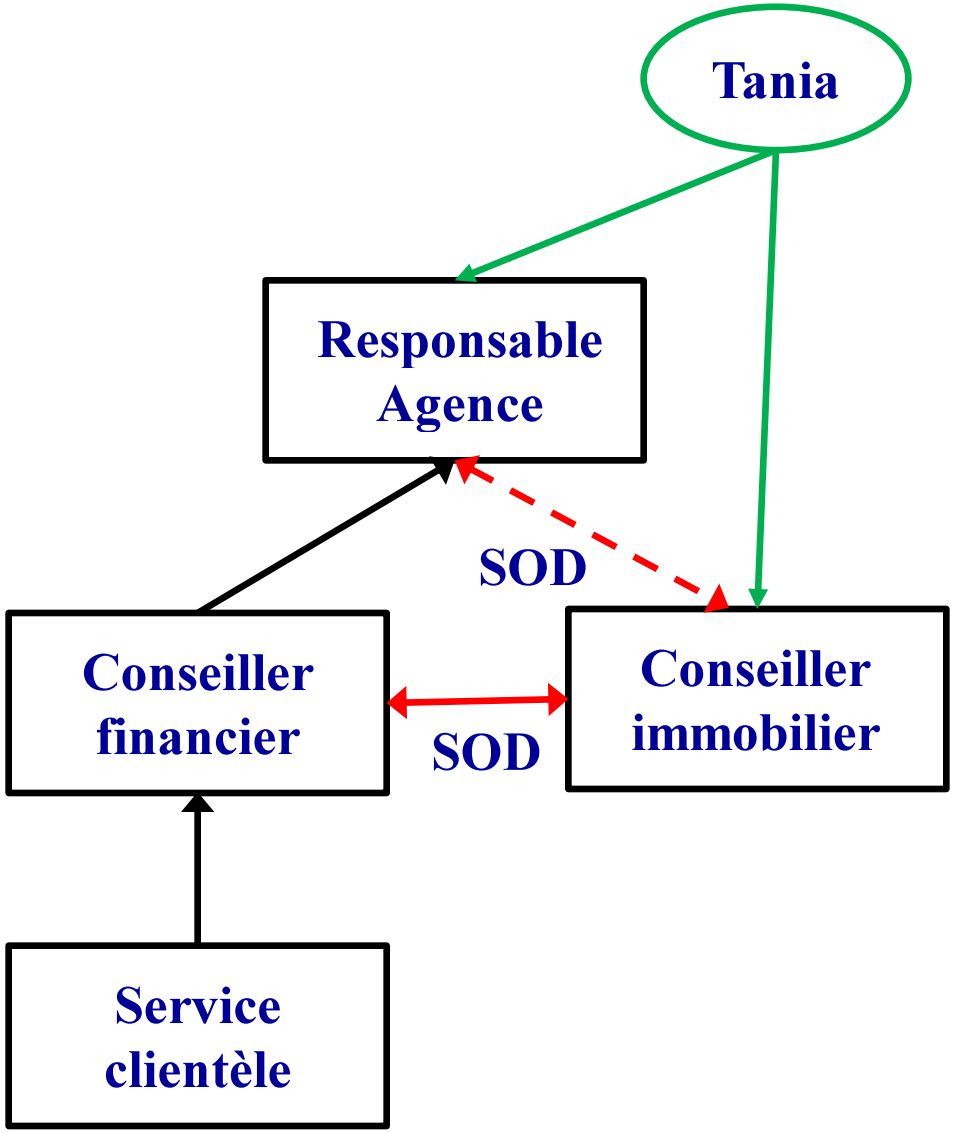
Exercices Autorisation, Contrôle d'accès

- Réponse question 6 :
  - Pour satisfaire la contrainte 1, il faut créer une règle de type « Séparation of Duty » entre les rôles :
    - Conseiller financier
    - Conseiller immobilier



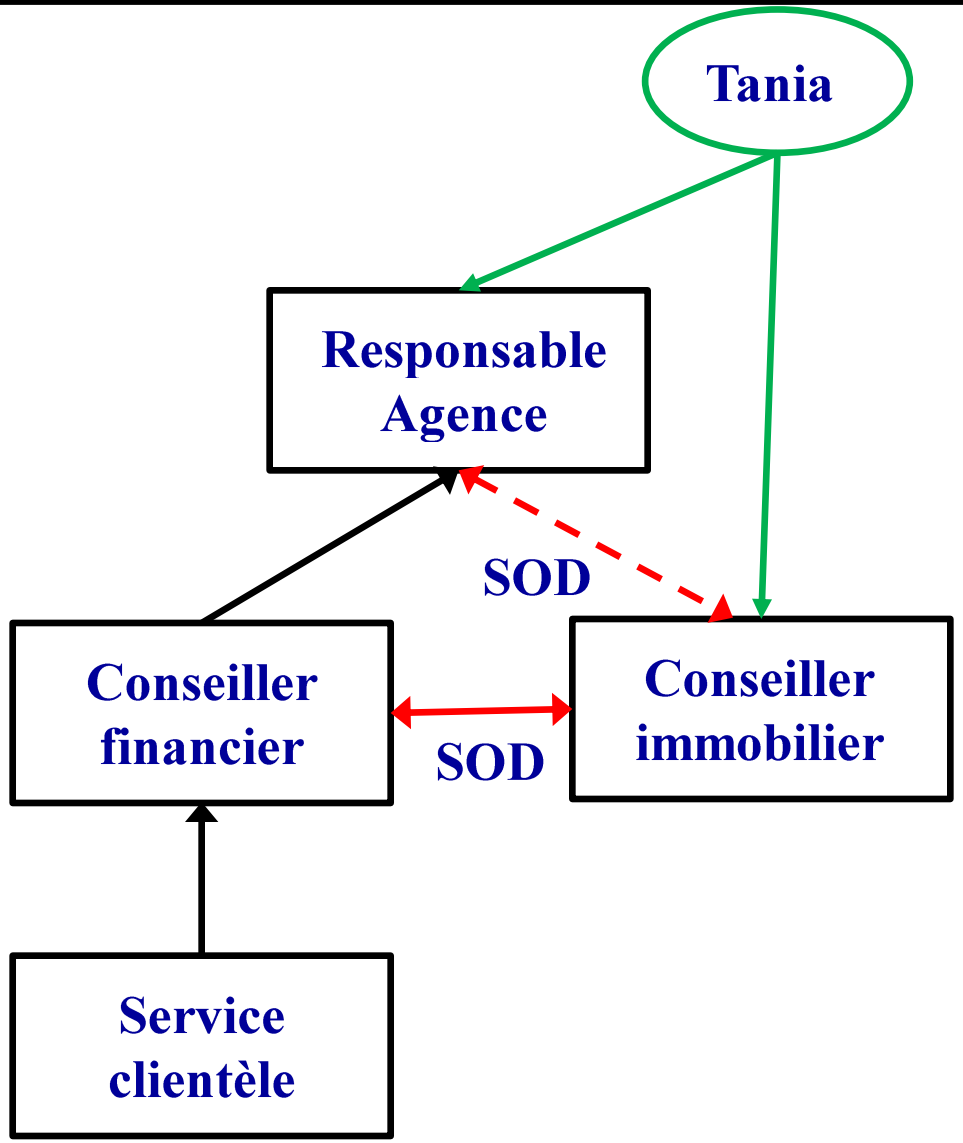
Exercices Autorisation, Contrôle d'accès

- Réponse question 6 :
  - Le responsable d'agence hérite implicitement de cette SOD



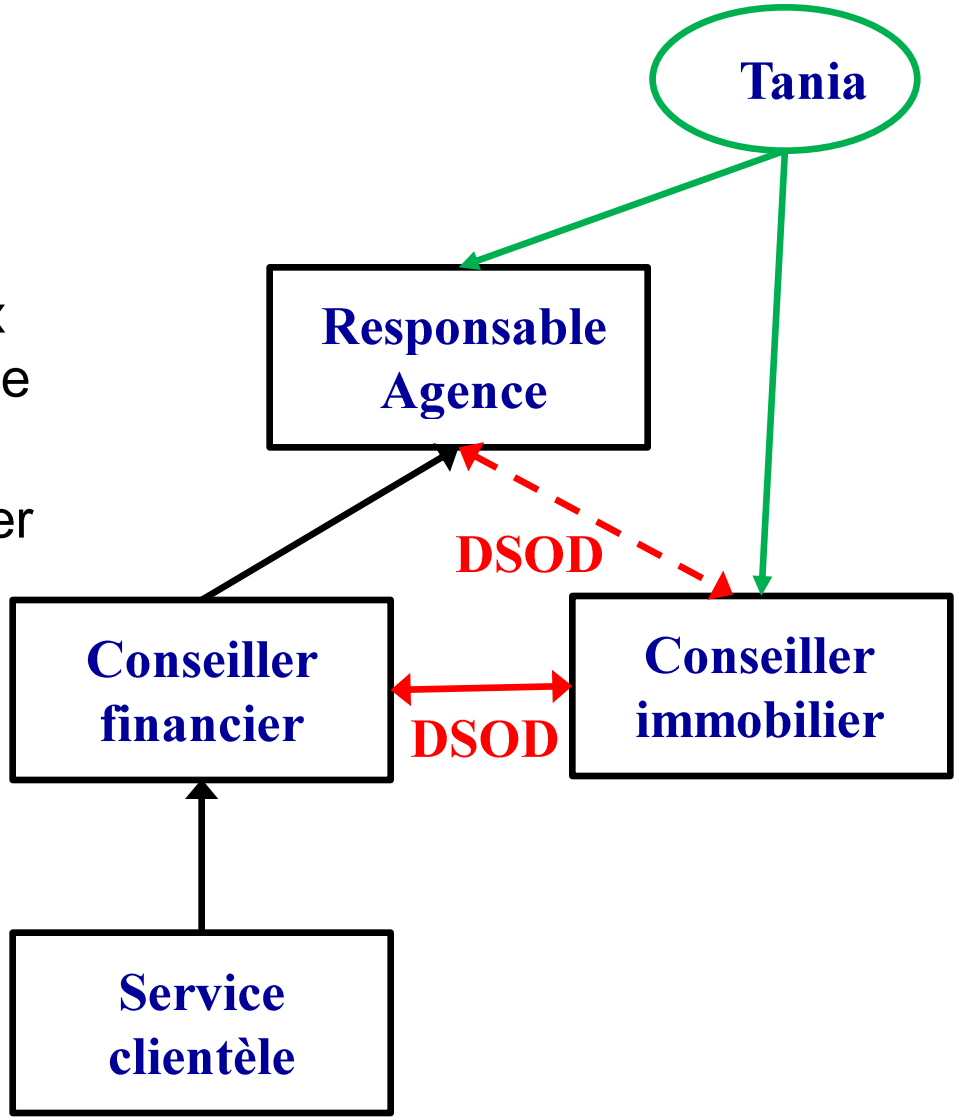
Exercices Autorisation, Contrôle d'accès

- Réponse question 6 :
  - Si la SOD est statique (SSOD), alors Tania ne peut pas être affectée aux rôles Responsable Agence et Conseiller immobilier
  - Problème !



Exercices Autorisation, Contrôle d'accès

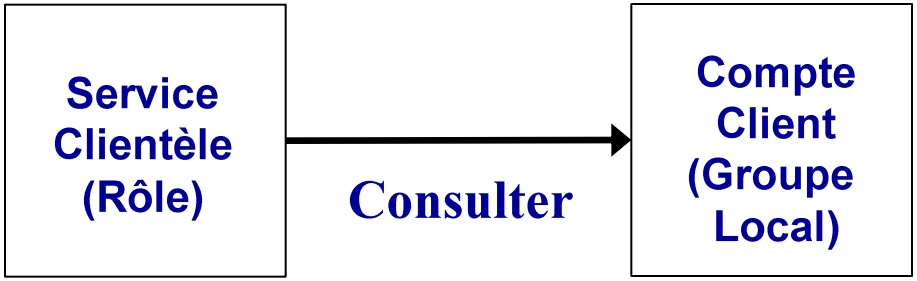
- Réponse question 6 :
  - Solution : La SOD doit être dynamique (DSOD)
  - Tania est affectée aux deux rôles Responsable d'agence et Conseiller Immobilier
  - Mais elle ne peut pas activer ces deux rôles en même temps



Exercices Autorisation, Contrôle d'accès

- Vous devez maintenant utiliser le modèle RBAC / AGLP pour exprimer les règles d'autorisation de la politique d'autorisation s'appliquant à l'agence
- Exemple de règle :
  - Le rôle service_client a la permission de consulter (lire) le compte des clients

- Il n'y a pas de difficulté pour exprimer ce type de règle avec AGLP



Exercices Autorisation, Contrôle d'accès

- Vous rencontrez des difficultés pour exprimer les règles d'autorisation s'appliquant au rôle client
- Exemples
  - Un client peut consulter ses comptes
  - Un client peut consulter les comptes d'un autre client à condition que ce client lui ait donné procuration

- Question 7 : Est-il possible d'exprimer ce type de règle en utilisant AGLP ?

- Question 8 : Si oui, quelle est votre solution ?

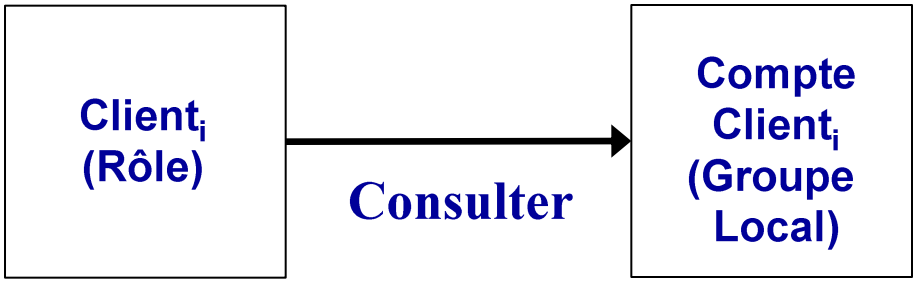
Exercices Autorisation, Contrôle d'accès

- Réponse question 7 : La réponse est oui, mais c'est compliqué !

Exercices Autorisation, Contrôle d'accès

- Réponse question 8 :
  - Il faut créer autant de rôles qu'il y a de clients :
    - Ensemble de rôles : $Client_i$ où i est un client
  - Il faut aussi créer des groupes locaux pour chaque client :
    - Ensemble de groupes locaux : $Compte\_client_i$ où i est un client

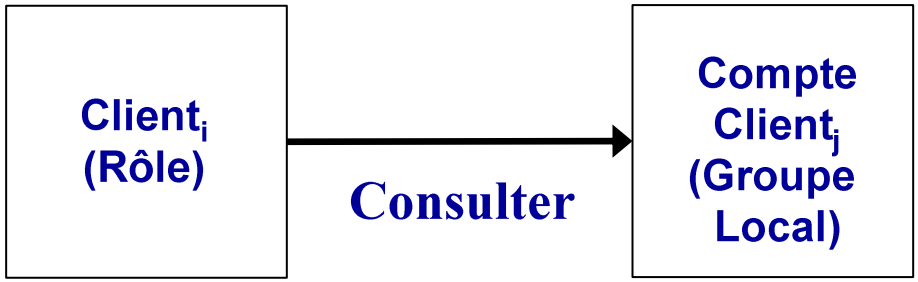
- Expression de la règle :
  - Un client peut consulter ses comptes



Exercices Autorisation, Contrôle d'accès

- Réponse question 8 :

- Et si le client j a donné procuration au client i pour qu'il puisse consulter ses comptes



Exercices Autorisation, Contrôle d'accès

- On perd complètement l'intérêt de RBAC !
  - Autant utiliser DAC !

- Un collègue vous recommande de continuer à utiliser RBAC :
  - En conservant le rôle Client et le groupe local Compte_client
  - En codant dans l'application « Consulter » le test que le compte consulté est bien un compte du client ou bien un compte pour lequel le client a procuration

- Question 9 : Que répondez-vous à ce collègue ?

Exercices Autorisation, Contrôle d'accès

- Réponse question 9 :

Exercices Autorisation, Contrôle d'accès

- Réponse question 9 :
  - Il faut séparer l'expression de la politique d'autorisation de l'implantation de l'application « Consulter » (comme des autres applications d'ailleurs)
  - Sinon, c'est compliqué de savoir si la politique d'autorisation est correctement appliquée
  - Sinon, c'est compliqué de faire les mises à jour (politique & applications)
  - Et ce n'est pas le rôle du développeur d'application d'implanter la politique de sécurité
    - Separation of Duty appliqué au développeur d'application !

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices Autorisation, Contrôle d'accès

- Vous décidez d'utiliser le modèle ABAC (Attribute Based Access Control) pour exprimer la politique de sécurité associée au rôle Client

- Vous considérez les attributs suivants pour les sujets :
  - Attributs du sujet : Nom, Rôle

- Vous considérez les attributs suivants pour les ressources :
  - Attributs de la ressource : Type, Ident, Nom_client, Liste_procuration

Exercices Autorisation, Contrôle d'accès

- Question 10 : En utilisant le modèle ABAC, exprimer les règles suivantes :
  - Un client peut consulter ses comptes
  - Un client peut consulter les comptes d'un autre client à condition que ce client lui ait donné procuration

Exercices Autorisation, Contrôle d'accès

- Réponse question 10 :

Exercices Autorisation, Contrôle d'accès

- Réponse question 10 :
  - Un client peut consulter ses comptes
  - Permettre si Role(Sujet)=Client et Type(Ressource)=Compte_client et Non(sujet)=Nom_client(Ressource) et Ident(Action)=Consulter

  - Un client peut consulter les comptes d'un autre client à condition que ce client lui ait donné procuration
  - Permettre si Role(Sujet)=Client et Type(Ressource)=Compte_client et Nom(sujet) $\in$ Liste_procuration (Ressource) et Ident(Action)=Consulter