5.4 Übungsaufgabe: RBAC & SoD

Alice ist Professor. Barbara und Charlie sind Beisitzer. Barbara, Charlie, Don und Egon sind Studenten. Das Informationssystem der Hochschule sieht folgenden Ablauf einer mündlichen Prüfung vor. Der Beisitzer fertigt zur Prüfung ein Protokoll an, das er im Anschluss im System speichert. Der Professor trägt die Note ins System ein. Abschließend signieren der Student, der Beisitzer und der Professor das Protokoll und die Note digital.

a) Formalisieren sie dieses Szenario als RBAC-Modell. Geben Sie dazu das Tupel (U, R, P, UA, PA, SESSION) mit den passenden Mengen und Relationen an. Geben Sie bei SESSION alle möglichen Sitzungen an.
b) Definieren Sie eine geeignete Rollenhierarchie und die daraus resultierende neue Relation Permission Assignment PA.
c) Geben Sie ein geeignetes Beispiel für eine SSoD-Regel an (textuell und formell).
d) Geben Sie ein geeignetes Beispiel für eine DSoD-Regel an (textuell und formell)

a)

RBAC = (U, R, P, UA, PA, SESSION)

U = {u_1, u_2, u_3, … } Menge der User
 R = {r_1, r_2, r_3, … } Menge der Rollen
 P = {p_1, p_2, p_3, …} Menge der Rechte (Permissions)
 UA (=User Assignment) ist eine Relation, die den Usern Rollen zuweist. Formell: UA: U → 2^R, z.B. UA(u_1) = {r_1, r_2}
 PA (=Permission Assignment) ist eine Relation, die den Rollen Rechte zuweist. Formell: PA: R → 2^P, z.B. PA(r_1) = {p_1, p_2, p_3}
 SESSION ist eine Relation, die Sitzungen definiert. Formell
SESSION ⊆ U × 2^R, wobei für (u, R) ∈ SESSION gelten muss: R ⊆ UA(u)

Beispiel: (u_1, {r_1, r_2}) ∈ SESSION, d.h. u_1 verwendet in einer Sitzung gleichzeitig die Rollen r_1 und r_2 und besitzt damit die Berechtigungen der Rollen r_1 und r_2.

U={Alice, Barbara, Charlie, Don, Egon}

R={Prof, Beisitzer, Studenten}

P={P_Protokoll, P_Note, P_Signieren}

UA(Alice)={Prof}

UA(Barbara)={Beisitzer, Student}

UA(Charlie)={Beisitzer, Student}

UA(Don)={Student}

UA(Egon)={Student}

PA(Prof)={P_Note, P_Signieren}

PA(Beisitzer)={P_Protokoll, P_Signieren}

PA(student)={P_Signieren}

E=Element von

(Alice,{Prof}) E Session

(Babara,{Beisitzer}) E Session

(Babara,{Beisitzer, Student}) E Session

(Babara,{ Student}) E Session

(Charlie,{Beisitzer, Student}) E Session

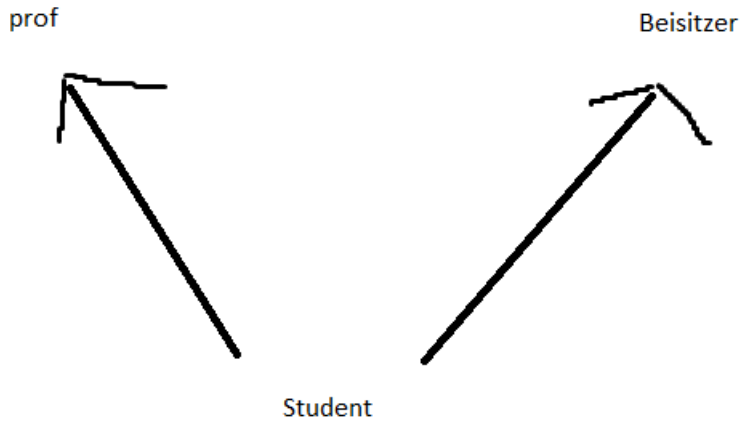
(Charlie,{ Student}) E Session

(Charlie,{Beisitzer }) E Session

(Don,{Student}) E Session

(Egon,{Student}) E Session

b)



PA(Prof)={P_Note,}

PA(Beisitzer)={P_Protokoll}

PA(student)={P_Signieren} P_Signieren wird vererbt an prof, beisitzer

c) die gleichzeitige Mitgliedschaft in den Rollen Beisitzer und Student ist ausgeschlossen

$\forall$ Beisitzer, Student $\in R$ $\forall u \in U$ gilt: $u \in member(\text{Beisitzer})$ und $u \in member(\text{Student}) \Rightarrow (r_i, r_j) \notin SSoD.$

d)

die gleichzeitige Aktivität seines Subjekts in der Rolle r_1 und r_2 ist unzulässig

$\forall$ Beisitzer, Student $\in R$ und $\forall u \in U$ muss gelten: $(u, \{\text{Beisitzer, Student}\}) \Rightarrow (r_i, r_j) \notin DSoD$