Adatbiztonság és Kriptográfia

Megbízható MarkMyProfessor alkalmazás a magyarországi felsőoktatásban

A második **gyak**orlaton *megb****esz****éltek* alapján az alkalmazásnak a Neptuntól külön kell futnia, azonban a megbízhatóság (egyediség, relevancia) miatt célszerű lenne mégis a Neptunhoz kötni az accountok létrehozását. **Ennek több módja is lehetne.**

Az egyik, hogy a regisztrációt kulcsh*oz* kötjük. Ezt úgy képzelem el, hogy a neptun felületén lenne egy opció (*esetleg* mező, szóval külön kérés nélkül generált kulcs), ami csak bejelentkezés után elérhető, amivel minden felhasználó egy egyedi kulcsot tudna generálni. Ezt a kulcsot kellene a regisztrációkor megadni az oldalon, amivel biztosítani tudnánk, hogy személy és account között 1:1 kapcsolat jöjjön létre. A kulcs generálása lehet véletlenszerű vagy a hallgató adataiból is képezhető (persze nem teljesen). A kulcsot el kell tárolni, mivel az alkalmazásunk a regisztráció beküldésével a neptunnal összehasonlítaná azt.

A másik, hogy a regisztrációt közvetlenül a neptunból kellene indítani, szóval az oldalon nem lenne erre lehetőség. A neptunhoz csatolt email címre kapnánk egy limitált ideig működő linket, ami átirányítana a regisztrációs felületre. Ezzel az a probléma, hogy valahogy tárolnia kell a neptunnak, hogy az adott linket felhasználták-e már (ha nem akarunk további személyes adatokat kérni a felhasználótól az egyediség biztosítására). Ha igen, akkor nem lehetne új mailt kiküldeni.

Személy szerint én az első lehetőséget preferálnám, ha sikerül kellően egyedi kulcsot előállítani. A másodikban több buktatót látok, hiszen a mail rossz kezekbe is keveredhet, aki ha véletlenül vissza akarna élni a lehetőséggel, akkor könnyen meg is teheti. Valamint rögtön bevonnánk egy harmadik szereplőt (email) a játékba, amivel rögtön tovább nő a kockázat.

A másik felvetődött kérdés ezzel a megvalósítással kapcsolatban, hogy az oldalunk hogyan férne hozzá a neptunban tárolt adatokhoz. Az alkalmazásnak a hiteles működéshez szüksége van a hallgató aktuális és múltbéli kurzusaira, illetve az azt oktatók nevére is.

Erre a problémára azt javasolnám, hogy minden félévben –amikor már lezárult a tárgyfelvétel – az első bejelentkezéskor, az alkalmazás indítson egy lekérdezést a neptun szerver felé, amivel össze tudnánk szinkronizálni a szükséges információkat. A múltbéli kurzusokat nyilván elég lenne az account létrehozásakor lekérdezni.

A felmerült ötletekhez mindenképp bele kell nyúlni valamilyen szinten a neptunba, plusz funkciókat kell hozzáadni. (Kulcs generálás, kulcs összehasonlítás, lekérdezés kiszolgálása) Ha biztonságos és hiteles alkalmazást szeretnénk, akkor ennek ez az ára. Ha a neptun szerverek az egyes intézményekben egymástól teljesen külön verzión futnak, akkor ez probléma lehet, de nem feltétlenül megoldhatatlan.