Specifikáció

# Követelmények

## Funkcionális követelmények (use-case-ek)

### OAuth2 alapú autentikáció

|  |  |  |
| --- | --- | --- |
| Azonosító | Összefoglaló | Leírás |
| F1.01 | Bejelentkezés | A felhasználó egyedi felhasználónévvel és jelszóval azonosítja magát. |
| F1.02a | Regisztráció | A felhasználó a következő adatok megadásával regisztrál: név, felhasználónév, email, jelszó. |
| F1.02b | Regisztráció adattárolás | A felhasználó által megadott adatok az adatbázisban lesznek eltárolva, a jelszó nem tiszta szövegként. |
| F1.02c | Regisztrációs szerepkörök | A felhasználó jogosultságai regisztráció után minden esetben azonosak, melyet később egy admin bővíthet. |
| F1.03a | Szerepkörök | A felhasználók különböző szerepkörökkel rendelkeznek, melyekhez eltérő jogosultságok kapcsolódnak. A szerepkörök a következők: tanuló, kutató, admin, tanár, szülő. |
| F1.03b | Szerepkör megszemélyesítése | A tanári és szülői szerepkörrel rendelkező felhasználók megszemélyesíthetnek egy tanuló felhasználót, és annak nevében járhatnak el. |
| F1.04 | Külső alkalmazások számára autentikáció | Az autentikációs szerver bizonyos előre definiált külső alkalmazásokkal is kapcsolatban áll, azok kérésére elvégzi a felhasználók azonosítását. És rendelkezésre bocsátja a felhasználó adatait. |
| F1.05 |  |  |

### A játékosok képességeinek tárolása

|  |  |  |
| --- | --- | --- |
| Azonosító | Összefoglaló | Leírás |
| F2.01 | Játékos kognitív profiljának tárolása | Minden játékoshoz az összes CHC képesség és ahhoz tartozó legfrissebb érték lesz eltárolva. |
| F2.02 | Egyéb képesség tárolása | A játékosokhoz más tetszőleges értéket felvevő (pl. bináris) képesség is tárolható. |
| F2.03 | Képességek visszakövethetősége | Az alkalmazás lehetőséget biztosít a játékos tetszőleges időpontbeli képességének lekérdezésére. |
| F2.04 |  |  |

### Játékok kezelése

|  |  |  |
| --- | --- | --- |
| Azonosító | Összefoglaló | Leírás |
| F4.01 | Játékok adatainak tárolása | Az alkalmazás külső játékokhoz tartozó információkat tárol. Az ehhez tartozó adatok: azonosító, érintett képességek, nehézség, elérési útvonal (url) |
| F4.02 | Játékok adatainak frissítése | Az játékosok eredményei alapján a játékok nehézsége folyamatosan frissül. A játékok egymásra is hatnak? |
| F4.03 | Játékok elérése | Az applikációból egy hivatkozásra klikkelve a játék egy új oldalon elindul. |
| F4.04 | Játékok számára biztosított adatok | A játékost közvetlenül azonosító adat nem hozzáférhető a játék számára (név, email, felhasználónév)  A játék lekérdezheti a játékos képességeit, de csak az aktuális játék az aktuális játékos képességeit. (Ehhez az alkalmazás hozzáférési tokent generál a játék számára, mellyel az azonosítja magát.) |
| F4.05 | Játékmenetek elkülönítése | A játékokat játékmenet azonosító különbözteti meg, melyet új játék esetén a játék generál. |
| F4.06 | Játék által küldött adatok | A játék minden játékmenethez adatokat küldhet az alkalmazás számára. Az adatküldéshez szintén azonosítja magát. A küldött adat tartalmazza a játékmenet azonosítót és a játék eredményét (bármilyen mért érték). |
| F4.07 | Játékmenetek és játékosok összekapcsolása | Minden felhasználóhoz az összes általa játszott játékmenet adatai el lesznek tárolva. A játékmenetekről az alábbi adatok: játék verzió, időpont, eredmény. |
| F4.08 | Játék keresése | Jogosult felhasználók különböző szempontok alapján kereshetnek a rendelkezésre álló játékok között. |
| F4.09 | Adatmentés játékindításkor | Egy játék elindításakor a játékos aktuális kognitív adatai el lesznek mentve időbélyeggel ellátott rekordként. Legfeljebb napi egyszer készül ilyen mentés. |
| F4.10 |  |  |

### Játékok ajánlása

|  |  |  |
| --- | --- | --- |
| Azonosító | Összefoglaló | Leírás |
| F5.01 | Játék elérésének lehetőségei | A játékos többféleképp érhet el egy játékot: egy arra jogosult felhasználó beállít számára egy konkrét játékot vagy a rendszer ajánl számára egy játékot |
| F5.02 | Játék kijelölése egy másik felhasználónak | Az arra jogosultak (pl. tanár, kutató) kijelölhetnek egy vagy több játékot más felhasználók számára. |
| F5.03 | Játék ajánlása képesség alapján | Az alkalmazás a játékos képességének megfelelő nehézségű játékot ajánl. |
| F5.04 | Profil és tréning elkülönítése  Mitől lesz különböző? | Amennyiben a játékosnak hiányos a profilja, azaz nem minden képességéhez tartozik érték, a rendszer profil teszteket ajánl, melyek a képességeket mérik.  Teljes profil esetén tréning teszteket ajánl, melyek növekvő nehézségűek. |
| F5.05 |  |  |
| F5.06 |  |  |
| F5.07 |  |  |

### Funkciócsoport6

|  |  |  |
| --- | --- | --- |
| Azonosító | Összefoglaló | Leírás |
| F6.01 |  |  |
| F6.02 |  |  |
| F6.03 |  |  |
| F6.04 |  |  |
| F6.05 |  |  |
| F6.06 |  |  |
| F6.07 |  |  |

## Műszaki követelmények

# Részletes terv

## Vizuális tervek (elérhető oldalak)

## Adatmodell

## Interfészek (REST API)

## OAuth2 – ezt szívesen megcsinálom (Anna)

Az elkészült szoftver OAuth2 autentikációt és autorizációt biztosít, mely lehetővé teszi, külső alkalmazások számára a felhasználók azonosítását, és jogosultságaik elérését. Az OAuth 2.0 specifikációban ismertetett szerepeknek megfelelően dedikált autorizációs szerver (a továbbiakban Authorization Server) lesz megvalósítva, illetve egy erőforrás szerver (a továbbiakban Resource Server) és egy kliens alkalmazás. Az első kettő Spring Security 6 keretrendszer felhasználásával készül el, míg a kliens (…?)

### Authorization Server

A komponens egy külön backendként funkcionál, melynek feladata a felhasználók azonosítása és jogosultságaik kezelése, valamint a kliens alkalmazások számára autorizáció biztosítása. Ez az alkalmazás a terhelés elosztása miatt különválik a projekt során elkészített többi komponenstől, önállóan futtatható.

Az alkalmazáshoz külön adatbázis kapcsolódik, melyben a felhasználók azonosításhoz szükséges adatai lesznek eltárolva (név, id, secret, jogosultságok). Emellett a regisztrált kliensalkalmazások azonosítására alkalmas adatai is innen elérhetők. A jelszóként funkcionáló titkos adatok az adatbázisba hashelt formában íródnak. Az adatbázis relációs sémára épül.

#### Regisztráció

A szerver regisztrációs felületet biztosít új felhasználók számára. A felhasználói adatok megadását követően új entitás kerül az adatbázisba. A felhasználó jogosultságait később az erre jogosult felhasználók állíthatják be.

#### Bejelentkezés

A felhasználót egy általa használt egy kliensalkalmazás átirányítja a bejelentkezési felületre, ahol a felhasználó az egyedi felhasználónevét és jelszavát megadva azonosítja magát. Sikeres bejelentkezést követően a szerver a kliens által megjelölt url-re irányít és elküldi a hozzáférési tokent.

A token egy jwt token, melybe a felhasználó neve, azonosítója és jogosultságai vannak kódolva. A kliens ezt a tokent használhatja a Resource Serverhez intézett kéréseknél azonosításra.

#### Kliensek azonosítása

Az Authorization Servert csak előre meghatározott kliensalkalmazások érhetik el, ezeket előre regisztrálni kell. A regisztrált kliensek azonosítót és titkos adatot kapnak, mellyel azonosíthatják magukat. Emellett a klienshez tartozó átirányítási url-ek is előre definiáltak.

### Resource Server

Ez egy REST API szerver, mely bizonyos privát endpoint-jait védi. Ezekhez csak azonosított és megfelelő jogosultsággal rendelkező felhasználók férhetnek hozzá.

Az alkalmazás a kérések fejlécében jwt-tokent vár, melyet az Authentication Server segítségével validál. A Resource Server nem kezeli a felhasználók jogosultságait, csupán felhasználja az Authentication Server-től kapott információt. Érvényes token esetén kiszolgálja a kérést.

### Client

A kliens alkalmazás az Authentication Server-t felhasználva igényel hozzáférési tokent a felhasználó számára. Ehhez egy kliens ID-val, titkos adattal és átirányítási címmel (ide várja a válasz tokent) felparaméterezett kérést intéz az Authentication Server felé. A válaszban kapott jwt-tokent felhasználja a Resource Server felé intézett kéréseknél.

### Szerepkörök, jogosultságok

Minden felhasználó egy vagy több szerepkörrel rendelkezik, melyek különböző jogosultságokat biztosítanak. Az Authentication Server kizárólag a felhasználók szerepkörét tárolja, és azonosítás után ezt továbbítja a Resource Server (illetve más külső alkalmazás) számára. A szerepkörökhöz tartozó jogosultságokat a Resource Server oldja fel, mivel ez minden alkalmazásnál eltérő lehet, és idővel változhat.

Bizonyos felhasználói szerepkörök (pl. tanár, szülő) más felhasználókat személyesíthetnek meg (pl. tanuló). A megszemélyesítés az Authentication Server szintjén történik. Miután a felhasználó azonosította magát, a sikeres belépés után az alkalmazás felkínálja (amennyiben lehetséges), hogy mely felhasználó nevében szeretne bejelentkezni. Emiatt a kiváltságos felhasználókhoz további felhasználók vannak rendelve az adatbázisban, akiknek a szerepében felléphet. Megszemélyesítés esetén az Authentication Server olyan hozzáférési tokent továbbít a Resource Server számára, melyben a megszemélyesített felhasználó adatai, illetve egy megszemélyesítést jelző flag szerepel.

Az adatbázisban tárolt szerepkör lehetséges értékei a következők: tanuló, kutató, admin, tanár, szülő.

## Technológiák, keretrendszerek