Tervezés

A tervezési fázisban el kellett készítenünk a rendszer architektúrális terveit, különböző ábrákat, szekvencia diagramokat és tesztelési tervét.

Követelmények

Funkcionális követelmények

- felhasználóknak kell tudni regisztrálni és belépni
- felhasználóknak kell tudni CAFF fájlt feltölteni, letölteni, keresni
- felhasználóknak kell tudni CAFF fájlhoz megjegyzést hozzáfűzni
- a rendszerben kell lennie adminisztrátor felhasználónak, aki tud adatokat módosítani, törölni

Use-case-ek

A felhasználóknak két csoportja van: a sima felhasználó, illetve az adminisztrátor. Az adminisztrátor mindent tud, amit egy alap felhasználó, de rendelkezik ezen felül más jogosultságokkal is.

A felhasználók a következő interakciókat tudják folytatni a rendszerrel:

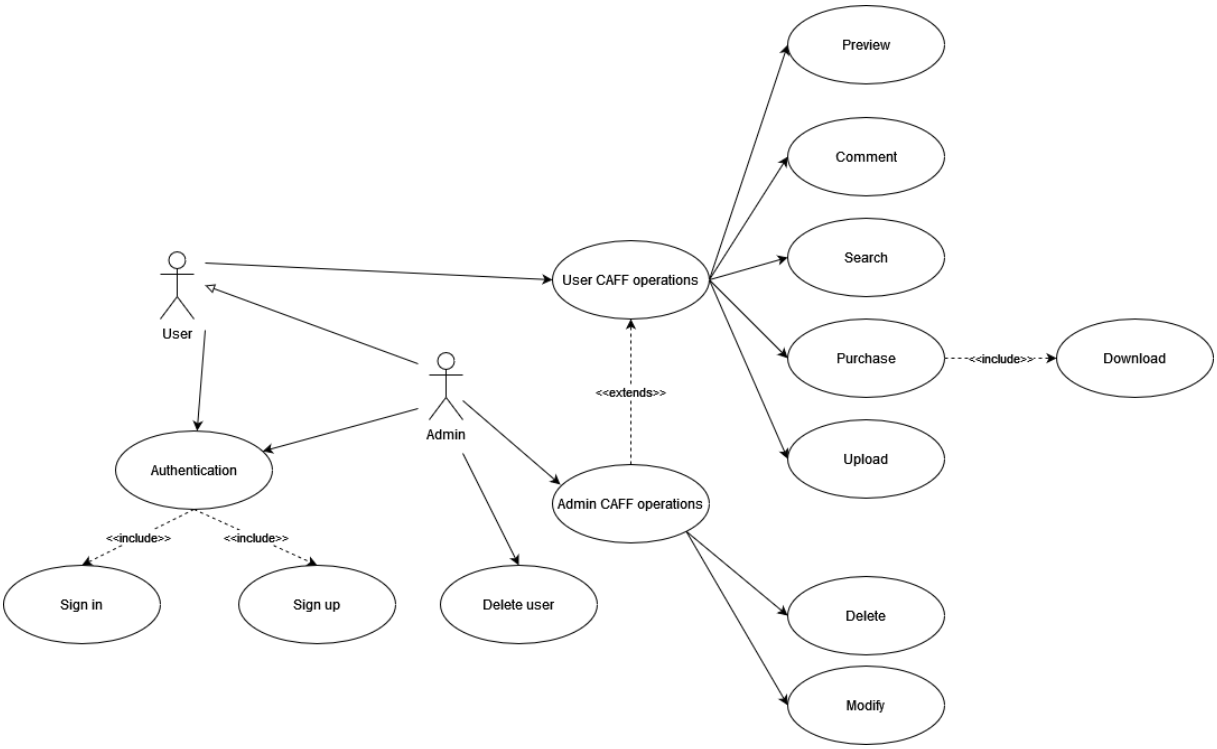
- Regisztrálhatnak a rendszerbe, amivel jogosultságot kapnak a rendszer használatához.
- Bejelentkezni is tudnak, ha korábban regisztráltak a rendszerbe, ezzel bizonyítják kilétüket és kapnak hozzáférést a szolgáltatáshoz.
- Előnézetben meg tudják tekinteni a CAFF file-okat az oldalon.
- Tudnak kommentelni egy-egy file-hoz az oldalon.
- Az oldalon tudnak keresést indítani, amivel szűrhetik a megjelenített file-okat.
- Tudnak CAFF file-t feltölteni az oldalra.
- Fizetés útján tudnak letölteni is az oldalról.

Az adminisztrátornak ezen felül az alábbiakhoz van jogosultsága:

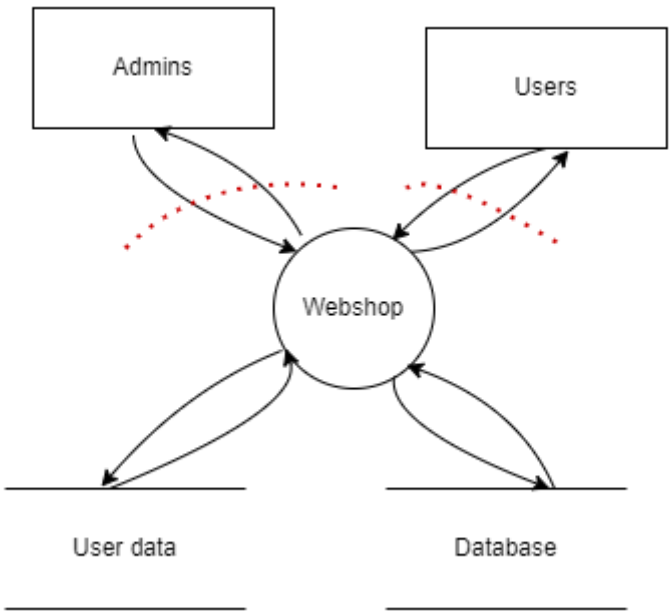
- Tud felhasználót törölni.
- Tud CAFF file-okat törölni, illetve módosítani.

Use-case diagram

Az alábbi képen a felhasználók, illetve adminisztrátorok felhasználói szcenárióit ábrázoltuk.



Rendszer és környezete



A fenti ábrán látható a rendszer és környezetének határai. A felhasználók, adminisztrátorok lépnek interakcióba a rendszerrel. A tőlük érkező inputok, viselkedések a rendszer határain túl vannak, hiszen ezt nem lehet szabályozni, a velük történő együttműködés kérdéseket vet fel. Ennek megfelelően ez egy kritikus pont, amit szaggatott piros vonallal látszik az ábrán. Ehhez hasonlóan a rendszernek szüksége van a felhasználók, illetve a file-ok adataira is, így ezekhez is biztosítani kell a kapcsolatot a rendszer felé. A felhasználókat pedig csak a számukra releváns adattal kell összekapcsolni.

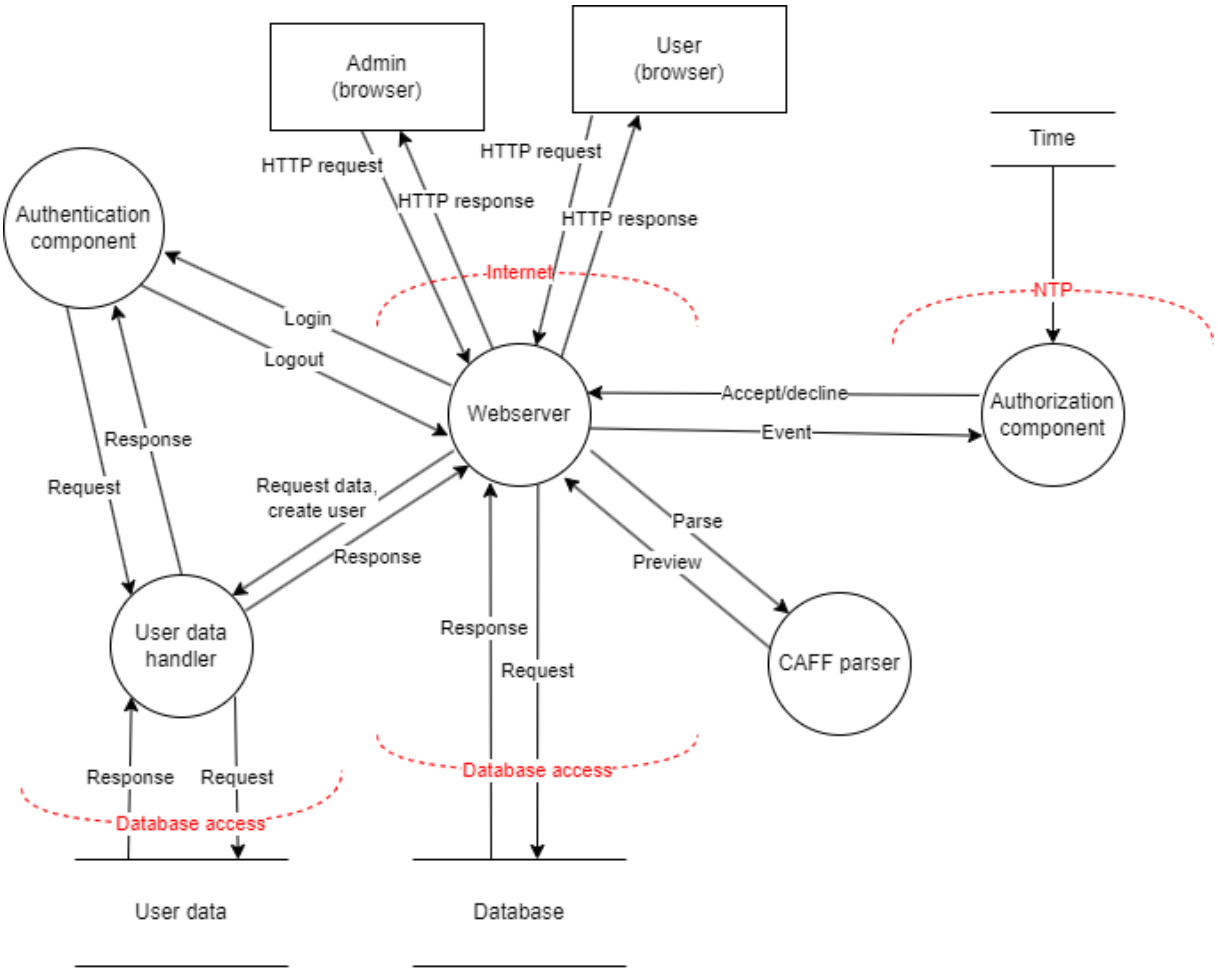
Biztonsági követelmények

A CIA és AAA elvek alapján:

- Bizalmasság
    - A felhasználók adatait csak ők maguk, illetve az adminisztrátorok láthatják. Az adminisztrátorok számára is szükséges ez, hiszen nekik lehetőségük kell legyen a felhasználó törlésére, ehhez pedig el kell tudniuk érni a felhasználó adatait, hogy lássák azt.
    - A felhasználók csak a saját adataikat láthatják, hiszen mások adatainak megismerése nem szükséges a rendszer használatához.
    - A webshopon keresztül a felhasználók és adminisztrátorok egyaránt hozzáférnek a CAFF file-ok előnézetéhez, tehát ehhez a hozzáférést biztosítani kell számukra. Tudnak keresni és előnézetet megtekinteni.
- Integritás
    - A felhasználóknak nincs semmilyen felhasználókkal kapcsolatos módosítási képessége. A felhasználók eltávolítására csak az adminisztrátorok képesek.
    - A CAFF file-ok módosítására és törlésére az adminisztrátorok képesek.
    - CAFF file-okat feltölteni, letölteni, keresni is tud a felhasználó.
- Elérhetőség
    - A rendszer, mivel webshopról van szó, 0-24 elérhetőnek kell lennie a felhasználók és adminisztrátorok számára is.
- Autentikáció
    - Csak regisztrált felhasználók férhetnek hozzá a rendszerhez és csak bejelentkezés után. Adminisztrátoroknak szintén szükséges a bejelentkezés alapján történő azonosítás a rendszer használata előtt.
- Autorizáció
    - Letöltés csak a szükséges pénzügyi tranzakció elvégzése után lehetséges a felhasználóknak.
    - Bejelentkezés után az adott felhasználó, adminisztrátor a saját szerepkörének megfelelő cselekvéseket hajthat végre.
- Auditálás -

Adatfolyam ábra

Az alábbi ábrán a fenti, csak nagyvonalakban felvázolt rendszer és környezetének kifejtése látható, vagyis az általunk fejlesztett rendszer komponenseinek, részeinek kifejtése is. A külső szereplőkkel való interakció is részletesen látszik és az azokkal kapcsolatos esetleges felmerülő biztonsági kockázatokat is jelöltük piros szagatott vonallal.



Threat assessment

Alább a STRIDE keretrendszer szerint szedtük össze a fenyegetett területeket, illetve ezen területekkel való visszaélési esetekre hoztunk példákat.

- Megszemélyesítés - hozzáférésvédelem, belső folyamatok (valamelyik komponenst megszemélyesítve megváltoztathatják annak viselkedését)
    - felhasználó módosítani akarja a CAFF file-okat
    - felhasználó törölni akar más felhasználót, pedig ezt csak adminisztrátor teheti meg
- Hamisítás - belső folyamatok információáramlása, adattár
    - adatbázisok tartalmának módosítása, jogtalan módosítások: felhasználók szerepkörének módosítása, CAFF file-ok korrupciója
- Tevékenységek letagadása -
- Információ szivárgás - belső folyamatok, tárolt adatok, adatáramlás
    - felhasználók adatainak megszerzése, jogtalan hozzáférés CAFF file-okhoz, belső információkhoz
- Szolgáltatás megtagadás
    - a rendszer és a szolgáltatás működésének szabotálása, amivel működésképtelenné, ezáltal értéktelenné teszik a rendszert
- Jogosultsági szint emelése - jogtalanul olyan funkciókhoz való hozzáférés, ami nem lehetséges szerepek szerint:

- felhasználó fizetés nélkül szeretné letölteni a file-okat
- felhasználó szeretne más felhasználót törölni

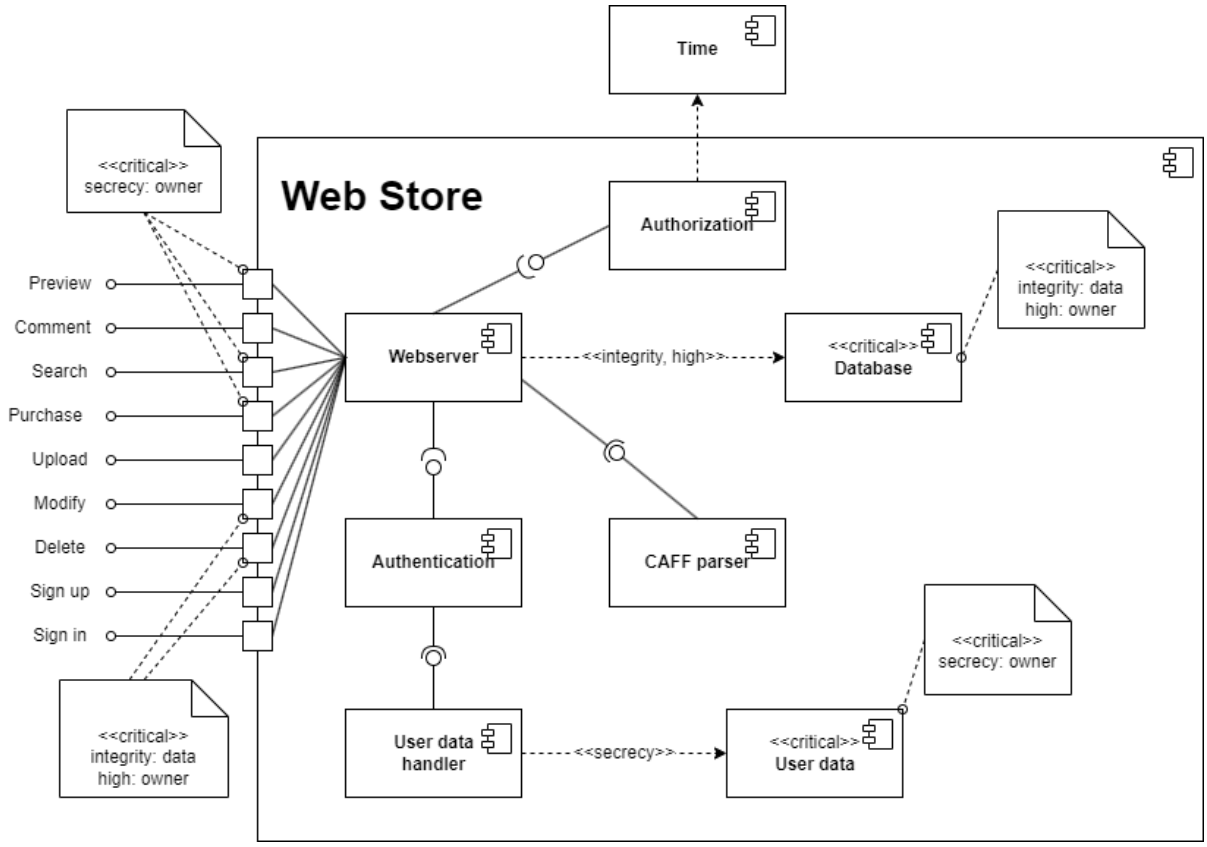
Biztonsági célok

- Szerepkör alapú hozzáférés védelem
- Felhasználói fiókok, hozzájuk tartozó adatok megfelelő kezelése
- Biztonságos adattárolás
- Hálózaton való biztonságos kommunikáció

Architektúra tervek

Az alábbi alfejezetben a rendszer felépítésével, viselkedésével kapcsolatos részleteket fejtjük ki. A komponensdiagramon szerepelnek a rendszer részei, illetve a rendszer által nyújtott kapcsolódási pontok, interfészek a felhasználók, adminisztrátorok felé. Későbbiekben az interfészek leírását, a rendszer és felhasználók közötti interakciók lépésenkénti lebontását láthatjuk.

A rendszer architektúrája



A rendszer kilenc interfészt nyújt a felhasználók számára, ezek közül a törlés és módosítás csak az adminisztrátor felhasználóknak érhető el.

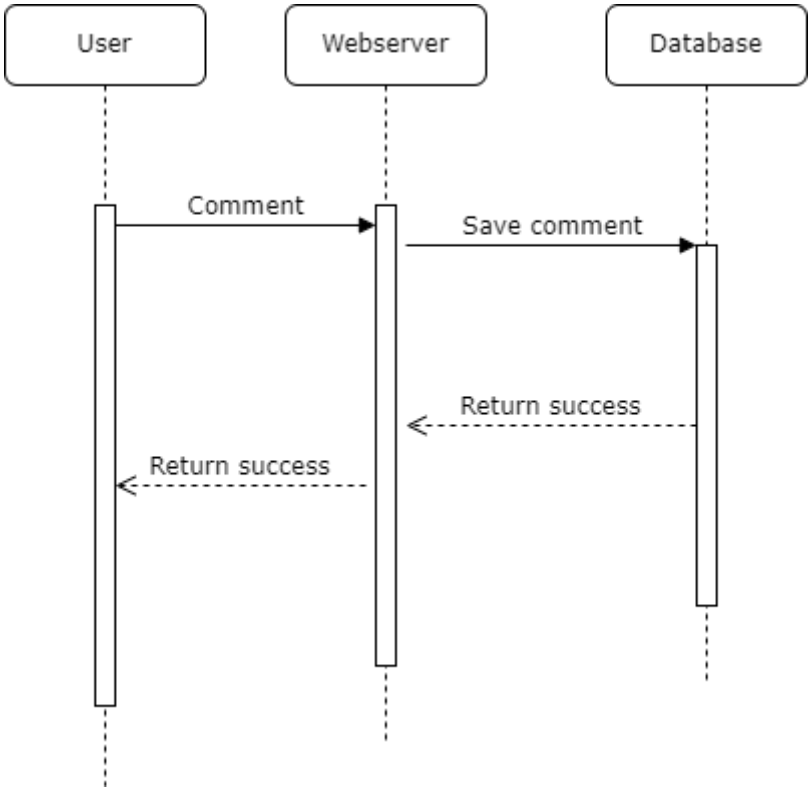
- Preview: Ezen az interfészen keresztül tudják a felhasználók és adminisztrátorok megtekinteni a file-okat a webshopon keresztül.
- Comment: Ezen az interfészen keresztül tudnak a felhasználók és adminisztrátorok kommentelni az adott file-hoz.

- Search: Ezen az interfészen keresztül tudnak a felhasználók és adminisztrátorok keresést indítani a file-ok között.
- Purchase: Ezen az interfészen keresztül tudnak a felhasználók és adminisztrátorok vásárlást indítani a file-ok között.
- Upload: Ezen az interfészen keresztül tudnak a felhasználók, illetve adminisztrátorok file-okat feltölteni
- Modify: Az adminisztrátorok ezen az interfészen keresztül tudják módosítani a felhasználók adatait, illetve a CAFF file-ok adatait.
- Delete: Az adminisztrátorok ezen az interfészen keresztül tudnak file-okat és felhasználókat törölni a rendszerből.
- Sign up: Ezen az interfészen keresztül tudnak regisztrálni a felhasználók és adminisztrátorok.
- Sign in: Ezen az interfészen keresztül tudnak bejelentkezni a felhasználók és adminisztrátorok.

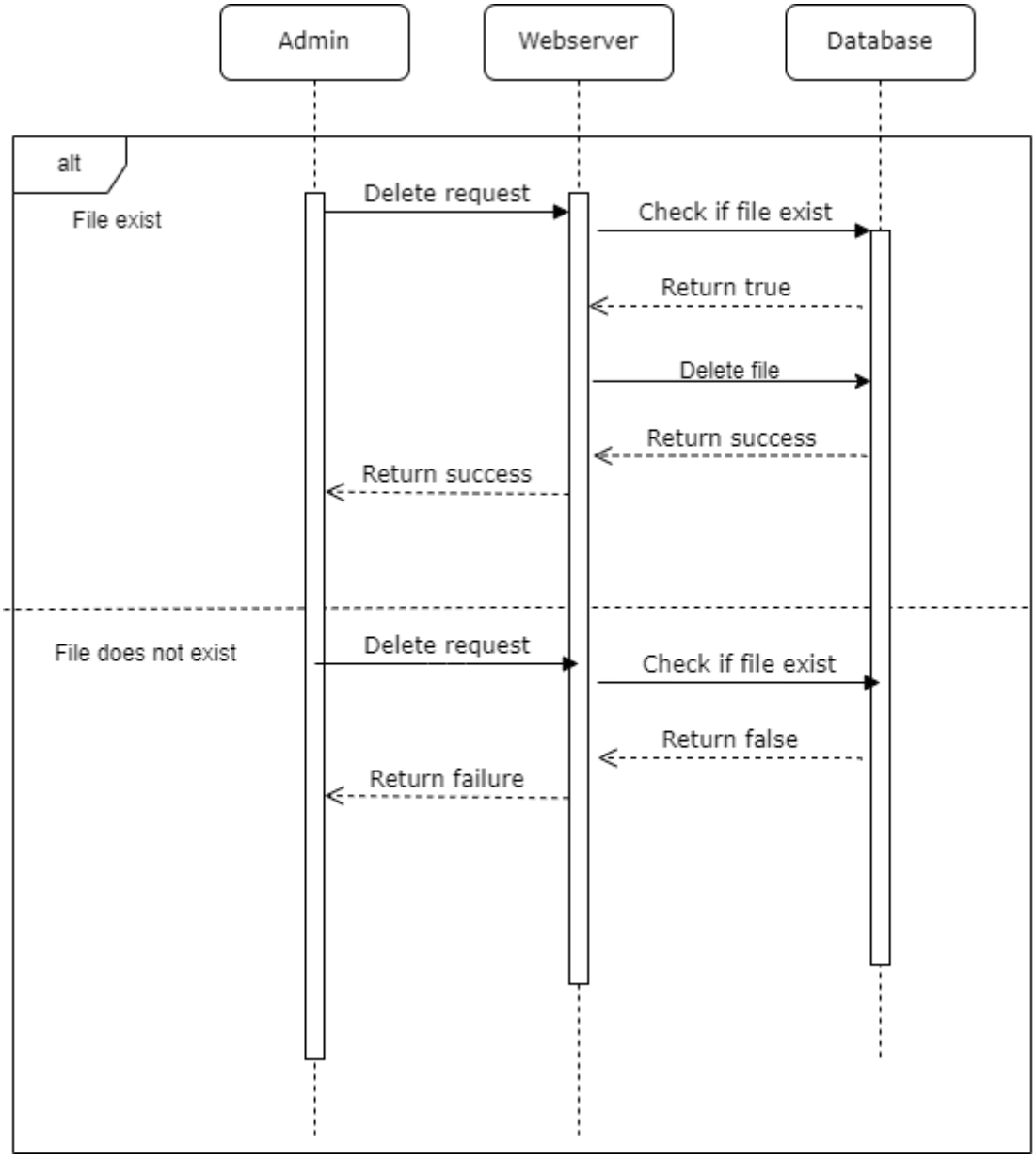
A rendszer viselkedése

Az alábbi szekvenciadiagramok minden egyes use case-hez levezetik, hogy milyen lehetséges lefutása lehet egy-egy interakciónak.

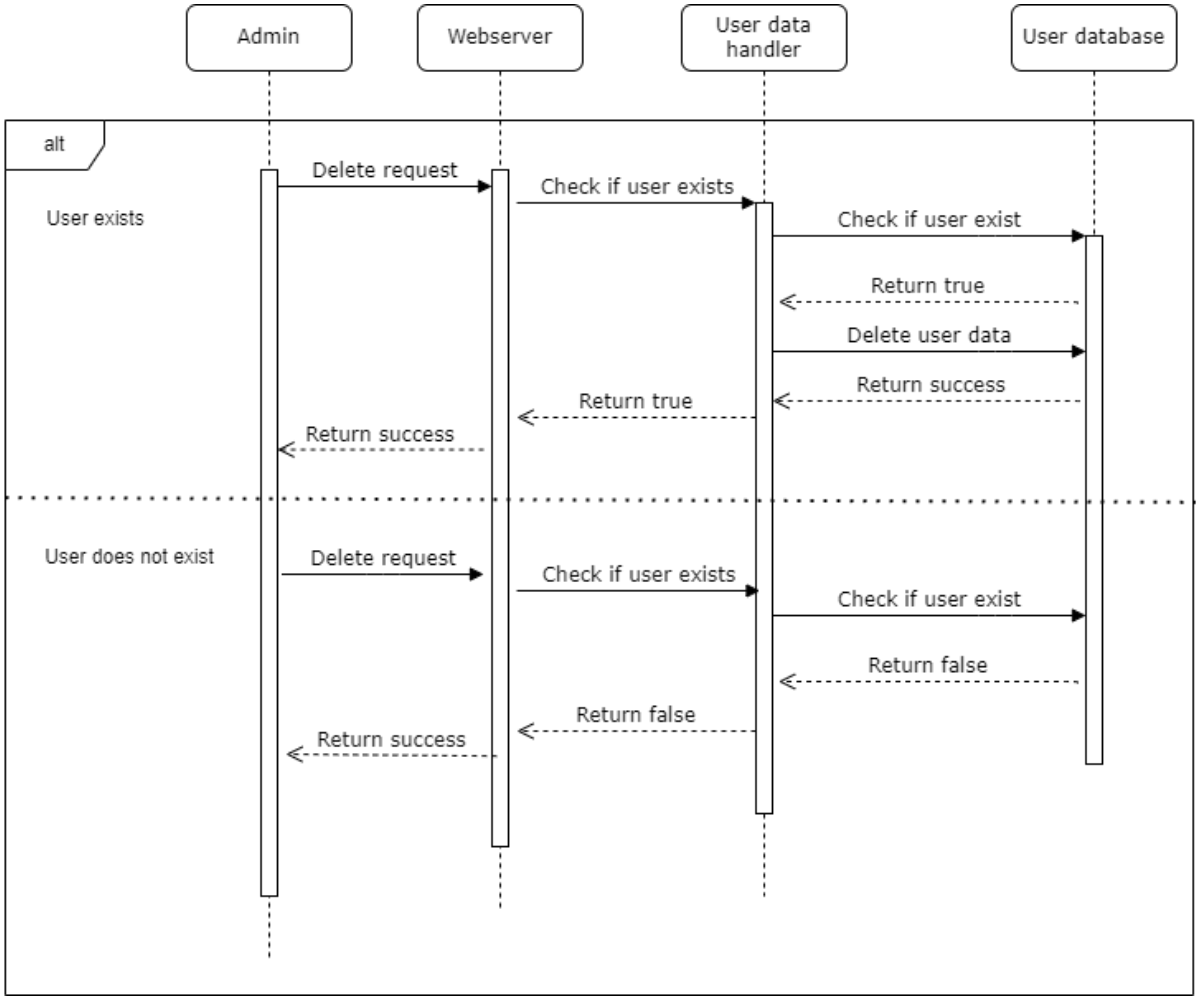
Komment



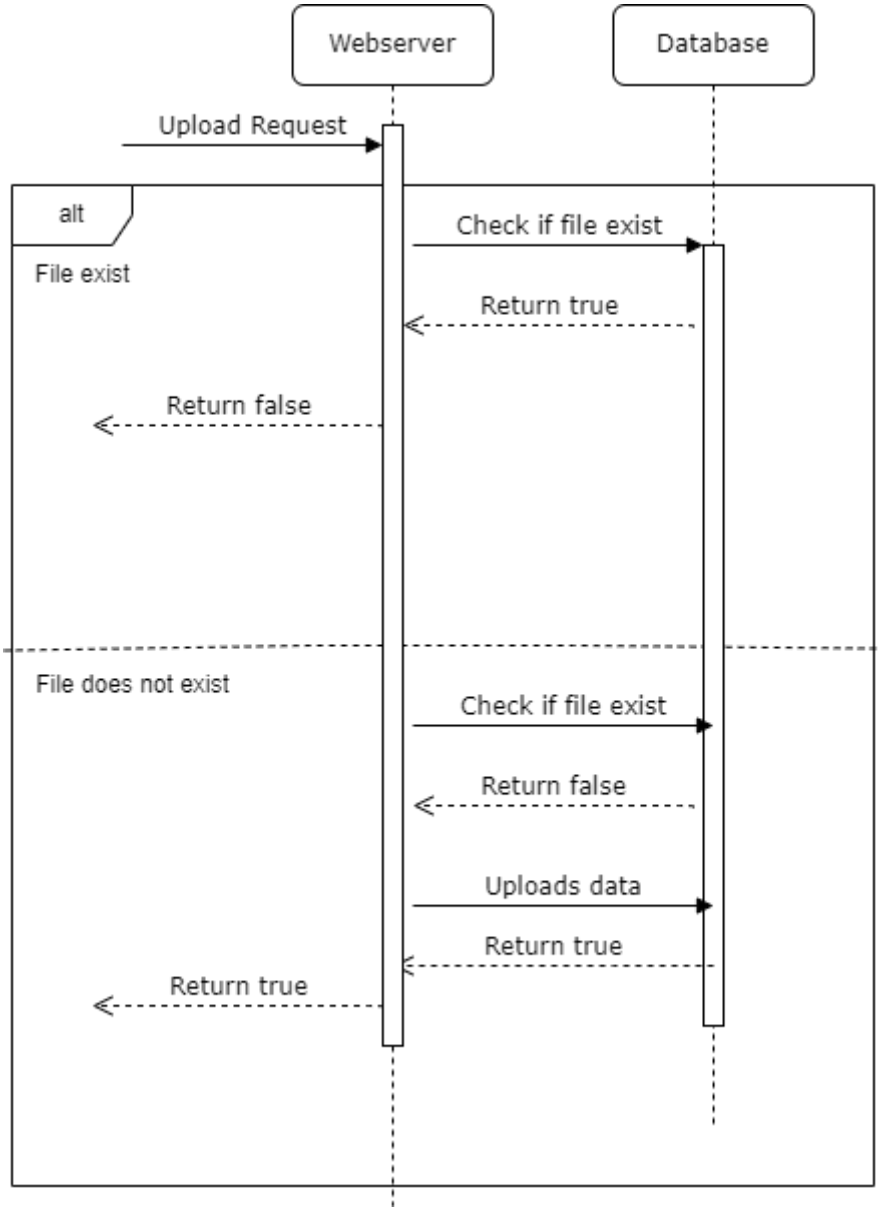
Fájl törlése



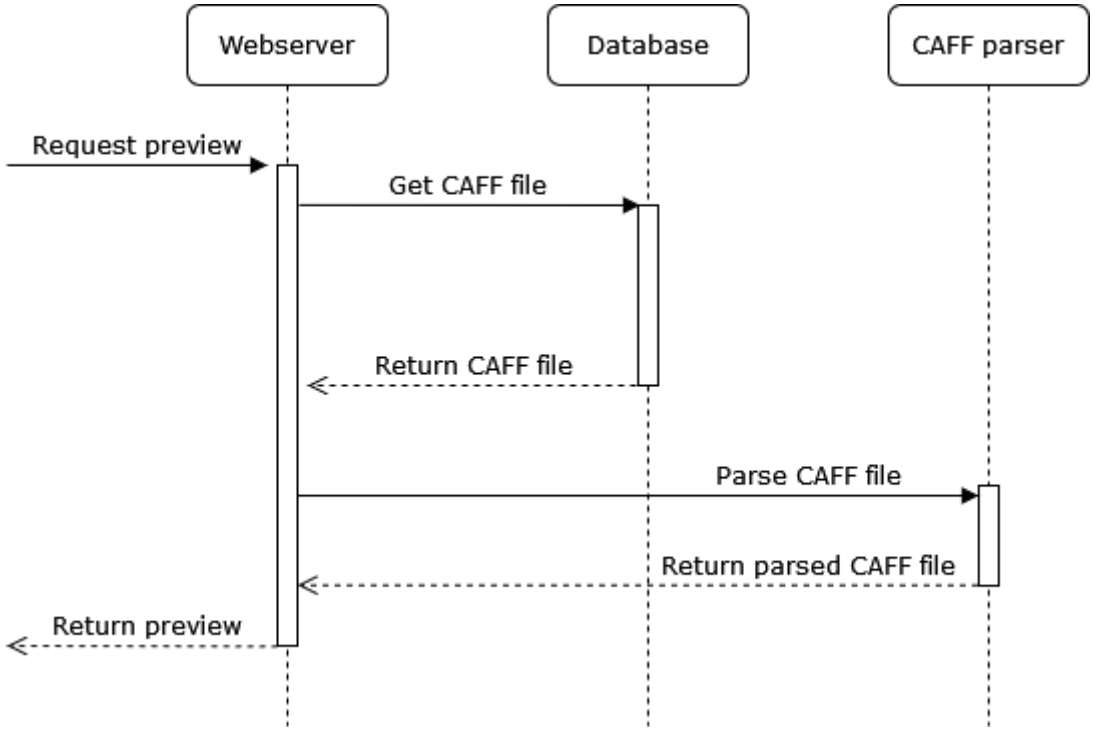
Felhasználó törlése



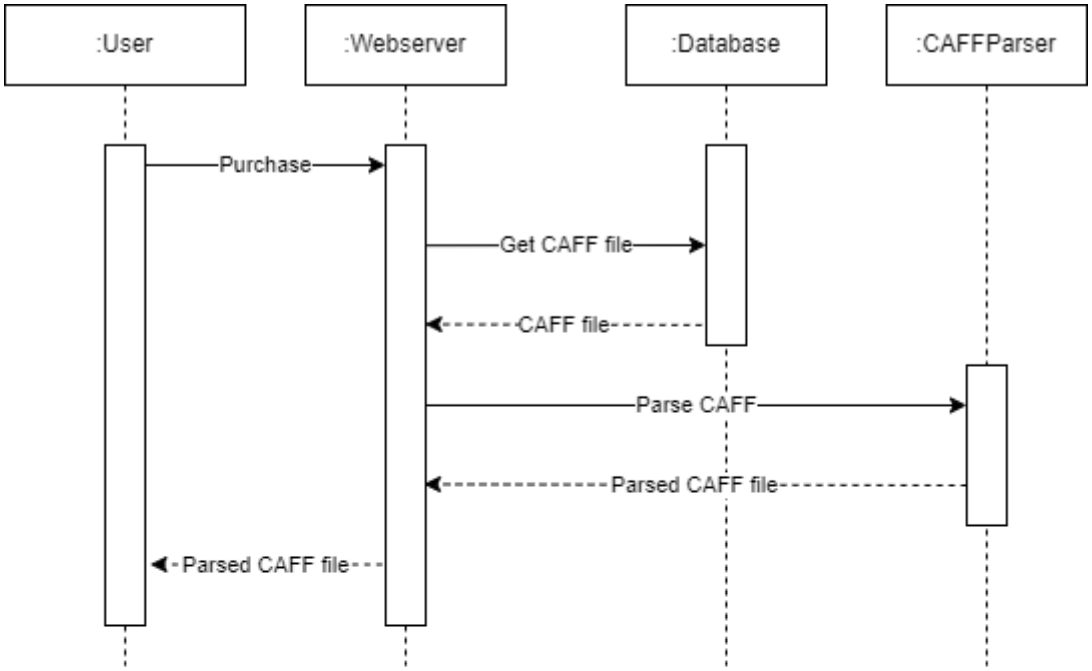
CAFF módosítása

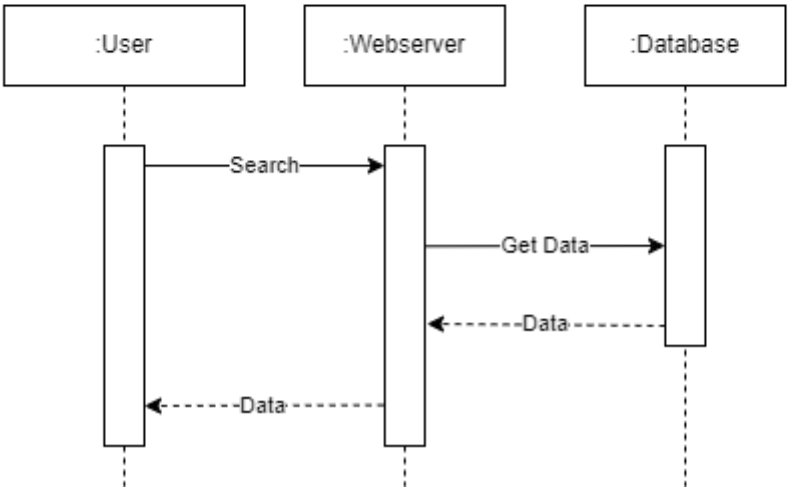


Előnézet

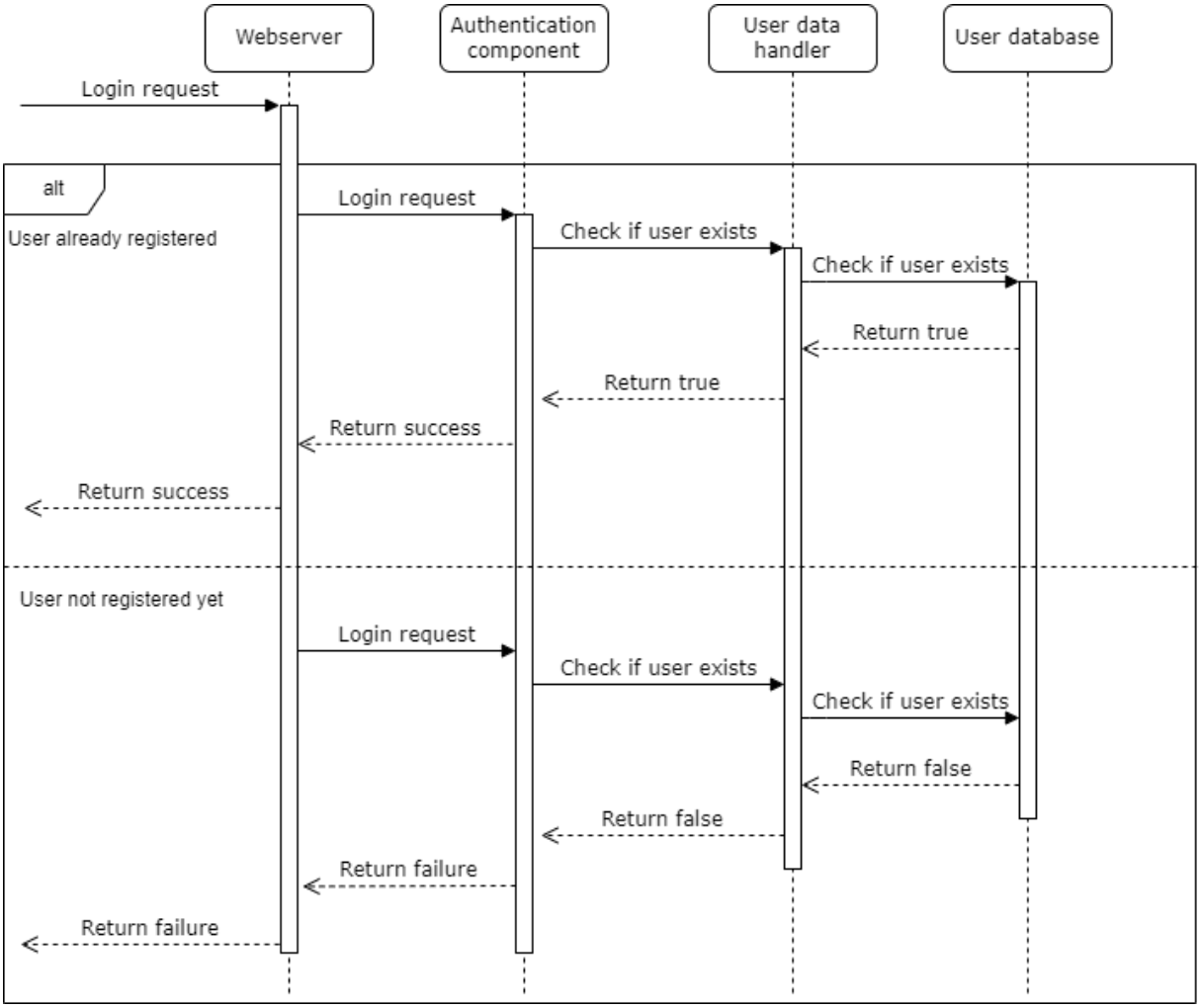

Webserver
Database
CAFF parser
Request preview
Get CAFF file
Return CAFF file
Parse CAFF file
Return parsed CAFF file
Return preview

Vásárlás és keresés





Bejelentkezés



Regisztrálás