Titkosított chat alkalmazás

Projektfeladat specifikáció

Informatikai Biztonsági és Adatvédelmi Tanácsadó Kft.

1 Tartalomjegyzék

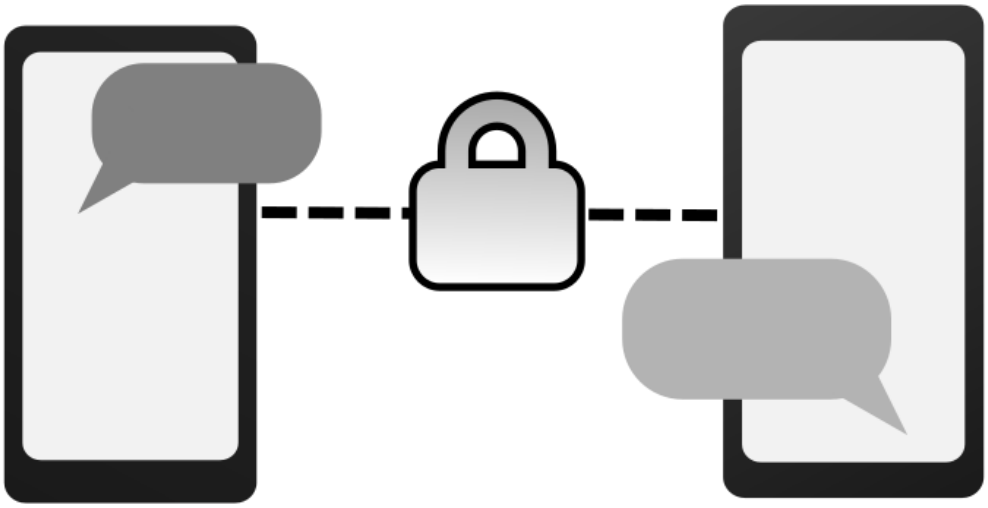
2 Bevezetés

2.1 A feladat címe

Titkosított chat alkalmazás

2.2 A feladat rövid ismertetése

A projekt célja egy E2EE (végponttól végpontig titkosított) chat alkalmazás megvalósítása.



3 Elvárások a feladattal kapcsolatban

3.1 Operációs rendszer, környezet

- Android vagy Chrome/Firefox böngésző

3.2 Felhasználandó programozási nyelv

- Nincs megkötés

3.3 Megoldás formátuma

- Forráskód állományok
- Teljes projekt környezet
- Forráskód dokumentáció
- Technikai dokumentáció (odt/docx és pdf formátumban)
- Felhasználó dokumentáció
- Erőforrás terv és munkaidő nyilvántartás

3.4 Szoftverfejlesztés

A feladat egy titkosított chat alkalmazás készítése, amelyben lehetőség van chatszoba létrehozására és meghívó küldésére.

A fejlesztés közben be kell tartani a meghatározott kódolási konvenciókat, amelyek az aktuális gyakorlatvezető szab meg.

Az elkészült megoldásnak maradéktalanul meg kell valósítania az 4-es fejezetben megfogalmazott követelményeket. Amelyik követelmény nincs pontosan definiálva, a megvalósítás során a fejlesztő szabad kezet kap. Fontos viszont, hogy a választott megoldás megfelelő színvonalú legyen mind felhasználói, mind fejlesztői szempontból.

3.5 Modulok

A projekt keretében történő megvalósítás egy lehetséges felbontási lehetősége az alábbi:

- Felhasználóbarát frontend (GUI) tervezése, kivitelezése
- Saját backend megvalósítása, vagy a célnak megfelelő platform (pl. firebase) használata, kezelése.
- Projektvezetéssel kapcsolatos dokumentáció, nyilvántartások vezetése, feladatok összehangolása, felhasználói dokumentáció elkészítése, tesztelés.

Lehetőség szerint a fejlesztői dokumentációkat minden esetben a ténylegesen fejlesztést végző projekttagok készítsék el. A felhasználói dokumentáció külön egységet képezhet, érdemes a teszteléssel összekapcsolni a megfelelő minőség biztosítása érdekében

4 Specifikáció

4.1 Megjelenés

- Főoldal
  Az alkalmazás/weboldal megnyitása után megjelenő felület (ha a felhasználó nincs bejelentkezve).
  A felületen található:
  - felhasználónév
  - jelszó mező
  - bejelentkezés gomb
  - regisztráció gomb

- Regisztráció
  A főoldalon található regisztráció gomb megnyomása után megjelenő felület, amely a következő beviteli mezőket tartalmazza
  - felhasználónév
  - jelszó
  - jelszó újra

- Chat lista
  Bejelentkezett felhasználóknak megjelenő felület, ahol listás nézetben megjelenik a felhasználó számára elérhető összes chatszoba.

- Chat felület
  A chat listán egy chat szobára kattintva megjelenik annak felülete. A felhasználók ezen a felületen tudnak a chat szoba tagjainak üzenetet küldeni, illetve itt láthatják a többi felhasználó által küldött üzeneteket. Az üzenetek felett fel kell tüntetni az üzenetet küldő felhasználók becenevét (ha nincs beállítva, a felhasználónevét).
  A felületen a szobát létrehozó felhasználónak legyen lehetősége meghívó generálására/másolására a szobához.

- Profil felület
  Bejelentkezés után elérhető felület. A felhasználó ezen a felületen tudja módosítani a jelszavát és az üzenetküldéskor megjelenő becenevét.

4.2 Funkciók

- Regisztráció
  A program használatához regisztráció szükséges (regisztráció felület).

- Üzenetküldés
  Az alkalmazás legfőbb funkciója.
  A küldött üzeneteket tetszőleges módon megvalósított E2E titkosítással kell kezelni.

- Chatszoba létrehozás, meghívások
  A felhasználónak lehetősége van saját chatszoba létrehozására, melyhez meghívó küldésével további felhasználóknak is hozzáférést tud biztosítani.
  A meghívók kezelése megvalósítható alkalmazáson belül (tehát a felhasználó az alkalmazásban tud meghívót küldeni és itt látja a kapott meghívókat) vagy más tetszőleges módon (pl. link vagy kód).

- Profil kezelés
  Saját jelszó és becenév módosítás.

4.3 Titkosítás

Az üzenetek titkosításához bármilyen tetszőleges algoritmus használható.

A végponttól végpontig titkosított kommunikációhoz az egy chatszobában lévő felhasználók között kulcscsere (vagy közös kulcs előállítása) szükséges. A kulcsok kezelését az alkalmazásban kell megvalósítani (nem kézzel beírt jelszó).

Aszimmetrikus titkosítás esetén a kulcsok megosztása történhet például a következő módokon:

- Minden felhasználó rendelkezik egy kulcspárral (privát és publikus). A felhasználók megosztják egymással a publikus kulcsaikat. Ebben az esetben, ha egy felhasználó üzenetet küld a vele egy chatszobában lévő összes felhasználó számára külön-külön kell titkosítania a küldött üzenetet a hozzájuk tartozó publikus kulccsal.
- Az egy chatszobában lévő felhasználóknak közös kulcs előállítása (pl. Diffie-Helman)

Szimmetrikus titkosítás esetén elegendő chatszobánként 1 közös kulcs, mellyel a felhasználók kódolhatják és dekódolhatják az üzeneteket.

5 Dokumentáció

5.1 Erőforrás-terv, munkaidő nyilvántartás

A specifikáció birtokában a projekt résztvevői készítsenek erőforrás-tervet. Ez tartalmazza a feladatban részt vevő projekttagokat, akik legyenek hozzárendelve a tervezés során azonosított részfeladatokhoz. Minden részfeladat mellé kerüljön egy munkaidő ráfordítási becslés munkaórában számolva. Ezt a tervet a tényleges fejlesztés előtt le kell adni. A feladat megoldása során az elvégzett munkáról készüljön nyilvántartás részfeladatonként és személyenként a tényleges munkaórák számának megjelölésével. A projekt végén a két dokumentum összehasonlításra, az eltérések elemzésre kerülnek.

5.2 Technikai dokumentáció

Az elkészült kódot, függvényeket és osztályokat megfelelő kommentekkel kell ellátni, továbbá el kell készíteni a teljes alkalmazás dokumentációját. A dokumentáció a feladat bonyolultságától függő hosszúságúnak kell lennie, maximális terjedelem nincs meghatározva. A technikai dokumentáció szövegezésénél előírás, hogy a nem hozzáértő személyek számára is feldolgozható legyen, így az egyes fogalmak, rövidítések, idegen kifejezések magyarázatát a dokumentumnak tartalmaznia kell.

5.3 Forráskód dokumentáció

A fontosabb függvények és osztályok előtt szerepelnie kell megjegyzéseknek, melyeknek tartalmazniuk kell az azt követő metódus rövid szöveges – akár magyar nyelvű – leírását. A forráskód dokumentációt a munka során folyamatosan kell készíteni.

5.4 Felhasználói dokumentáció

Az alkalmazás használatának részletes bemutatása, képernyőképekkel, funkciók pontos leírásával.

6 A projekt értékelése

6.1 A feladat értékelésének felhasználó oldali szempontjai

A működő alkalmazás tesztelése alapján az alábbiak a legfontosabb jellemzők:

- Kiírást teljes egészében lefedő funkcionalitás
- Ergonomikus kialakítás
- Kényelmes használat
- Igényes felhasználói felület
- Stabil működés
- Igényes felhasználói dokumentáció

6.2 A feladat értékelésének technikai szempontjai

Informatikai szakmai szempontból a megoldás értékelésének alapja:

- Kódkép, a kód tisztasága, kommentelés minősége
- Kódolási konvenciók betartása
- Fejlesztői dokumentáció színvonala
- Dokumentált tesztelés
- Erőforrás felhasználásának pontos nyilvántartása

6.3 Projekt megvalósításának piaci jellegű értékelése

A projekt lezárultával összehasonlításra kerül a kezdeti erőforrás-terv, valamint a megvalósítás során dokumentált munka. Ezen dokumentumok elemzéséből levezetésre kerülnek azok a jellemző problémák, melyek a piaci környezetben jellemzően megjelennek. Végigtekintjük ezen problémák okait, következményeit, lehetséges elkerülésüknek vagy hatásuk mérséklésének módjait. A jellemző hibák ebből a megközelítésből:

- Határidő csúszása
- Nem megfelelő minőség
- Hiányos, vagy elmaradó tesztelés
- Használhatatlan, pontatlan dokumentáció
- Pontatlan erőforrás becslés
- Aránytalanul magas önköltség
- Az elkészült termék továbbfejlesztésének, karbantartásának nehézségei

A fentiek értékelésén túl fejlesztői szemszögből elemezzük a megvalósítás tapasztalatait, a lehetséges továbbfejlesztés, átalakítás, támogatás kérdéseit és piaci lehetőségeit.

7 Projekt adatlap

Projekt neve: -Titkosított chat alkalmazás

Feladat rövid ismertetése: Végponttól végpontig titkosított chat alkalmazás megvalósítása.

Specifikációt összeállította: Antal Norbert