Aegis

Aplicație pentru păstrarea sigură a documentelor



Aplicație dezvoltată de echipa Cretzu Cafe:

* Student caporal CORDUNEANU Arian-Andrei
* Student caporal IVAN Florentin-Marian

Cuprins

[Capitolul 1. Introducere 3](#_Toc193639971)

[1.1. Scopul proiectului 3](#_Toc193639972)

[1.2. Lista definițiilor 3](#_Toc193639973)

[1.3. Lista referințelor 3](#_Toc193639974)

[1.4. Structura DCS 3](#_Toc193639975)

[Capitolul 2. Descrierea generală a produsului software 3](#_Toc193639976)

[2.1. Descrierea generală 3](#_Toc193639977)

[2.2. Platforma HW/SW 3](#_Toc193639978)

[2.3. Constrângeri 3](#_Toc193639979)

[Capitolul 3. Cerințe specifice 3](#_Toc193639980)

[3.1. Cerințe funcționale 3](#_Toc193639981)

[3.2. Cerințe ne-funcționale 3](#_Toc193639982)

[Capitolul 4. Anexe 3](#_Toc193639983)

[Descriere model logic 3](#_Toc193639984)

[Diagrama claselor 3](#_Toc193639985)

# Capitolul 1. Introducere

## Scopul proiectului

Această aplicație este dezvoltată pentru a stoca într-un mod sigur documentele utilizatorilor prin utilizarea unor metode avansate de criptare și partajare securizată. Aplicația își propune să asigure un nivel înalt de confidențialitate, integritate și accesibilitate pentru utilizatorii săi.

Conexiunea dintre client și server va fi privată, iar transferul de date se va realiza prin intermediul unor canale de comunicație securizate utilizând protocoale de securitate precum HTTPS/TLS. Acest lucru protejează datele utilizatorilor împotriva interceptării și asigură confidențialitatea.

Documentele vor fi criptate local pe dispozitivul utilizatorului înainte de a fi încărcate pe server. Criptarea va fi realizată printr-o cheie simetrică generată individual pentru fiecare fișier, garantând astfel o protecție personalizată și fiabilă.

Pentru confidențialitate sporită, aplicația oferă utilizatorilor opțiunea de a ascunde denumirea fișierelor prin generarea unui hash unic. Pe lângă acest proces, cheile simetrice vor fi stocate local de către client, iar pentru partajare, acestea vor fi criptate folosind cheia publică a destinatarului, garantând astfel că doar destinatarul poate decripta fișierul cu cheia sa privată.

Aplicația permite partajarea securizată a fișierelor, oferind utilizatorilor posibilitatea de a selecta contactele dorite pentru partajare. Sistemul gestionează cu ușurință distribuirea cheilor de criptare, notificarea destinatarilor și procesul de partajare, oferind o experiență simplă și eficientă.

Autentificarea utilizatorilor se va realiza pe baza unui sistem de nume de utilizator și parolă, unde parola va fi stocată local sub formă de hash pentru a preveni accesul neautorizat.

De asemenea, aplicația include funcționalități de jurnalizare, înregistrând toate acțiunile efectuate la nivelul clientului și serverului pentru a asigura trasabilitatea și identificarea eventualelor probleme sau erori.

## Lista definițiilor

Cheie simetrică: tipul de cheie utilizat atât pentru criptare, cât și pentru decriptare. Această cheie este împărțită între expeditor și destinatar

Cheie publică/privată: sunt folosite în sistemele de criptate asimetrice unde cheia publica este utilizată pentru criptare, iar cheia privată pentru decriptare (cheia privată fiind strict confidențială)

TLS (Transport Layer Security): un protocol de securitate care protejează comunicațiile prin criptarea datelor transmise între client și server

HTTPS: o extensie securizată a HTTP care utilizează TLS, nepermițând atacuri cum ar fi MitM (Man-in-the-Middle)

Hash: funcție matematică care transformă un set de date într-un șir unic de caractere, utilizat pentur verificarea integrității sau ascunderea datelor

## Lista referințelor

Work in progress

## Structura DCS

Capitolul 1 – Introducere: oferă o imagine de ansamblu asupra scopului aplicației, termenilor tehnici și referințelor relevante utilizate în dezvoltarea proiectului. Oferă contextul și terminologia necesară

Capitolul 2 – Descrierea generală a produsului software: se concentrează pe o descriere detaliată a aplicației, a platformei hardware/software necesare și a eventualelor constrângeri de proiectare. În plus aici se găsesc detalii despre mediul operațional și specificațiile platformei

Capitolul 3 – Cerințe specifice: este cel mai detaliat capitol, incluzând cerințele funcționale și cerințele nefuncționale.

Capitolul 4 – Anexe: oferă suport grafic și documentație suplimentară pentru cerințele definite. Include modele logice, diagrame ale claselor, fluxuri de date și alte elemente grafice relevante pentru implementare

# Capitolul 2. Descrierea generală a produsului software

## 2.1. Descrierea generală

Aplicația Aegis este o soluție software concepută pentru stocarea și partajarea sigură a documentelor utilizatorilor. Scopul său principal este de a asigura protecția datelor personale și confidențialitatea informațiilor prin utilizarea unor tehnologii avansate de criptare, autentificare și comunicare securizată.

Sistemul este bazat pe un model arhitectural client-server și include următoarele funcționalități principale:

**Client:**

* Utilizează interfața grafică pentru interacțiunea directă cu utilizatorii.
* Realizează criptarea fișierelor local prin generarea unei chei simetrice individuale pentru fiecare fișier.
* Stochează local cheile simetrice, utilizând hash-uri pentru anonimizare (opțional).
* Trimite fișierele criptate către server prin conexiuni securizate HTTPS/TLS.
* Primește de la server cheile publice ale altor utilizatori pentru partajare.

**Server:**

* Găzduiește fișierele criptate primite de la client.
* Stochează cheile simetrice, criptate folosind cheia publică a utilizatorului.
* Menține o listă centralizată cu utilizatorii înregistrați pentru facilitarea partajării fișierelor.
* Notifică destinatarii atunci când un fișier a fost partajat.
* Asigură jurnalizarea tuturor acțiunilor efectuate de utilizatori.

## 2.2. Platforma HW/SW

## 2.3. Constrângeri

# Capitolul 3. Cerințe specifice

## 3.1. Cerințe funcționale

## 3.2. Cerințe ne-funcționale

# Capitolul 4. Anexe

## Descriere model logic

## Diagrama claselor