Cryptochat – aplicatie de mesagerie securizata

Dezvoltatori:

Std. Cap. Ionescu Andrei Ianis Echipa Ciresarii

Std. Cap. Birsan Cristian

Grupa: C-112-A

Data: 23.03.2025

Academia Tehnica Militara “Ferdinand I”

# Cuprins

1. Introducere  
   1.1 Scopul proiectului  
   1.2 Lista definițiilor  
   1.3 Lista referințelor  
   1.4 Structura DCS
2. Descrierea generală a produsului software  
   2.1 Descrierea produsului software  
   2.2 Detalierea platformei HW/SW  
   2.3 Constrângeri
3. Detalierea cerințelor specifice  
   3.1 Cerințe funcționale  
   3.2 Cerințe ne-funcționale

# Capitol 1 – Introducere

**1.1 Scopul proiectului**

Aplicația **CryptoChat** este o platformă de mesagerie securizata dezvoltată în **C++**, având ca scop furnizarea unui mediu **sigur și rapid** pentru comunicarea utilizatorilor prin mesaje text și fișiere.

Aceasta va integra un **server proxy de comunicație**, chei de criptare unice pentru fiecare utilizator la înregistrare, **grupuri de chat**, **agendă la nivel client**, jurnalizare a acțiunilor atât pe client, cât și pe server și partajare de fișiere securizată prin chei de criptare individuale.

**1.2 Lista definițiilor**

| **Abreviere** | **Definiție** |
| --- | --- |
| DCS | Document de Cerințe Software |
| HW | Hardware |
| SW | Software |
| API | Application Programming Interface |
| TLS | Transport Layer Security |

**1.3 Lista referințelor**

* RFC 6455 - WebSocket Protocol
* Standarde de securitate **TLS/SSL**
* Documentație **Qt** pentru GUI

**1.4 Structura DCS**

Acest document descrie cerințele funcționale și nefuncționale ale aplicației **CryptoChat**, detalierea platformei HW/SW, precum și modelele logice și diagramele utilizate în dezvoltarea sa.

**Capitolul 2 - Descrierea generală a produsului software**

**2.1 Descrierea produsului software**

**CryptoChat** este o aplicație de mesagerie care permite:

* Trimiterea de **mesaje text**, imagini și fișiere
* Criptare end-to-end utilizând **chei de criptare unice** pentru fiecare utilizator
* Funcționarea printr-un **server proxy de comunicație** pentru redirecționarea mesajelor
* **Grupuri de chat** și gestionarea utilizatorilor într-o **agendă locală**
* **Jurnalizarea acțiunilor** utilizatorului și a serverului pentru audit și securitate

**2.2 Detalierea platformei HW/SW**

* **Hardware**:
  + PC-uri cu minim **2GB RAM**, procesoare **dual-core**
* **Software**:
  + **Windows, Linux**
* **Tehnologii utilizate**:
  + **C++** pentru backend
  + **Qt** pentru interfață grafică
  + **WebSockets** pentru comunicare în timp real
  + **SQL** pentru baza de date

**2.3 Constrângeri**

* **Dimensiunea maximă a fișierelor transferate**: 100MB
* **Necesitatea unei conexiuni active la internet** pentru mesagerie
* **Criptare obligatorie** pentru orice fișier transmis

**Capitolul 3 - Detalierea cerințelor specifice**

**3.1 Cerințe funcționale**

* **Înregistrare utilizatori**:
  + La înregistrare, serverul generează și transmite o **cheie de criptare unică** utilizatorului
* **Autentificare și conexiune**
  + Autentificare prin **număr de telefon**
* **Trimiterea și primirea mesajelor**
  + Mesaje text individuale și în **grupuri de chat**
  + Serverul funcționează ca **proxy** și nu stochează conținutul mesajelor
* **Partajarea fișierelor**
  + Fiecare fișier transmis are o **cheie de criptare individuală**
* **Gestionarea agendei**
  + Utilizatorii pot **adăuga și gestiona contacte** local
* **Jurnalizare**
  + Acțiunile utilizatorului sunt **logate la nivel client și server** pentru audit

**3.2 Cerințe ne-funcționale**

* **Cerințe de performanță**
  + Timp de răspuns **sub 1 secundă** pentru trimiterea mesajelor
  + **Optimizare memorie**: consum maxim de **200MB RAM**
* **Cerințe de interfață**
  + Interfață intuitivă, **UX modern**, suport **dark mode**
  + Compatibilitate **desktop**
* **Cerințe operaționale**
  + **Mecanism de backup** local pentru mesaje
* **Cerințe impuse resurselor fizice**
  + Aplicația trebuie să ruleze pe **hardware low-end**
  + Stocare locală criptată pentru datele sensibile
* **Cerințe de verificare**
  + Testare pe **diferite platforme** și rețele lente (3G, 4G, Wi-Fi)
* **Cerințe de securitate**
  + Jurnalizare a **acțiunilor utilizatorului și serverului**