Key Manager

Rust Project Proposal

Leon Rado, Dokaniev Andrii

Introduction

Cieľom projektu je vytvoriť bezpečný a efektívny manažér na generovanie, spracovanie, šifrovanie a ukladanie hesiel a rôznych špeciálnych kľúčov (napr. SSH kľúče, API kľúče). Aplikácia umožní používateľom bezpečne spravovať svoje citlivé dáta pomocou šifrovania a autentifikácie používateľa pred prístupom k údajom. Manažér bude podporovať ukladanie hesiel a kľúčov v databáze a bude obsahovať používateľské rozhranie (UI) pre jednoduchú správu a bezpečný prístup k údajom. V aplikácii bude tiež možné vytvoriť SSH spojenie so vzdialeným serverom.

Konkrétne prípady použitia

- **Administrátori serverov** – Bezpečné generovanie, ukladanie a správa SSH kľúčov na vzdialenú správu serverov.
- **Vývojári** – Ochrana a šifrovanie API kľúčov, prístupových tokenov a iných citlivých údajov používaných v aplikáciách.
- **Firmy a organizácie** – Centrálna správa a bezpečné zdieľanie autentifikačných údajov pre interné systémy a cloudové služby.
- **Jednotlivci** – Generovanie, uchovávanie a správa hesiel a ďalších citlivých údajov

Dôvod výberu jazyka Rust

- **Bezpečnosť pamäte** – Rust automaticky predchádza chybám typu buffer overflow a dereferencii nulových ukazovateľov.
- **Vysoký výkon** – Rust je porovnateľne rýchly s *C/C++*, ale poskytuje vyššiu úroveň bezpečnosti.
- **Silná podpora kryptografie** – K dispozícii je široká škála bezpečnostných knižníc, napríklad *ring, openssl, aes-gcm*.
- **Dobrá paralelizácia** – Rust umožňuje bezpečné asynchrónne spracovanie s nízkymi režijnými nákladmi vďaka runtime knižnici *tokio*.

Cieľom projektu je naučiť sa

- **Vytvoriť bezpečný systém** na správu kľúčov v programovacom jazyku Rust.
- **Navrhnúť a implementovať** bezpečnú autentifikáciu používateľov.
- **Implementovať kryptografické knižnice** na zabezpečenie šifrovania a hashovania.
- **Vytvoriť jednoduchý server** na spracovanie používateľských požiadaviek.
- **Integrovať databázový systém** na bezpečné ukladanie hesiel a kľúčov.
- **Implementovať používateľské rozhranie** pre pohodlnú správu a prístup k údajom.

Requirements

- Autentifikácia používateľov
- Ukladanie údajov v zašifrovanej podobe
- Generovanie a ukladanie hesiel a kľúčov
- Možnosť exportu a importu hesiel a kľúčov
- Grafické používateľské rozhranie
- Integrácia s databázou
- Asynchrónne spracovanie požiadaviek
- Pripojenie k serveru pomocou SSH

Dependencies

- ★ **ring** - kryptografické operácie ako šifrovanie a hashovanie
- ★ **sqlx** - interakcia s SQL databázou
- ★ **russh** - bezpečné pripojenie k vzdialeným serverom
- ★ **bcrypt** - hashovanie používateľských hesiel
- ★ **tokio** - vykonávanie asynchrónnych operácií
- ★ **rocket** - vytvorenie webového API alebo servera
- ★ **egui** - grafické používateľské rozhranie
- ★ **serde** - serializácia a deserializácia dát do JSON
- ★ **openssl** - kryptografické operácie, generovanie SSH kľúčov
- ★ **reqwest** - vykonávanie HTTP požiadaviek
- ★ **uuid** - generovanie unikátnych identifikátorov
- ★ **chrono** - práca s dátumami a časmi