Password Manager

Mini Project in SSD Esbjerg Erhvervs Adademi Sydvest

The Password Manager Security Documentation outlines the security features of the application, including encryption methods (AES, SHA-256, bcrypt), key management, and Two-Factor Authentication (2FA). It highlights the main security objectives: confidentiality, integrity, and availability. The document also identifies potential threat actors, such as external attackers and malicious insiders, and discusses potential pitfalls like key loss and local storage risks. The conclusion emphasizes the importance of user awareness and responsible management of key files and passwords to maintain security

Klaus Hviid

11-10-2024

11-10-2024

Password Manager

Password Manager Security Documentation

Indholdsfortegnelse

Overview

This document provides an overview of the security features implemented in the Password Manager application, identifies potential threat actors, explains my security model, and highlights any pitfalls or limitations.

Purpose

The primary purpose of this documentation is to ensure users understand the robust security measures I have taken to protect their data, as well as to highlight the potential threats and limitations within the current setup.

Security Objectives

My main objectives are:

Confidentiality: Ensuring that sensitive user data, including passwords and personal information, is kept confidential and accessible only by authorized users.

Integrity: Maintaining the accuracy and completeness of the stored data.

Availability: Ensuring that authorized users have reliable access to their data whenever needed.

Threat Actors

The primary threat actors I am protecting against include:

1. **External Attackers**: Individuals or groups attempting to gain unauthorized access to user data through hacking or other cyber-attacks.

2. **Malicious Insiders**: Authorized users who misuse their access privileges to compromise data security.

3. **Casual Intruders**: Unauthorized individuals attempting to access user data without sophisticated tools or methods.

Security Model

Encryption

1. **AES (Advanced Encryption Standard)**: I use AES for encrypting sensitive data, such as passwords stored in the database. This ensures that even if the database is compromised, the data remains secure.

2. **SHA-256**: Utilized for hashing master passwords and key handling. This ensures secure storage and comparison of password data.

3. **bcrypt**: Used for hashing user passwords, adding an extra layer of security with built-in salting and adaptive workload capabilities.

Key Handling

1. **Key Management**: Encryption keys are derived from the user's master password using SHA-256, and combined with random data generated from mouse movements. These keys are then used to encrypt sensitive data. The master password is never stored in plain text.

2. **Random Data**: Secure random data generation techniques are used for initialization vectors (IV) and key derivation. This random data is generated from mouse movements when generating the master key and is stored securely.

3. **KeyFilePath**: The KeyFilePath is used for hiding the actual path to the MasterPassword.key file, which the user selects. This path is also securely stored and encrypted using AES.

WORKFLOW

User Registration and Setup:

- During initial setup, the user creates a master password.
- The master password is hashed using bcrypt and stored securely.
- Random data is generated from mouse movements and used to derive encryption keys.
- A MasterPassword.key file is created and encrypted using AES, and the file path is stored securely. The MasterPassword.key file must be securely stored by the user, as they are responsible for its safekeeping.
- A QR code is generated for Two-Factor Authentication (2FA), which the user can scan to set up TOTP (Time-based One-Time Password). The 2FA seed is created from a secure random generation process and kept secret within the secure storage mechanisms of the application.

Login and Verification:

- Upon login, the user provides their master password.
- The provided password is hashed and compared with the stored hash.
- The user is prompted for a TOTP code generated by their 2FA app.
- If verified, the user's encrypted data is decrypted using keys derived from the master password and random data.

Data Storage and Retrieval:

- User passwords and sensitive data are encrypted using AES before storing in the database.
- Encrypted data is decrypted only when accessed by the authenticated user.

Potential Pitfalls and Limitations

1. Key Loss: If users lose their MasterPassword.key file or forget their master password, they will be unable to access their encrypted data.

2. Single Point of Failure: The MasterPassword.key file is critical. Ensuring its security is paramount.

3. Local Storage: Storing the MasterPassword.key file locally may present a risk if the user's device is compromised.

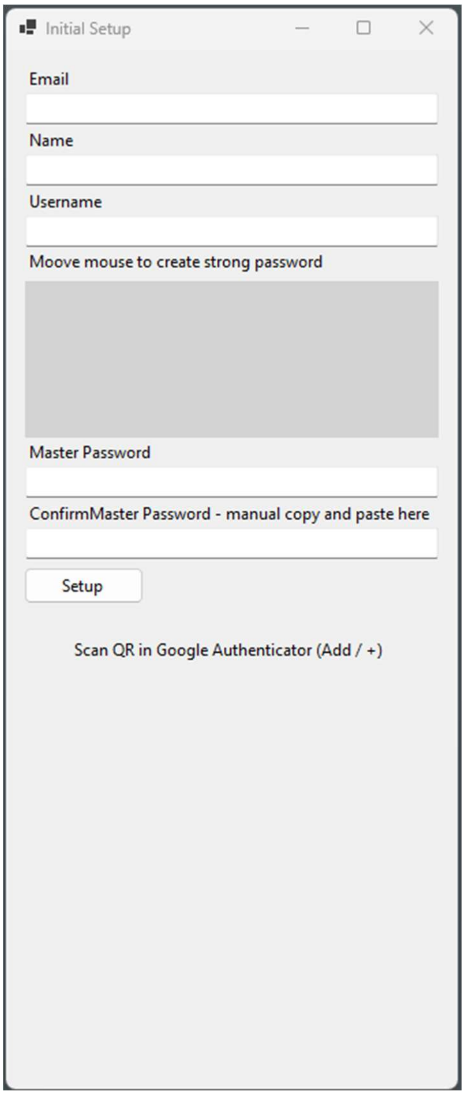
4. User-Managed Security: The security heavily relies on the users managing their master passwords and key files responsibly. Users must ensure their master password is strong and not reused across multiple platforms. The user has the responsibility of the Master Key and password.

Conclusion

My solution aims to provide robust security through advanced encryption and key management techniques. By integrating Two-Factor Authentication (2FA) and TOTP, I further enhance the security against unauthorized access. However, user awareness and responsible management of key files and passwords are critical to maintaining security. Regular updates and continuous monitoring for potential vulnerabilities are essential to enhance the security posture. While the current setup provides strong protection, users must remain vigilant and proactive in safeguarding their credentials.

Screenshots and usage

Initial Setup Form


Initial Setup
Email
Name
Username
Moove mouse to create strong password
Master Password
ConfirmMaster Password - manual copy and paste here
Setup
Scan QR in Google Authenticator (Add / +)

Here you fill out:
Email

Name

Username

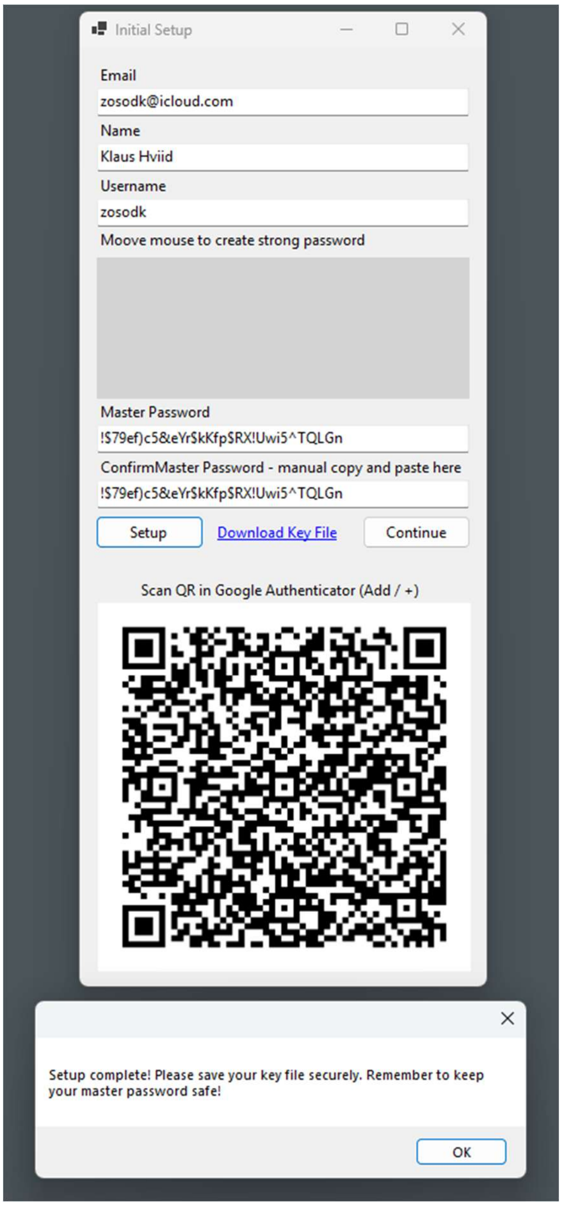
Then you move the mouse around in the dark-grey field – it will then create a random 32 character Master Password in the equally named text field.

Select the Master Password from the field and manually copy/paste it into the Confirm Master Password field below

Also Save this password in a safe place of you own choosing

Press the button Setup

Click on the Setup button



Initial Setup

Email

zosodk@icloud.com

Name

Klaus Hviid

Username

zosodk

Moove mouse to create strong password

Master Password

!$79ef)c5&eYr$kKfp$RX!Uwi5^TQLGn

ConfirmMaster Password - manual copy and paste here

!$79ef)c5&eYr$kKfp$RX!Uwi5^TQLGn

Scan QR in Google Authenticator (Add / +)

Setup complete! Please save your key file securely. Remember to keep your master password safe!

Klik on the Blue link and select a safe place to store your keyfile for the program.

Open you phone and find your favorite authenticator – this program has been tested with Google Authenticator, but any should work

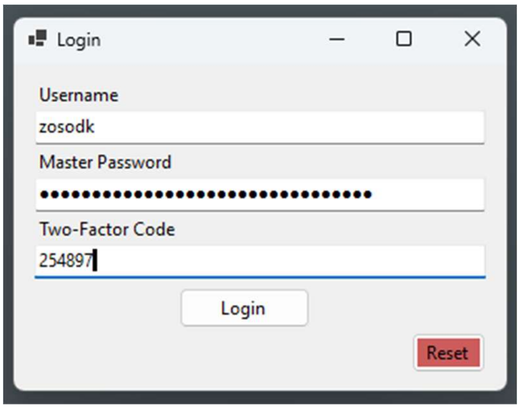
Make sure your phone and computer has automatic time synchronization set to ON Most have – so this shouldn't be necessary to make any changes.

Add this QR key to you Authenticator this should create a key that you must use to logon.

When this is done – press Continue

If you cannot press Continue, then make sure you have pressed the OK button on the Setup Complete dialogue box

Login Form



Username: zosodk

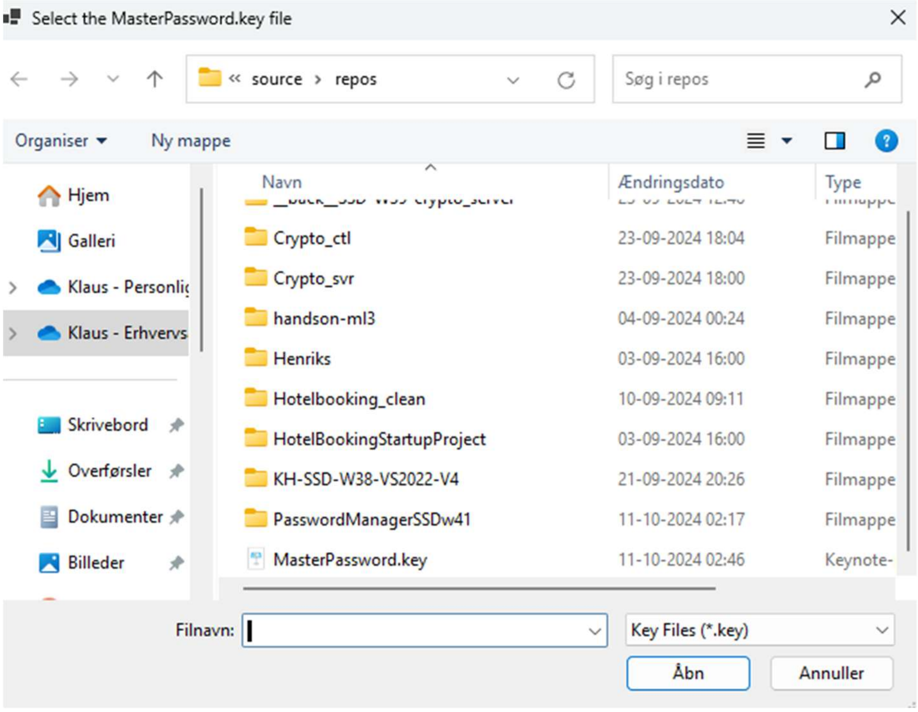
Master Password: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Two-Factor Code: 254897

Input your username, password from earlier

If you somehow managed to forgot to save your password, create your 2FA authenticator. Then you can press the Reset button. This will delete all files related to your creation – except for the MasterPassword.key.

Click Login – this will prompt you with the opportunity of supplying the path to your Keyfile.Locate the file and select open.

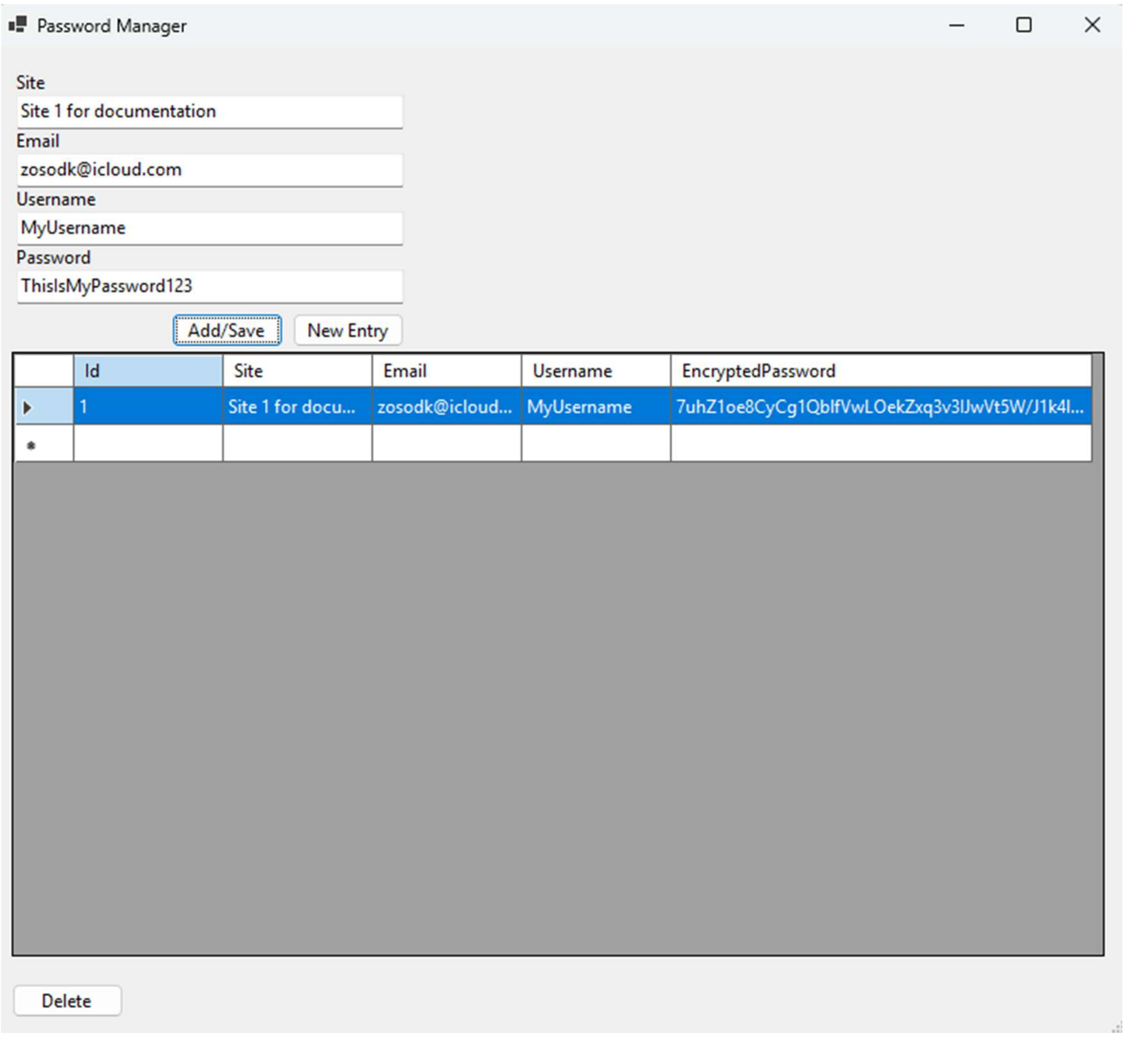


Navn	Ændringsdato	Type
Crypto_ctl	23-09-2024 18:04	Filmappe
Crypto_svr	23-09-2024 18:00	Filmappe
handson-ml3	04-09-2024 00:24	Filmappe
Henriks	03-09-2024 16:00	Filmappe
Hotelbooking_clean	10-09-2024 09:11	Filmappe
HotelBookingStartupProject	03-09-2024 16:00	Filmappe
KH-SSD-W38-VS2022-V4	21-09-2024 20:26	Filmappe
PasswordManagerSSDw41	11-10-2024 02:17	Filmappe
MasterPassword.key	11-10-2024 02:46	Keynote-

Filnavn:

Key Files (*.key)

Password Manager Form



Site

Site 1 for documentation

Email

zosodk@icloud.com

Username

MyUsername

Password

ThisIsMyPassword123

	Id	Site	Email	Username	EncryptedPassword
▸	1	Site 1 for docu...	zosodk@icloud...	MyUsername	7uhZ1oe8CyCg1QblfVwLOekZxq3v3lJwVt5W/J1k4l...
*					

This is rather self explanatory.

Add/Save is for creating entries or editing by selecting from the table

New Entry clears the input fields for new entries

Delete, at the bottom left, deletes a selected record.