Software Design Specification

# Project Title: Password Manager

Version: 1.0

Supervisor: Sir Shaheer Ahmed

Project Team: M. Tamseel Khanzada (23k-2063), Abdul Ahad (23p-0625),

Abdul Samad (23k-3042)

Submission Date: 4/29/2025

**Table of Contents**

**1. Introduction**

**1.1 Purpose of Document**

**1.2 Intended Audience**

**1.3 Document Convention**

**1.4 Project Overview**

**1.5 Scope**

**2. Design Considerations**

**2.1 Assumptions and Dependencies**

**2.2 Risks and Volatile Areas**

**3. System Architecture**

**3.1 System Level Architecture**

**3.2 Software Architecture**

**4. Design Strategy**

**5. Detailed System Design**

**5.1 Database Design**

**5.2 Application Design   
 5.3 RMM Table**

**6. References**

**7. Appendices**

# Document Sign-Off

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Sign-off Authority | Project Role | Signature | Sign-off Date |
| 1.0 | Ahad | Lead Developer | A. | 2025-04-17 |
| 1.0 | Tamseel | Support | T. | 2025-04-29 |
| 1.0 | Samad | Support | S. | 2025-04-29 |

# Document Information

Customer: FAST-NU

Project: Password Manager

Document: Software Design Specification

Document Version: 1.0

Status: Draft

Author(s): M. Tamseel Khanzada, Abdul Ahad, Abdul Samad

Approver(s):

Issue Date:

Document Location:

Distribution:

# Definition of Terms, Acronyms and Abbreviations

|  |  |
| --- | --- |
| Term | Description |
| AES | Advanced Encryption Standard |
| GCM | Galois/Counter Mode |
| JSON | JavaScript Object Notation |
| MFA | Multi-Factor Authentication |
| IV | Initialization Vector |
| UI | User Interface |

**1. Introduction**  
1.1 Purpose of Document  
This document defines the design details for the Password Manager project. It targets students and developers aiming to implement or understand the system's architecture. The project uses Object-Oriented Design methodology.

1.2 Intended Audience  
This document is intended for project team members, advisors, evaluators, and future developers.

1.3 Document Convention  
This document uses Times New Roman, size 12 for body text and bold headings.

1.4 Project Overview  
The Password Manager is a desktop application for securely managing user credentials. It allows password storage, retrieval, encryption/decryption, and backup functionality. Built in Python using Tkinter and the Cryptography library.

1.5 Scope

* Allows user account creation with secure login.
* Stores encrypted credentials for multiple sites.
* Provides backup and restore options.
* Generates strong passwords.
* Works offline only.
* Master password recovery is not supported.
* **2. Design Considerations**

2.1 Assumptions and Dependencies

* Python 3.10 or higher must be installed.
* System depends on external Cryptography libraries.
* User is responsible for data backups.

2.2 Risks and Volatile Areas

* Security breaches if encryption is poorly implemented.
* Data loss without backups.
* Changes in encryption library API.
* GUI compatibility across OS platforms.
* **3. System Architecture**  
  3.1 System Level Architecture
* Modules: UI Module, Logic Module, Encryption Module, Storage Module.
* External Interface: JSON file system, local file access.
* Components communicate through well-defined APIs.

3.2 Software Architecture

* **Presentation Layer**: Built with Tkinter, handles user interaction.
* **Application Logic Layer**: Handles authentication, CRUD operations.
* **Data Access Layer**: Encrypts/decrypts and stores data in JSON.
* Uses AES-GCM encryption with unique IV per entry.

**4. Design Strategy**

* Modular design for easy updates.
* Clean UI for non-technical users.
* Offline-first design.
* AES-GCM ensures secure storage.
* All decrypted data is held in memory only.

**5. Detailed System Design**  
5.1 Database Design  
(See below for tables)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |

## Data Dictionary - User Table

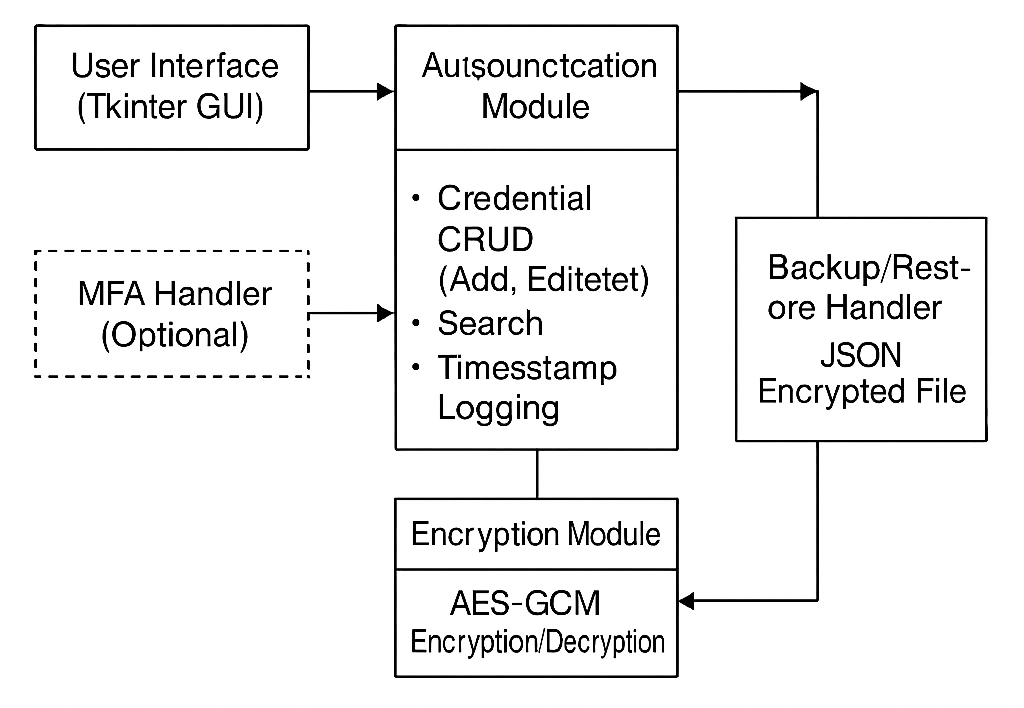
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Column Name | Description | Type | Length | Nullable | Default Value | Key Type |
| user\_id | Unique ID | int | N/A | No | Auto | PK |
| master\_hash | Hashed master password | string | 256 | No | - |  |
| salt | Salt for hashing | string | 128 | No | - |  |

## Data Dictionary - Credential Table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Column Name | Description | Type | Length | Nullable | Default Value | Key Type |
| cred\_id | Unique ID | int | N/A | No | Auto | PK |
| user\_id | Foreign Key | int | N/A | No | - | FK |
| site | Website name | string | 100 | No | - |  |
| username | Username | string | 100 | No | - |  |
| password | Encrypted password | string | 256 | No | - |  |
| iv | Initialization Vector | string | 128 | No | - |  |
| timestamp | Created/Modified time | datetime | - | No | CURRENT\_TIMESTAMP |  |

**5.2 Application Design**

**Architecture diagram**



**Class diagram**

A diagram of a computer system

AI-generated content may be incorrect.

**5.3 Rmm Table:**

| **Risk** | **Likelihood** | **Impact** | **Mitigation Strategy** | **Owner** | **Status** |
| --- | --- | --- | --- | --- | --- |
| Weak encryption implementation | High | High | Use AES-GCM for strong encryption, review code regularly. | Ahad | Ongoing |
| Data loss without backups | Medium | High | Implement backup feature and educate users on backup steps. | Samad | Planned |
| Changes in Cryptography library API | Medium | Medium | Regularly check for library updates and adjust as necessary. | Ahad | Ongoing |
| Compatibility issues across platforms | Low | Medium | Test on different OS platforms (Windows, macOS, Linux). | Tamseel | Planned |

**6. References**

* NIST AES Specifications
* OWASP Password Storage Guidelines
* Python Cryptography Documentation

**7. Appendices**

* Use Case Diagrams
* UI Wireframes (to be added)
* JSON File Structure

**End Of Document**