Dominik Kędzia
PL6793186013

Savepass.net

Web service

User Requirements Document

Issue:	Draft
Revision:	0
Reference:	1/2019
Created:	October 1st 2019
Last modified:	October 23rd 2019
Prepared by:	**Dominik Kędzia**

Abstract

This User Requirements Specification Document describes the business needs for what users require from the Savepass.net web platform. The newest version can be found in GIT repository under the following URL:

github.com/dkedzia/savepass-urd

Table of contents

User Requirements Document **1**

Abstract **3**

Table of contents **4**

1 Introduction **6**
1.1 Purpose of the document 6
1.2 Scope of the software 6
1.3 Definitions, acronyms and abbreviations 6
1.3.1 Definitions 6
1.3.2 Acronyms 6
1.3.3 Abbreviations 7
1.4 References 7
1.5 Overview of the document 7

2 General Description **7**
2.1 Product perspective 7
2.2 General capabilities 7
2.3 General constraints 7
2.4 User characteristics 7
2.5 Operational environment 7
2.6 Assumptions and dependencies 8

3 Specific Requirements **8**
3.1 Capability Requirements 8
3.1.1 Passwords Generator 8
3.1.1.1 Length input 8
3.1.1.2 a-z selection 8
3.1.1.3 A-Z selection 8
3.1.1.4 0-1 selection 8
3.1.1.5 Special characters selection 8
3.1.1.6 Profile selection 9
3.1.2 Password Encryptor 9
3.1.2.1 Text field 9
3.1.2.2 Profile selector 9
3.1.2.3 Submit button 9
3.1.3 Password Decryptor 9

3.1.3.1 Copy button 9
3.1.3.2 Edit button 9
3.1.3.3 Delete button 9
3.2 Constraint Requirements 9
3.2.1 There is no constraint requirements. 9

4 List of User Requirements **9**
4.1 Logging 9
4.2 Change password 10
4.3 Delete password and account 10
4.4 Generate password 10
4.5 Encrypt password 10
4.6 Decrypt password 10

1 Introduction

1.1 Purpose of the document

The purpose of this document is to specific the service provided by Savepass.net.

1.2 Scope of the software

The main goal for software described in this document is to provide cryptographic service for the users. Web platform is intended to provide two main functionalities.

The first is about auto-generating random passwords for users, based on their expectations - length and complexity.

The second one is to encrypt given passwords with user's main password.

1.3 Definitions, acronyms and abbreviations

1.3.1 Definitions

- "ready-to-go" - describes software that do not need any configuration steps to work correctly,
- "hash" - random string,
- "password" - secret string known only to user.

1.3.2 Acronyms

- "LAN" - Local Area Network
- "GDPR" - General Data Protection Regulation

1.3.3 Abbreviations

1.4 References

1.5 Overview of the document

2 General Description

2.1 Product perspective

Huge demand on passwords encryption services seems to put Savepass.net web service on very safe position. Software development should focus on providing ready-to-go services especially provided for governments which are potential clients with need of this type of service

2.2 General capabilities

1. Passwords generator - allows user to generate random string using given characters of given length.
2. Passwords encryptor - allows user to encrypt given string into secure hash, using given main password, Initialization vector and random hash generated for every user.
3. Passwords decryptor - allows user to decrypt the password using given main password, Initialization vector and random hash generated for every user.

2.3 General constraints

The is no any constraints.

2.4 User characteristics

1. Normal user - this is default and only one type of user. There is no separation for moderators, pro users, basic users. It is just a user who has got the access to all parts of the software.

2.5 Operational environment

Software from the client-side must be able to run on the following platforms:

- Microsoft Windows
- GNU/Linux

- Apple macOS
- Google Android
- Apple iOS

All devices must be connected to Internet or LAN where Savepass.net service is provided in order to communicate with server.

Server-side must be able to run on servers based on GNU/Linux.

2.6 Assumptions and dependencies

Software must run on standard Web server, equipped with PHP interpreter and MySQL Database.

It cannot depends on any foreign frameworks considering the level of safety provided by this service.

3 Specific Requirements

3.1 Capability Requirements

3.1.1 Passwords Generator

3.1.1.1 Length input

Software must allow user setup the length of the generated password.

3.1.1.2 a-z selection

Software must allow user to choose if he needs a-z characters in generated password.

3.1.1.3 A-Z selection

Software must allow user to choose if he needs A-Z characters in generated password

3.1.1.4 0-1 selection

Software must allow user to choose if he needs 0-1 characters in generated password

3.1.1.5 Special characters selection

Software must allow user to choose if he needs special characters, like !@#$ in generated password

3.1.1.6 Profile selection

Software must allow user to select the profile of known services to provide the most secure password.

3.1.2 Password Encryptor

3.1.2.1 Text field

Software must allow user to encrypt password given by his own.

3.1.2.2 Profile selector

Software must allow user to select generator profile if he wants to generate and encrypt new password

3.1.2.3 Submit button

Software must allow user to execute encryption process.

3.1.3 Password Decryptor

3.1.3.1 Copy button

Software must allow user to copy password to clipboard.

3.1.3.2 Edit button

Software must allow user to change option of the saved record.

3.1.3.3 Delete button

Software must allow user to deleted encrypted and saved password.

3.2 Constraint Requirements

3.2.1 There is no constraint requirements.

4 List of User Requirements

4.1 Logging

User must be able to login to his account, because he needs to stay in touch with his encrypted passwords.

4.2 Change password

User must be able to change his main password in order to stay safe.

4.3 Delete password and account

User must be able to delete his passwords and account in order to GDPR.

4.4 Generate password

User must be able to generate new passwords, because he wants to make it as most safe as possible.

4.5 Encrypt password

User must be able to encrypt new passwords, because he wants to keep them in the safest way possible.

4.6 Decrypt password

User must be able to decrypt all his passwords in order not to lose access to any services.