

Software Requirements Specification

for

Egnog

Version 0.1.0

Prepared by

Group Name: *Matthew and Hunter*

|  |  |  |
| --- | --- | --- |
| Matthew Droege | 11524046 | Matthew.droege@wsu.edu |
| Will Purviance | 11538155 | william.purviance@wsu.edu |

|  |  |
| --- | --- |
|  |  |
| Date: | 10/7/2018 |
|  |  |
|  |  |
|  |  |

Contents

Revisions iii

1 Introduction 1

1.1 Document Purpose 1

1.2 Product Scope 1

1.3 Intended Audience and Document Overview 1

1.4 Definitions, Acronyms and Abbreviations 1

1.5 Document Conventions 1

1.6 References and Acknowledgments 2

2 Overall Description 3

2.1 Product Perspective 3

2.2 Product Functionality 3

2.3 Users and Characteristics 3

2.4 Operating Environment 3

2.5 Design and Implementation Constraints 4

2.6 User Documentation 4

2.7 Assumptions and Dependencies 4

3 Specific Requirements 5

3.1 External Interface Requirements 5

3.2 Functional Requirements 6

3.3 Behaviour Requirements 6

4 Other Non-functional Requirements 7

4.1 Performance Requirements 7

4.2 Safety and Security Requirements 7

4.3 Software Quality Attributes 7

5 Other Requirements 8

Appendix A – Data Dictionary 9

Appendix B - Group Log 10

Revisions

| Version | Primary Author(s) | Description of Version | Date Completed |
| --- | --- | --- | --- |
| 1st draft  Version 0.1.0 | Matthew Droege  William Purviance | Initial project proposal, with an outline of its basic functionality. | 10/07/18 |

# Introduction

This section gives a brief overview of this document’s intent. It also gives a brief description of the proposed software’s functionality.

## Document Purpose

This document gives a detailed description of the web application “Egnog”. Its purpose and functionality are outlined here. It will provide an overview concerning the customer attributes and a guideline for the development team to follow.

## Product Scope

“Egnog” is a multi-purpose software utility, specifically concerned with allowing users the ability to manage personal information, catering towards password keeping.

Users will be able to create an account to easily access tabs to store their information. Included in these tabs will be one to store a website name along with login information that will be kept private exclusively to the user. Other tabs will be able keep information such as to-dos, or a calendar.

## Intended Audience and Document Overview

The target audience for this software is anyone who can benefit from having a place to securely store passwords and manage information. This could be for the user wishing to store social media or gaming login information, or for professionals wishing to have a secure place to store important information like banking and company information.

## Definitions, Acronyms and Abbreviations

A password manager/keeper is any software used for generating and storing passwords, for future retrieval.

## Document Conventions

The body of this document is in Ariel, 11 point. It is divided into 5 sections.

# Overall Description

## Product Perspective

The system will consist of a login in page where you are able to enter your username and password or create a new account. These options include being able to add a new username and password along with what site the login information is for.

TBA

Users

Support

Saved Passwords

Login

Egnog

## Product Functionality

- Store login credentials

-Store user imputed passwords

-Generate passwords

-TBA

-TBA

## Users and Characteristics

This web application will be catering towards users who need some place to store multiple passwords and information they use in an easy and efficient way.

## Operating Environment

Egnog is a web application. It will run on any web browser running off current distributions of Windows, Mac OS, and most Linux distros.

## Design and Implementation Constraints

To be determined later.

## User Documentation

Documentation will cover how to use the main functionalities of the software, and how the user can be most efficient in accomplishing task with its utilities. These tasks include: storing passwords, usernames, or login-credentials; retrieving these stored credentials for use; auto-generating passwords; and creating and updating the to-dos list utility.

## Assumptions and Dependencies

1. The user will likely end up storing a significant number of passwords in the software database, for future access.
2. The user will likely not want to spend much time within the application, but will be using it to quickly reference information, or add information.
3. The user will need to store passwords that favor complexity, over simplicity, for security.

# Specific Requirements

## External Interface Requirements

### User Interfaces

At the time of version 1 the development team plans to have a login window then at least 4 different sections to get access to. There will be a page to keep track of your passwords, 2 pages that will be announced later and 1 page that will have support information if something goes wrong (Revisions to this section could be made in later versions).

### Hardware Interfaces

TBA, not sure if we will need external libraries yet (Revisions to this section could be made in later versions).

### Software Interfaces

The user will be able to input information and save it to the database to be fetched when the user needs it (Revisions to this section could be made in later versions).

### Communications Interfaces

The security of our users will be top priority as keeping their passwords safe a secure is the only way our application will not fail. We plan to use encryptions but to which standards is to be determined (Revisions to this section could be made in later versions).

## Functional Requirements

### 3.2.1 Store login credentials

Exact method is to be determined.

**3.2.2 Store user imputed passwords**

Exact method is to be determined.

**3.2.3 Generate passwords**

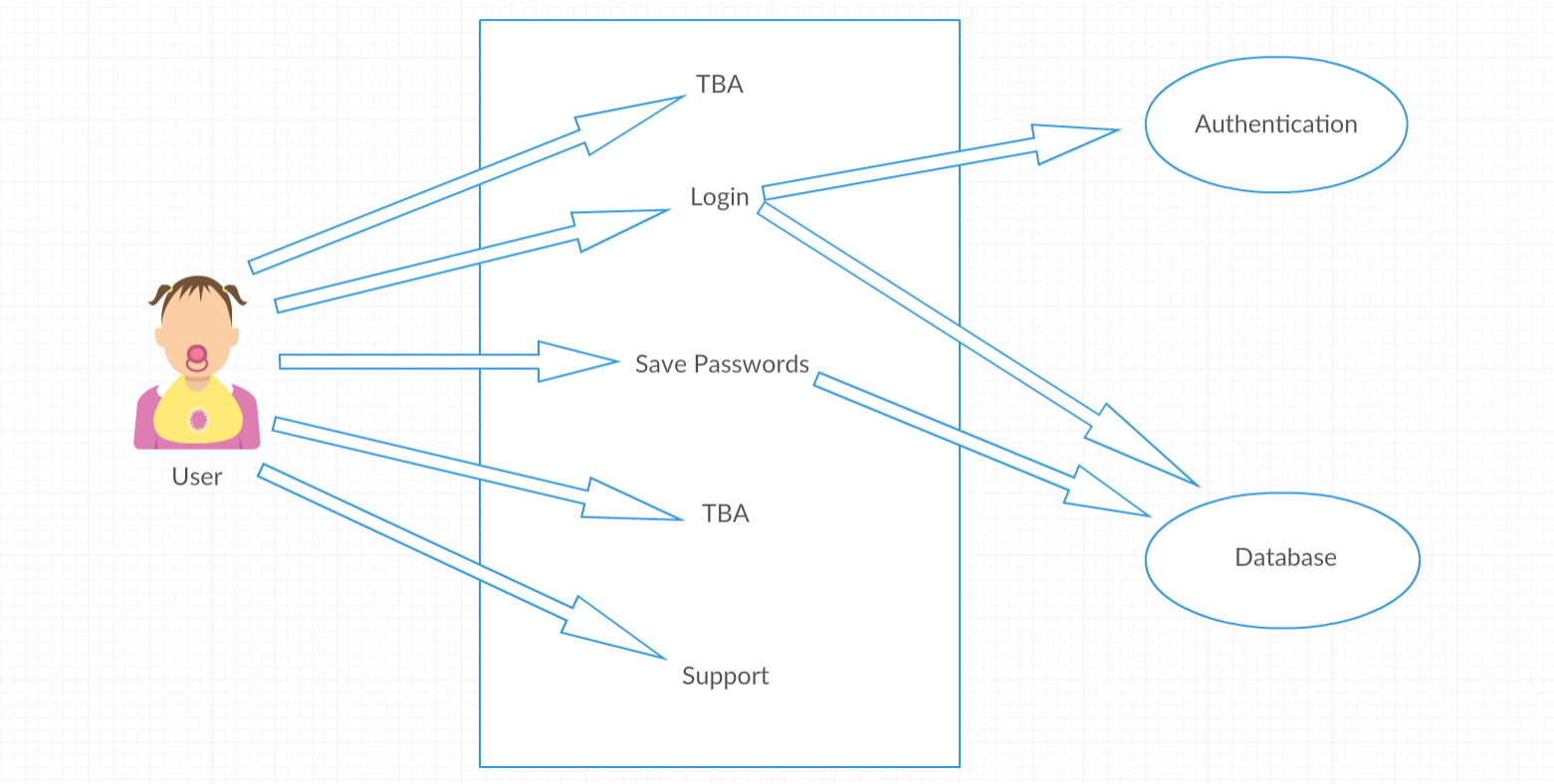
Exact method is to be determined.

**3.2.4 TBA**

**3.2.5 TBA**

## Behaviour Requirements

### Use Case View



user

# Other Non-functional Requirements

## Performance Requirements

TBD

## Safety and Security Requirements

The only safety concern at this time would be data loss from a 3rd party source. Since keeping your data safe will be our number one priority, we will continually work on our encryptions and make sure the passwords you enter will only be viewed by you.

(encryptions and authenticators will be provided upon further consideration.)

## Software Quality Attributes

**4.3.1 TBA**

**4.3.2 TBA**

# Other Requirements

Appendix A – Data Dictionary

Appendix B - Group Log

10/2/2018 – 2pm-5pm

10/3/2018 – 3pm-5pm