

**Bachelor of Computer Science**

**(Digital System Security)**

CSCI321 – Final Year Project

Project Proposal

**Project Particulars**

|  |  |
| --- | --- |
| Supervisor | Dr Ta Nguyen Binh Duong |
| Project Group | SS18/1F |
| Project Title | Two Factor Authentication |

**Project Team’s Particulars**

|  |  |  |
| --- | --- | --- |
| Student Number | Student Name | Email Address |
| 5363536 | Koh Hong Wei | hwkoh003@mymail.sim.edu.sg |
| 5710923 | Chua Han Ming Adler | hmachua002@mymail.sim.edu.sg |
| 5711356 | Ong Wei Hao | whong012@mymail.sim.edu.sg |

**Document Control**

Title: Project Proposal

Document Name: FYP\_ProjectProposal

**Distribution List**

|  |  |  |
| --- | --- | --- |
| Name | Title/Role | Where |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Record of Revision**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Revision Date | Description | Section Affected | Changes Made By | Version after Revision |
| 23/01/18 | Initial Setup of project proposal | - | Adler | 1.0 |
| 24/01/18 | Populating Data into project proposal | - | Team | 1.1 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[Project Team Structure 1](#_Toc504576566)

[Project Gantt chart 1](#_Toc504576567)

[1. Introduction 2](#_Toc504576568)

[1.1. Background 2](#_Toc504576569)

[1.2. Project Purpose 2](#_Toc504576570)

[1.3 Target Users 2](#_Toc504576571)

[1.4 Proposed Features 2](#_Toc504576572)

[2. Market Survey 2](#_Toc504576573)

[2.1. Market Research and Current Products 2](#_Toc504576574)

[3. Development Methodologies 4](#_Toc504576575)

[3.1 Waterfall Model 4](#_Toc504576576)

[3.2 Prototyping Model 5](#_Toc504576577)

[3.3 Agile Model 5](#_Toc504576578)

[3.4 Rational Unified Process 6](#_Toc504576579)

[References 6](#_Toc504576580)

# Project Team Structure

|  |  |  |
| --- | --- | --- |
| Name | Email | Roles |
| Koh Hong Wei | hwkoh003@mymail.sim.edu.sg |  |
| Chua Han Ming Adler | hmachua002@mymail.sim.edu.sg |  |
| Ong Wei Hao | whong012@mymail.sim.edu.sg |  |

The above team structure is implemented to clearly distinguish the area each member of the team is to focus on but it does not infer that he/she will be the only one involved in doing that task.

SmartSVN and a private GitHub repository will be use as version controlling and team collaboration tool. Each team member will have local repository which will then be merged with the central repository. All members will be working on different part of the project at a given point in time to prevent clashes when committing to central repository. All documents and source codes will be stored in this central repository.

Meeting minutes will be noted down during every meeting summarising the content of the meeting and what actions to be taken.

# Project Gantt chart

# 1. Introduction

## 1.1. Background

This project proposal was written to document the research and proposed idea for the Final Year Project entitled “Two Factor Authentication”. Impersonating others has always been an issue when it comes to cyber security. Password alone is no longer as effective as before as more and more ways of attacks, like brute force attack, will allow malicious attacker obtain a password.

The Final Year Project group is tasked to create a two factor authentication to enhance current security authentication that are already implemented in current applications, systems or devices.

## 1.2. Project Purpose

This project aims to provide the following to users:

* To enhance security on file management
* Provides 2 factor authentication to unlock files
* A secure vault that only allows intended users to access files

## 1.3 Target Users

According to our market research, we found our application suitable for the following group:

1. Employees in a workplace that wants to keep documents with different security level confidential from other employees using the same machine.
2. Student using school machine for assignment or homework and wants to keep it confidential from other students who might use the same machine after.
3. General public using shared machine with documents or information saved on such machine.

## 1.4 Proposed Features

Setting up an account

Locking of File/Folder

Unlocking of File/Folder

Secure Cryptographic Algorithm

Account Recovery

# 2. Market Survey

## 2.1. Market Research and Current Products

Below are a few ways of user authentication that are already in the market and example of products in the market that are using them.

### 

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Application | Platform | Description | Security | Features |
| 1Password | Android | This application remembers all your passwords for the user, the user would need a master password or using fingerprint authentication before being able to access the rest of the passwords | Login using master password or fingerprint authentication  Lock the app automatically to ensure data is protected, even if device is lost or stolen | Create strong, unique passwords for all online accounts  Fill usernames and passwords into websites and apps  Access information on all user’s mobile devices and computers  Share passwords securely with family or company  Unlock using fingerprint unlock |
| Authenticator Plus | Android | Authenticator Plus generates 2-step verification to protect accounts with your password and phone/tablet | Secure – 256-bit AES encryption and Pin lock for security  Automatic back/restore- accounts are automatically backed up to cloud  Fingerprint support – Unlock the app through fingerprint | Generates a 6 digit OTP after scanning QR code generate from facebook or other site. This OTP serves as a second authentication factor before being able to access to the account  Organize – group accounts with categories and re-order frequently used accounts to top |
| App Lock: Fingerprint Password | Android | A secure and easy-to-use application locker with pin, pattern or fingerprint password protection | Second authentication factor even though the user’s phone is unlock.  App Lock able to prevent others from opening locked apps, deleting or purchasing anything while on the user’s phone | Put a Pin, Pattern or fingerprint lock in front of any app on your phone like Facebook, Snapchat. When opening a protected app, App Lock will ask to confirm password the user have set to let the user in |
| Google Authenticator | iOS, Android, website | A software token that implements two-step verification using Time-based One-time algorithm and HMAC-based algorithm. | Google account (username and password)  Implements algorithm specified in RFC 6238 & 4226 | Uses QR code to register account  One google account to manage multiple 2FA applications  Password Managers  File hosting services |
| Hardware token |  | A keychain sized security token which generates OTP. Each time user logs in, user will press the button on the token to generate the OTP and the OTP will be displayed on the screen of the token. | Only generates OTP when user press on the button on the token | OTP is generated based on time and last for a certain amount of time before a new OTP will be generated upon request. |
| SMS OTP | Mobile with SIM card | SMS containing OTP will be sent to mobile phone registered. OTP sent whenever user log in with Username and Password | OTP is sent to registered mobile number. | OTP is sent via SMS to user.  OTP last a certain amount of time |
| Yubikey | NFC devices/ computer | Touch the button to trigger security based on public-key cryptography: works instantly, no need to re-type passcodes from a device — replacing SMS texts, authenticator apps, legacy tokens, and similar devices | Only allow accessing when the key is plugged in or detected by NFC. | Can be used for any accounts, by NFC or USB form. Key allows 2FA done when accessing account-based sites(fb/gmail) |

# 3. Development Methodologies

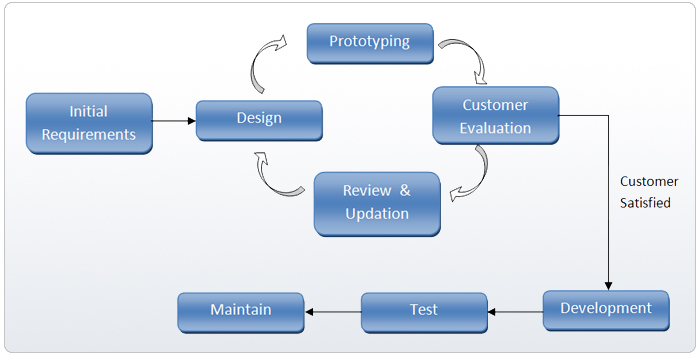
## 3.1 Waterfall Model

The waterfall model is a relatively linear sequential design development methodology. It tends to be one of the less iterative and less flexible approach to adopt. As its name suggest, it is a downwards model that flows through the different phases. By adopting this model, it is challenging and more costly to support changes once its phase has passed.



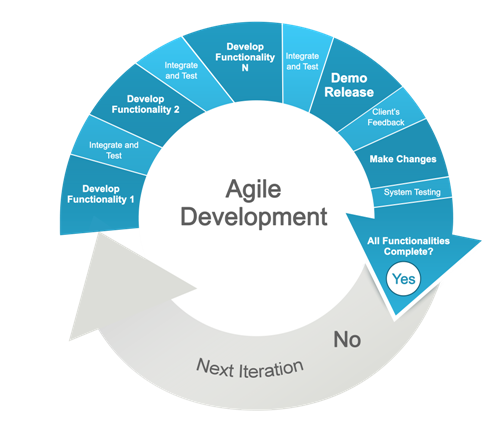
## 3.2 Prototyping Model

This model is based on requirements gathered from a user. A prototype is then built based on requirements gathered. Prototype is reviewed by the user an a new prototype is built again. This iteration repeats until the final design is confirmed and accepted by the user.



## 3.3 Agile Model

The initial planning and analysis is kept at a high level, just enough to outline the scope. After every iterations, an end product is released. At every iteration, product is refined.



## 3.4 Rational Unified Process

RUP is an iterative software development framework. It consists of 4 main stages:

* Inception

In this phase, the scope of the project is defined.

Requirements are gathered.

Mitigate the key risk items identified through analysis.

* Elaboration

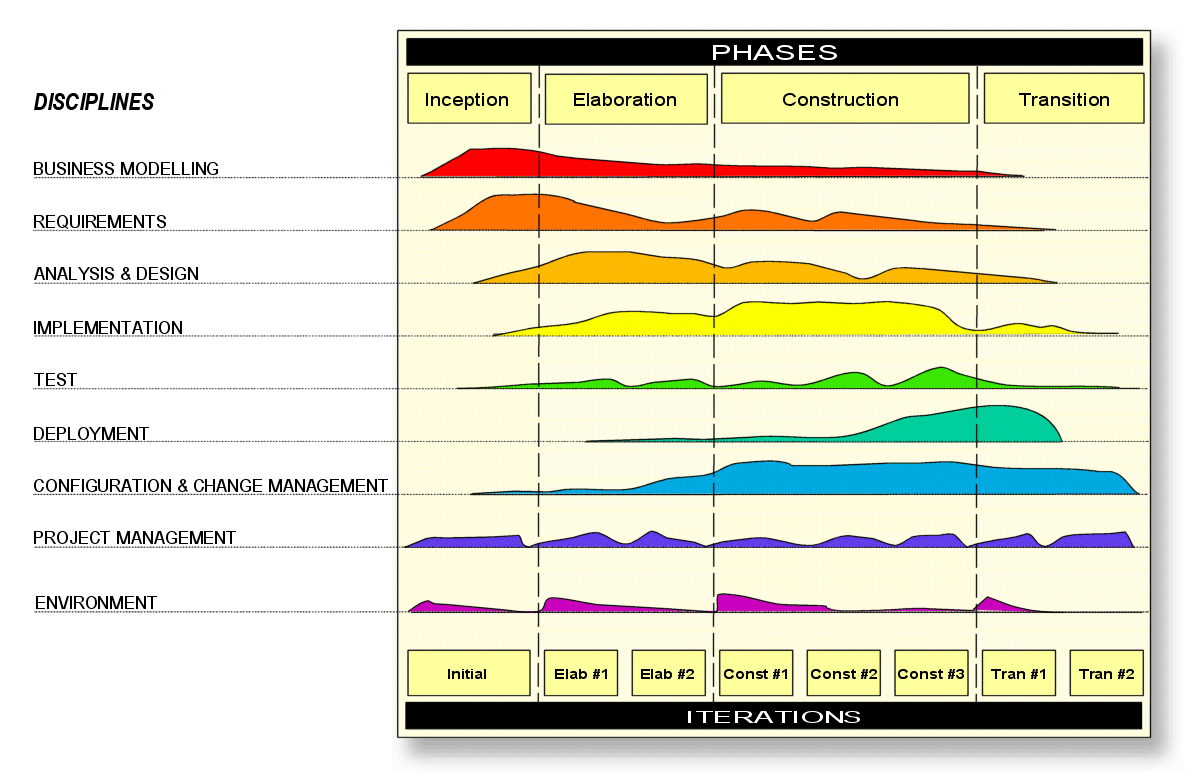
Develop detailed design of the system with diagram aids (use case diagram, activity diagram etc)

* Construction

In this phase, the actual product is being developed.

* Transition

Primary objective is to transit from development phase into production, making it ready for the market. This phase includes testing the system and providing training to its user.



# References

<https://en.wikipedia.org/wiki/Google_Authenticator#Pseudocode_for_one-time_password_(OTP)>

<https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/2fa-the-use-of-otp-token>

<https://www.yubico.com/products/yubikey-hardware/fido-u2f-security-key/#toggle-id-10>