Turtl
Use Case Specification

Submitted to:

Asst. Prof. Ma. Rowena C. Solamo
Faculty Member
Department of Computer Science
College of Engineering
University of the Philippines, Diliman

Submitted by:
Nikki Balugay
Ram Mangaoang
Brian Sy

In partial fulfillment of academic requirements
for the course
CS 191 Software Engineering I
of the
1st Semester, AY <2017-2018>

Unique Reference:

The documents are stored in the https://github.com/brianpesy/turtlios.

https://github.com/brianpesy/turtlios/tree/master/02%20-%20Requirements%20Engineering

Document Purpose:

This document is for further explaining different functionalities within the program to a more specific and clear extent while also maintaining readability as well.

Target Audience:

Businesses, clients, and those people who are interested in the whole project and how exactly we are going to go about designing the whole project are within the scope of our target audience.

Revision Control

History Revision:

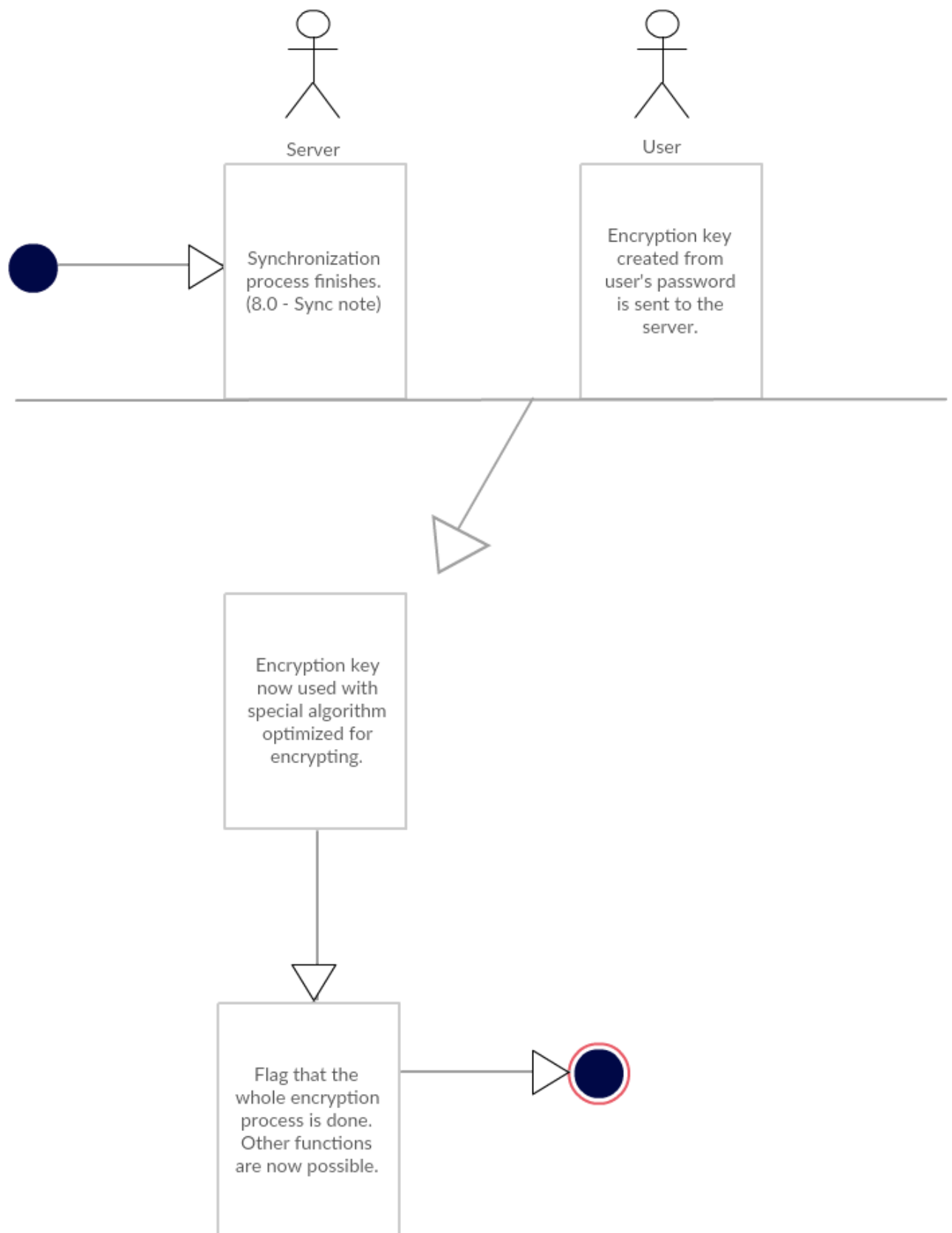| Revision Date	Person Responsible	Version Number	Modification
10/07/2017	Brian Nicholas Sy	1.0	Initial document, document purpose, target audience, use case name, description, preconditions, and diagram

Use-Case Name: 8.1 Encrypt Note

Description: Using the unique encryption key provided when a user makes a new account in Turtl, this process is for securing and keeping different notes private to the user. It kicks in after synchronizing in order to signal that it is now private and ready to share.

Preconditions: Synchronization process must be finished.

Flow of Events:

Scenario Name	Description
Scenario 1 (Basic Flow) The server synchronized the note and will now immediately encrypt.	1. The synchronization process finishes. 2. The encryption key is accessed by the user's client sending it over. 3. The encryption key is now used along with an algorithm used for encryption in order to keep data private. 4. After encryption, it will flag that the note is ready for sharing and is now private.

Activity Diagram of the Flow of Events:

Server

User

Synchronization process finishes. (8.0 - Sync note)

Encryption key created from user's password is sent to the server.

Encryption key now used with special algorithm optimized for encrypting.

Flag that the whole encryption process is done. Other functions are now possible.

Postcondition: The server will now hold the note, and it is saved.

Relationships: It extends 8.0 - Sync Note

Special Requirements:
Synchronization must be complete, user must have made an account (However, it is not possible to use the app without making the account itself. The app merely authenticates it.)