**Software Development Tools**

**laboratory work 1**

**Exercise 01 – SoftWare Requirments specification**

**Doc Type:** Requirements Description

**System:** Biometric System

**Revision:** V.0\_0

**Revision Date:** << to be filled in by course instructor to make relevant >>

**Requested by:** Komekbay Dinmukhammed, Amanzhol Azat

The Miri app is available for only devices which has faceID or touchID. Our app help users to protect their data with biometric system, it means that only the person who created security with his biometric data can access, no one else.

App divides into two type: Free and Paid. Free version has limited functions. In paid version functions will be more complex.

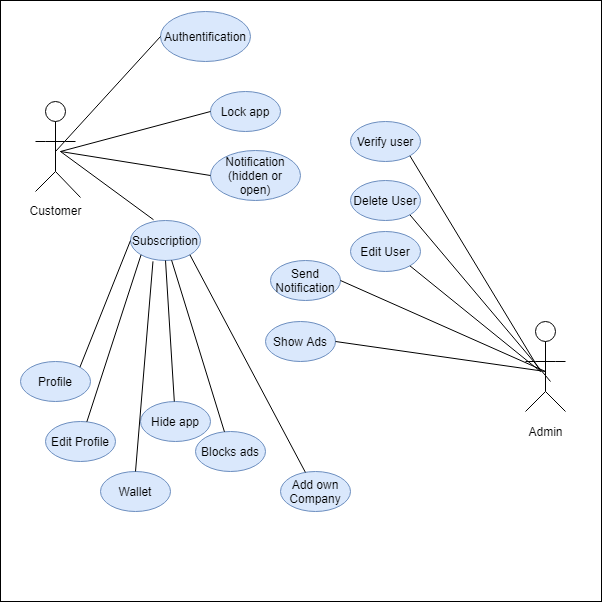
The Smart Biometric System must be able to provide the following services to the users:

1. It provides to customer high quality of protection. For example, in the regular protection if somebody knows your privacy data like(Pin-code), they can easily access to your personal information, but with Biometric System Security it’s impossible.

2. Convenience. Biometric System doesn’t need to input or remember any passwords and emails. Identifying the right individual is very simple when you know the person, or you have to recognize him or her from a few persons. But what will happen when you have to identify hundred or thousand individuals from thousands or millions of persons? It was challenging and even almost impossible. But biometrics technology allows to conveniently determine the right person from millions or authenticate the right one within less than a second.

3. Saving of Investment. Implementation of biometrics technology ensures the return on investment in a significant way. On the one hand, it saves the organization from unnecessary costs like ID card issuing, time theft, buddy punching, and ghost employees, and on the other had it increases accuracy and accountability to ensure higher ROI.

EXERCISE 02 – Identifying Use Cases



**EXERCISE 03 – CREATING USE CASE TEMPLATE**

| **ID** | **Description** | **Actors** | **Assumptions** | **Steps** | **Variations** | **Quality Concerns** | **Issues** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Sign Up | Users,  Application | Users finger or face | 1. User pass on the face control or finger print 2. User should agree with terms | * Re-pass validations | Security concerns:  Be able to show all sides of head and eyes should be open or press all sides of finger | Incorrect navigated face.  Closed eyes. |
| 2 | Hide app’s icon | Users, Application | User has paid version | 1. User press hide app’s icon  2. Create pin-code to enter app.  3. Re-enter pin-code to verify | 1.User re-entered wrong pin-code |  | Incorrect re-entered pin-code |
| 3 | Go to hidden app | Users, Application | User has pin-code | 1. Go to call section  2. Enter the pin-code start with \* and end with #  3.After entering pin-code call | 1.User don’t know pin-code  2. User don’t know ways go to hidden app | Security concerns: | Happens nothing if smth is wrong |
| 4 | Lock apps | Users, Application | User select the apps (only 5 apps if free version) | 1.User in app selects apps to lock  2.User press lock | 1. App is already locked  2.User has free version | Security concerns: | You don’t have a subscription for lock more apps |
| 5 | Unlock app | Users, Application | User has  Device which has faceID or touchID | 1.User open app  2.User confirm biometric data by faceID or touchID | Face is not match or finger is not match. | Security concerns:  User should show all sides of face | User’s face doesn’t match |