**Software Requirements Specification**

Mobile Electronic Training Jacket

Version 1.0 approved

Prepared by Jake Strojny, Kevin MacAllister, Tyler MacInnis, Robert Huard

NUWC

12/4/2016

**Table of Contents**

**1.** Product Overview................................................................................................................... 2

**1.1** Problem Overview................................................................................................................ 2

**1.2** Project Scope....................................................................................................................... 2

**2**. Overall Description................................................................................................................. 2

**2.1** Product Features................................................................................................................. 2

**2.2** User Classes and Characteristics........................................................................................ 3

**2.3** Operating Environment........................................................................................................ 3

**2.4** Design and Implementation Constraints.............................................................................. 3

**2.5** User Documentation............................................................................................................ 3

**2.6** Assumptions and Dependencies.......................................................................................... 3

**3.** Requirements Specifications.................................................................................................. 4

**3.1** Features -- Functional Requirements................................................................................... 4

**3.2** Nonfunctional Requirements................................................................................................. 5

**3.2.1** Performance Requirements............................................................................................... 5

**3.2.2** Safety Requirements.......................................................................................................... 5

**3.2.3** Security Requirements....................................................................................................... 5

**3.2.4** Software Quality Attributes................................................................................................. 5

**4**. External Interface Requirements............................................................................................. 6

**4.1** User Interfaces...................................................................................................................... 7

**4.2** Hardware Interfaces.............................................................................................................. 7

**4.3** Software Interfaces............................................................................................................... 7

**4.4** Communications Interfaces................................................................................................... 8

**5.** Other Requirements................................................................................................................ 8

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Date** | **Reason For Changes** | **Version** |
| Initial Creation | 12/4/2016 | Created the document | 1.0 |
|  |  |  |  |

# **1.** **Product Overview**

## **1.1** **Problem Overview**

The ability to give the sailors access to training and education information from their mobile devices while maintaining a level of security. Training and Education information is currently only accessible from desktop computers.

**1.2** **Project Scope**

A mobile Android application that will allow sailors to access their training, education, and career history from their mobile devices. This will make the information far more accessible, especially for offshore sailors and officers who need to see an enlisted sailor’s relevant credentials.

The mobile application will be able to download this information from a database and store it locally so that it can be accessed even while underway. The information will be protected by a new authentication system that does not consist of a username and password.

# **2.** **Overall Description**

## **2.1** **Product Features**

* Non-Username / Password based authentication system
  + Users login using something they know and something they have
* Downloads username information from online database and stores it locally
* Displays this information in a way that is easy to navigate and understand
  + Information will be accessible through a categorized menu structure

## **2.2** **User Classes and Characteristics**

**Enlisted Sailors**: Main users, will have access to all functionality associated with enlisted sailor rank and information, technical expertise will vary. Will potentially have diverse credentials and education.

**Officers**: Similar to Enlisted Sailors, except they access all functionality associated with Officer rank and information.

**NTMPS**: Non-sailor user who is in charge of training information. Catch-all class for those associated with app but are not sailors.

## **2.3** **Operating Environment**

**Environment**: Should function with or without an internet connection

**Hardware**: Mobile phones

**Operating System:** Android 6.0

## **2.4** **Design and Implementation Constraints**

**Policies:** Must be secure, users should only see their own records.

**Hardware Limitations**: Not all mobile devices come with the same features(Fingerprint scanners, camera quality, etc).

**Technologies**: SQLite, Java

**Tools**: Android Studio, SQLite. Git, GitHub

**Protocols**: Network Communications

**Programming Standards**: Follow Java design style.

## **2.5** **User Documentation**

Will include a short description of how to log in and set up your account.

## **2.6** **Assumptions and Dependencies**

**Assumption**: All phones have a unique IMEI and it is not easily duplicated. Assuming the sailor has an Android based smartphone. Assuming all phones have fingerprint scanners. Assuming the phone will have internet access for initial installation of application.

**Dependencies:** Android API on the phone.

# **3.** **Requirements Specifications**

## **3.1** **Features -- Functional Requirements**

**3.1.1** **Secure Login Functionality:**

3.1.1.1. Description

Login to access the ETJ on a mobile device without using a username and password.

Enlisted Sailors and Officers.

3.1.1.2. Functional Requirement

Fingerprint scanning using the Android fingerprint scanning API and encrypted password storing. Checking entered PIN against encrypted PIN stored in Android Keypass. Checking user entered IMEI against IMEI found in phone using TBD. Access external database for first time authorization TBD.

If the fingerprint does not match initial fingerprint, or pin does not match initial pin, reject authorization. Allow user to enter information again. On first login, if entered IMEI does not match

**3.1.2 Access to ETJ data:**

3.1.2.1. Description

Sailors and officers have access to view the ETJ data in a readable format.

3.1.2.2. Functional Requirement

Pull information from external database, parse through data to display on screen, display in a logical and clear manner to the user.  
  
If there is an error another attempt should be made to parse and display the data. If this second attempt fails then the user should be prompted to try again later or contact an admin about the problem.

**3.1.3 Download, store, and access encrypted ETJ data while offline:**

3.1.3.1. Description

Ability to download the enlisted member’s specific ETJ data in an encrypted format to be able to view and access while not connected to a network.

3.1.3.2. Functional Requirement

Store and retrieve database information in an encrypted format on local storage  
  
If a database connection can not be established the download attempt should be aborted and if possible a reason should be displayed to the user so that they can correct it, for example if they try to download without a network connection they should be informed that they need to be connected to the internet for initial download.

## **3.2** **Non Functional Requirements**

### **3.2.1** **Performance Requirements**

The Mobile Electronic Training Jacket should be able to access the database in a short period of time, not exceeding 30 seconds. Once the database has been accessed and the information transferred to the user, the user should be able to access specific parts of the data (classes completed, test grades, etc.) near instantaneously. The navigation of menus and subsequent display of data should be smooth and uninterrupted. Saving records to the phone should also not exceed 30 seconds.

### **3.2.2** **Safety Requirements**

Possible damage of this system is the unauthorized acquisition of training records. This can be damaging in many ways due to this information being confidential. Parties that have something to lose is the U.S. Navy, Naval Academies and Individual Sailors. Regulations that must be met to avoid this damage would be that records shouldn’t be able to be accessed without authorization, all records should be encrypted if saved, any online transfer of data should be encrypted and the web server should not dispense any data without authorization.

### **3.2.3** **Security Requirements**

The records obtained by the application should not be able to be viewed by anyone but the registered user. The information acquired and viewed by this app is personal and confidential military information so it is important that this requirement is met. This is the only requirement but since it is a web application there must be many safe-guards. One such safe-guard is a secure login to the system. The login will use a verification method that requires one thing that the person knows, and one thing that the person owns. Also, any records saved to the phone should be encrypted to avoid unauthorized offline record acquisition. The transfer of data from the server to the phone should be encrypted to avoid acquisition via interception. Finally, the app should time out and require the user to do the login verification method again if the user is inactive for a period of time.

### **3.2.4** **Software Quality Attributes**

Correctness : The app should be able to verify a user’s identity without using a username and password, access the correct training information correlating with that identity and save that information for offline use.

Flexibility : If the customer decides that the app should provide more functionality, we should be able to add/remove or modify any existing functionality to the system without it breaking.

Maintainability : Code in the app should be well documented and commented so that if a fault occurs late in the development it can be easily understood and fixed.

Portability : The app should have backwards compatibility to android phones and at the very least handle faults presented by older versions. Compatibility to other phone Operating Systems is not required for this product due to it’s nature as a prototype for a final product.

Robustness : Any faults in the app should be handled in such a way that the data handled by the app is still secure. Ideally, faults will never result in a crash, but if they do data should be secure from leaking. It is not required that records be saved in this crash since users are able to choose when to copy records to their phone, however, old records should not be broken due to a crash.

Reusability : Components for this app should be designed in such a way that they rely on abstraction instead of concretion. This would open up the higher level components to be re-used if desired by the customer in the final product. Since this is in essence a horizontal prototype we don’t expect the customer to re-use the exact code, but we would like it to be easy for them if they do.

Testability : Test cases for valid and invalid authorization should be developed. It is important that we uncover instances where invalid information is used to successfully access information and where valid information is used and is unsuccessful in accessing information. Something to watch out for here is SQL injection since our product is heavily reliant on SQL.

Usability : The app should be easy to use and easy to learn. Logging in, navigating menus and accessing/saving data should be self-explanatory. If possible, functionality should be maintained for users who have disabilities.

# **4.** **External Interface Requirements**

## **4.1** **User Interfaces**

**Layout Constraints:** Data must be neat and easily navigable on a variety of small device screens.

**Style**: Layout and Visuals to be determined

**Menu Buttons Description**

* Sign In (Appears on Login Screen)
* Sign Out (Appears in Main Menu)
* Refresh (Appears in Main Menu)
* Personal Information Button (Appears in Main Menu)
  + Awards
* Enlisted Sailor Skill Info (Appears in Main Menu if user is Enlisted Sailor)
  + Navy Enlisted Classifications
  + Enlisted Language Skills
  + Enlisted Career History
* Officer Skill Info Button (Appears in Main Menu if user is an Officer)
  + Navy Officer Classifications
  + Officer Language Skills
  + Officer Career History
* Credentials (Appears in Main Menu)
  + Trainings
  + Qualifications/Certifications
  + ASVAB/BTB

The buttons that appear in the Main Menu will bring the user to a new page that displays their sub buttons. These sub buttons will then bring the user to another new page that displays the relevant information. This keeps all information within two clicks of the home page.

## **4.2** **Hardware Interfaces**

**Device**: Smartphone

**Interface**: Touch screen

**Interface:** Fingerprint scanner

## **4.3** **Software Interfaces**

The product will connect to an external server from the phone. Authentication data is sent securely from the phone to the server, and if accepted, the server securely sends the correlating training info back to the phone. The server generates this data by querying a SQLite database local to it. Once the data is on the phone, the phone can access certain parts of it by navigating menus on the screen. A record can be saved to the phone, which should be encrypted, and the phone can then read from that record at a later time if the phone is offline.

The product will take advantage of the Android SDK for it’s functionality, we will be using the fingerprint scanner technology on the Android as well.

## 

## **4.4** **Communications Interfaces**

All data transfer, namely authentication information sent to the server and training record information sent to the app, will be encrypted. The app will use a public key infrastructure to ensure that the data sent to and from the server are properly encrypted. We will also be using SSL to ensure a secure socketing. Depending on the success and security of this interface we may change our protocols to suit our needs better.

# **5.** **Other Requirements**

* Reliability will be a concern. The mobile app should perform smoothly for Android version 6 and newer. The presentation of information is a main component of the requirements and should be uniform and well laid out to be easily readable on a mobile device.
* The mobile app will have the flexibility or modularity to accommodate different authentication processes that are designed. Different and creative authentication methods are being developed to move away from the standard username and password authentication processes. Keeping them modular will make it easy to integrate one or another.
* Database files that are downloaded will be encrypted. Individual’s database files are currently planned to be stored on their personal smartphone to accommodate the ETJ’s information offline.
* The menu level structure will be kept to one sublevel and clustered by like categories. Maintaining a shallow submenu structure will allow for more intuitive navigation through the menu options.
* Automatic inactivity logoff will provide another level of security. A disconnect mechanism will be utilized in the instances the user leaves the app unattended to help preserve the integrity of the information stored.

Appendix A: Glossary

**ETJ**: Electronic Training Jacket - The application we are building to store and list users information

Appendix B: Analysis Models

<Optionally, include any pertinent analysis models, such as use-case models, data flow diagrams, class diagrams, state-transition diagrams, or entity-relationship diagrams.>

Appendix C: Issues List

**TO BE DECIDED:**

* How the data will be laid out on the screen
* How we initially set up authorization to access data
* How we access the database for initial pull of data
* If we use IMEI as part of authentication how do we access it(Android API does provide a few methods)