Department of Computer Science & Engineering
The University of Texas at Arlington

System Requirements Specification
CSE 4316: Senior Design I
Fall 2023

ESMS
Encrypted SMS

Jacob Holz
Nam Huynh
Gilbert Lavin
Landon Moon
Parker Steach

Revision History

Revision	Date	Author(s)	Description
0.1	9.27.2023	JH	document creation
0.2	10.16.2023	ALL	complete draft

CONTENTS

List of Figures

1 Product Concept

This section describes the purpose, use, and intended user audience for ESMS. ESMS is a system that uniquely leverages SMS as its communication protocol, which in turn eliminates the need for proprietary relay servers. Users of ESMS will be able to communicate securely without the risk of back-doors in relay servers, as the reliance on SMS ensures that there are no relay servers accessible to parties capable of decrypting communications. Users of ESMS will also be able to decide on the level of security they want to use and be informed about the nature of the methods they are using.

1.1 Purpose and Use

ESMS should allow the user to send text-based messages to other users of the application. These communications should be encryptable to multiple levels of security based on settings selected by the user. ESMS should allow the user to easily switch between conversations in a way similar to existing messaging applications. The user should be able to use the application to learn about several communication security concepts such as encryption, key-exchange, cracking encryption, and older cryptographic methods.

1.2 Intended Audience

The intended audience of ESMS is anyone with an interest in communication privacy. ESMS should be accessible to general audiences as far as ease of use and functionality are concerned. ESMS will be especially valuable to a user interested in having control over the systems used to secure their communications. It is intended for general use as a stand alone communication application.

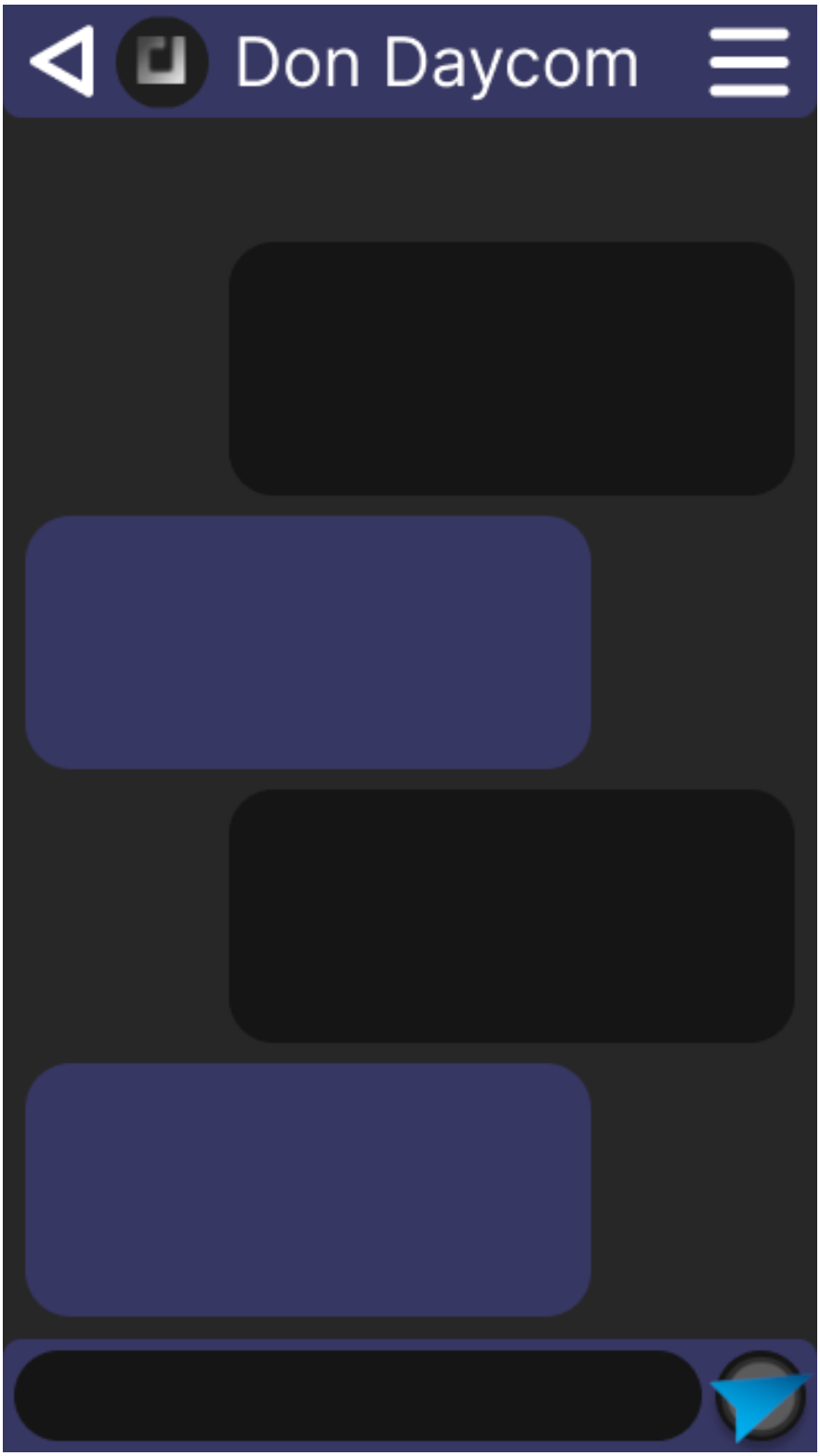

Figure 1: Chat Screen Conceptual Drawing

2 PRODUCT DESCRIPTION

This section provides the reader with an overview of the ESMS system. The primary operational aspects of ESMS, from the perspective of end users, are defined here. This application will have a messaging system for the user, that will encrypt their messages. Users will be able to select an encryption method but the default will be a secure industry standard protocol. Each message will be sent and received through the phone's SMS service, with an express avoidance of internet services. The phone's SMS service will be used as an insecure channel that encrypted data will be transmitted through.

2.1 FEATURES & FUNCTIONS

ESMS is built on top of SMS and will implement a secure interface similar to common phone SMS components. These features are the contacts, and conversations implementations through ESMS. The look and feel of these components follow industry standards from other messaging applications. Figure 1 is a sample UI for a conversation. This diagram shows the messaging history in the center with a text field to send messages at the bottom. Additionally, there is a hamburger button in the top right that is intended for chat settings. A back button will be included to go back to a contacts list. The conversation history and contacts list will depend on the phone's data.

2.2 EXTERNAL INPUTS & OUTPUTS

CDE[1]	Name	Description	Use
1	User Text	User will type a message to be encrypted and sent	Messaging
2	Incoming Text	User will receive encrypted messages from contacts	Messaging
3	SMS API	The app will utilize the Android API to perform SMS messaging	Phone Usage
4	Contacts information	The app will utilize the Android API to show contact information	Phone Usage
5	Messaging history	The app will utilize the Android API to show messaging history	Phone Usage

Table 2: Overview of External Inputs & Outputs

2.3 PRODUCT INTERFACES

The end-user will have 3 main interfaces to move between. [Figure 2] On the Contacts View the user will be able to see all of their contacts. This will include the contact's profile picture and profile name. When the user taps on a thread, they will be brought to the messaging view for that contact. [Figure 3] The Messaging View will allow the user to view previous messages and send new messages to the selected thread. This Page will utilize the User Text, Incoming Text, and SMS API external input and outputs. [Figure 4] The Settings and Properties View will allow the user to set preferences about the app, including choosing which encryption method they would like to use. Another preference choice will be color scheme. There will be application wide and message thread specific settings. Contact properties will also be accessible through the properties of a specific thread as it is attached to that contact.

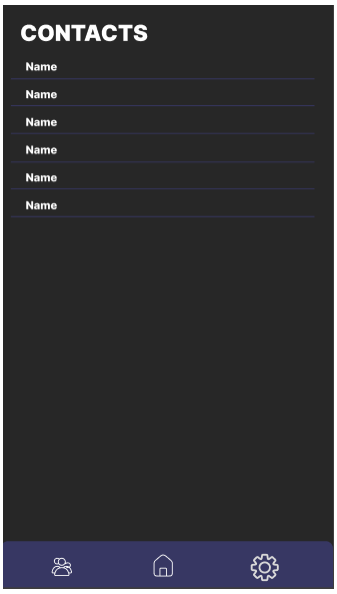

Figure 2: Contacts View

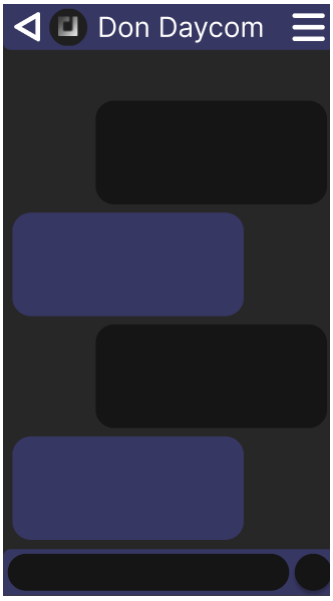

Figure 3: Messaging View

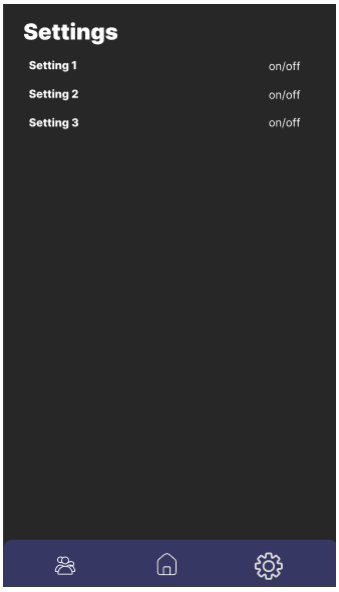

Figure 4: Settings and Properties View

3 Customer Requirements

3.1 Standard Messaging UI/UX

3.1.1 Description

To ensure an intuitive user experience, the ESMS interface will adopt a design paradigm consistent with prevailing messaging applications. This includes the incorporation of contacts and conversation sections, essential for a seamless messaging experience.

3.1.2 Source

The customer

3.1.3 Constraints

While the UI/UX design will be influenced by existing messaging applications, it will not replicate any specific components directly. Instead, it will emulate the overarching design themes common to these applications.

3.1.4 Standards

N/A

3.1.5 Priority

High

3.2 Encryption

3.2.1 Description

The application will employ a comprehensive encryption framework. Users will have the option to choose from a preselected set of encryption algorithms, ensuring the confidentiality and integrity of their messages.

3.2.2 Source

The customer

3.2.3 Constraints

The available encryption methods will be restricted to those supported by the chosen library.

3.2.4 Standards

TBD

3.2.5 Priority

Critical

3.3 Messaging

3.3.1 Description

Users can send and receive messages with other application users.

3.3.2 Source

The customer

3.3.3 Constraints

The application will support the exchange of text messages only, excluding file transfers.

3.3.4 Standards

N/A

3.3.5 Priority

Critical

3.4 Contacts

3.4.1 Description

Users can add individuals to their in-app contact list, enabling message exchanges.

3.4.2 Source

The customer

3.4.3 Constraints

Contact additions are limited to individuals who have the application installed. Encrypted messaging will only be feasible between application users.

3.4.4 Standards

N/A

3.4.5 Priority

Critical

3.5 Local Storage

3.5.1 Description

Users have the option to store data locally on their devices. To ensure user trust, no messages sent or received will be stored in our database.

3.5.2 Source

The customer

3.5.3 Constraints

Storing a significant number of messages might consume a substantial amount of local storage, potentially causing issues for users with limited available space.

3.5.4 Standards

N/A

3.5.5 Priority

Critical

3.6 Color Customization

3.6.1 Description

Users will have the flexibility to customize the application color using an RGB palette. This feature aims to enhance user personalization without requiring manual RGB value calculations.

3.6.2 Source

The customer

3.6.3 Constraints

Customization capabilities might be limited to specific interface elements.

3.6.4 Standards

N/A

3.6.5 Priority

Low

4 Packaging Requirements

The product will be packaged as an Android Application Package (APK). Users will obtain the app from the Google Play Store. Upon successful installation, an application icon will be accessible from the device's home screen, enabling users to launch the application. This product exclusively consists of software components, without any associated hardware.

4.1 APK Delivery

4.1.1 Description

The ESMS application is designed for Android devices, necessitating its packaging as an APK for compatibility and distribution purposes.

4.1.2 Source

The application is open-source and will be hosted on GitHub, facilitating direct cloning. Additionally, for user convenience, it will be available for download from the Google Play Store.

4.1.3 Constraints

The delivery method for the application is restricted to the APK format, ensuring compatibility with Android devices.

4.1.4 Standards

The application will support devices with Android 13 (API 33) and above. It will adhere to the standards and guidelines set by the Google Play Store. [1]

4.1.5 Priority

Critical

5 Performance Requirements

Because ESMS is a mobile app, there are a couple of performance requirements that apply to all mobile applications. Additionally, because ESMS is dependent on the phone's SMS system, considerations to message delays and encryption power consumption need to be taken.

5.1 Responsive UI

5.1.1 Description

As a mobile application that interacts with users, in order to provide a smooth and easy use of ESMS, ESMS shall not hang or freeze for more than half a second.

5.1.2 Source

Customer

5.1.3 Constraints

Phone processing power can change between phone models. This variety constrains ESMS to be usable on phones with low processing power.

5.1.4 Standards

N/A

5.1.5 Priority

High

5.2 Responsive Startup

5.2.1 Description

As a mobile application that interacts with users, in order to provide a smooth and easy use of ESMS, ESMS shall not take longer than 5 seconds to cold start the application. Cold start means that the application isn't already running and its state isn't saved in memory.

5.2.2 Source

Customer

5.2.3 Constraints

Phone processing power can change between phone models. This variety constrains ESMS to be usable on phones with low processing power.

5.2.4 Standards

N/A

5.2.5 Priority

High

5.3 Messaging Overhead Delays

5.3.1 Description

As an application that is used to message other users, customers expect a message to be sent in a timely manner if possible. ESMS shall not add any more than 10 seconds to send and encrypted message.

5.3.2 Source

Customer

5.3.3 Constraints

A phone's SMS capabilities might temporarily be unable to send a message.

5.3.4 Standards

N/A

5.3.5 Priority

High

5.4 Power Requirement

5.4.1 Description

As a mobile application, phones have a limited amount of battery life. ESMS shall not cause a noticeable increase in power consumption when compared to their phone's SMS message application.

5.4.2 Source

Customer

5.4.3 Constraints

A phone's battery life and SMS optimizations can cause power consumption to vary between devices. The phone with the worst power performance shall be used as a comparison.

5.4.4 Standards

N/A

5.4.5 Priority

Medium

6 Safety Requirements

As a software product, physical safety impact is not especially difficult to minimize. There are dangers related to the development location, but not any of the processes to be completed during development or by the customer.

6.1 Laboratory equipment lockout/tagout (LOTO) procedures

6.1.1 Description

Any fabrication equipment provided used in the development of the project shall be used in accordance with OSHA standard LOTO procedures. Locks and tags are installed on all equipment items that present use hazards, and ONLY the course instructor or designated teaching assistants may remove a lock. All locks will be immediately replaced once the equipment is no longer in use.

6.1.2 Source

CSE Senior Design laboratory policy

6.1.3 Constraints

Equipment usage, due to lock removal policies, will be limited to availability of the course instructor and designed teaching assistants.

6.1.4 Standards

Occupational Safety and Health Standards 1910.147 - The control of hazardous energy (lockout/tagout).

6.1.5 Priority

Critical

6.2 Epileptic Seizure and Eye Strain Prevention

6.2.1 Description

ESMS will take measures to prevent eye strain from the use of ESMS. Additionally, ESMS will avoid any situation that may cause an epileptic seizure from rapidly flashing sections of the screen.

6.2.2 Source

Customer

6.2.3 Constraints

People with epilepsy may not be used to test the potential of epileptic seizures from the ESMS app.

6.2.4 Standards

N/A

6.2.5 Priority

Medium

7 Security Requirements

Our team is developing a platform that relies on SMS as its communication foundation. We recognize the inherent vulnerability to man-in-the-middle attacks over this medium. In light of this, and mindful of our commitment to security, our application will offer a comprehensive array of features designed to fortify the simplicity of SMS communication. These features will include multiple encryption options, allowing users to select the type of protection that aligns with their security preferences. Furthermore, all messages will be securely stored within the device's internal storage, benefiting from encryption protocols integrated into the phone's native systems, ensuring the utmost data security for our users.

7.1 Use of Safe Encryption Algorithms

7.1.1 Description

Many encryption algorithms exist, so the user must be able to use the most secure algorithms as are feasible for inclusion. There must be a framework for installing new encryption algorithms.

7.1.2 Source

The customer

7.1.3 Constraints

There will only be a limited number of algorithms initially. Mobile devices are not as powerful as purpose built cryptography machines, so the encryption strength will be unavoidably limited, but still rather high due to the mathematical fortitude of modern algorithms. No algorithm intended for security may be manually implemented by the team as cryptography is beyond the scope of the project timeline.

7.1.4 Standards

There are Standard algorithms that are approved and used in industry.

7.1.5 Priority

Critical

7.2 Cache Decryption Screen

7.2.1 Description

Users may toggle cache encryption with a pass-code provided on startup to heighten the security of stored data.

7.2.2 Source

The customer

7.2.3 Constraints

Up to one user defined password will be used to decrypt the cache.

7.2.4 Standards

Standard high security encryption algorithms for cache encryption

7.2.5 Priority

Medium

8 Maintenance & Support Requirements

Maintenance and support requirements outline the provisions and activities necessary for the ongoing upkeep and user support of the product post-release. This section highlights essential considerations for ensuring product reliability, addressing user feedback, and ensuring continued compatibility with technological advancements. Here, we detail the approaches and methodologies we will employ to maintain and enhance the ESMS application post-deployment.

8.1 Encryption Algorithms Maintenance

8.1.1 Description

To ensure robust and up-to-date encryption capabilities, routine tests will be conducted to validate the proper functionality of implemented encryption methods. Additionally, as encryption standards evolve, we will introduce new algorithms to bolster security. Compatibility with existing encryption libraries will be continuously verified.

8.1.2 Source

Development Team

8.1.3 Constraints

As hardware improves, older devices will no longer be able to perform the required computation in a reasonable time for more advanced encryption algorithms. This will lead to the phasing out of support for older devices as the encryption algorithms they can support become less secure.

8.1.4 Standards

N/A

8.1.5 Priority

High

8.2 Bug Fixes and User Feedback

8.2.1 Description

Regular monitoring of user feedback and reported bugs will be conducted on a monthly basis. This approach ensures the application performs as expected and allows for timely resolution of any identified issues.

8.2.2 Source

Development Team

8.2.3 Constraints

Detecting bugs can be contingent on user reports. Some feedback may be ambiguous or lack the detailed context required for immediate resolution.

8.2.4 Standards

N/A

8.2.5 Priority

High

8.3 UI Optimization

8.3.1 Description

The ESMS application's user interface (UI) will undergo periodic optimizations to maintain alignment with contemporary design trends in messaging applications. Feedback-driven refinements and proactive updates aim to deliver a consistent and user-friendly experience.

8.3.2 Source

Development Team

8.3.3 Constraints

While our goal is to provide a universally appealing UI, we acknowledge that design changes might not resonate with all user preferences. When feasible, the ability to return to the old UI should be maintained. If systems for this are put in place at the time of creation, it will be more consistently feasible.

8.3.4 Standards

N/A

8.3.5 Priority

Medium

9 Other Requirements

ESMS will allow users to change the type of encryption used during messaging, this will require a modular setup to allow multiple encryptions to be added over time.

9.1 Encryption Modularity

9.1.1 Description

The app will be constructed in a way that allows for multiple encryption methods. This allows for flexibility for knowledgeable users to have more diverse choices.

9.1.2 Source

Customer.

9.1.3 Constraints

Need to have at least one encryption method.

9.1.4 Standards

N/A

9.1.5 Priority

Medium

10 FUTURE ITEMS

This section reiterates all requirements designated with a priority of 5. Although these requirements have been discussed and documented, they will not be addressed in the prototype version of the product due to constraints such as budget, time, skills, technology, and feasibility.

REFERENCES

[1] Developer policy center. https://play.google.com/about/developer-content-policy/.