Nuslack Software Requirements Specification

Section 1: Introduction

1.1 Purpose

This document serves as the single source of requirements for the application Nuslack. It contains a detailed account of the purpose, components and requirements of the software. It details what the software will do and the standards it must adhere to.

1.2 Scope

Nuslack is a server-based application that allows the secure sharing of messages between individuals and groups. It supports the creation of groups of users that are overseen by moderators who have the power to add/remove users. Users are authenticated by third-party services with an option to require additional authentication to access group content.
Users can customize their friend circles, interact with them using a variety of media types (text, video, audio, images, etc.), follow other users, and build conversations. The application supports the English, Spanish and French character sets.
In addition, users can customize their privacy experience with options to modify lifetime of messages, view forwarding history of a message, end-to-end encryption, and the ability to delete messages.
Enforced by the US government is CALEA, a rule on communications. The application is obligated to provide an unaltered copy of the conversations involving parties that get a subpoena, along with their IP addresses.
Nuslack aims to provide a secure, yet featureful experience for communication via the Internet.

1.3 Audience

This document is intended to be viewed internally but any parties interested in the development of Nuslack can have access to it.

Section 2: Overall description

2.1 Product perspective

This system is designed to be deployed to a remote server that can be accessed by any user who has an internet connection. Its use does not require a specific operating system or user interface, only a browser capable of rendering HTML and sending/receiving HTTP requests/responses.

2.2 Product functions

The high level functions of this system are:

- The ability for an individual to register as a user
- The ability for a registered user to form and join groups of other users/groups
- The ability for a registered user to send secure messages to other users/groups
- The ability for a registered user to search for other users/groups
- The ability to ensure CALEA compliance

2.3 User characteristics

Our product is open to all kinds of users. Students may use it for chit-chat and they probably would keep in a free service tier or lower level tier as they might not need some complicated encryption for their communications. Companies may use it for business purposes and probably they care more about the security of their communications.

2.4 Constraints

(a) Regulatory policies:
    (i) Full CALEA compliance.
(b) Standards:
    (i) SRS adheres to IEEE standard.
(c) Hardware Limitations:
    (i) Client Side:

(1) Any device with a user-agent capable of sending HTTP requests, and processing responses with CSS layout information (as well as standard sub-resources).

(ii) Server Side:

(1) Server must be capable of running a java application on a linux OS

(d) Interfaces to other Applications:

(i) Processing HTTP requests, and responses from unaffiliated services.

(e) Parallel operation:

(i) No constraints

(f) Audit functions:

(i) No constraints. (no salaries paid, no income collected)

(g) Control Functions

(i) No constraints.

(h) Higher-Order Language Requirements:

(i) Java8 based server

(ii) Junit4 Testing

(iii) Jenkins

(iv) SonarQube

(i) Signal Handshake protocols:

(i) No Constraints

(j) Reliability Requirements:

(i) None

(k) Criticality of application:

(i) Non-critical

(l) Safety and security considerations

(i) At least basic encryption will be available to clients.

2.5 Assumptions and dependencies

We assume all of our users have a device that has Internet access as our app only relies on a stable Internet connection. And users should be able to click and type with the device. We don't think our product needs really high level hardware.

Section 3: Specific requirements

3.1 Users and Groups

#	Type *	Priority	Requirement
1.1	F	1	The system shall allow individuals to register and login as users
1.2	F	1	The system shall allow users to form groups with other users
1.3	F	1	The system shall allow users to form groups of other groups
1.4	NF	1	A group shall require at least one user to be a moderator
1.5	NF	1	Any member of a group shall be able to invite other users or groups to join the group
1.6	NF	1	Only a moderator of a group shall be able to remove a user from that group
1.7	NF	1	A group shall not be able to be disbanded except by a moderator of the group
1.8	NF	2	Users shall be able to validate login through third party APIs, which may include Google, LinkedIn, or Facebook
1.9	NF	2	Users shall be able to be part of 0, 1, or many groups
1.10	NF	2	When a group (group A) is added to another group (group B), and a message is sent to group B, all users who are members of group A and group B shall receive the message
1.11	NF	2	A moderator of a group shall be able to decide whether or not they need to approve new users joining the group
1.12	NF	2	A moderator of a group shall be required to approve another group joining a group
1.13	F	2	A moderator of a group, and only a moderator shall be able to set a password for that group.
1.14	NF	2	If a password is set for a group, that password must be correctly entered by a user who is a member of the group before they can see messages sent to the group
1.15	F	3	The system shall allow a user to select filters on incoming messages
1.16	NF	3	Filters may include any combination of: vulgar language, sexual language, or bigotry
1.17	NF	3	The system shall allow a user to decide whether filtered content is (1)not sent to them, (2)is censored for filtered content, or (3)is flagged as containing filtered content, but not actually filtered

1.18	F	3	The system shall allow a user to send private messages.
1.19	NF	3	Private messages shall be encrypted during transport and storage.
1.20	NF	3	Private messages shall not be able to be forwarded
1.21	NF	3	Private messages shall not be able to be copied
1.22	F	3	The system shall allow a user to schedule events and invite other users
1.23	NF	3	When a user is invited to an event by another user, that user shall be able to respond to the invitation to indicate whether or not they will attend
1.24	F	3	The system shall allow a user to create keywords in messages by prepending a '#' character to the message
1.25	NF	3	A user shall be able to search a message's history for keywords
1.26	F	3	The system shall allow users to associate picture icons with their accounts
1.27	NF	3	Users shall be able to choose which icons are visible to to which other users, i.e. User A shall be able to choose to show Icon A to User B and User C while showing Icon B to User D and User E.

3.2: Communicating

#	Type *	Priority	Requirement
2.1	F	1	Users shall be able to search for other users
2.2	F	1	Users shall be able to search for groups
2.3	F	1	User shall be able to send messages to other users
2.4	F	1	User shall be able to send a message to a group
2.5	F	1	User shall be able to add another user as a friend
2.6	F	1	User shall be able to reply to a message in a group where they are a member
2.7	F	1	Delivered messages shall contain time stamps depicting the sender's local time.
2.8	F	1	Users shall be able to reply to the entire group
2.9	F	1	Messages shall be stored permanently
2.10	F	1	Character sets in English/Spanish/French shall be supported
2.11	F	1	Users shall be able to include other media (i.e. emojis, emoticons, tunes/recording, video) in the messages
2.12	F	2	Users shall be able to follow other users and receive updates about a change

			in status
2.13	F	2	User shall be able to see who is connected (online/offline/do not disturb) in their friend circle
2.14	F	2	User may be able to forward a message to another user
2.15	F	2	The system shall be able to record message forwarding history
2.16	F	2	User shall be able to start a conversation by replying to a specific message in a group
2.17	F	2	The system shall deliver messages to a user in the order in which they were sent, when the user is online
2.18	F	2	Users shall be able to recall/delete a message
2.19	NF	2	If a user deletes a message before it is seen, then it shall never be seen
2.20	F	2	Messages may be encrypted
2.21	F	2	Messages sent to a User when the User is offline shall be received by the user in the order in which they were sent when the user next signs in
2.22	F	3	Users may be able to turn off the ability to be found (hidden mode)
2.23	F	3	User shall be able to see a fixed number of past messages in a conversation (the number of messages may vary depending on service tier of the user)
2.24	F	3	Users may be able to only reply to the sender or a subset of the group
2.25	F	3	Message may be translated into the receiver's default language
2.26	F	3	Character sets in non-English languages may be supported

3.3: The Government

#	Type *	Priority	Requirement
3.1	F	1	Service shall be able to provide a copy of all messages sent to and by a defined person of interest, exactly as they are received (even if they are encrypted), for a predefined fixed length of a subpoena.
3.2	F	1	Users with a subpoena will not be informed, specifically by requests for the receivers of their sent communications, requests for which users are online, requests for which users are connected in their circles, requests to find a specific user/group, requests for users they follow/are followed by, and requests for the members of any group (if such requests are supported), of this change of state.
3.3	F	1	Service shall be able to provide a copy of all logged communications received/sent by the user with a subpoena, exactly as they are stored (even if this is in an encrypted state).
3.4	F	3	Messages provided by a subpoena request will additionally contain the IP address (as we receive it) of both the sender and the receiver of said message.

3.4 Other

#	Type *	Priority	Requirement
4.1	F	3	The system shall allow a user to select filters on incoming messages
4.2	NF	3	Filters may include any combination of: vulgar language, sexual language, or bigotry
4.3	NF	3	The system shall allow a user to decide whether filtered content is (1)not sent to them, (2)is censored for filtered content, or (3)is flagged as containing filtered content, but not actually filtered
4.4	F	3	The system shall allow a user to send private messages.
4.5	NF	3	Private messages shall be encrypted during transport and storage.
4.6	NF	3	Private messages shall not be able to be forwarded
4.7	NF	3	Private messages shall not be able to be copied
4.8	F	3	The system shall allow a user to schedule events and invite other users
4.9	NF	3	When a user is invited to an event by another user, that user shall be able to respond to the invitation to indicate whether or not they will attend
4.10	F	3	The system shall allow a user to create keywords in messages by prepending a ‘#’ character to the message
4.11	NF	3	A user shall be able to search a message’s history for keywords

* F is for Functional; NF is for Nonfunctional