Secure Chat Requirements Specification

Version 1.0

October 16, 202020

**Team Members:**

**Brendan Curran**

Table of Contents

[1. Executive Summary 3](#_Toc53770177)

[1.1 Project Overview 3](#_Toc53770178)

[1.2 Purpose and Scope of this Specification 3](#_Toc53770179)

[2. Product Description 3](#_Toc53770180)

[2.1 Product Context 3](#_Toc53770181)

[2.2 Primary User Characteristics 3](#_Toc53770182)

[2.3 Assumptions 3](#_Toc53770183)

[2.4 Constraints 3](#_Toc53770184)

[3. Requirements 4](#_Toc53770185)

[3.1 Functional Requirements 4](#_Toc53770186)

[3.2 Non-Functional Requirements 4](#_Toc53770187)

[3.2.1 Operational Requirements 4](#_Toc53770188)

[3.2.2 Performance 4](#_Toc53770189)

[3.2.3 Security 4](#_Toc53770190)

[3.2.4 Cultural/Political 4](#_Toc53770191)

[3.3 System Interface/Integration 4](#_Toc53770192)

[3.3.1 Network and Hardware Interfaces 4](#_Toc53770193)

[3.3.2 Systems Interfaces 4](#_Toc53770194)

[4. Use Cases 5](#_Toc53770195)

[5. Class Diagram 6](#_Toc53770196)

[6. Entity-Relationship Diagram 6](#_Toc53770197)

[7. Requirements Confirmation sign-off 7](#_Toc53770198)

[APPENDIX 8](#_Toc53770199)

[Appendix A. Definitions, Acronyms, and Abbreviations 8](#_Toc53770200)

[Appendix B. References 8](#_Toc53770201)

# Executive Summary

## Project Overview

This project is a secure chat program that allows for all of its users to post in a single chat room. It is intended for any user that is computer literate. The program will be a 2-tier, database-driven application that is only made to run on desktops.

## Purpose and Scope of this Specification

This program is meant to provide a secure chat room to computer-literate users.

**In Scope**

* Let users create accounts
* Let users logon
* Let users post to the chat room
* Encrypt communications

**Out of Scope**

* Modifying user accounts
* Multiple chat rooms
* Other devices (such as mobile)
* Admin accounts
* Data integrity checking

# Product Description

## Product Context

This system is not independent. The user will need an internet connection to connect to the database.

## Primary User Characteristics

* Computer-literate
* Has potentially used other chat programs in the past

## Assumptions

* Operating Systems: Windows, Mac, Unix
* Internet Connection
* Working Computer that can run a small program (maybe 8 MB)

## Constraints

Describe any items that will constrain the design options, including

* C++, Azure SQL Server, Qt, GCC
* Only regular users, no admins
* Password hashing and salting
* Program will be no more than 8 MB in size
* Program must retrieve from the database every 4 seconds
* SHA256 for password hashing
* Internet connection required

# Requirements

## Functional Requirements

**3.1.1 System Tasks**

* The system allows existing users to login to the chat room
* The system allows a new user can create an account to login with
* The system allows a user that is logged to post to the chat room
* When a user leaves or enters, the system tells the chat room to say so
* Upon logging in, the system shows the user the last 5 messages posted

**Information Tasks**

* Users: Stores username, encrypted password, salt, email, and user ID#
* Messages: Stores the poster’s username, content, message timestamp, and message ID#

## Non-Functional Requirements

### Operational Requirements

* Work on any Windows, Mac, and Unix operating system
* Work with Azure SQL Server

### Performance

* Must not exceed 8 MB in size
* Checks for new messages every 4 seconds
* Logging in should take less than 5 seconds
* Posting a new message should take less than 5 seconds

### Security

* SHA256 encryption and salting for passwords
* Messages and user activity is logged in the database
* Users cannot access chat room until logged in
* Authentication Factor: Password

### Cultural/Political

* In case of any data protection laws, all messages will be stored in the database

## System Interface/Integration

### Network and Hardware Interfaces

The only interface is between the program and the Azure SQL Server. The program will connect to port 1433 on the server using the ODBC protocol use TCP/IP for networking in general.

### Systems Interfaces

The program will create a connection to the SQL server on port 1433.

The database will be used to receive account information (for the account creating and logon processes) and receiving and sending messages that have been posted.

The account SQL entries will have a password, a username, and an email address.

The message SQL entries will have the username of the one who sent it and the content of the message.

# Use Cases

Provide a summary of the major functions that the product will perform. Organize the functions to be understandable to the customer or a first time reader. Include all required use cases, or provide a link to a separate document (or documents):

Name: Log In to Chat Room

Identifier: SC-001

Preconditions:

1. User has an account

Postcondition: User is able to see the chat room and post to it

Basic Course of Action

1. User is greeted with login form
2. User inputs username and password and submits the form
3. The user is authenticated
4. The user is greeted with the chat room, which now has the message “User has arrived”

Alternative Course A: User does not have an account

1. User clicks “Sign Up” button on the login form
2. User enters email address, username, and password for the account
3. Account is created
4. User is greeted again by the login form

Name: Post to Chat Room

Identifier: SC-002

Preconditions:

1. User has logged into the chat room and has been authenticated

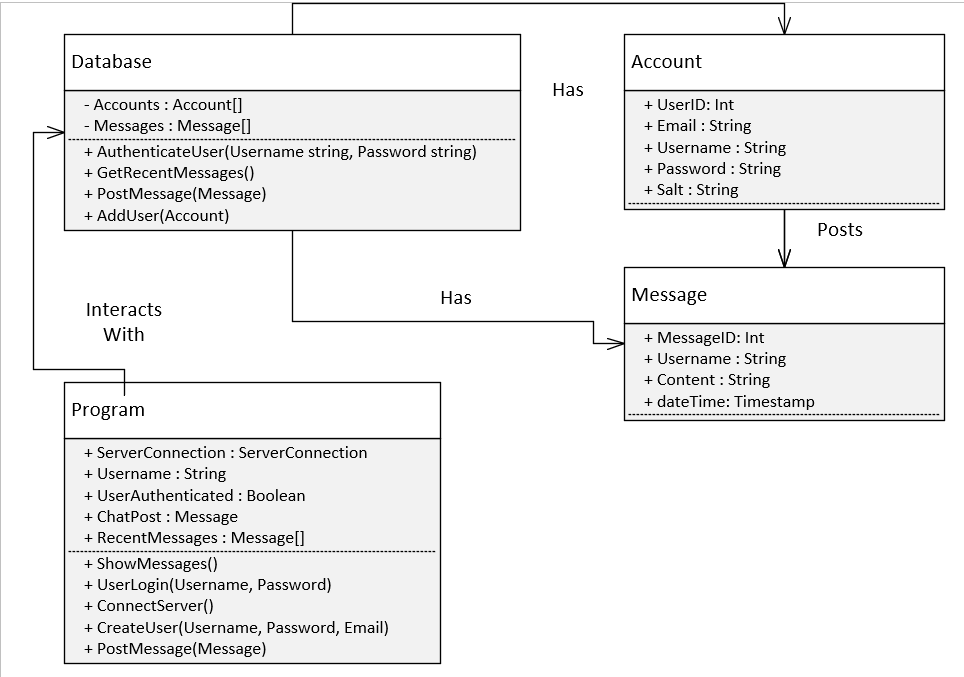
Postcondition: The user’s message has been posted to the chat room

Basic Course of Action

1. User sees the chat room’s past messages and text field to write message in.
2. User writes message in the text field
3. User clicks “Post” button
4. User’s message is written to the chat room

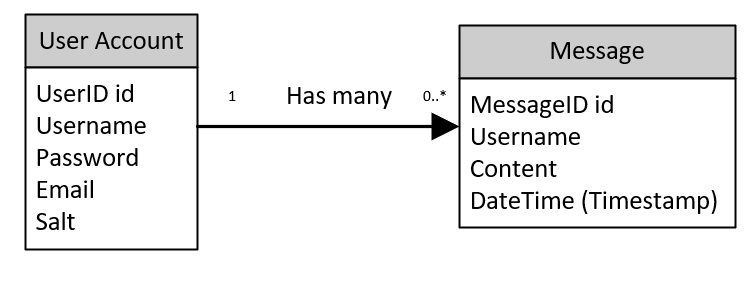
# Class Diagram

Include a UML class diagram, or provide a link to a separate document (or documents):



# Entity-Relationship Diagram

Include an Entity-Relationship diagram for your relational database design, or provide a link to a separate document (or documents):



# Requirements Confirmation sign-off

Include documentation of the approval or confirmation of the requirements here. For example:

|  |  |  |
| --- | --- | --- |
| Meeting Date | Attendees (name and role) | Comments |
| 10/15/2020 | Brendan Curran, Student  Professor Grady, Faculty/Project sponsor | Gathered initial requirements |

APPENDIX

1. Definitions, Acronyms, and Abbreviations

Azure: Cloud computing service that provides an SQL database.

C++: Language used to program the program.

GCC: Runtime compiler to create the program.

ODBC: The protocol to communicate with Azure’s SQL Server.

Qt: Used to make the user interface.

Salt: Added to the password before it gets hashed and stored.

SHA256: Hashing algorithm, used for encryption.

SQL: Language used to communicate with the database.

TCP/IP: Protocol used to communicate on a network.

1. References

*.*