# PROJECT PROPOSAL

## CredHub – Protecting Your Credentials

**by**
**Megan Steeves, Selma Samet, Kellen Mentock, and Tamara Linse –**
**Programmers in Senior Design at the University of Wyoming**

## Project

CredHub is a next-gen identity and credentials manager that includes verification by issuing institutions and control of data by user.

## User Experience

For first-time login, the user will enter their username and password and establish two factor authentication and facial recognition. In the case of a forgotten password, the user resets their password via pin code sent via text to their phone.

To begin verification of a credential or ID, the user will enter information into a form about the ID or credential and, if necessary, upload images of that credential or related documents. The app will then interface with the issuing organization to verify it.

The process of verification—which we will have established ahead of time through a relationship with that organization—will be in one of two ways: 1) if the organization has an API, we will establish an electronic link that will digitally verify the ID or credential, 2) but if the organizations does not have an API, we will establish a manual procedure to verify that ID or credential and then the organization will send a verification.

The app's home screen will have a button for each ID or credential, and the user will use a pin code—the same pin code for all IDs or credentials for ease of use—to access these to ensure security. In this way, the user will give permission for IDs and credentials to be accessed and viewed, and the phone will be locked so that if it needs to be handed to someone, the other person cannot access the user's information. Each ID or credential will also have an expiration date and prompt the user to confirm or renew, if needed.

We will ask the issuing organization to put a page on their website that verifies the legitimacy of our app, which we will link to on our app. And so, if a person viewing an ID or credential questions the validity of the app, they can click that button and see that it is legitimate.

## Back End

- An Android UI/UX in Java and/or Kotlin designed with the user in mind.
- Secure authentication, login, and password recovery, which will use Android's facial recognition, Android SMS Retriever API, and Google SMS multi-factor identification.
- An AWS backend server in Python and/or C++, which will be our cloud hosting service, run our business logic, and host our database.
- A PostgreSQL database through AWS RDS that will be mirrored on both the server and the user's device.
- IDs and credentials stored to an Ethereum blockchain using Solidity, with smart contracts for execution. The server will be able to read and write to the blockchain, but user devices will only be able to read from them.

## Our Team

**Tamara Linse –** Originally from Lovell, Tamara is a senior in computer science who is planning on going on to get her master's and Ph.D. in computer science. She also has a bachelor's and master's in English and serves as manager of content and web strategy for the UW Foundation. Tamara is developing verification procedures and databases (with Selma).

**Kellen Mentock** – Kellen is a senior at UW pursuing a bachelor's degree in computer science with a minor in blockchain. Originally from Sheridan, he hopes to be able to help develop this emerging technology in his home state. Kellen is developing the server (with Megan) and blockchain and smart contracts (with Tamara).

**Selma Samet –** Selma is an international student majoring in computer science and pursuing a certificate in cybersecurity. She works as a resident assistant at UW. Selma is developing security and authentication (with Megan).

**Megan Steeves –** From just north of Denver, Colorado, Megan is a senior in computer science with a minor in blockchain. She works in the University IT Walkin Service Center. Megan is developing the Android UI (with Selma).