# Unify: All Access Key

## Spring 2023 Group 5

## Arijus Trakymas, Sharva Darpan Thakur, Russel Tjahjadi, Mohammad Zaid

Unify is an all-access key application. It is an application that utilizes an RFID card which will be connected to an application. This card aims to be an all-in-one card that can not only access certain areas but also support different payment methods when being charged. The application aims to also have the list of subscriptions/memberships that the user is currently enrolled in. Additionally, the app also aims to implement a chatting feature where users can talk to other users so that they can share their experiences with one another and discover new places to go to or share their experiences with one another. We are building this product because we have noticed the difficulty in people having to keep track of their multiple cards. In the end, we want to create a product that shall just have everything all at once and in the event, they forget the card, they could resort to opening the app installed in their mobile phones.

Without using this app, a person needs to bring their cards, and this unfortunately takes up a lot of space in their wallet, purse, etc. We shouldn't forget that sometimes people tend to be forgetful and that they might lose or did not remember to bring their card for their passes/membership cards. This then wastes a lot of time and money if they need to go back and retrieve it from their own homes or if they need to buy a pass again. Using this app helps solve that problem.

To get our project moving, we will also need input from our customers because we need to know how the experience was like for the users. First question that we will ask is how they feel before using the app (meaning that they would have a lot of cards that they need to carry) and after using the app (when they do not need to worry about the different cards they need to carry because Unify is an all-in-one card that has the ability to pay their charges in a much simpler and efficient way).

We have three types of stakeholders that we wish to target as of this current moment: client, customer and the hands-on users of the product. The client would be the developing organization. The second stakeholder, being the customer, will be anyone that has not even used a product like this before and is willing to use the product that just wants to simplify their cards and passes/memberships. The third stakeholder, the hands-on users of the product will be the people who have experience with technologies like this (the RFID chips and applications integrated with the card). The two types of hands-on users would be businesses that support our cards with their systems and the actual users that use our cards to access and / or purchases things.

There are a few solutions to combat certain constraints that we have thought of in this project. Firstly, the user must accept our terms and conditions to use the app because every user that plans on using the app must adhere to the rules and regulations placed upon the app. Secondly, the app shall work in different operating systems like the iOS, Android devices that a lot of users currently have on their phones. Third is that we plan on making the file of the app as small as possible to not take up a lot of space once the user downloads the app. Fourth is to increase security because the app will be dealing with sensitive information like user's card information, username, password, email, phone number, etc. Fifth is to have a respectful

community because the app feature will allow users to interact with one another, we need to keep the interactions between them to be respectful and if any of the existing users has violated that rule, other users can report the specific user and the team shall revoke their use of the app in the future. Finally, our product aims to be user friendly because we understand that some people have a hard time getting used to a new app, the app should have buttons which tell them exactly where they would go once pressed.

The anticipated workplace environment for this product is that the product can be used anywhere and anytime because there will be a lot of people relying on the product itself to grant them access and/or the experience of the things they want to do. In addition to that, since the app will be an online app, it must be resistant to viruses and malware that could potentially also unfortunately corrupt the central database where all the other user's information is stored.

As the app will have multiple users trying to access their own accounts, we will need to implement a validation functional requirement which only allows the user to access their accounts if they have their correct credentials entered and the way we are going to test this is to have a validation test. In addition to that, since again, important information will be stored in a database, we want to keep a consistent record of each user's information and to test this, we will also need a database test.

Our app will handle multiple requests from a lot of users and because of this, we also considered the speed and latency requirements. When processing multiple requests, our app shall have already implemented an efficient algorithm to decrease the lag and have optimal performance. In addition to that, we also want the user to have a seamless transaction when they tap their card on a scanner because we want to have a fast response time when they are trying to enter a building.

We also want our app to be dependable for the users. Hence, we aim to have no long downtime and we expect to have the app undergo maintenance every month and as the app is undergoing maintenance, the app should be back up again at most 60 minutes. In addition to that, we would like to state that the app shall go through the update process in the hours when people usually do not need to use it which is around the 2am to 3am. Other than that, the app shall remain available 99% of the time.

The application contains a common database for login accounts to store respective information for businesses and users. However, only application users have direct access to the RFID card whereas businesses will use this platform to promote, allow access to access their services and display user information. The user must also have access to a mobile device to run the application which ultimately administers the RFID card.

The proposed system architecture utilizes a client-server architecture for sending and receiving data, user authentication, and storage. The client side is responsible for displaying the application interface to the user and collecting input information to send to the server and display relevant outputs. The server receives, processes, and stores information like user data, account details, membership information. To enhance and address security measures, a proxy server must be implemented to protect data.