
# CS491/492 Weekly Log

**2024/2025 Bilkent**

**Serhat Merak**

**22002414**

**IAWIA**

**T2424**

**18/11/2024 Week**

I worked on the Project Specifications Report. For this report and to complete our project, I have read the following reports and papers about zero-knowledge proofs and blockchain technology. These reports and papers are mainly suggested by our supervisor Cemil Şinasi and his friend who is working at Ethereum Foundation Onur Kılıç.

https://tlsnotary.org/use-cases

This is not a report or paper but a product that provides an open-source protocol to enable zero-knowledge proofs on the request and response flow. This link is the use cases of tlsnotary.

https://zkp2p.xyz/

This is another application that provides a bridge between on-chain and off-chain using traditional bank payment reports. This was an important example for our topic because in Turkey, Granti Bank is working with this system and I have analyzed this application.

https://rarimo.medium.com/zk-identity-registry-35c8856a0ea5

This was the best blog that made our project clear. It was about a Georgian politician Rarimo who proposed an online voting system using zero-proof knowledge. It explains how to generate a unique personal device that is impossible to copy.

**25/11/2024 Week**

We met as a group to discuss how to divide our tasks for the Analysis and Requirements report and discuss our project. I was responsible for first implementing the design for the mobile application to scan passports. I used Figma to design our application. It is a small mobile application that contains at most 10 screens because all the logic lies behind the zero-knowledge part. I have added the design and explanation for the pages. Then, I have continued on my research about the zero-knowledge proofs and contributed the report with technical details

**02/12/2024 Week**

I have started to implement the mobile application. Even though it will contain a few pages to scan a passport and show the details on the screen, I wanted to start with a whole structure from language support to the light-dark theme. Because I am currently working part-time on the frontend in a startup, I have combined my knowledge from my part-time job into our mobile application project.

We decided to use react-native on the mobile side because it is easier to access the native part of the codes and makes it easier to create a good structure to use some parts of the codes to develop a website. I have spent this week implementing the basic structure and folder structure.

09/12/2024 Week

Besides the mobile development, this week I have mainly researched the Zero-Knowledge proofs and proved something on-chain using the Google Chrome extension. Even though we will not show this part in the first demo, there were some questions to answer in order to draw the roadmap for our project.

1- How we can ensure uniqueness on the passport wallet in order to produce zero knowledge on the blockchain?

2- In order to increase security, we decided to add security properties. However, how should we store the private key of the wallet encrypted with security properties. Is it safe?

16/12/2024 Week

I worked mainly on implementing a passport scan system for mobile phones. Using NFC features requires writing native code on kotlin and swift separately. However, we have to be registered to the developer system of apple in order to use NFC feature

- We have bought the developer system however, it was not approved for 3 days so we have to write kotlin code. It was not our intention, we had decided to show scanning passports using the NFC feature of the iPhone, however, because our registration was not approved, we decided to implement it for Android for now.