Supervisor: Le Ngoc Son

17983859 | Nguyen phan tan duy

17984048 | Luu dieu co

17983603 | Tran hoang chuong

17983612 | Tran Phuoc nhan

17983478 | Ngo vinh hien

Mid-project progress preview

App data security team

# Executive summary

- Our client is from the University Hospital in Zurich which wants to improve the rating trainees system. The workload increases but the workforce decreases so the amount of paperwork is overwhelming for assessors. Furthermore, rating is currently based on emotion so that it’s not precise. Besides, our client wants the data is possessed by only the trainees.

- In current time, the collaboration team is developing an application which can interact between trainees and trainers. Our team and collaboration team will be working together to bring out a solution which helps the client solve this problem and secure all of the data.

- Risk : We haven’t had experience in this field so that would be challenging for our team. And also, we have to work on security frameworks and a new technology specifically Blockchain which having sparse information about it.

# Project description

The team will study and analyze and further define the specifications of the case study application, identify and document all the actors, data usage situations and security requirements, and then recommend suitable data security solutions to best meet the complex requirements. This can include public key encryption, certificate and / or block chain techniques. The team should build an independent prototype to demonstrate the setup, configuration and functionality of the security features. This can be done on an independent demonstration platform and does not need to focus on user interface or actual application usability aspects.

The application in question is an in-job-skills assessment solution which has many independent data creators, holders, validators and signers. The solution will need to enable the distribution of learning badges and maintain their qualities and trust. The team should explore the use of existing learning badge solutions and protocols to see how they can be integrated in the solution

# Project objectives, scope, approach, major milestones and deliverables

## Project objectives

To have an application that can capture the data of trainees in the training course and prove that trainees are able to do the task afterwards. And also, this application can use have multi-source feedback (360 degrees evaluation) for assessing trainees in order to know their competence and have further training plan provided to improve trainees’ skills.

## Scope

## Approach

## 3.4 Milestones and deliverables

# A response to how the proposal conditions or recommendations have been addressed

After 3 times talking to clients and development team with three following results:

1) The document did not match the requirement of our development team.

2) After re-analyse all the workflow, the development team approved our solutions but with some adjustments.

3) We sent the lastest version of our document and got approved by the development team.

Our team also documented a feature which related to blockchain which also was approved by development team after discussions. Based on the agreements between two teams, our team is currently working on two aspects:

## Security modules

These security modules are used for securing data and connection between all the parties in the system( trainee-supervisor-server, supervisor-server-email server,…)

## Webservice

Web services is mainly used for demo prerequisite functions, based on the project workflow. With web services, user could interact with client page to transmit data in for server page to execute the data then return the requested result.

Essential modules that could be built by using Web services application component :

+ Cryptography: Encrypting and decrypting classified information. Applied and executed with RSA method.

+ Digital Signature: Signing and verifying information.

+ Database connection: Assets would be transferred between client and server for interaction or extraction.

## Blockchain

The purpose of using Blockchain for this project is for everyone to look up the trainee competency

Users can interact with Blockchain via a web application in which users can freely look up not only trainee information but also the hospital that trainee works for.

Besides, most of the functions in the web application are for the hospitals. Hospitals can use these functions :

+ Authorize Employee  
+ Add Records to trainee profile

+ Delete Employee

+ Signing

Overall, the web application has these functions below :

+ Authorise Hospitals : National Authority will use this function to authorise hospitals.  
+ Authorise Trainees : Only authorised hospitals can use this function to add the trainee to their hospitals.

+ Add Trainee Records : Only authorised hospitals can use this function to add records to trainee who works for their hospital.

+ Look-up Trainee / Hospital Info : Everyone can use this function.

+ Delete Trainee / Hospital : To delete hospital, it must be the National Authority. Once the hospital is deleted, all trainees work for that hospital is also deleted. To delete Trainee, it must be the authorised hospitals and trainee has to work for that hospital.

+ See Trainee Records : Everyone can use this to see trainee records which the trainee has achived.

+ Signing : This function is for making sure the Certificate is valid and signed by the hospitals.

+ Verifying : To verify the Certificate if it is validated by the authorised hospital.

# New variations from the original proposal with a rationale for them

At first our mission in this project was to get customer requirements then analyse them to design the security modules that needed for each sections. However, after a period of time both our team and development team both created our own workflow from the requirements of our client which leads us to do only analyse and design security models later on since the workflow was made by the development team.

The second thing that changed was in the system workflow, at the start of the project, the project had only two type of profiles which were called “live profile” and “national authority profile” but our client want to add one more type of profile which was called “snapshot profile”. Moreover, in the description of project, we have to imply “learning badget” but after our lastest discussion with development team and proxy client there was no meantioning about it.

# Summary of current project status

## Workflow analysis document

After 3 times meeting with client and development team, our team has confirmed the workflow analysis document. Each workflow process in this document will have its own diagram describing the detail of security modules including interaction between actors, key exchange storage and transmission security when transmitting data, encryption, decryption. Furthermore, each workflow process will be implemented in the web service for further usage.

## Web Services

### b.1 Completed

* + - Build a cryptography module based RSA method, which included:
      1. Data encrypting
      2. Symmetric method (formerly, this was mixed in RSA method for previous security planning)
    - Build a signing-verifying algorithm for data verification, also:
      1. Signing data with private key.
      2. Verifying data with public key.
    - Verifying document from email server’s encrypted data and supervisor’s signature. This objective was combines with both cryptography and digital signing module.
    - Build a database then connect to IDE.
    - Extract requested data from the database. This data was the public key of trainee which could be carried to use for encrypting such relevant documents as trainee profile, trainee record or supervisor evaluation form.
    - Establish connection between server and client. Allow interaction between both parties as well as build the components with essential functions, this included:
      1. Cryptography (encrypting and decrypting data)
      2. Digital Signature (generating a data signed and verifying the data with that signature)

### b.2 For future updates

* + - Improve the client page decoration (with html and css)
    - Build the database connection and run its essential modules within Web Services.
    - Update the Select Task function.
    - Creating assessment and sharing profile will be added.
    - Improve the replying signing email function.

## Blockchain:

### b.1 Completed

- Built front-ent for the web application which easily for users to use.

- Finish a smart contract which is used for executing conditions before the data goes into the Blockchain.

- Run Blockchain local test and Use Web3 to help interact between Blockchain and Web application.

- Can get data input and execute it through smart contract. Then can return the data back to the application.

### b.2 For future updates

- Decoration for the web application

- Functions added (if requirements changed)

- Review code and fix to make it more secure.

## Issues

* Client in Switzerland is quite busy and the time zone is also different from our team so when it comes to scheduling meetings, it’s quite difficult for us to have a meeting.
* Proxy client and development team are quite busy with their own business, so when it comes to replying email to confirm our suggested documents, it was quite slow.
* The biggest issue that our team has been facing with is that the requirements at first was not quite clear, our team had to spend a lot of time specifying the requirements, but in the end, analysis documents we have made are not accepted because development team analyzed their own documents and used those documents instead of using our analysis documents. While our project scope is to take, analyze requirements from clients and design.

# Recommendations for improving the project team’s performance

* Communicating with development team more frequently
* Writing logs more often after having a meeting describing what we have done.

# Summary of individual member contributions and learning achieved so far in the R&D Project

## Duy

* + - I analysed the business process, use case, workflow of the system and thought of security features can be applied to the system to make it more secure. I also built from scratch a website to interact with Blockchain and write a smart contract in Solidity.
    - So far, I have learned about some security concepts and how it works such as symmetric encryption, asymmetric encryption, digital signature, Caesar Cipher, Diffie-hellman key exchange protocol, hashing, salting. And also, data transmit encryption protocol such as ssl, ssh. Besides, I have also learned Blockchain concepts and its component for our project like smart contract. Programming languages I have learned up to now : Python, Solidity, HTML, CSS, Boostrap, Jquery, Web3.js, Truffle.

## Hiển

## Cơ

## Chương

## Nhân