WORKFLOW ANALYSIS DOCUMENT

# Workflow analyse

Trainee will log in using their provided ID and password. After successful log in, trainee will select a game, if there is any game record, the server will return all records for the trainee, if not server will create a new empty one. After joining the game, the trainee application will check if there is any tasks that still available to select, each time they submit the task’s answer, the record of that trainee will be updated and the loop keeps going until there is no task left.

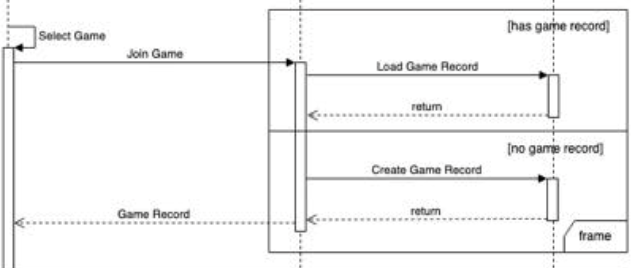
When all tasks completed, trainee will inform to the server that all tasks have been done and request a QR code in order to let supervisor scan and assess the performance based on the record. The supervisor has to log in in to the application. Supervisor will send request assessment to server, then server will load the game record from database and return it to the supervisor. Supervisor will fill a signing form then select signing with email by sending signing request to server, server will save the signing method (with email) of the record to database, and make a request to email server, email sever will return the confirm form to the supervisor. After choosing the signing method, supervisor makes optional feedback on that record.

Finally, supervisor will reply the signing email, email server then received the reply and will inform to server that the signing has been completed and update the record following the sign method to database. Server will confirm to email server that those signings are signed email, server will update those signings.

# Security analyse

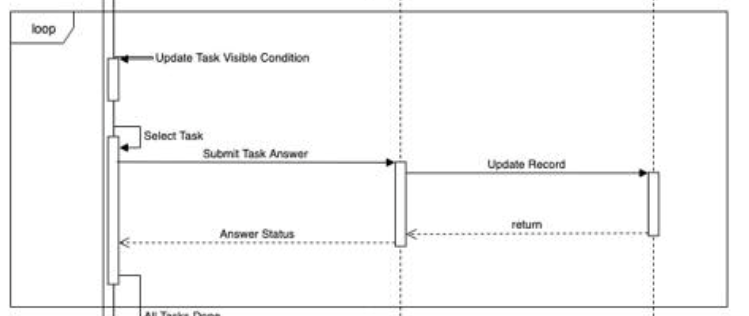
All users and server will have a key pair which called public key, private key and server’s public key, but the database stores all the public key of all users.

## Trainee join game



In this section, there could be new data created which is trainee record if the game trainee selected has no record before. All the records are encrypted at database using trainee public key. When the trainee load game record, server will take the record encrypted using trainee’s public key and return it to the trainee, it will be decrypted using trainee’s private key.

## Select task



Users will send public key and basic information to server, server will go to database and check public key and basic information, if it’s true, server will send public key to user, then user will generate a session key and encrypt the session key using server’s public key and send to server, server will decrypt by using server’s private key to get the session key and then two parties will use session key to transmit data (Task Answers, Answers Status).

After choosing and performing each task, trainee will submit answered task to server, then server using trainee’s public key to encrypt answered task and store in database.

## Supervisors see record and make assessment



Firstly, trainees will use supervisor’s public key to encrypt the session key and send to supervisor, then supervisor will decrypt using supervisor’s private key to get the session key, then trainees and supervisors will use session key to send data.

## Supervisors sign email

After supervisors reply signing email to sign the trainees’ record, there will be a sign email field that contain the signing of supervisors which will be encrypted using trainee’s public key.