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.

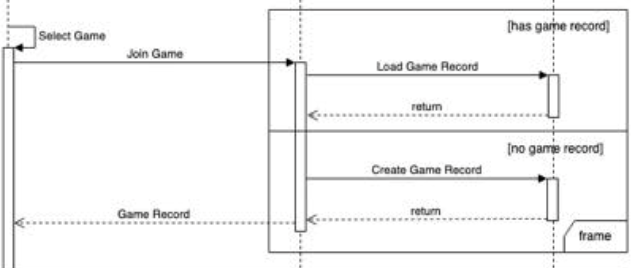
When all tasks completed, trainee will inform to the server that all tasks have been done and request a QR code in order to let supervisor scan and assess the performance based on the record. The supervisor has to log in in to the application. Supervisor will send request assessment to server, then server 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

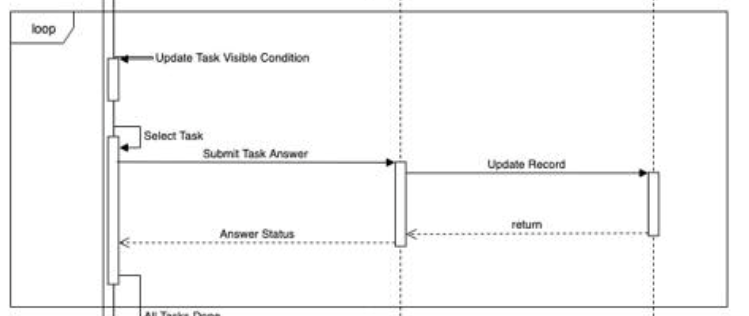
All users and server will have a key pair which called public key, private key and server’s public key, but the database stores all the public key of all users. All users also store the server’s public key.

## 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 in database using trainee public key. When the trainee load game record, server will take the encrypted record 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 response, 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, the server will decrypt by a session key then using trainee’s public key to encrypt answered task and store in database.

## Supervisors see record and make assessment



Firstly, trainee shows QR to supervisor to scan and encrypt it using server public key and send it to server include supervisor public key, QR code will be decrypted using server private key and use it to find trainee record, if found server will send that encrypted record to trainee, trainee will decrypt it using private key and use supervisor’s public key to encrypt the record and send to supervisor, then supervisor will decrypt using supervisor’s private key to get the record,after making assessment, the supervisors will use sever public key to encrypt all the data including signing method and evaluation form to server. At server, the data will be decrypted using server private key and then encrypted with trainee public key.

## Sending request to email server

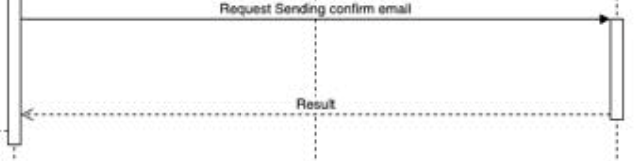


Figure 1 Sending confirm email



Figure 2 Sending result email

Server will create a new session key using email server public key to encrypt, then send it to email server and email server uses its private key to decrypt the session then send a confirm message to server inform connection has been created. After that all the data which is sent by server and email will be encrypted and decrypted using the session key.

## Trainee shares profile to supervisor

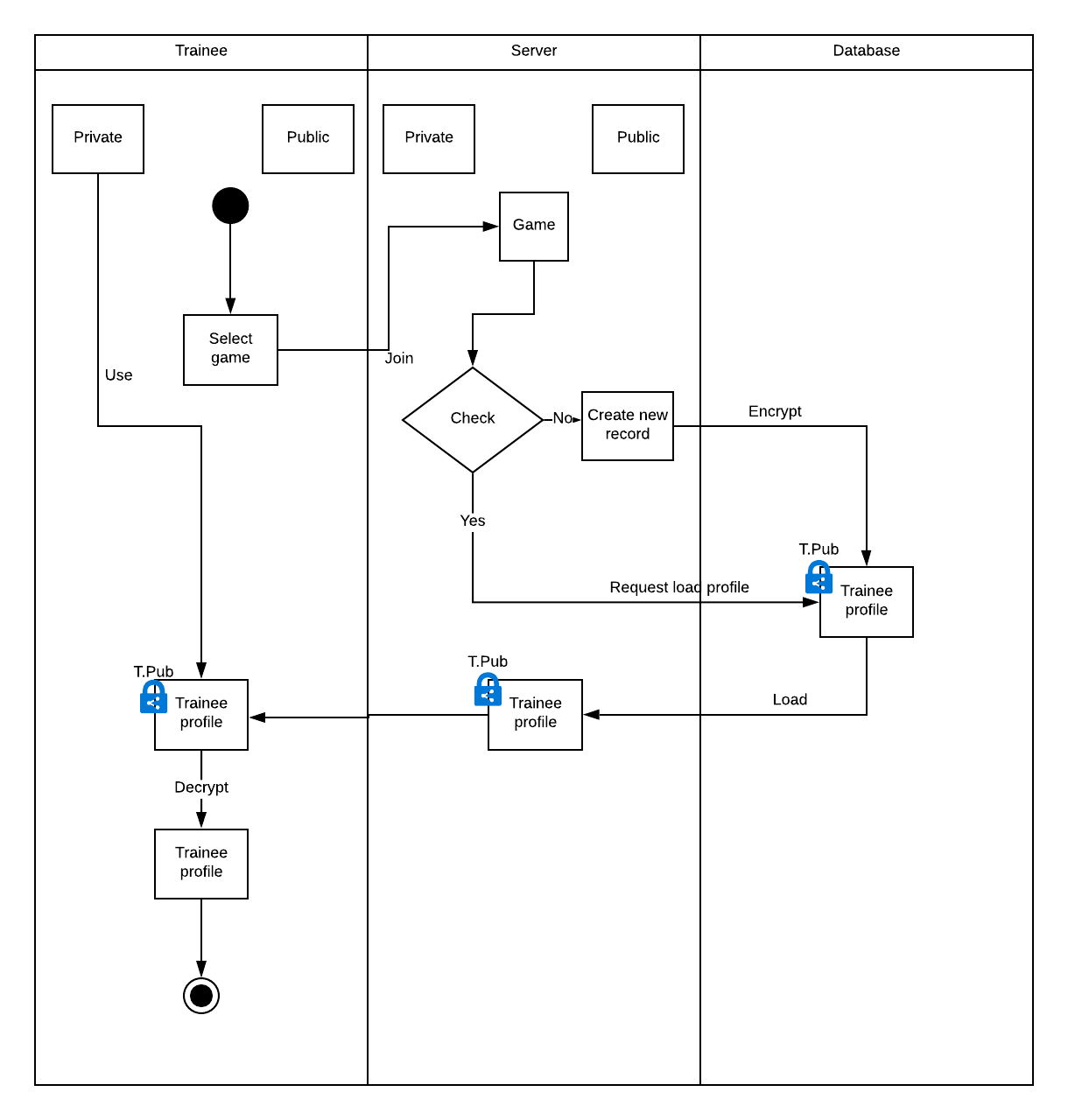
Trainee will show profile QR code (not record QR code) to supervisor, supervisor scans the QR code then send it to server include with supervisor information (QR code and public key), server uses that QR code to check if the trainee exists or not. If yes server will send the trainee encrypted profile and supervisor public key to trainee in order to decrypt it using trainee private key. Then trainee will create a session then use supervisor public key to encrypt and send it to the supervisor, supervisor will decrypt the session key with his private key then send a response to trainee. After receiving the response trainee will use the session key to encrypte his profile and then it to the supervisor, he will use the session key to decrypte trainee profile.

Each session key indicates the connection between supervisor and trainee, both save the session on their phones for an assigned time. Whenever there is any update of trainee profile during valid time, session will be reused to send the lastest trainee profile and supervisor will delete outdated profile on his phone.

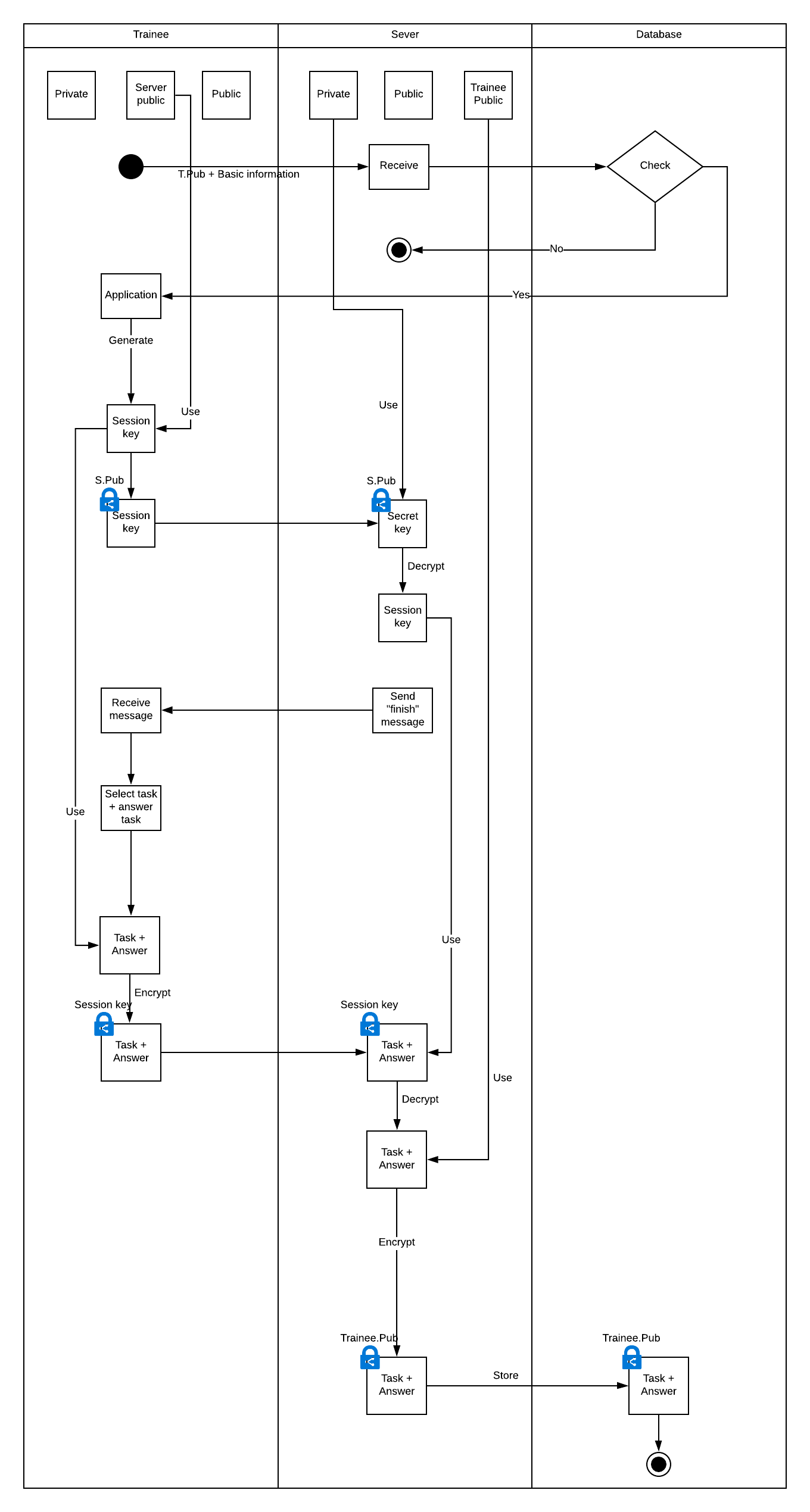
**Drawback**: everytime there is any new update to trainee profile, supervisors who can see the profile will have to update again from the trainee

# Security workflow diagrams

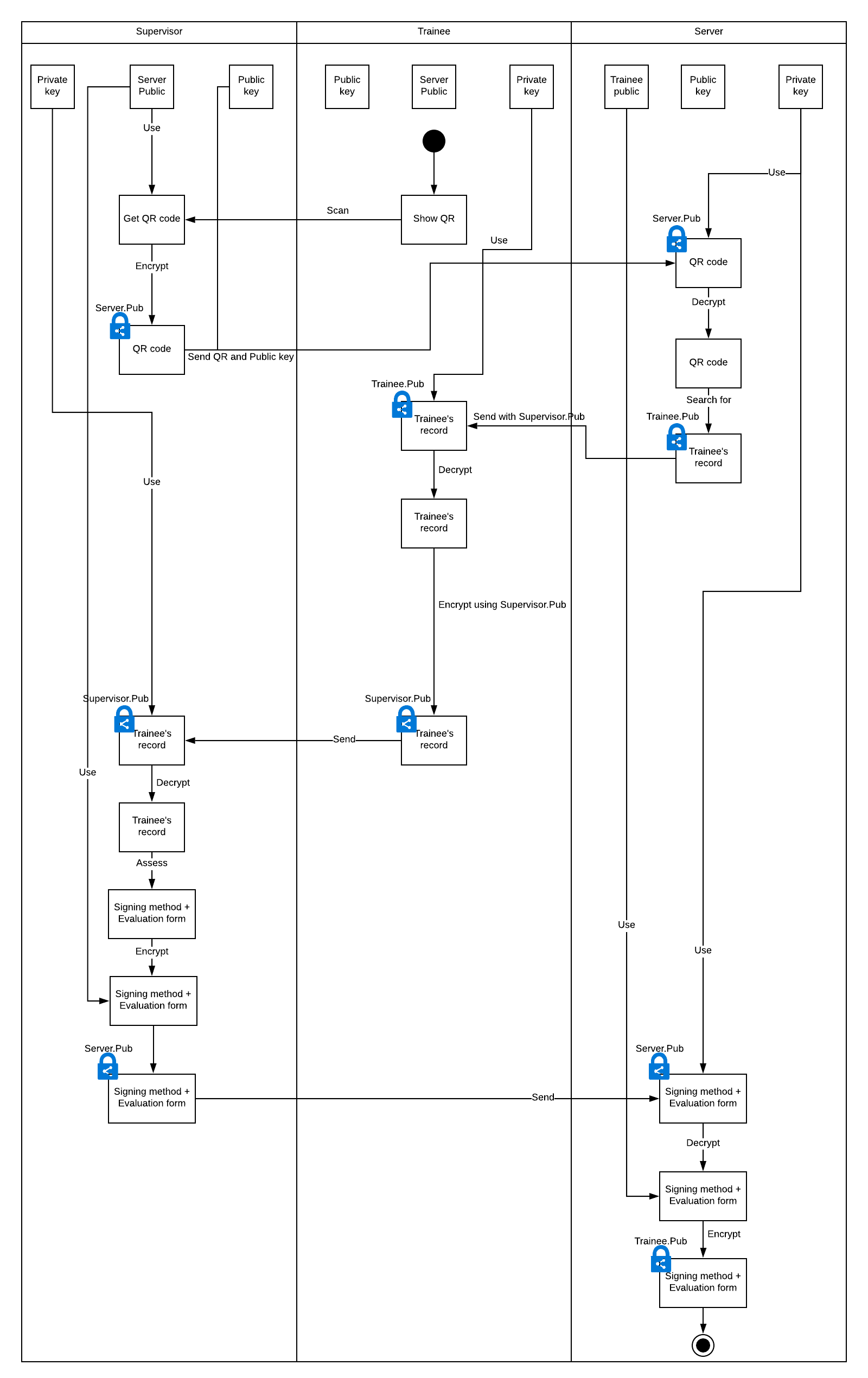
## Trainee join game



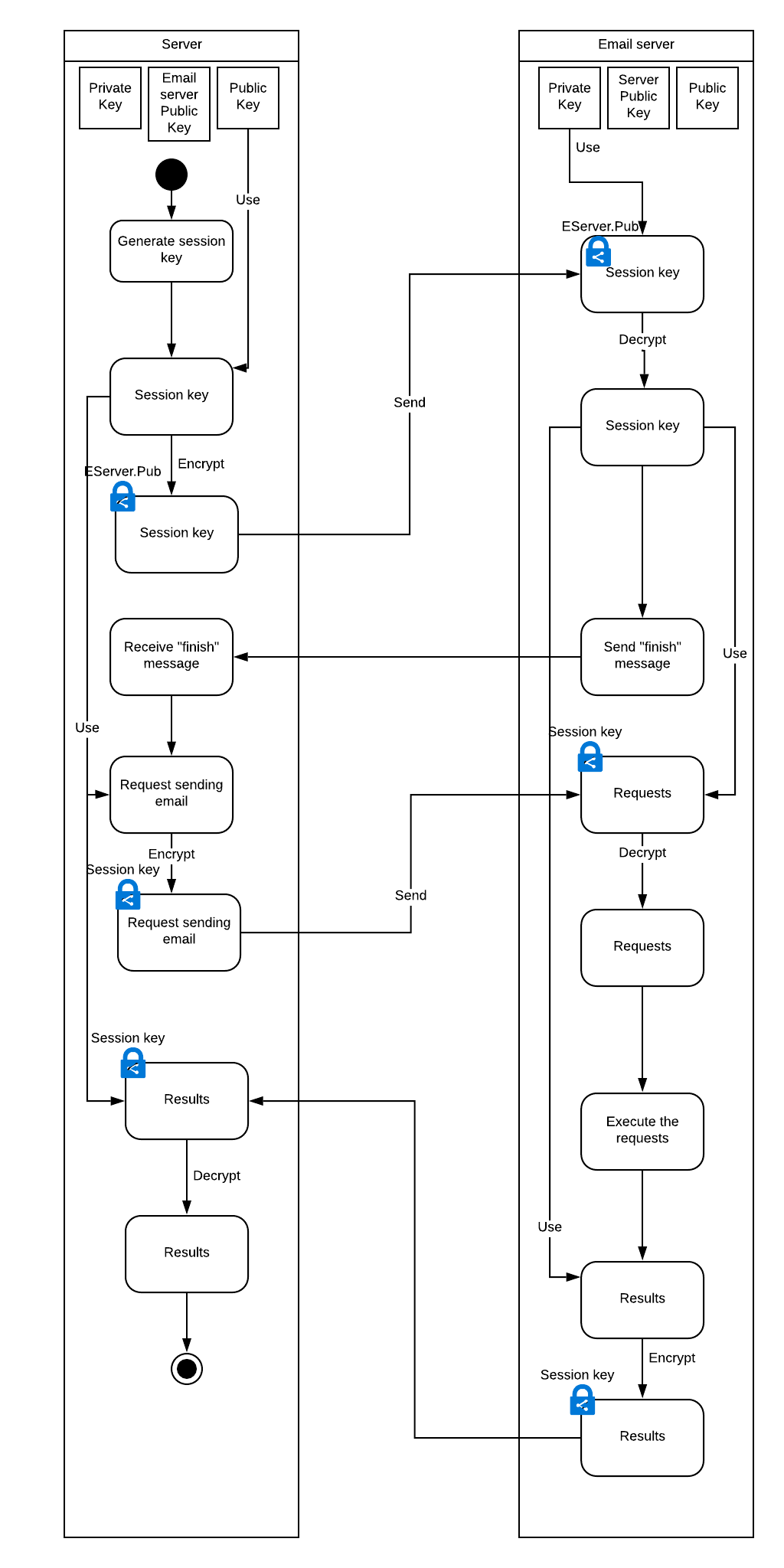
## Select task



## Make assessment



## Sending request to email server



## Trainee shares profile to supervisor

