# Business Analyze Process

## Summary:

This section has two Workflow analysis and Security analyses/solution document. One was created based on client workflow and because the security reasons, client cannot give their source code of the software to our team to integrate APIs, this led to the second Workflow analysis and analyses/solution document. The document is similar with the first one, but it also includes more about our team will create a draft software and database to integrate and run APIs.

## Workflow analysis and Security analyses/solution (Based on client):

### Workflow analyze:

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, when email server receives then it will respond to server then, server will update the game record in the database that it has been signed. Afterward, server will request sending result email to the email server then it will send the result to the server.

### Security analyze:

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. Firstly, the trainee will select game, then user 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 continue to check the game record, if the game record does not exist, server will create a new record, if the game record exists, server will load the game record that is being encrypted by trainee’s public key in the database and return it to the trainee . When the trainee load game record, it will be decrypted using trainee’s private key.

#### Select task:

#### 

Firstly, trainee 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, supervisor will scan the trainee’s QR code to get the code and send it to server include supervisor public key, server will check trainee’s game 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 evaluation form (result supervisor’s rating field) will be encrypted using server public key. Meanwhile, the trainee’s record will be encrypted using supervisor public key. Both will be sent to the server include with record’s QR code. On the server side, the evaluation form will be encrypted using supervisor public key and attached with the trainee’s record which was encrypted using supervisor public key, both will be sent to email server side to create a confirm email.

#### 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 encrypt his profile and then it to the supervisor, he will use the session key to decrypt trainee profile.

When trainee wants to create a snapshot, he can choose which section should be shown/hide to the supervisor.

When the trainee’s profile (snapshot) is sent, this snapshot profile will attach with sent and expire date, the supervisor’s application can check if it reaches the expire date, then the application will remove the trainee’s profile.

*(\*) Trainee encrypted profile: contains all the encrypted fields (ID, QR record).*

#### Reply signing email

#### 

When the supervisor signs, the evaluation form (result supervisor’s rating field) will be hashed then encrypted using supervisor private key to get the supervisor’s signature. Meanwhile, another evaluation form will be encrypted using email server public key. Both supervisor’s signature and evaluation form will be sent to the email server. On the email server side, the evaluation form will be decrypted using email server private key then hashed. The supervisor’s signature will be decrypted to get the hash. Both hashes will be compared if they match, email server will send record’s QR code to server to find the record and update it (change the sign status into signed), server will request email server to send evaluation form to server. On the email server side, the evaluation form will be encrypted by using server public key then decrypted in server side by using server private key. Finally, the evaluation form will be encrypted using trainee public key and updated to trainee’s profile.

### Security workflow diagrams:

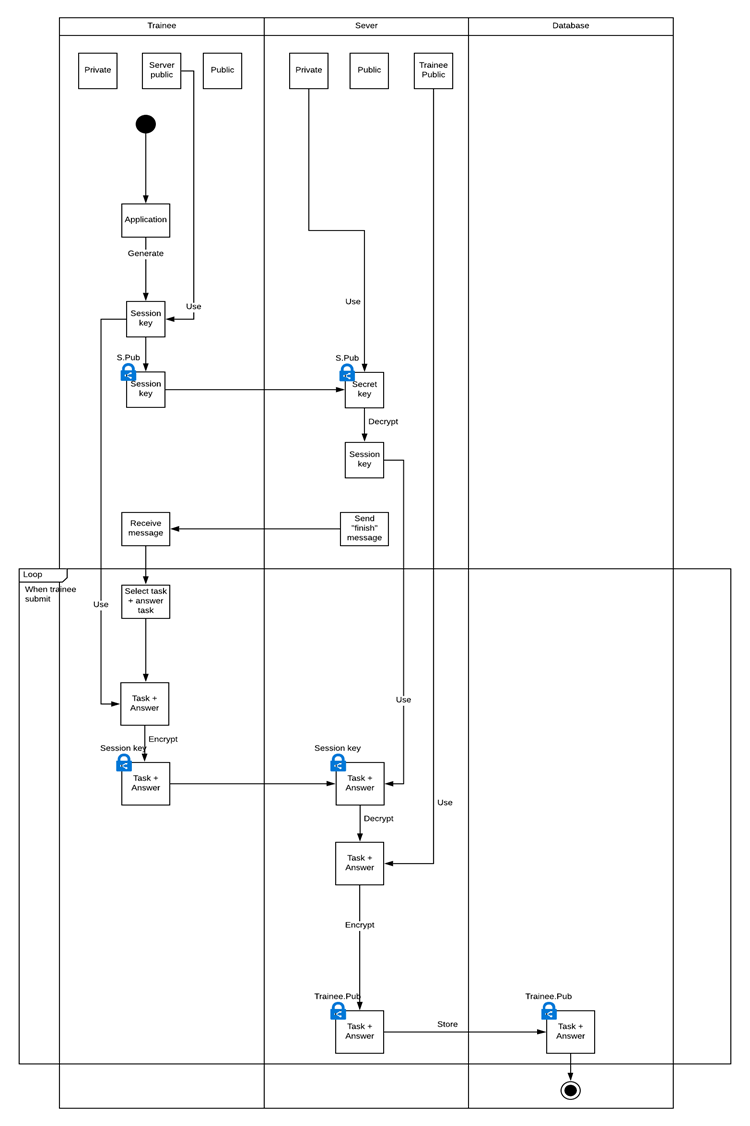
#### Trainee join game:

#### 

**Security Modules need to be used:**

* Decryption module (decrypt the game record).

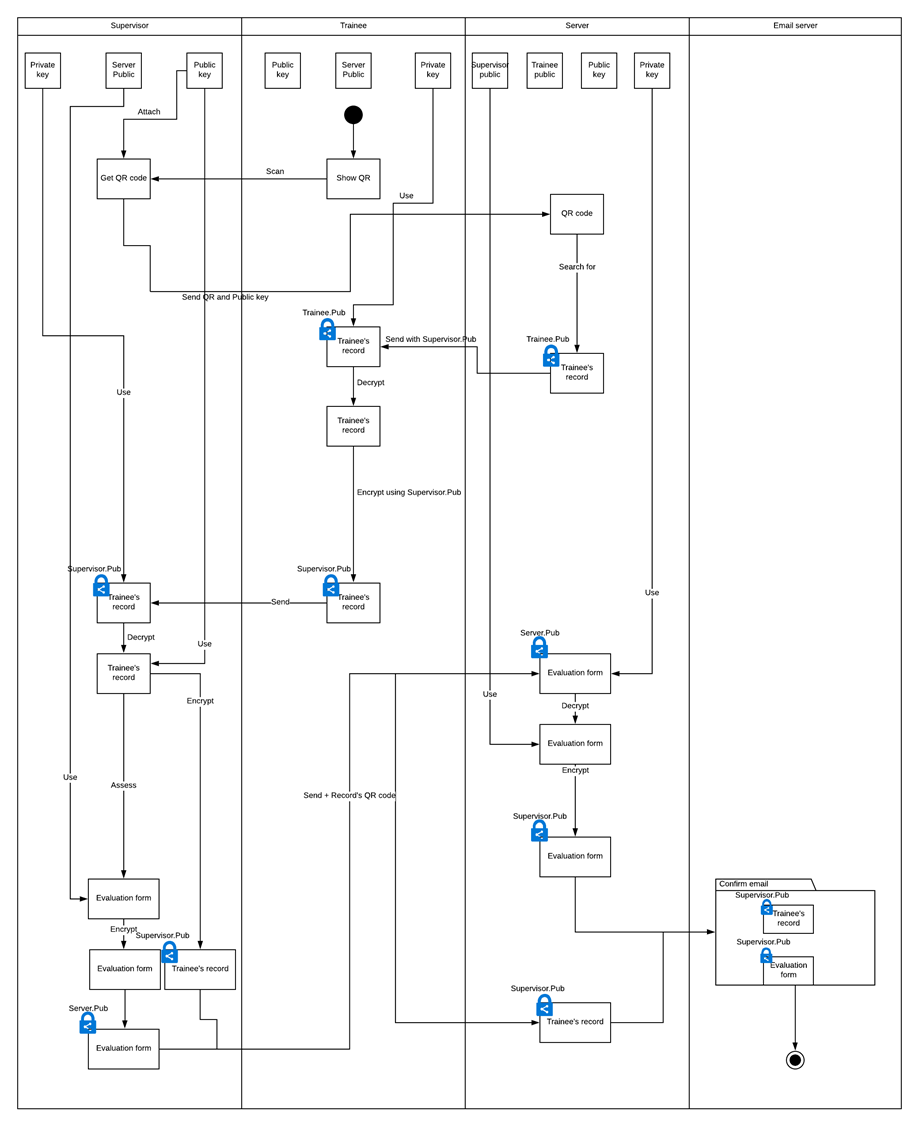
#### Select Task



**Security Modules need to be used:**

* Key generator Module (generate a session key)
* Encryption Module (encrypt the session key/Task Answers, Answers Status)
* Decryption Module (decrypt the session/ Task Answers, Answers Status)

1. *Make assessment*

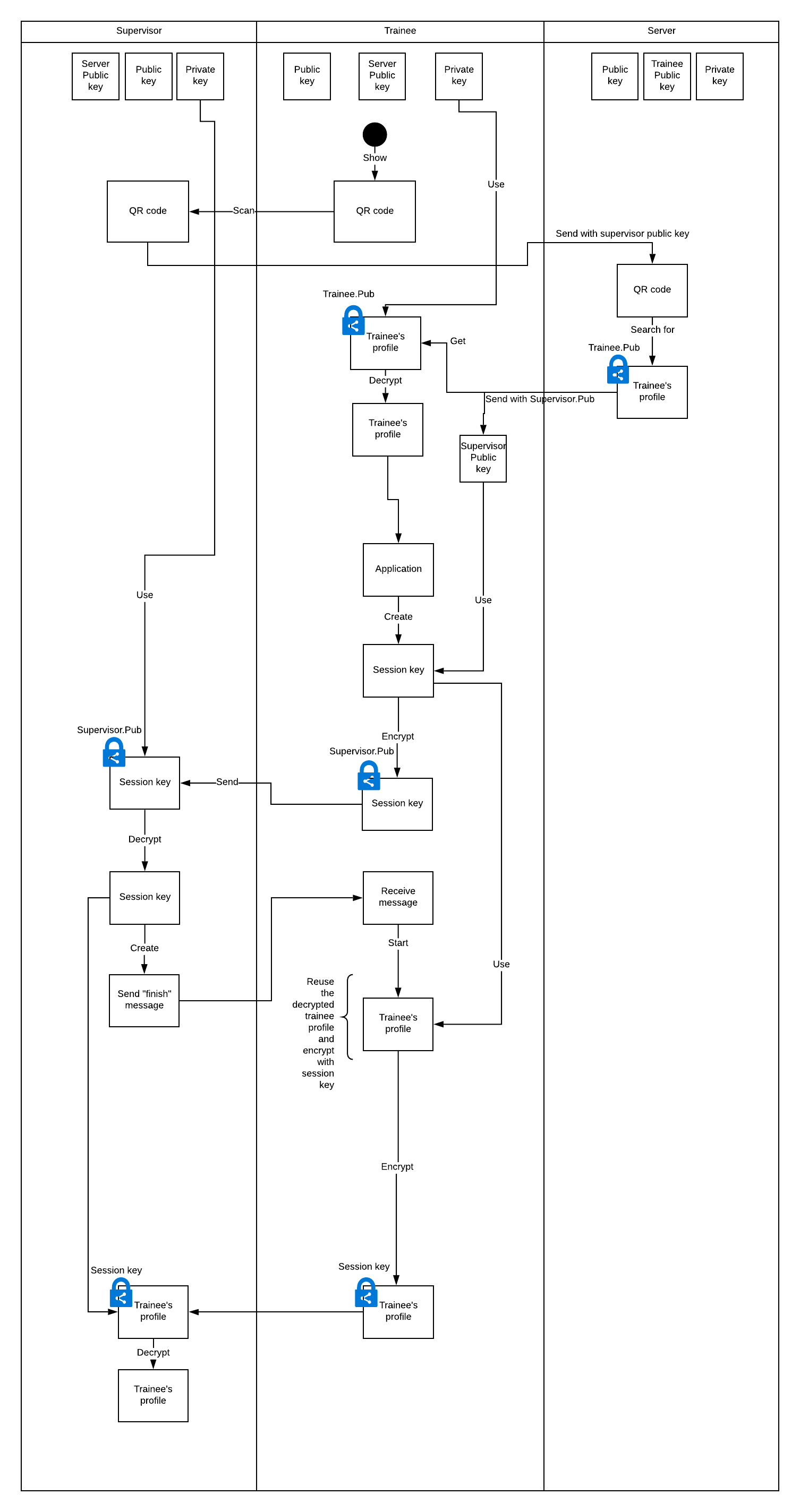
**

Security Modules need to be used:

• Decryption Module (decrypt the record)

• Encryption Module (encrypt the record for supervisor)

#### d. Trainee shares profile to supervisor



**Security Modules need to be used:**

* Decryption Module (decrypt the profile using trainee private key)
* Key generator Module (create a session key)
* Encryption Module (encrypt the profile)

#### e. Reply signing email

#### 

**Security Modules need to be used:**

* Digital signature module (the evaluation)
* Encryption module (encrypt the evaluation)
* Signer verification module.

## Workflow analysis and Security analyses/solution (Draft Software):

## 3.1 Database design

#### a. Employee list

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Name | DOB | Public key | Role |

* ID: each hospital’s employee has a unique number.
* Public key: unique public key of every employee.
* Role: there are 2 roles which are trainee and supervisor.

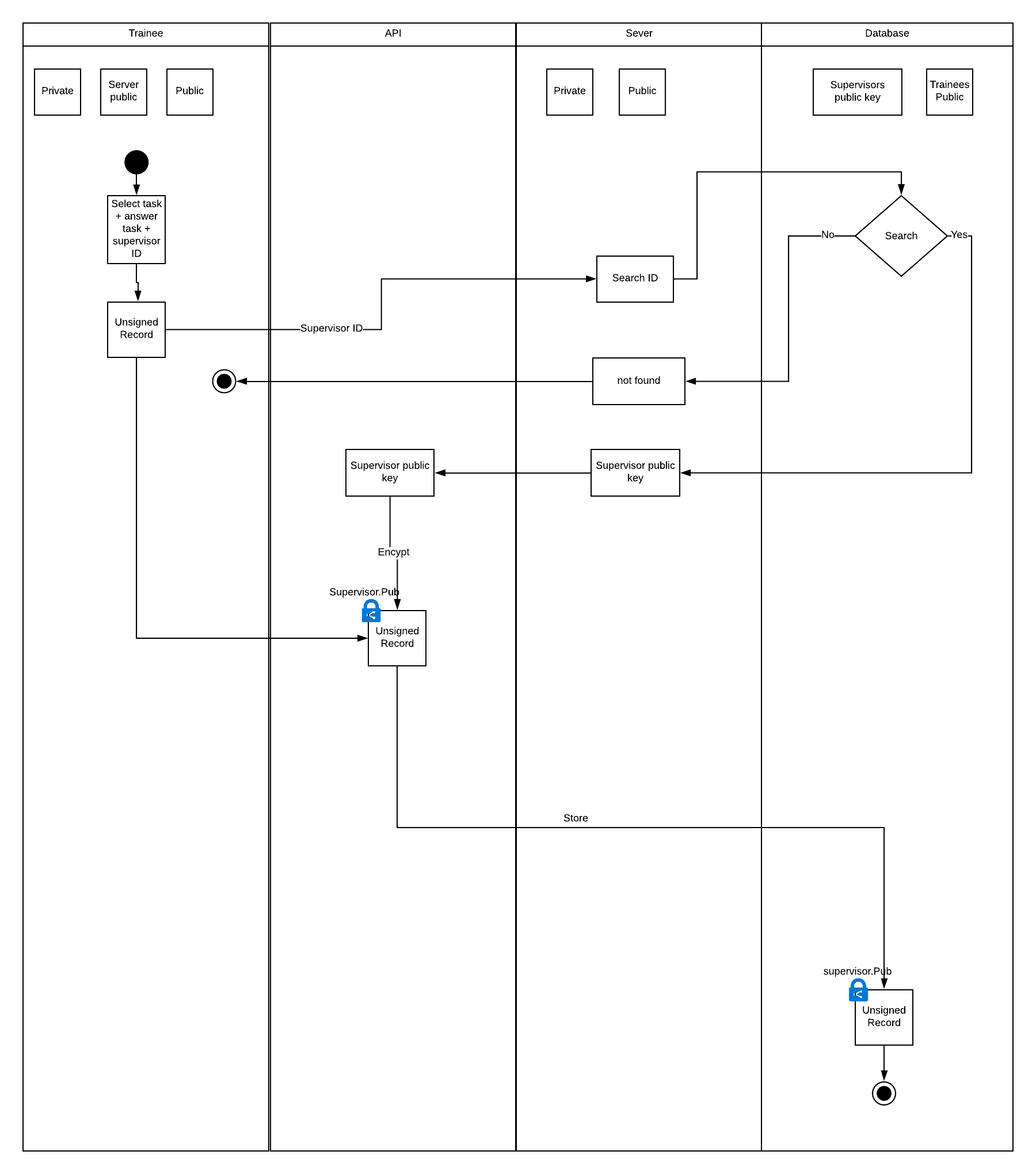
#### b. Trainee records

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| QR record | Trainee ID (encrypted) | Finished Tasks(encrypted) | Self-rating(encrypted) | Date(encrypted) | Supervisor ID | Sign status(encrypted) | Supervisor’s rating(encrypted) | Feedback(encrypted) | Hash |

* QR record: Each record has a unique QR code to identify the record.
* Trainee ID: has a reference to employee list’s ID.
* Finished tasks: contains all the tasks have been finished in the record.
* Self-rating: the level that the trainee rate by oneself.
* Supervisor ID: has a reference to employee list’s ID.
* Date: the date when the tasks finished.
* Sign status: shows if the record has been signed or not.
* Supervisor’s rating: the level that the supervisor rates the trainee.
* Feedback: optional opinions of the supervisor for the trainee.
* Hash: hashed Finished tasks, Self-rating, Supervisor’s rating, Feedback

### Security workflow

###### Make Record

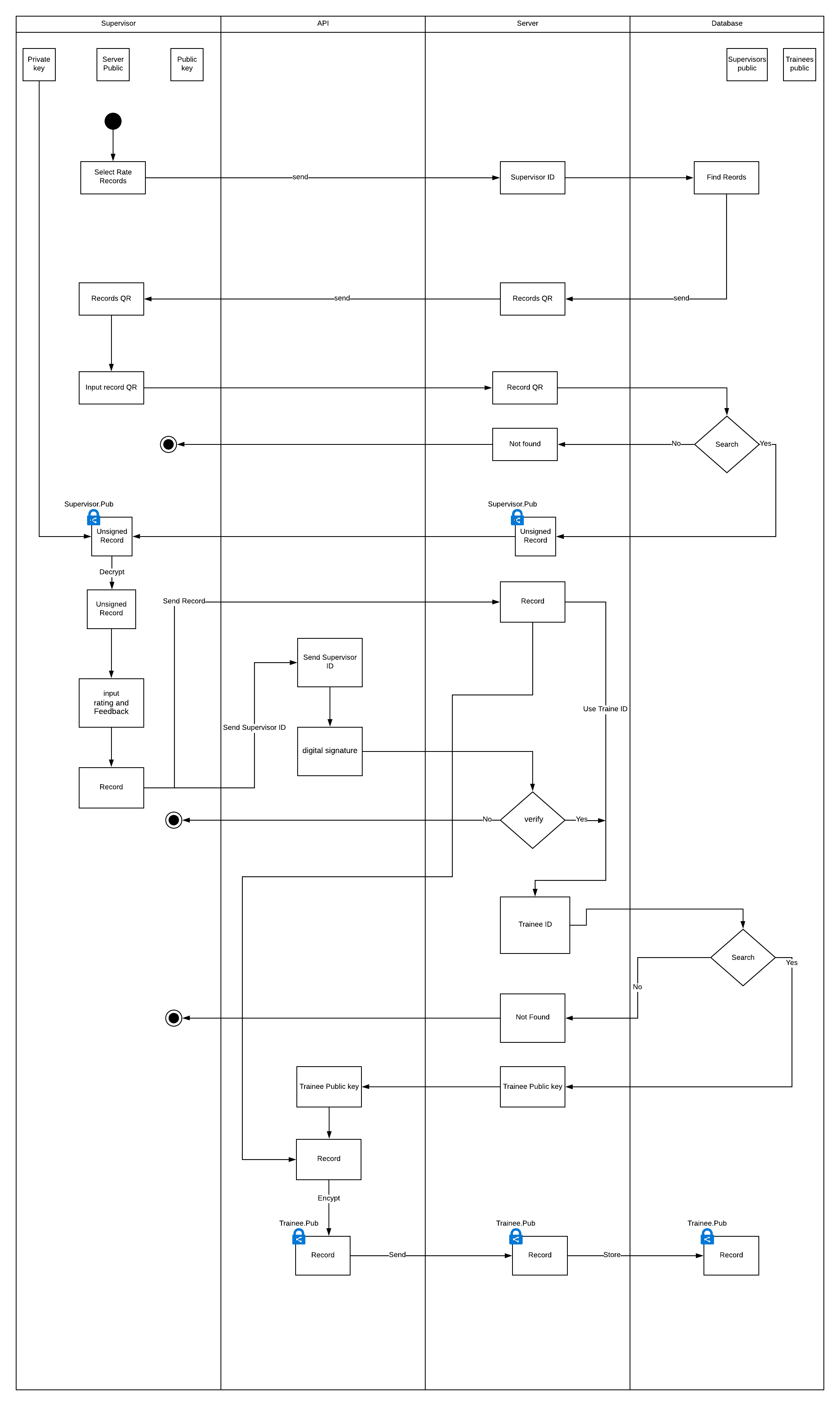


**Security Modules need to be used:**

* Encryption Module (encrypt the record for trainee)

#### When create a new record, train will fill in the Finished Tasks, Self-rating, Date and supervisor ID and this information will be encrypted by the supervisor public key. QR record will be generated by application automatically. Sign status will be “Unsigned” until the supervisor rates the record by fill in the Supervisor’s rating and Feedback.

#### Make assessment

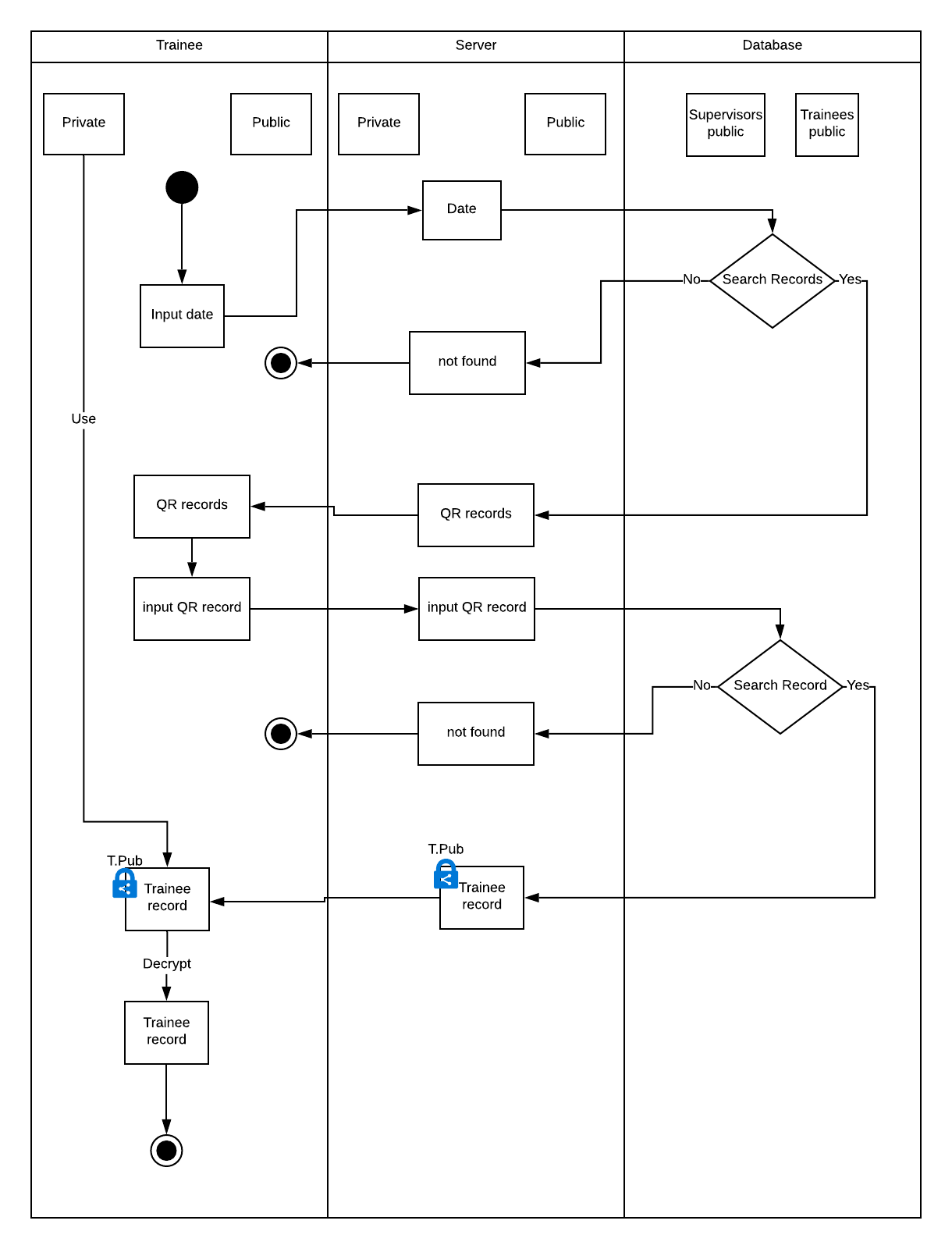


**Security Modules need to be used:**

* + Decryption Module (decrypt the record)
  + Encryption Module (encrypt the record for supervisor, trainee)
  + Digital signature Module
  + Hash Module

When supervisor want to rate records, application will use supervisor’s ID to find all the records need to be rated by the supervisor. Then supervisor will input the QR of the record. The application will load the record and supervisor will fill in the Supervisor’s rating and Feedback. After that supervisor select submit and the system will use supervisor’s ID to make digital signature for the server to verify if it is approved, the server will update the record and encrypt it by trainee public key.

#### c. Trainee see Profile:

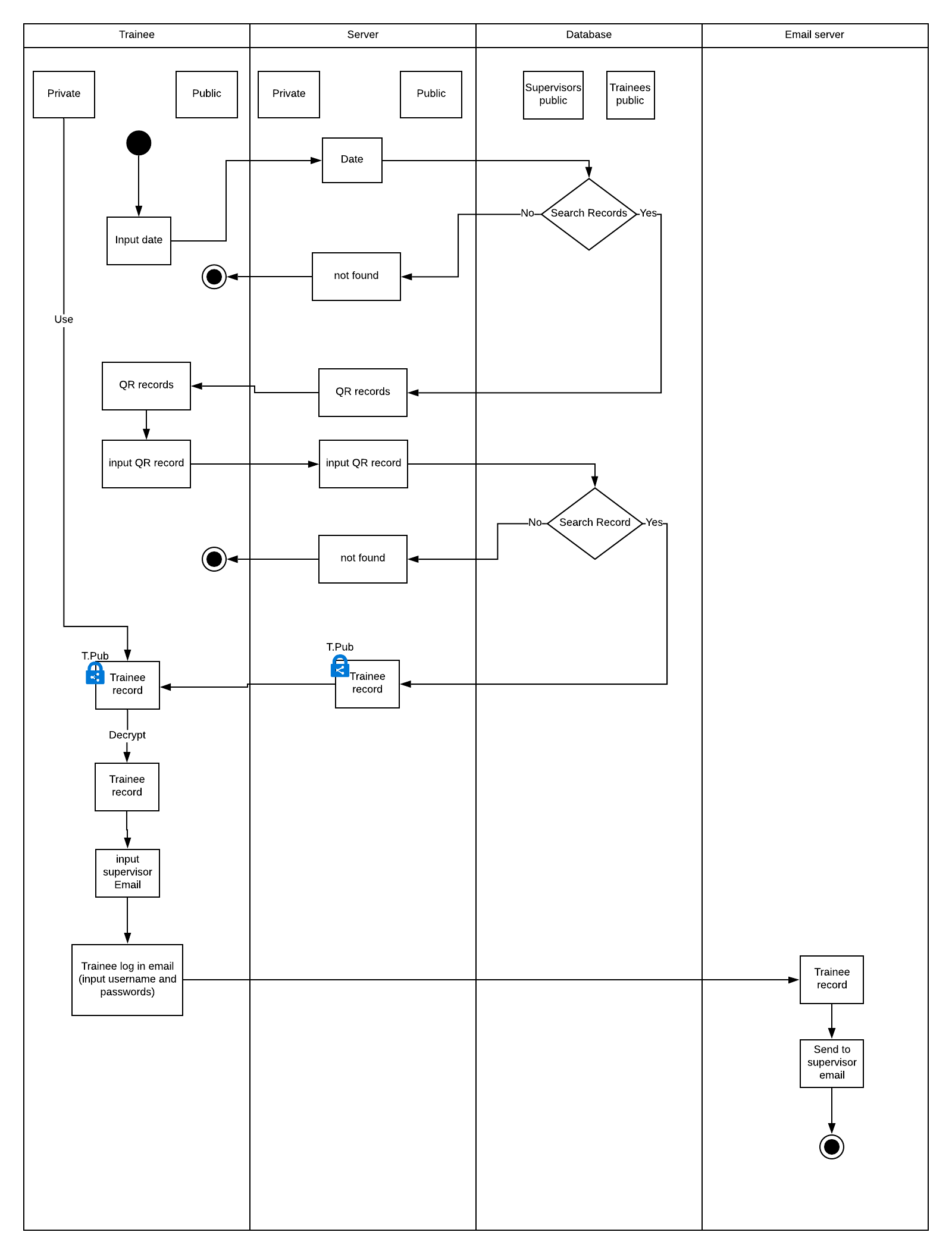


**Security Modules need to be used:**

* Decryption module (decrypt the game record).

#### To see the profile trainee will input the date of a record then application will return all the QR records of the date, so trainee can select one of those QR code to see the profile. After that the record will be decrypted on the trainee side.

#### d. Trainee shares profile to supervisor

 When trainee want to share profile to a supervisor. The trainee will select share profile then input his/her and the supervisors ’email then the record will be sent to the supervisor. The process of select a profile to share is like the See Profile Process.

## Blockchain Business Analyze:

For the sake of reliable trainee's records and competency, Blockchain is used for storing trainees' records because the data once is verified and created in a new block, it is immutable. Moreover, in the worst case, the data in that block is changed, it will create a new block and the history of the changed record also being written in the Hyperledger so that we can know what has been changed. Blockchain is also traceable so it would be much more convenient for tracking that new block was coming from which block in the chain. On top of that, the Blockchain usages in this project are to be comparing the hashing of the records in the Blockchain to the hashing of the records in Server's Database of the Rating Application and to verify the trainee's Certificate signed by the Hospital which they are working for.

In addition, comparing hashing between Blockchain storage and Rating Application Database is to know if a record has been changed in the database or not. For example: in the Rating Application database, we have a record of Record ID is 4791 and the hashing of that record is A1B2C3. So, when comparing the hashing stored in Blockchain which is equal to that record's hashing, that means it is still valid and hasn't been changed. So, we can trust the integrity of that record in the Database.

Besides, Verifying the Trainee's Certificate means every record of Trainees deployed in the Blockchain goes along with a Certificate signed by the Hospital which creates a new block of that record in the Blockchain, we can verify who signed that Certificate. If it is authorized hospital signed that record or it has been intercepted by someone who doesn't take charge of signing that Certificate.