WORKFLOW & SECURITY DOCUMENT

## 1.Database design

### 1.1Employee 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.

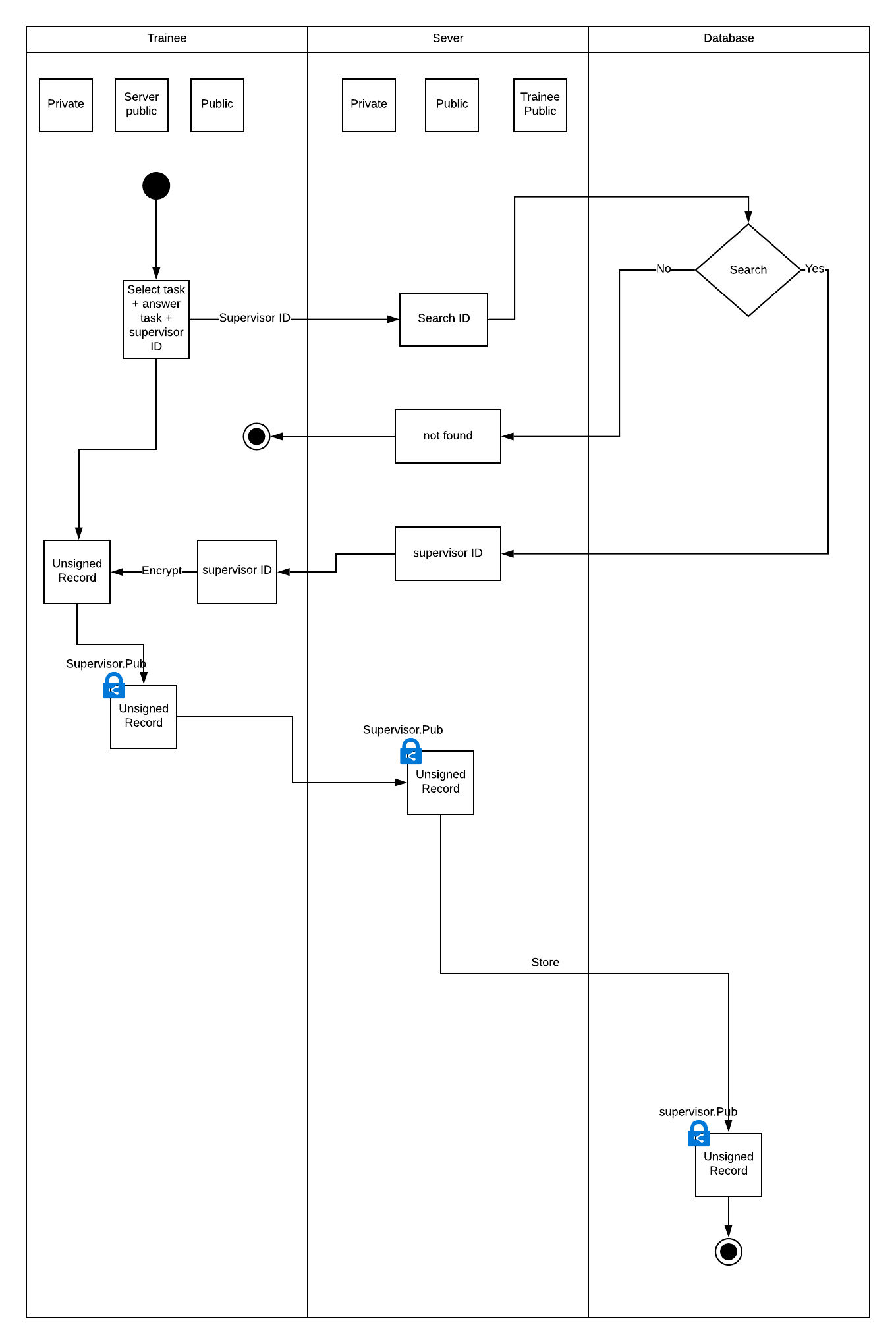
### 1.2Trainee records

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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

## 2.Security workflow

### 2.1 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 these information will be encypted by the supervisor public key. QR record will be generated by application automatically. Sign status will be “Unsigned” untill the supervisor rate the record by fill in the Supervisor’s rating and Feedback.

### 2.2 Make assessment

{PICTURE}

**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, aplication will use supervisor’s ID to find all the reocrds 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.

### 2.3 Train see Profile:

{PICTURE}

**Security Modules need to be used:**

* Decryption module (decrypt the game record).

Trainee log in the application and select see profile. The application will use trainee ID to find the records which have sign status are “SIGNED” then send back to trainee. After that the record will be decrypted on the trainee side.

### 2.4 Trainee shares profile to supervisor

{PICTURE}

When trainne want to share profile to a supervisor. The trainee will select share profile and then input the supervisor’email then the record will be sent to the supervisor.