WORKFLOW & SECURITY ANALYSIS DOCUMENT

# 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.

# Database design

## 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.

## Trainee records

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

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 pub: the public key of supervisor reference from employee list.

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.

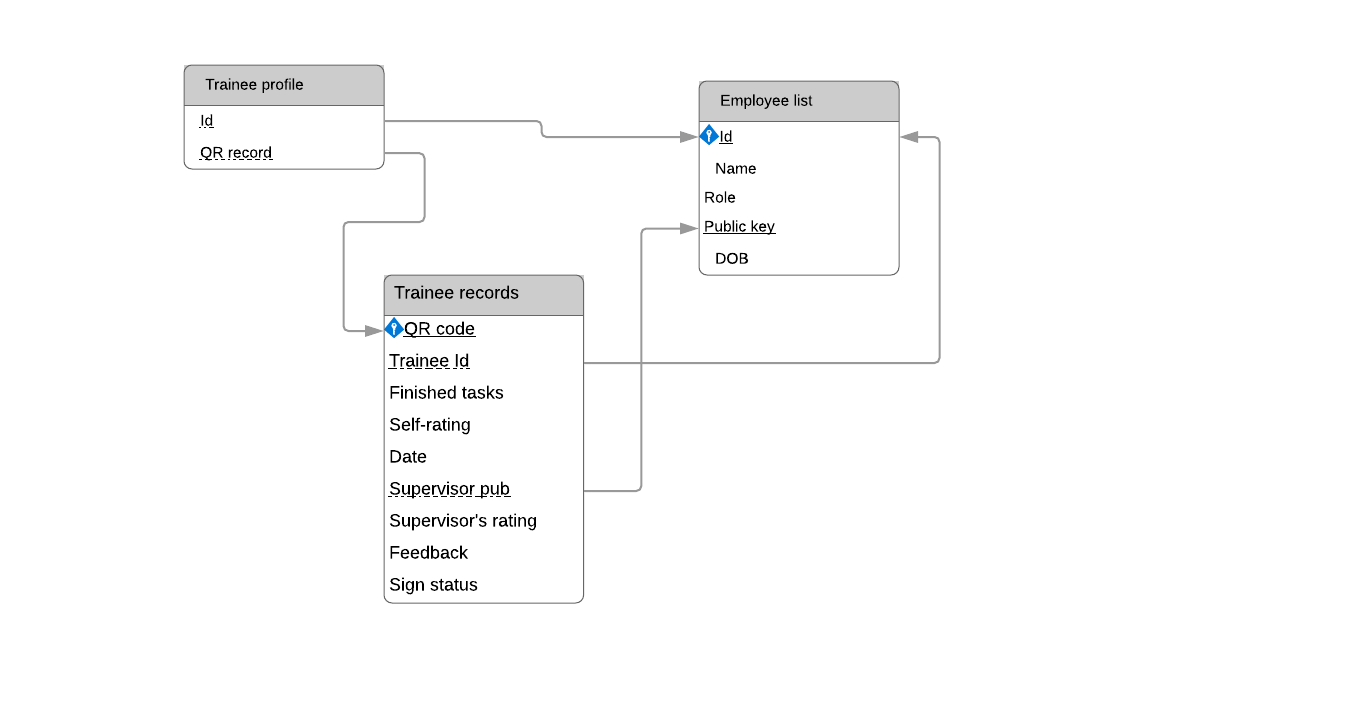
## Trainee profile

|  |  |
| --- | --- |
| ID (encrypted) | QR record(encrypted) |

ID: reference from employee list.

QR record: reference from employee list.

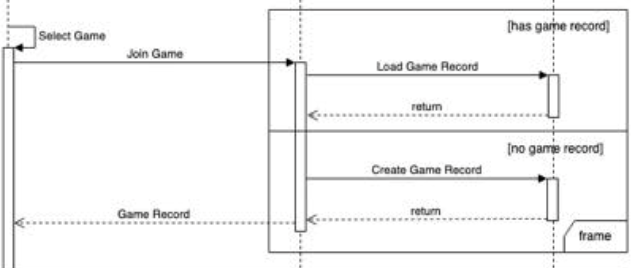
# Database scheme



# Security analyze

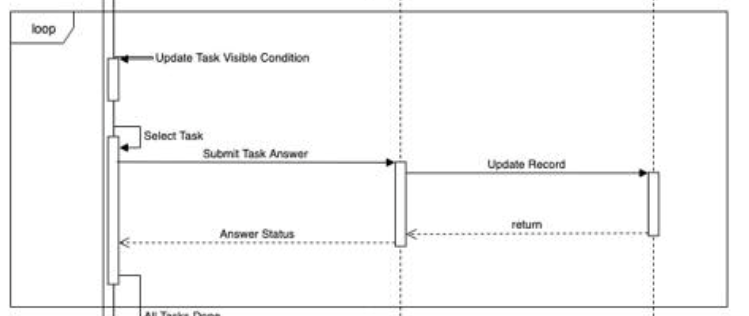
All users and server will have a key pair which called public key, private key and server’s public key, but the database stores all the public key of all users. All users also store the server’s public key.

## 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

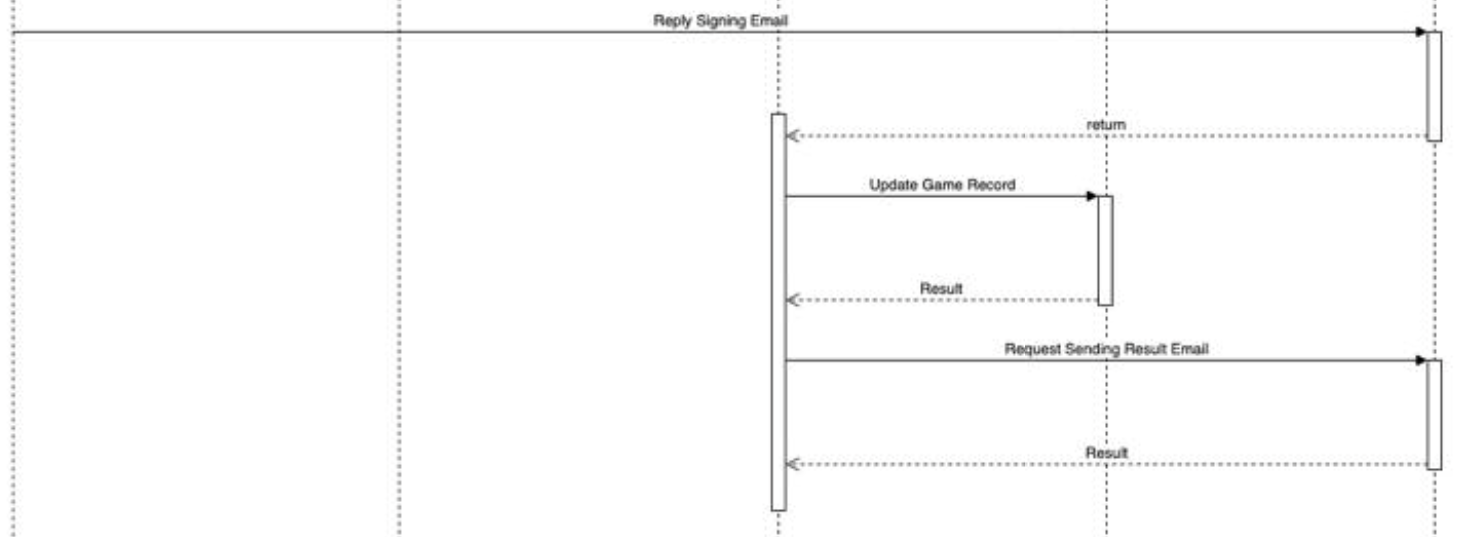
Trainee will show profile QR code (not record QR code) to supervisor, supervisor scans the QR code then send it to server include with supervisor information (QR code and public key), server uses that QR code to check if the trainee exists or not. If yes server will send the trainee encrypted profile\* 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.

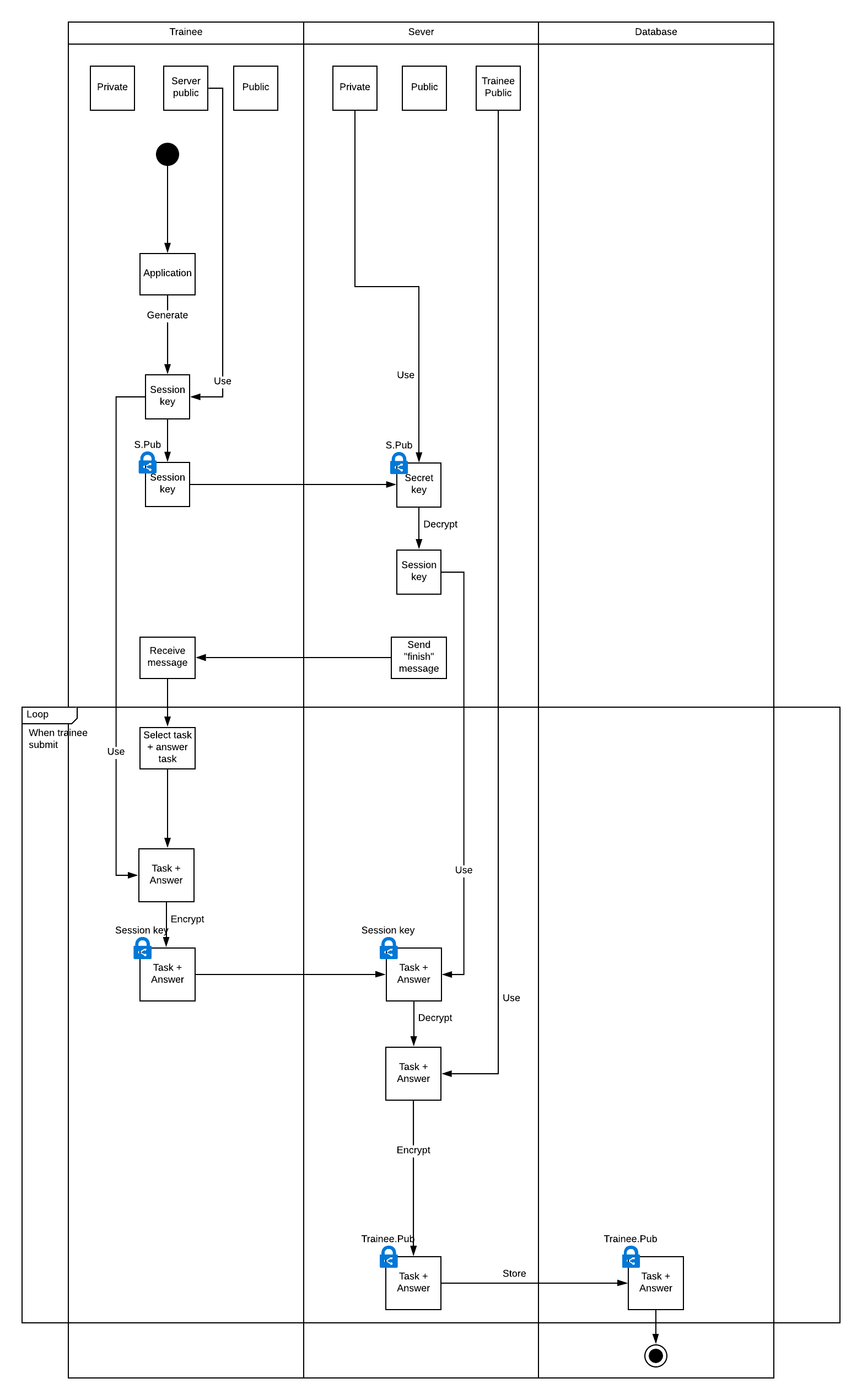
# Security workflow diagrams

## Trainee join game

**Security Modules need to be used:**

* Decryption module (decrypt the game record).

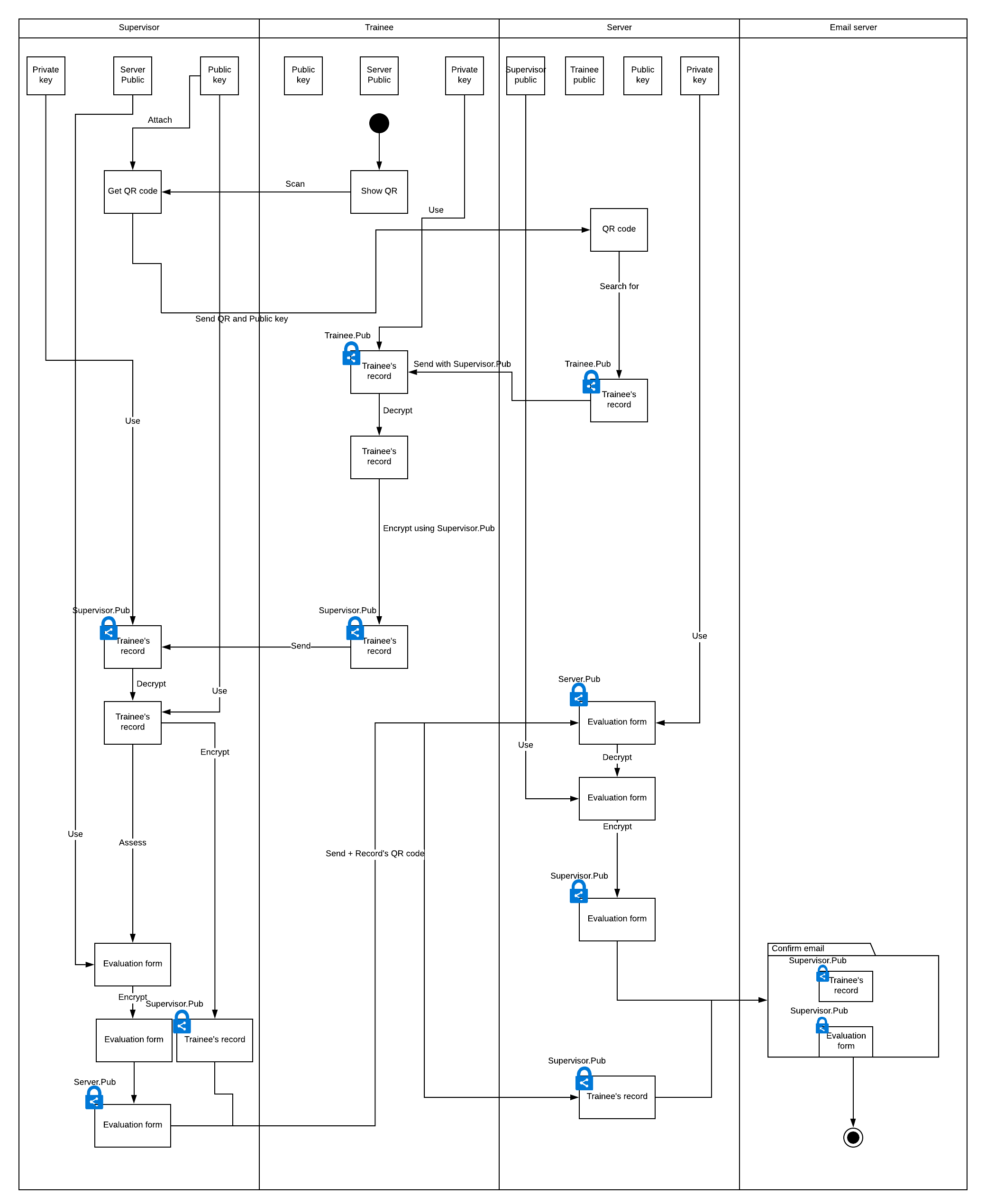
5.2 Select task



**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)

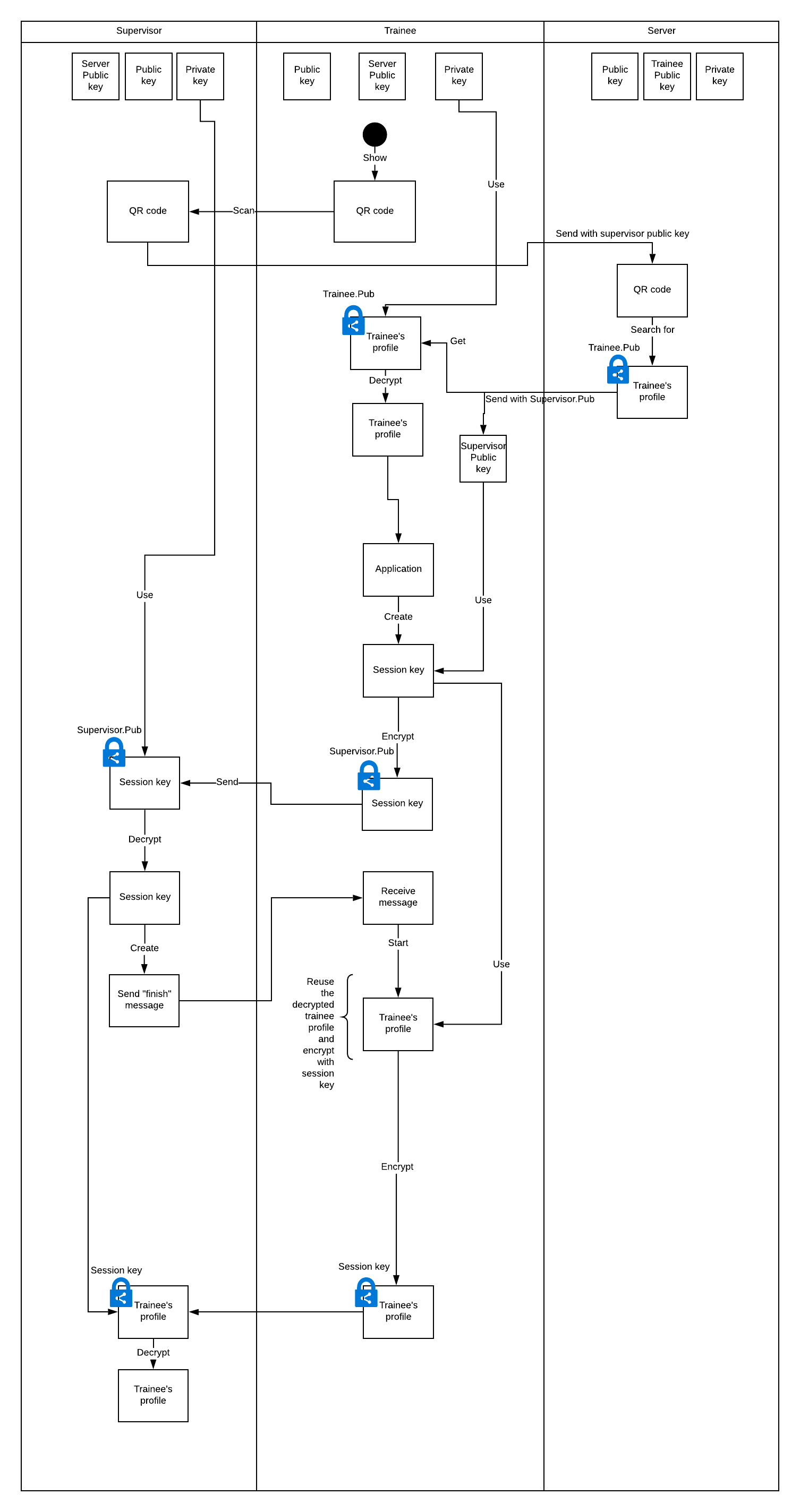
## Make assessment



**Security Modules need to be used:**

* Decryption Module (decrypt the record)
* Encryption Module (encrypt the record for supervisor)

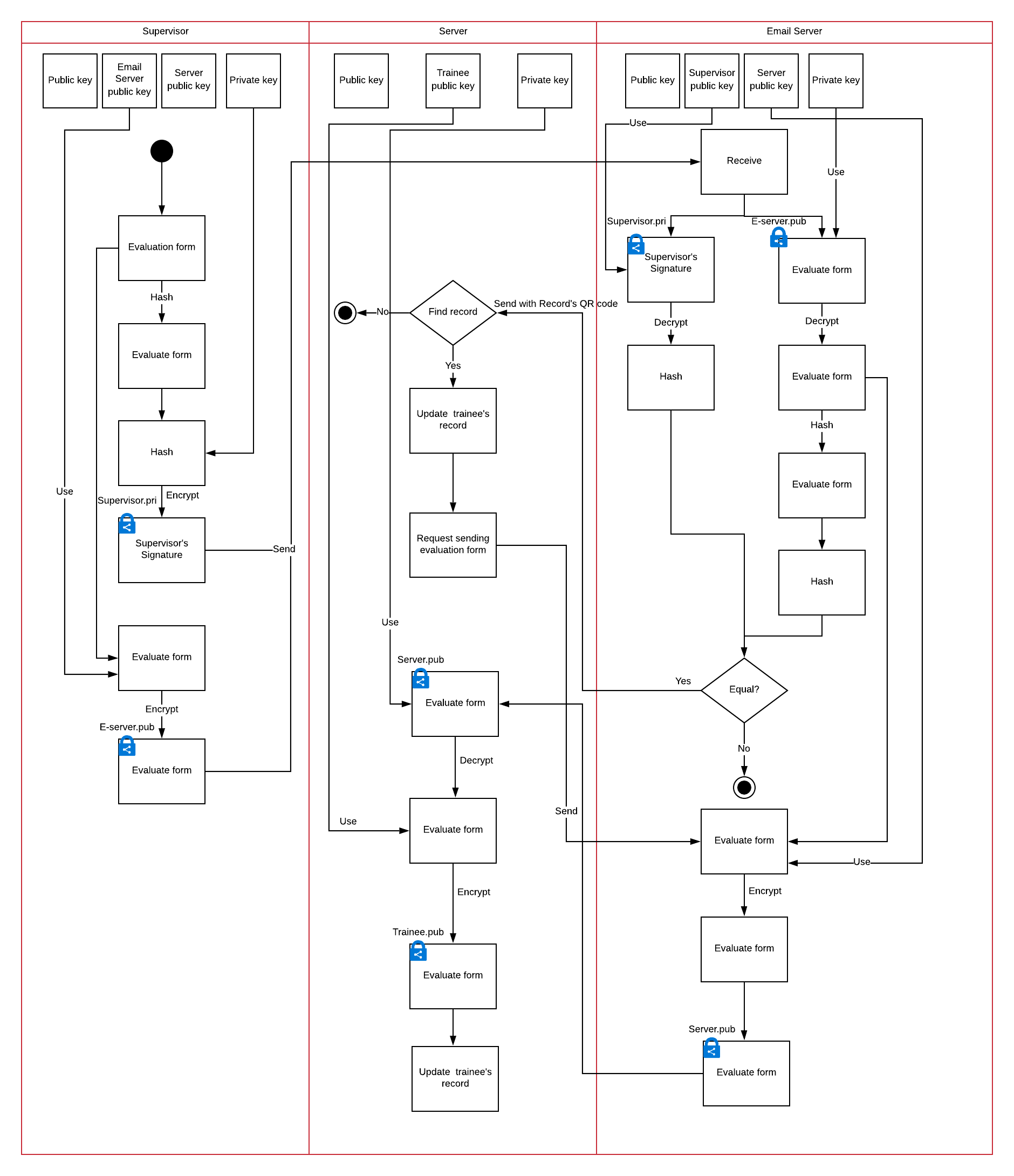
## Trainee shares profile to supervisor



**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)

## Reply signing email



**Security Modules need to be used:**

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