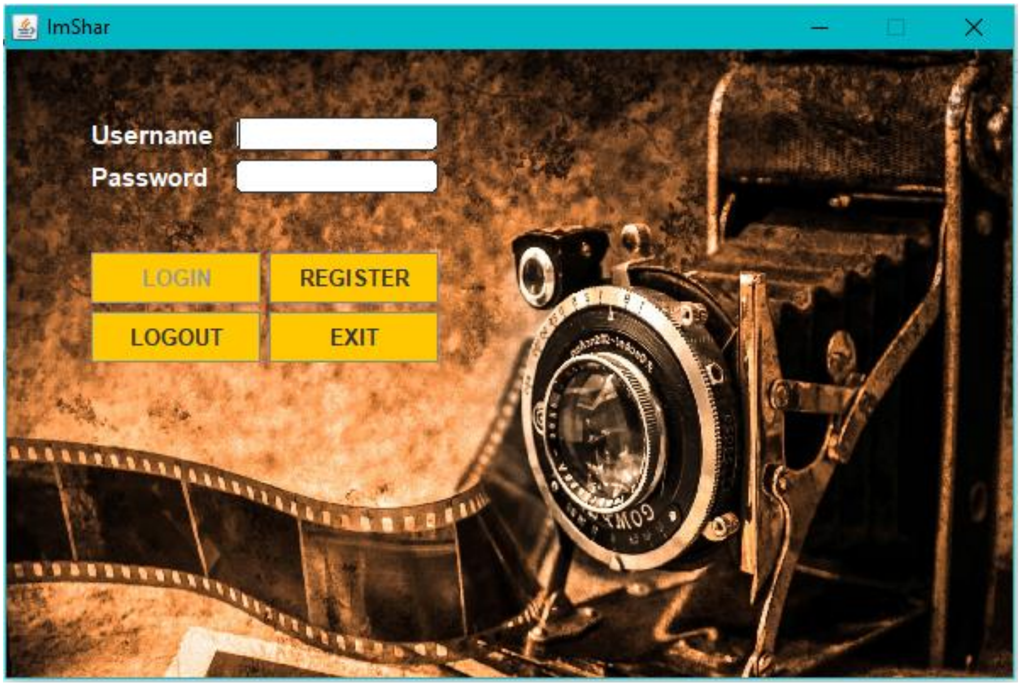
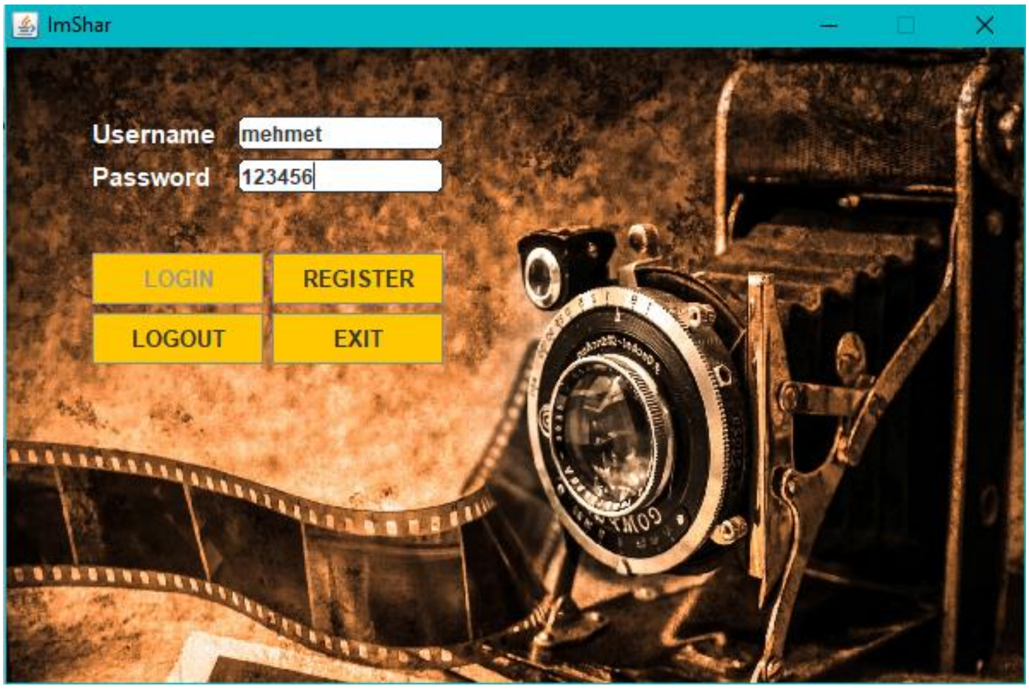
REGISTER PHASE



If user did not register, login button is disable. User can not login before register.



Username mehmet

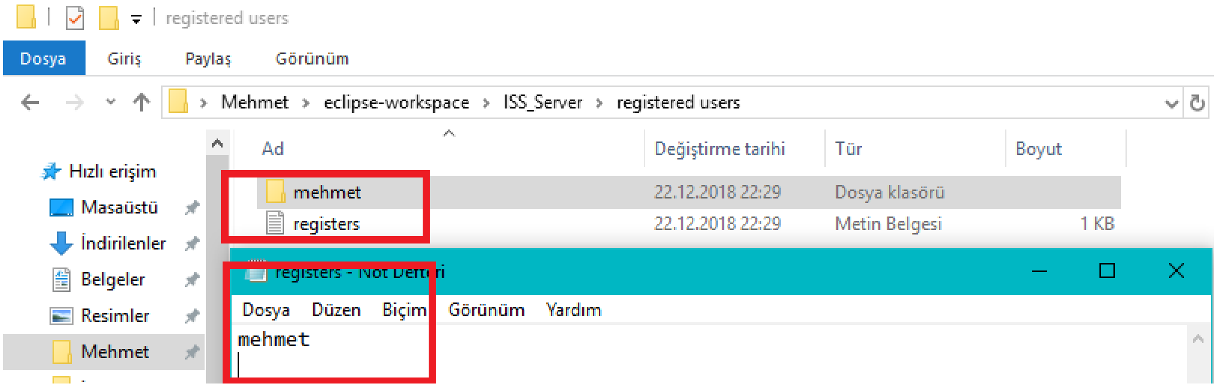
Password 123456

When user tries to register, server checks username if there is a registered user with same name, server refuse registration. If username is appropriate, then client side application creates public and private key pairs. Then send public key to the server, server certificates the public key with his/her username and send back to client. Client takes certificate and verifies it. If verify is succesful, public key, private key and username stored in client's computer.

Server , if register is succesful, for each registered user:

Appends the username to register.txt file

And creates a folder by name of username



Ad	Değiştirme tarihi	Tür	Boyut
mehmet	22.12.2018 22:29	Dosya klasörü	
registers	22.12.2018 22:29	Metin Belgesi	1 KB

```
mehmet
```

In the folder which is created by username

There is two folder image and notification

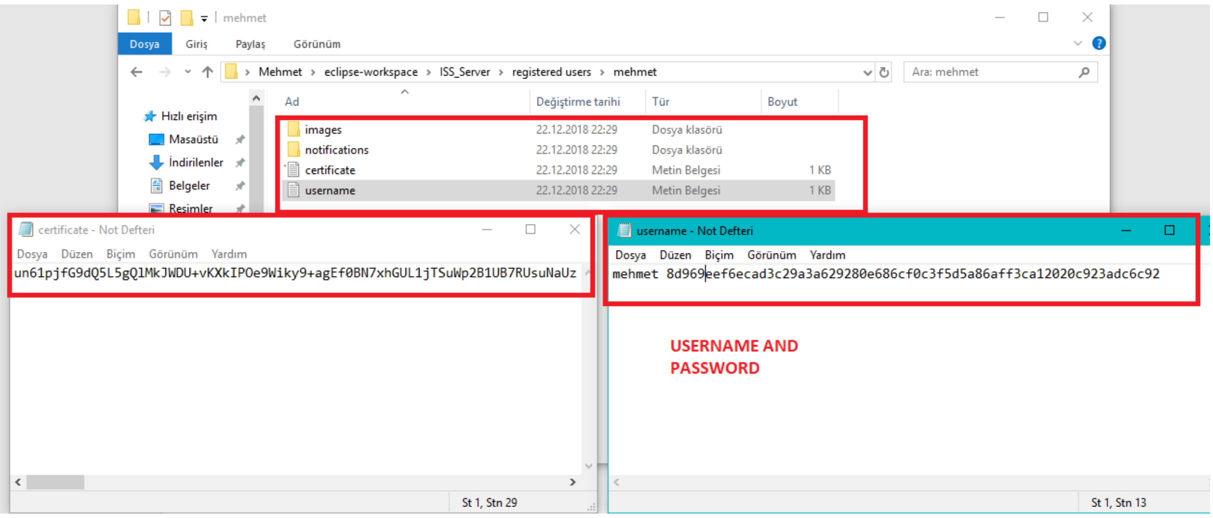
In the image folder, keept uploaded files for the user

(encrypted Aes key and encrypted IV)

In the notification folder, ketp notifications for the user

Certificate of the user stored in certificate.txt file

Username and password stored in username.txt file



Ad	Değiştirme tarihi	Tür	Boyut
images	22.12.2018 22:29	Dosya klasörü	
notifications	22.12.2018 22:29	Dosya klasörü	
certificate	22.12.2018 22:29	Metin Belgesi	1 KB
username	22.12.2018 22:29	Metin Belgesi	1 KB

```
un61pjfG9dQ5L5gQ1MkJWDU+vKXkIPOe9Wiky9+agEf0BN7xhGUL1jTSuWp2B1UB7RUsuNaUz
```

```
mehmet 8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92
```

USERNAME AND PASSWORD

Register features:

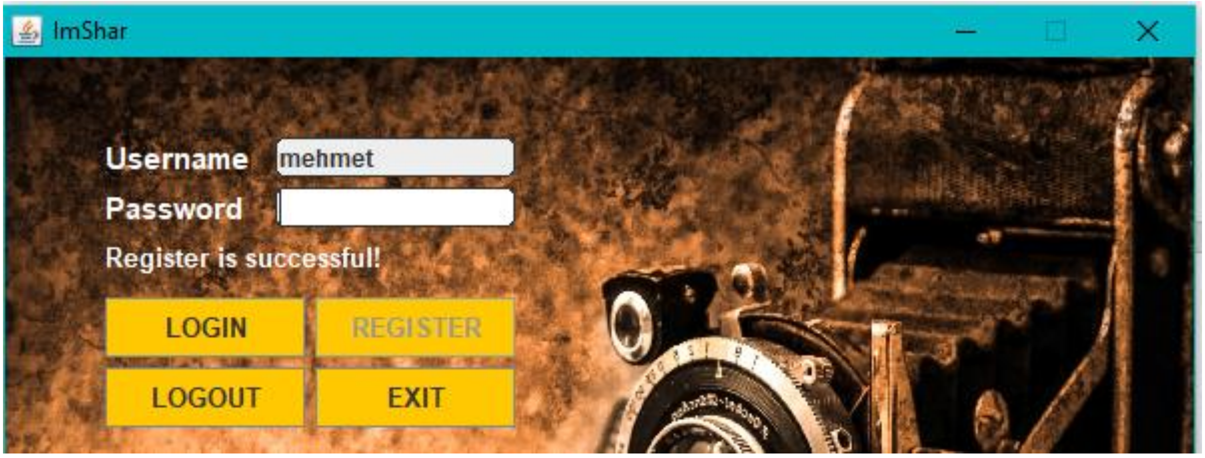
Can not register same name.

Can not login before register.

If certificate is not verified does not register.

LOGIN PHASE

In the client's pc, in the username.txt file there can be only one username. Application catch username from username.txt file and writes it to the field. Then, disable to edit the field. Client enters password to the field and clicks on login button. Server checks first username and password if it is correct then checks user online or not. If everything is ok clients logs in the server.



Username: mehmet

Password:

Register is successful!

Also, if there is someting in the username.txt file register button is disabled.

Login features

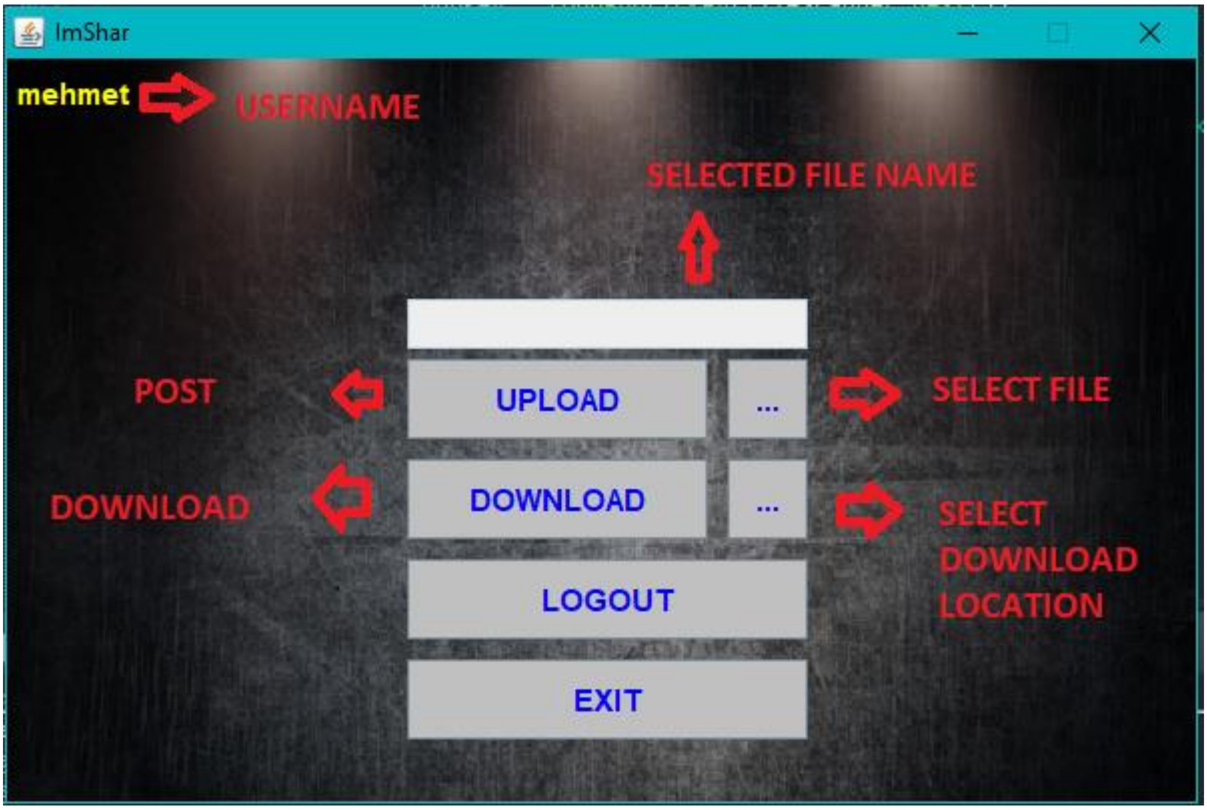
In this design, there is some advantages and disadvantages

Advantages :

Looking in terms of security, user can only login where the user is registered. Even, trudy knows password she can not login because can not login before register.

Disadvantages :

User can not login in another computer. Also, if he/she logs out can not login in any computer.



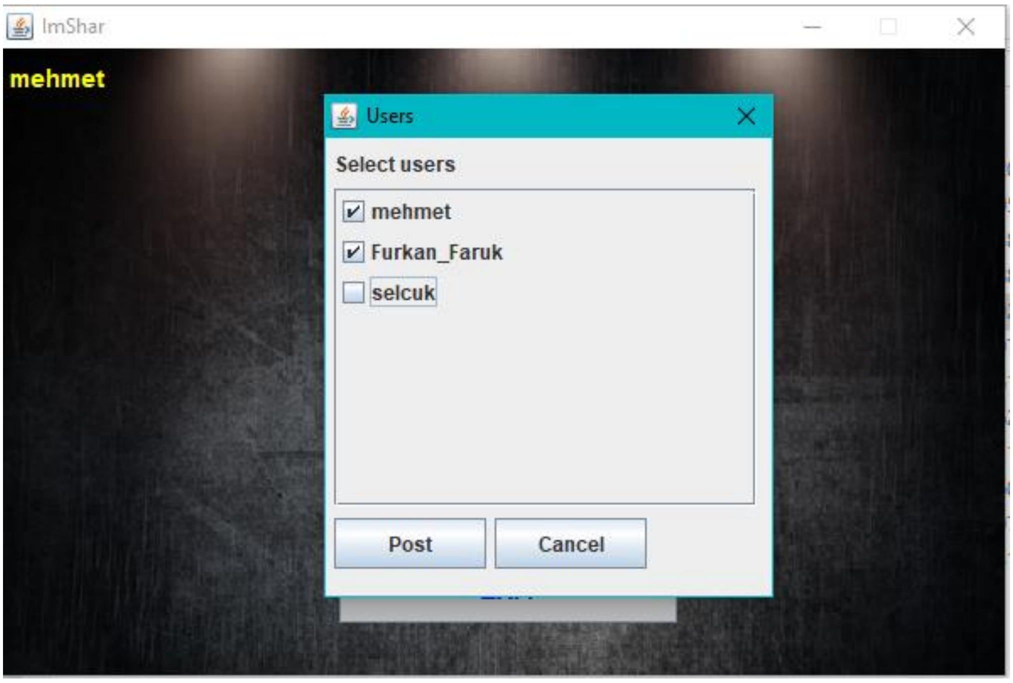
POST FILE PHASE

Post phase has 2 steps.

First step

Select a file from pc and click on upload button

At the background, client send file name to server. Server checks availability of file name. If it is available user get user list from server. Then, creates checkboxes.



Second step

User select the user, he/she want to post. Then clicks on post button.

At the background, client does as follow:

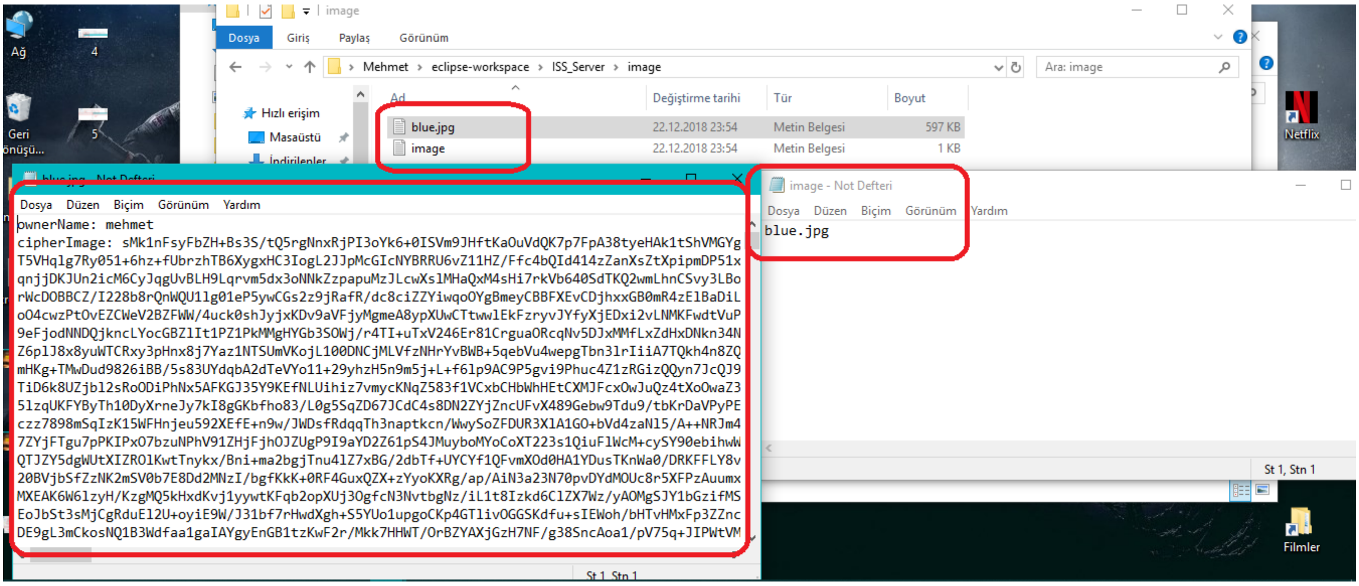
- Generates 16 bytes symmetric key and IV.
- Convert file to string.
- Encrypt the string with AES by the symmetric key and IV
- Take hash function of string (not encrypted one) and encrypt it with his/her private key. (digital signature)
- Send image name, cipher file, and digital signature to server.
- Check for each checkboxes selected or not, for selected ones want his/her certificate from server, verify it (with the name) and encrypt symmetric key and IV with the public key. And, send them to server

Server side:

On the public area:

Create a text file named with file name posted, and store owner name, cipher file, digital signature and certificate in this text file.

Also, append the file name to the image.txt file (this file makes easy to check file name in the first step)



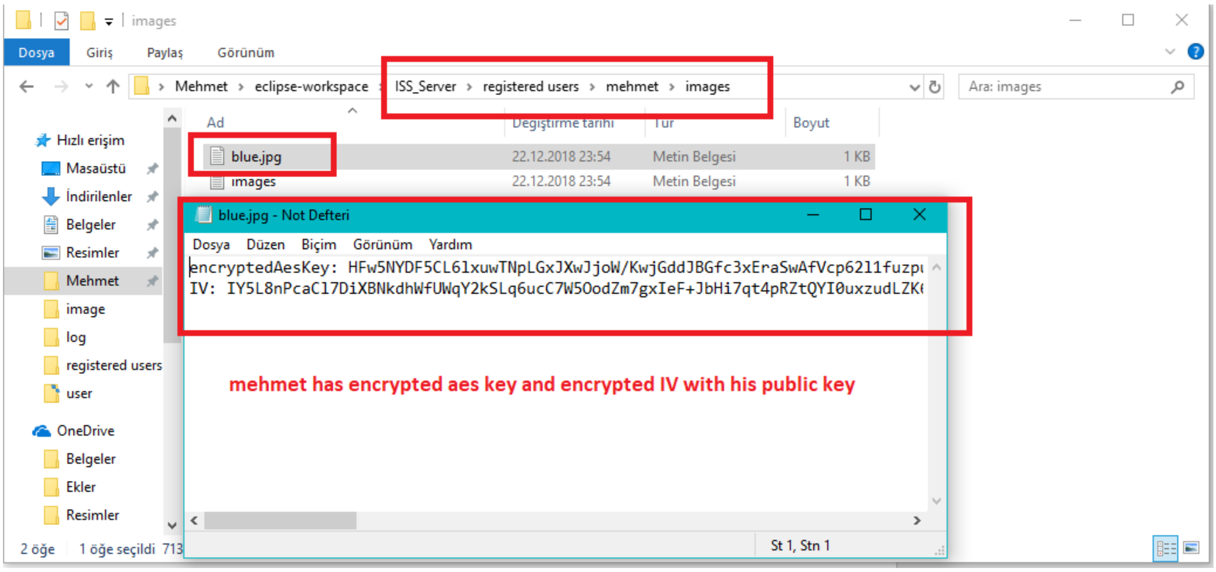
```
ownerName: mehmet
cipherImage: sMk1nFsyFbZH+Bs3S/tQ5rgNnxRjPI3oYk6+0ISVm9JHftKaOuVdQK7p7FpA38tyeHAk1tShVMGYg
T5VHqlg7Ry051+6hz+fUbrzhTB6XygxHC3IogL2JJpMcGIcNYBRRU6vZ11HZ/Ffc4bQId414zZanXsZtXpipmDP51x
qnjjDKJUn2icM6CyJqgUvBLH9Lqrvm5dx3oNNkZzpapuMzJLcwXslMHaQxM4sHi7rkVb640SdTKQ2wmLhnCSvy3LBo
rWcDOBBCZ/I228b8rQnWQU1lg01eP5ywCGs2z9jRafR/dc8ciZZYiwqoOYgBmeyCBBFXEvCDjhxxGB0mR4zElBaDiL
oO4cwzPtOvEZCWeV2BZFWW/4uck0shJyjxKDv9aVFjyMgmeA8ypXUwCTtwwlEkFzryvJYfyXjEDxi2vLNMKFwdtVuP
9eFjodNNDQjkncLYocGBZlIt1PZ1PkMMgHYGb3SOWj/r4TI+uTxV246Er81CrguaORcqNv5DJxMMfLxZdHxDNkn34N
Z6plJ8x8yuWTCRxy3pHnx8j7Yaz1NTSUmVKojL100DNCjMLVfzNHrYvBWB+5qebVu4wepgTbn3lrIiiA7TQkh4n8ZQ
mHKg+TMwDud9826iBB/5s83UYdqbA2dTeVYo11+29yhzH5n9m5j+L+f6lp9AC9P5gvi9Phuc4Z1zRGizQQyn7JcQJ9
TiD6k8UZjbl2sRoODiPhNx5AFKGJ35Y9KEfNLUihiz7vmycKNqZ583f1VCxbCHbWhHEtCXMJFcxOwJuQz4tXoOwaZ3
5lzqUKFYByTh10DyXrneJy7kI8gGKbfho83/L0g5SqZD67JCdC4s8DN2ZYjZncUFvX489Gebw9Tdu9/tbKrDaVPyPE
czz7898mSqIzK15WFHnjeu592XEfE+n9w/JWDsfRdqqTh3naptkcn/WwySoZFDUR3XlA1GO+bVd4zaNl5/A++NRJm4
7ZYjFTgu7pPKIPxO7bzuNPhV91ZHjFjhOJZUgP9I9aYD2Z61pS4JMuyboMYoCoXT223s1QiuFlWcM+cySY90ebihwW
QTJZY5dgWUtXIZROlKwtTnykx/Bni+ma2bgjTnu4lZ7xBG/2dbTf+UYCYf1QFvmXOd0HA1YDusTKnWa0/DRKFFLY8v
20BVjbSfZzNK2mSV0b7E8Dd2MNzI/bgfKkK+0RF4GuxQZX+zYyoKXRg/ap/AiN3a23N70pvDYdMOUc8r5XFPzAuumx
MXEAK6W6lzyH/KzgMQ5kHxdKvj1yywtKFqb2opXUj3OgfcN3NvtbgNz/iL1t8Izkd6ClZX7Wz/yAOMgSJY1bGzifMS
EoJbSt3sMjCgRduEl2U+oyiE9W/J31bf7rHwdXgh+S5YUo1upgoCKp4GTlivOGGSKdfu+sIEWoh/bHTvHMxFp3ZZnc
DE9gL3mCkosNQ1B3Wdfaa1gaIAYgyEnGB1tzKwF2r/Mkk7HHWT/OrBZYAXjGzH7NF/g38SncAoa1/pV75q+JIPWtVM
```

```
blue.jpg
```

On the private areas:

Stored encrypted symmetric key and encrypted IV

And also, image name in the image.txt file (makes download easy)



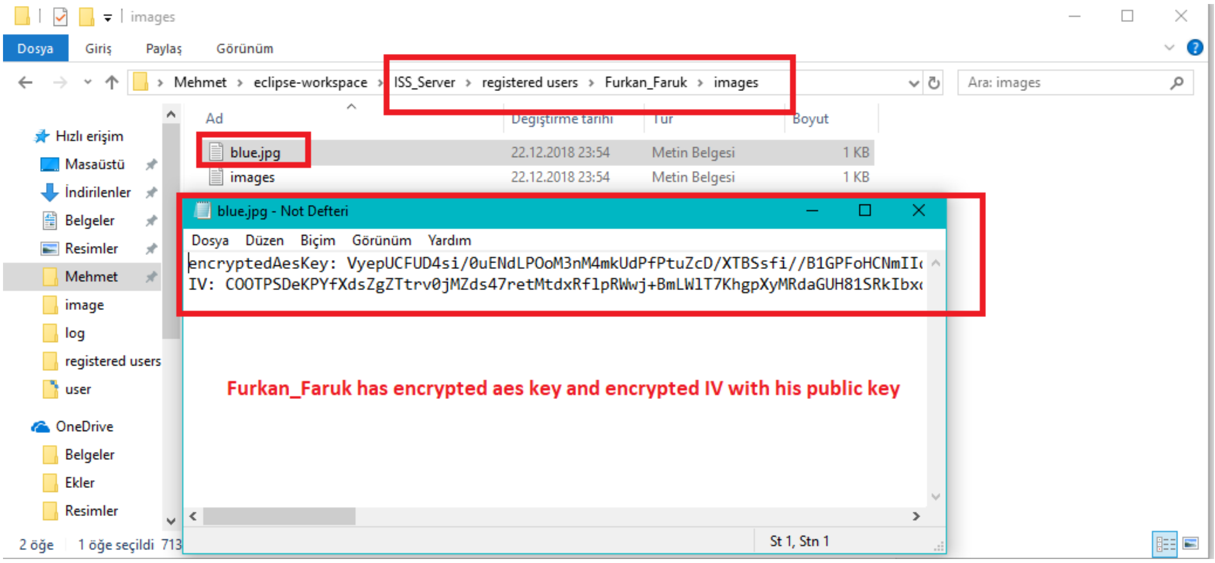
Mehmet > eclipse-workspace > ISS_Server > registered users > mehmet > images

Ad	Değiştirme tarihi	Tür	Boyut
blue.jpg	22.12.2018 23:54	Metin Belgesi	1 KB
images	22.12.2018 23:54	Metin Belgesi	1 KB

blue.jpg - Not Defteri

```
encryptedAesKey: HFw5NYDF5CL61xuwTNpLGxJXwJjoW/KwjGddJBGfc3xEraSwAfVcp6211fuzp
IV: IY5L8nPcaCl7DiXBNkdhWfUWqY2kSLq6ucC7W5OodZm7gxIeF+JbHi7qt4pRZtQYI0uxzudLZK
```

mehmet has encrypted aes key and encrypted IV with his public key



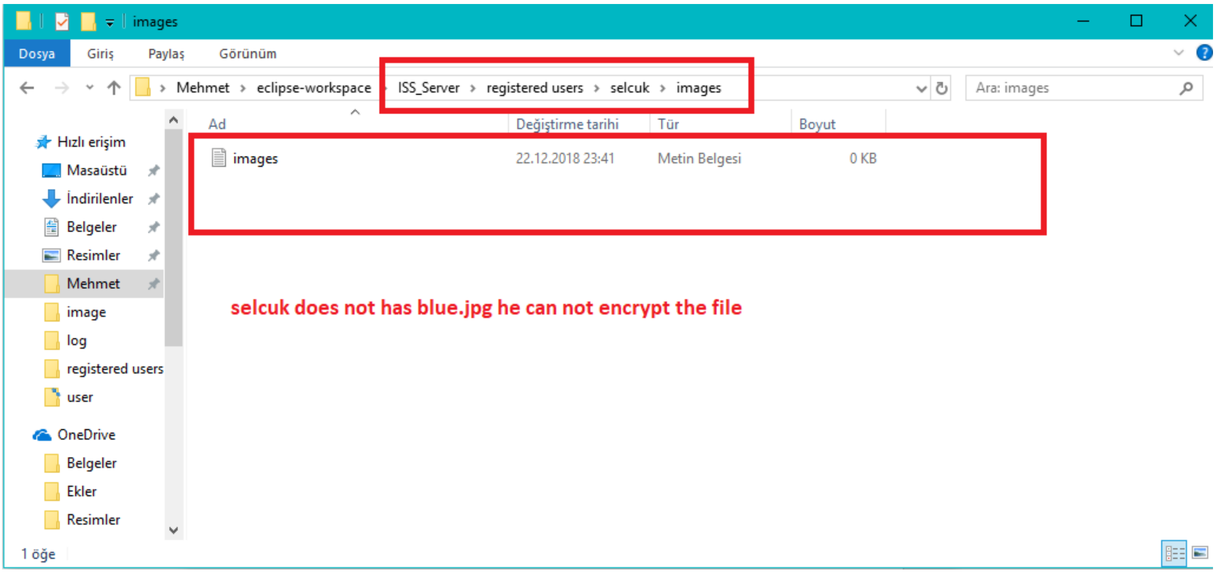
Mehmet > eclipse-workspace > ISS_Server > registered users > Furkan_Faruk > images

Ad	Değiştirme tarihi	Tür	Boyut
blue.jpg	22.12.2018 23:54	Metin Belgesi	1 KB
images	22.12.2018 23:54	Metin Belgesi	1 KB

blue.jpg - Not Defteri

```
encryptedAesKey: VyepUCFUD4si/0uENdLPOoM3nM4mkUdPfPtuZcD/XTBSsfi//B1GPFoHCNmII
IV: COOTPSDeKPYfXdsZgZTtrv0jMZds47retMtdxRflpRWwj+BmLWlT7KhgpXyMRdaGUH81SRkIbx
```

Furkan_Faruk has encrypted aes key and encrypted IV with his public key



Mehmet > eclipse-workspace > ISS_Server > registered users > selcuk > images

Ad	Değiştirme tarihi	Tür	Boyut
images	22.12.2018 23:41	Metin Belgesi	0 KB

selcuk does not has blue.jpg he can not encrypt the file

Post file features

Server does not be able to decrypt file either trudy. (in the scenario above only mehmet and Furkan_Faruk can do)

Download File Phase

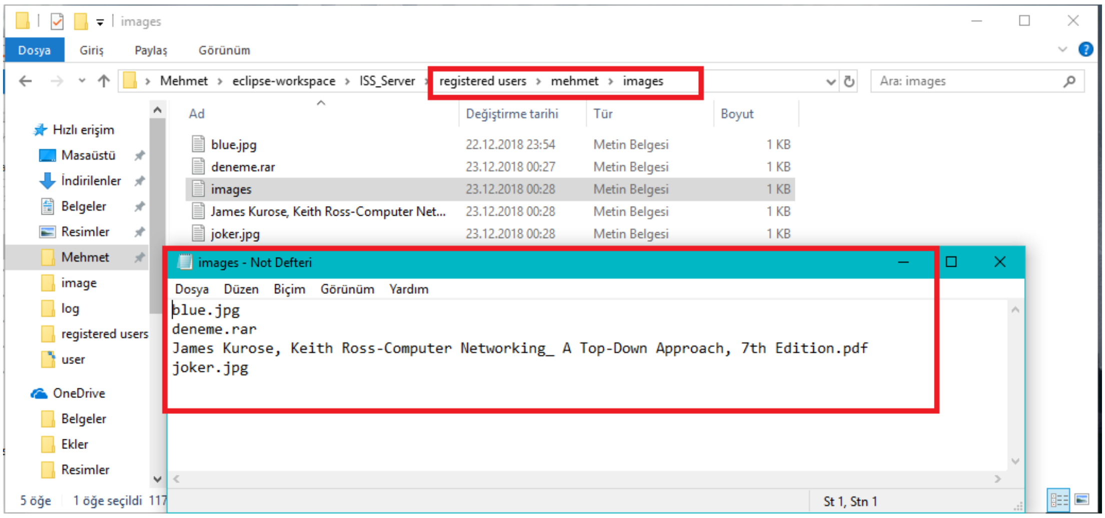
Download phase has also 2 steps.

First step

Select a download location and click on download button

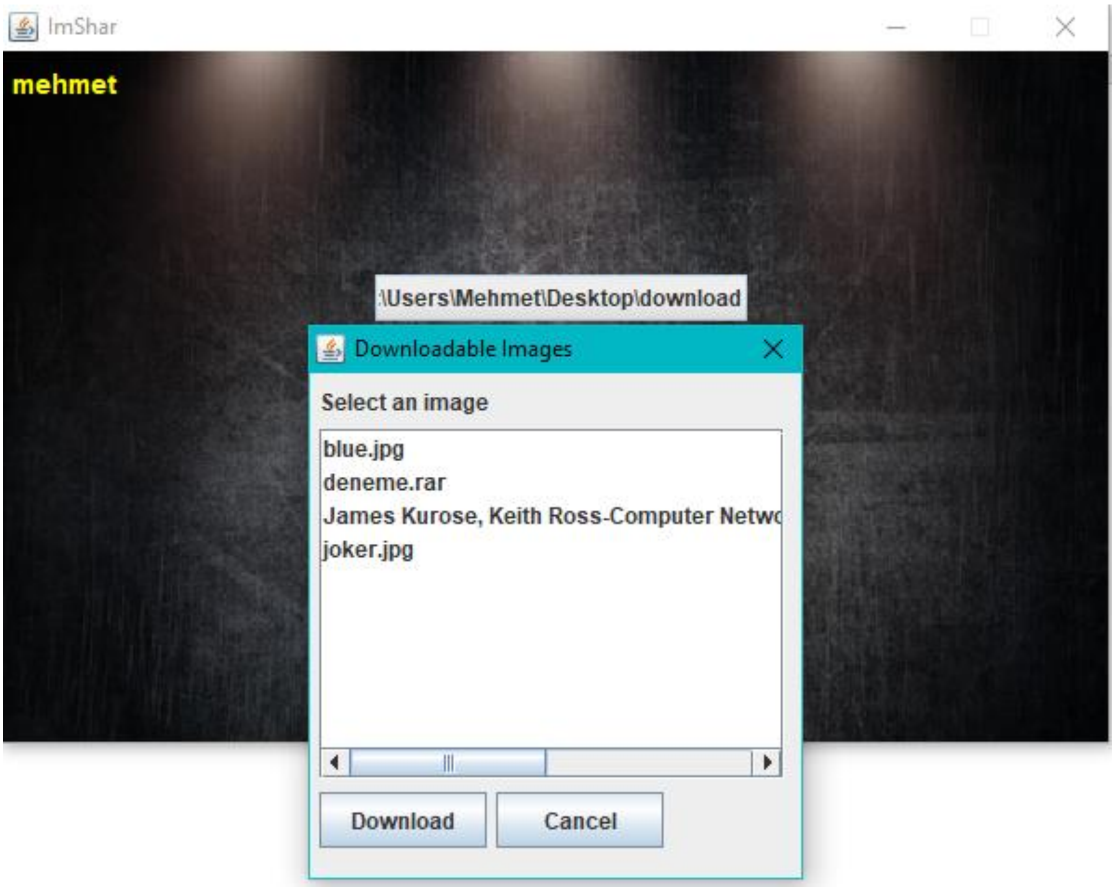
At the background, server send downloadable files to server. Client creates a list and a scroll pane from the list.

Downloadable file names in the list taken from private are in the image.txt name



Ad	Değiştirme tarihi	Tür	Boyut
blue.jpg	22.12.2018 23:54	Metin Belgesi	1 KB
deneme.rar	23.12.2018 00:27	Metin Belgesi	1 KB
images	23.12.2018 00:28	Metin Belgesi	1 KB
James Kurose, Keith Ross-Computer Net...	23.12.2018 00:28	Metin Belgesi	1 KB
joker.jpg	23.12.2018 00:28	Metin Belgesi	1 KB

```
blue.jpg
deneme.rar
James Kurose, Keith Ross-Computer Networking_ A Top-Down Approach, 7th Edition.pdf
joker.jpg
```



blue.jpg
deneme.rar
James Kurose, Keith Ross-Computer Netwo
joker.jpg

Step 2

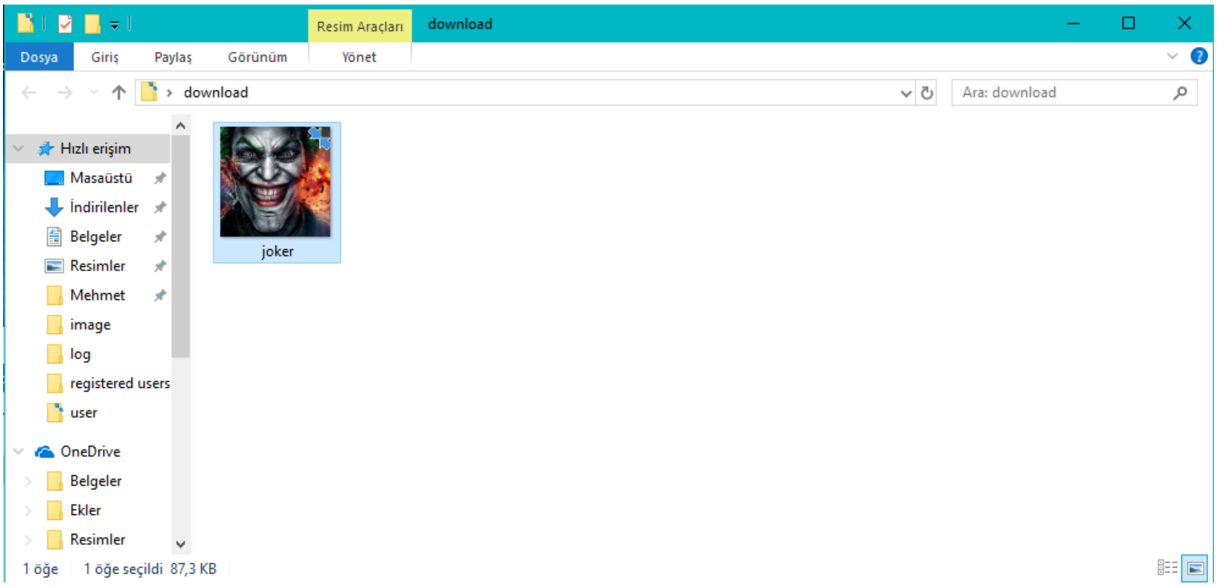
When user select a file and clicks on download button

Server sends to user

- Owner name from public area
- Cipher file from public area
- Digital signature from public area
- Certificate from public area
- Encrypted symmetric key from private area
- Encrypted IV from private area

User does as follows

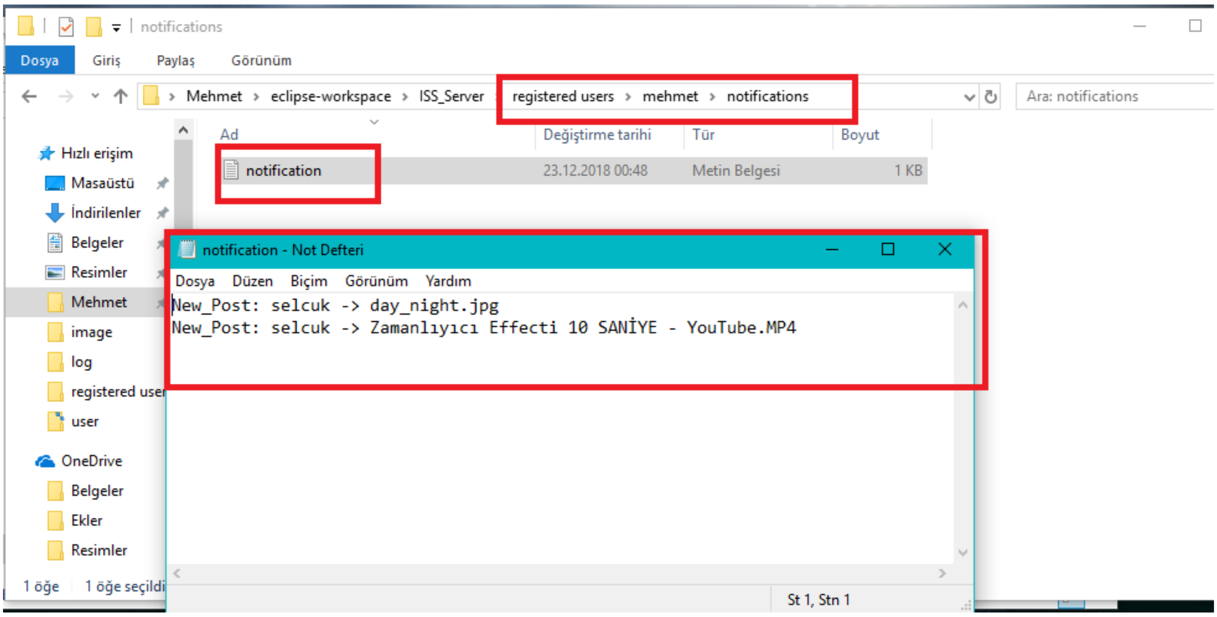
- Decrypt symmetric key with private key
- Decrypt IV with private key
- Decrypt file with symmetric key and IV
- Extract certificate and control certificate name with owner name
- Take hash funtion of file
- Decrypt digital signature with owner's public key
- Compare signature and hash function
- If everything is ok convert string to file



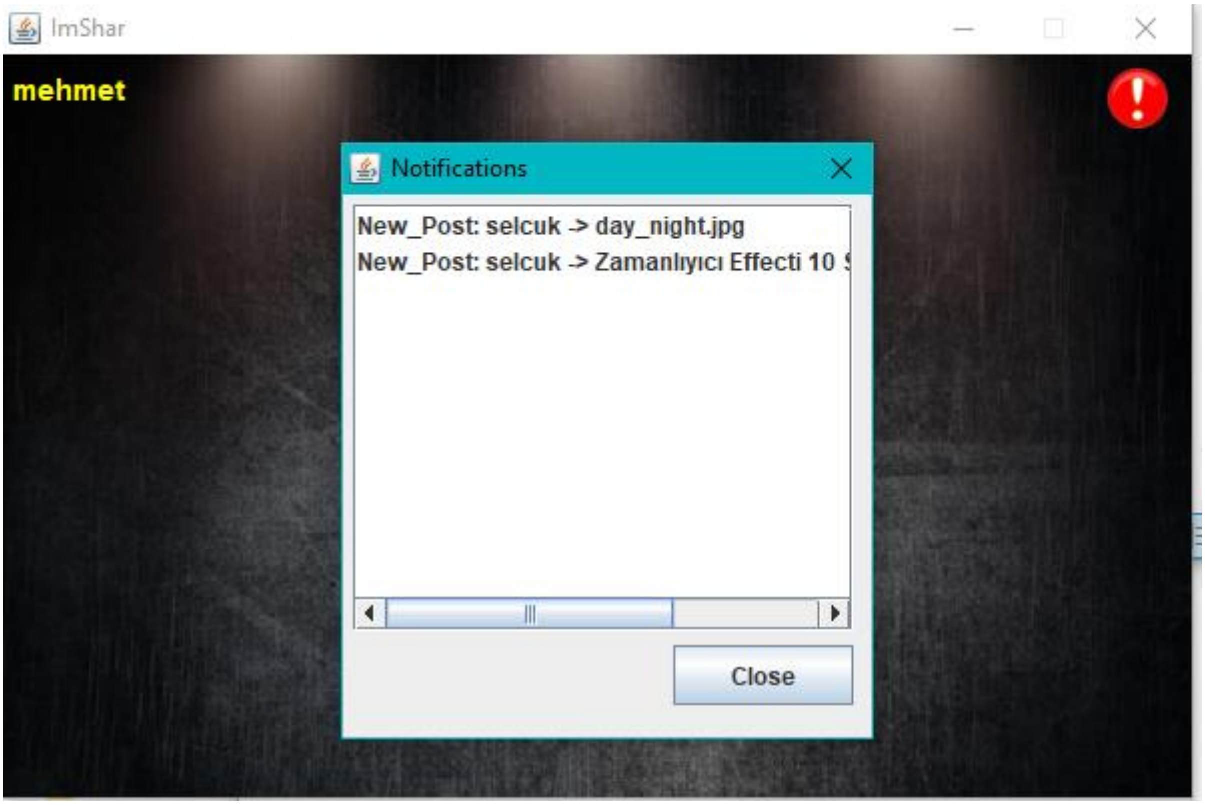
NOTIFICATON PHASE

Client ask every 5 second to server for notification if there is a notification server send it to client.

Notificaitons kept on private area in notification.txt file, even user is offline they stores when user is online send them to user.



```
New_Post: selcuk -> day_night.jpg
New_Post: selcuk -> Zamanlıyıcı Effecti 10 SANİYE - YouTube.MP4
```



```
New_Post: selcuk -> day_night.jpg
New_Post: selcuk -> Zamanlıyıcı Effecti 10 S
```

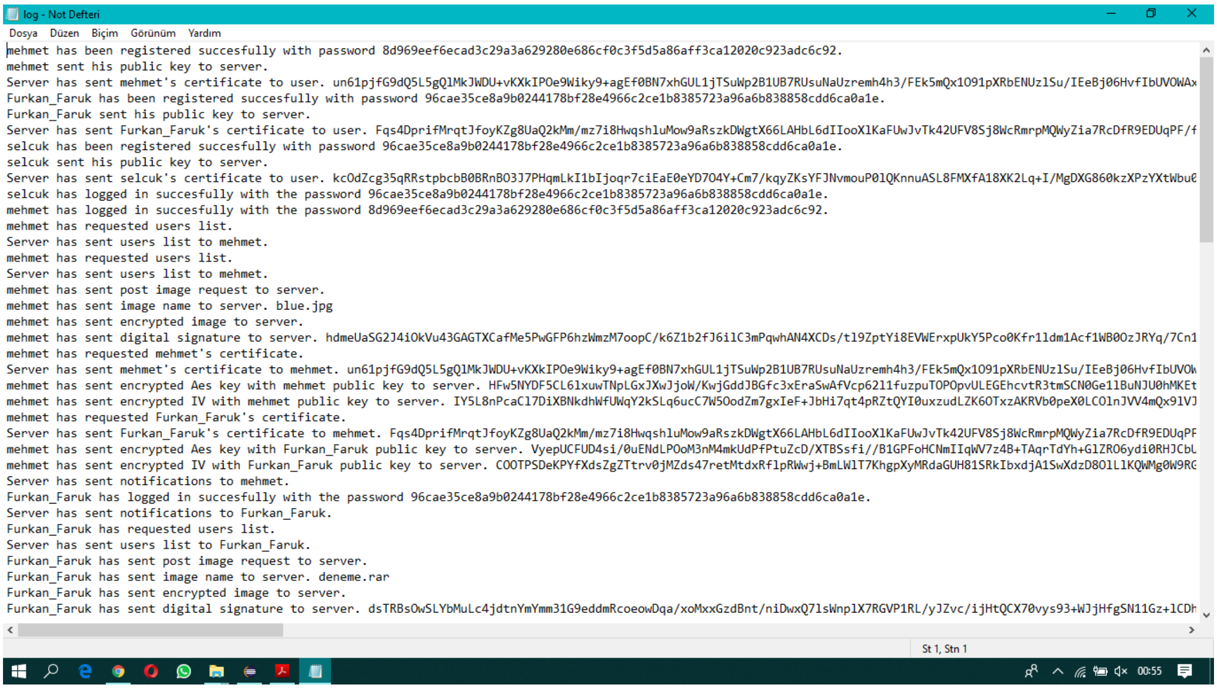
What did we do?

- Actually we believe we did everything wanted from us.
- Also our code supports any type of file. (we triyed pdf, mp4, rar, ppt, jpg, png, jpeg)

What we thinked but we couldn't implemented?

- Application get special to computer, do not let a user to login in another computer (actually we succeed this part) but, if user logs out , can login in whenever he wants and create public ,private key pairs again like WhatsApp (could not implement this part, why because in WhatsApp we can login with our tel. number it is easy to control but username is not special for a computer really huge different)
- Also something like WhatsApp web when the user is online can login in another computer create connection between main computer and post or download through main computer. (it is really hard to implement in pc , in security side)

LOG



```
mehmet has been registered succesfully with password 8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92.
mehmet sent his public key to server.
Server has sent mehmet's certificate to user. un61pjfG9dQ5L5gQlMkJWDU+vKXkIPOe9Wiky9+agEf0BN7xhGUL1jTSuWp2B1UB7RUsuNaUzremh4h3/FEk5mQx1O91pXRbENUzlSu/IEeBj06HvfIbUVOWAx
Furkan_Faruk has been registered succesfully with password 96cae35ce8a9b0244178bf28e4966c2ce1b8385723a96a6b838858cdd6ca0a1e.
Furkan_Faruk sent his public key to server.
Server has sent Furkan_Faruk's certificate to user. Fqs4DprifMrqtJfoyKZg8UaQ2kMm/mz7i8HwqshluMow9aRszkDWgtX66LAHbL6dIIooXlKaFUwJvTk42UFV8Sj8WcRmrpMQWyZia7RcDfR9EDUqPF/f
selcuk has been registered succesfully with password 96cae35ce8a9b0244178bf28e4966c2ce1b8385723a96a6b838858cdd6ca0a1e.
selcuk sent his public key to server.
Server has sent selcuk's certificate to user. kcOdZcg35qRRstpbcbB0BRnBO3J7PHqmLkI1bIjoqr7ciEaE0eYD7O4Y+Cm7/kqyZKsYFJNvmouP01QKnnuASL8FMXfA18XK2Lq+I/MgDXG860kzXPzYXtWbu
selcuk has logged in succesfully with the password 96cae35ce8a9b0244178bf28e4966c2ce1b8385723a96a6b838858cdd6ca0a1e.
mehmet has logged in succesfully with the password 8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92.
mehmet has requested users list.
Server has sent users list to mehmet.
mehmet has requested users list.
Server has sent users list to mehmet.
mehmet has sent post image request to server.
mehmet has sent image name to server. blue.jpg
mehmet has sent encrypted image to server.
mehmet has sent digital signature to server. hdmeUaSG2J4iOkVu43GAGTXCafMe5PwGFP6hzWmzM7oopC/k6Z1b2fJ6ilC3mPqwhAN4XCDs/tl9ZptYi8EVWErxpUkY5Pco0Kfr1ldm1Acf1WB0OzJRYq/7Cn1
mehmet has requested mehmet's certificate.
Server has sent mehmet's certificate to mehmet. un61pjfG9dQ5L5gQlMkJWDU+vKXkIPOe9Wiky9+agEf0BN7xhGUL1jTSuWp2B1UB7RUsuNaUzremh4h3/FEk5mQx1O91pXRbENUzlSu/IEeBj06HvfIbUVOW
mehmet has sent encrypted Aes key with mehmet public key to server. HFw5NYDF5CL6lxuwTNpLGxJXwJjoW/KwjGddJBGfc3xEraSwAfVcp62l1fuzpuTOPOpvULEGEhcvtR3tmSCN0Ge1lBuNJU0hMKEt
mehmet has sent encrypted IV with mehmet public key to server. IY5L8nPcaCl7DiXBNkdhWfUWqY2kSLq6ucC7W5OodZm7gxIeF+JbHi7qt4pRZtQYI0uxzudLZK6OTxzAKRVb0peX0LCOlnJVV4mQx9lVJ
mehmet has requested Furkan_Faruk's certificate.
Server has sent Furkan_Faruk's certificate to mehmet. Fqs4DprifMrqtJfoyKZg8UaQ2kMm/mz7i8HwqshluMow9aRszkDWgtX66LAHbL6dIIooXlKaFUwJvTk42UFV8Sj8WcRmrpMQWyZia7RcDfR9EDUqPF
mehmet has sent encrypted Aes key with Furkan_Faruk public key to server. VyepUCFUD4si/0uENdLPOoM3nM4mkUdPfPtuZcD/XTBSsfi//B1GPFoHCNmIIqWV7z4B+TAqrTdYh+GlZRO6ydi0RHJCbL
mehmet has sent encrypted IV with Furkan_Faruk public key to server. COOTPSDeKPYfXdsZgZTtrv0jMZds47retMtdxRflpRWwj+BmLWlT7KhgpXyMRdaGUH81SRkIbxdjA1SwXdzD8OlL1KQWMg0W9RG
Server has sent notifications to mehmet.
Furkan_Faruk has logged in succesfully with the password 96cae35ce8a9b0244178bf28e4966c2ce1b8385723a96a6b838858cdd6ca0a1e.
Server has sent notifications to Furkan_Faruk.
Furkan_Faruk has requested users list.
Server has sent users list to Furkan_Faruk.
Furkan_Faruk has sent post image request to server.
Furkan_Faruk has sent image name to server. deneme.rar
Furkan_Faruk has sent encrypted image to server.
Furkan_Faruk has sent digital signature to server. dsTRBsOwSLYbMuLc4jdtnYmYmm31G9eddmRcoeowDqa/xoMxxGzdBnt/niDwxQ7lsWnplX7RGVP1RL/yJZvc/ijHtQCX70vys93+WJjHfgSN11Gz+lCDh
```