



README.md

Image Encryption

2021-1 Software Engineering Team Project

source <https://nevonprojects.com/image-encryption-using-aes-algorithm/>

Team Notion <https://www.notion.so/e7b05fcf792b4be9a13e5264cabe0323>



Problem Statement

Introduction

기존의 주제 였던 Image encryption using AES algorithm 으로 프로젝트를 진행하기에는 프로젝트의 취지에서 좀 벗어난다는 판단이 들었다. 따라서, 팀 회의 끝에 가상의 고객을 선정한 뒤 고객의 문제상황과 그에 따른 요구사항을 도출해서 프로젝트를 해보자는 의견이 있었고, 은행이라는 가상의 고객을 대상으로 추가적인 기능을 더 구현해보기로 했다. 즉 우리의 프로젝트 주제는 원래 Image encryption using AES algorithm 이지만, 아래에 가상으로 제시한 문제 상황과 고객을 프로젝트의 문제상황과 고객이라 가정한 뒤에, 고객의 요구사항을 만족시킬 수 있는 몇 가지 기능들을 추가로 더 구현할 계획이다.

Problem

코로나 팬더믹 사태로 사람들은 언택트 시대에 적응하고 있고 은행 역시 비대면 계좌 계설 등 대다수의 업무를 전화 및 온라인으로 처리하고 있다. 젊은 세대부터 X세대까지 모두 코로나를 겪으면서 모든 세대가 그러한 언택트 환경을 경험하고 있다. 중요한 것은 은행 관련 업무를 온라인에서 처리하기 위해서는 신원 식별이 필수 불가결 하다는 점이다. 그러므로 은행에서는 은행 업무를 진행할 때 고객의 신원을 확인하기 위한 정보를 종종 요청하곤 한다. 법인이나 몇몇 개인들은 팩스를 통해서 서류를 전송 하기도 하지만, 대부분의 사람들의 집에는

팩스가 없다. 이런 상황에서, 중요한 문서를 사진으로 전송하면 개인정보 유출이나 보안사고가 발생할 수 있는 위험이 존재한다. 따라서 우리는 개인정보를 사진으로 보낼 때 안전하게 전송할 수 있는 플랫폼을 구축해달라는 요청을 받았고, 사용자가 전송한 사진을 은행으로 안전하게 전송하는 웹 플랫폼을 만들 계획이다.

Method

고객의 요구 사항

1. 비대면 은행 업무를 선호하는 사람들이 많아지면서, 고객의 개인정보를 사진으로 찍어서 주고 받는 일이 잦아짐
2. 이때 특별한 웹 페이지를 만들어서 사용자가 웹에서 은행으로 사진을 전송하면 그 사진이 안전하게 은행에 도착하여, 은행에서 업무에 그 사진을 사용하고 싶어함

선택한 방법론

- Agile 방법론

Sub-Problems

1. 사진을 안전하게 송수신 하는 기능 → feature/PictureHandler
2. 사용자가 은행으로 서류 사진을 전송하는 기능 → feature/Customer
3. 은행에서 사용자가 보낸 사진을 받아서 다운받는 기능 → feature/BankClerk

Subproblem

- **Feature/PictureHandler** 김영빈 박희수
- **Feature/Customer** 임혜정 정도현
- **Feature/Clerk** 방수원 장영욱

1. PictureHandler를 구현하는 그룹은 원본 사진의 Encryption, 암호화된 사진의 Decryption, 암호화 알고리듬의 Key 관리, 암호화된 파일의 저장 및 관리 등을 구현할 계획이다.
2. Customer를 구현하는 그룹은 고객의 회원가입 및 로그인, 고객 자신에게 주어진 요청 확인, 사진을 PictureHandler에게 전송하는 기능을 구현할 계획이다. 이때 자신에게 주어진 요청이란 은행에서 사용자에게 서류를 요청할 때 할당되는 이벤트이다.
3. BankClerk를 구현하는 그룹은 고객에게 서류 요청 기능, 고객이 사진을 보냈는지 확인하는 기능, 고객의 사진을 다운로드 받는 기능을 구현할 계획이다.

Scenario

Scenario

홈페이지에 접속하면 고객과 은행원을 선택하는 버튼이 표시된다. 은행원 선택 시 은행에서 각 은행원에게 부여한 아이디와 비밀번호로 로그인할 수 있다. 은행원 계정으로 로그인을 하면, 고객의 사진 서류 요청을 관리할 수 있는 페이지가 열리고 은행원은 요청을 생성하고 조회할 수 있다. 생성된 요청은 요청페이지에서 볼 수 있으며, 사진 전송이 완료된 요청, 사진 전송이 완료되지 않은 요청 두 가지 템이 존재한다. 홈페이지에서 고객은 회원가입과 로그인을 할 수 있다. 고객 계정으로 로그인을 하면 고객은 은행에서 자신에게 할당한 요청을 조회할 수 있다. 조회된 요청을 클릭하여 은행에서 요청한 사진 정보를 upload하여 전송할 수 있다. 전송된 사진은 암호화되어 은행으로 전송된다. 은행으로 사진이 전송되면 해당 요청은 사진전송이 완료된 요청으로 분류된다. 사진전송이 완료된 후, 은행원은 요청페이지에서 완료 여부를 조회가 가능하다. 전송된 사진의 다운로드 버튼을 클릭하면 암호화된 파일을 복호화하여 사진으로 다운로드 받을 수 있다. 또한 복호화 된 사진을 다운로드 받은 후에는 웹페이지 DB에 저장된 암호화된 파일은 삭제된다.

UseCase

Use Case

Actor		Actor's Goal	Use Case Name	Use Case Name
User	Customer	회원가입을 하고, 정보를 DB에 저장한다.	회원가입	Sign Up (UC-1)
	Clerk	회원가입을 하고, 정보를 DB에 저장한다.	회원가입	Sign Up (UC-1)
User	Customer	로그인을 통해서, 사용자에게 부여된 권한에 맞게 프로그램을 이용한다.	로그인	Log in (UC-2)
	Clerk	로그인을 통해서, 사용자에게 부여된 권한에 맞게 프로그램을 이용한다.	로그인	Log in (UC-2)
Customer		고객은 은행원이 자신에게 요청한 내역을 확인한다.	요청 확인	Identify (UC-3)
Customer		자신의 개인정보가 들어있는 사진을 넘겨 업무를 완료하기 위해서 서류를 업로드 한다.	사진 업로드	Upload (UC-4)
Picture Handler		전달받은 사진을 암호화하여 DataBase에 저장한다.	사진 암호화	Encryption (UC-5)
Picture Handler		은행원이 복호화된 사진을 다운받을 수 있다.	사진 복호화	Decryption (UC-6)
Clerk		선택한 고객에게 필요한 사진 혹은 서류를 요청한다.	요청 생성	Create request(UC-7)
Clerk		고객이 전송한 사진을 요청한다.	사진 다운로드	Download((UC-8))
User	Customer	알람을 설정하고, 원하는 알림을 받을 수 있다.	알림 설정	Select Notification(UC-9)
	Clerk	알람을 설정하고, 원하는 알림을 받을 수 있다.	알림 설정	Select Notification(UC-9)

Traceability Matrix For Use Case

Req't	PW	UC1	UC2	UC3	UC4	UC5	UC6	UC7	UC8	UC9
REQ1	10	X								
REQ2	7	X	X							
REQ3	3			X	X			X		
REQ4	3			X				X		
REQ5	2							X		
REQ6	8						X		X	
REQ7	10				X					
REQ8	5					X				
REQ9	5					X				
REQ10	4				X					
REQ11	2						X		X	
REQ12	5						X		X	
REQ13	2						X			
REQ14	5									X
MAX PW	10	7	3	10	5	8	3	8	5	
TOTAL PW	17	7	6	13	14	17	8	15	5	

Implementation

how to run in local

```
python manage.py runserver
```

after run enter in local web

```
http://127.0.0.1:8000/
```

Page Organization

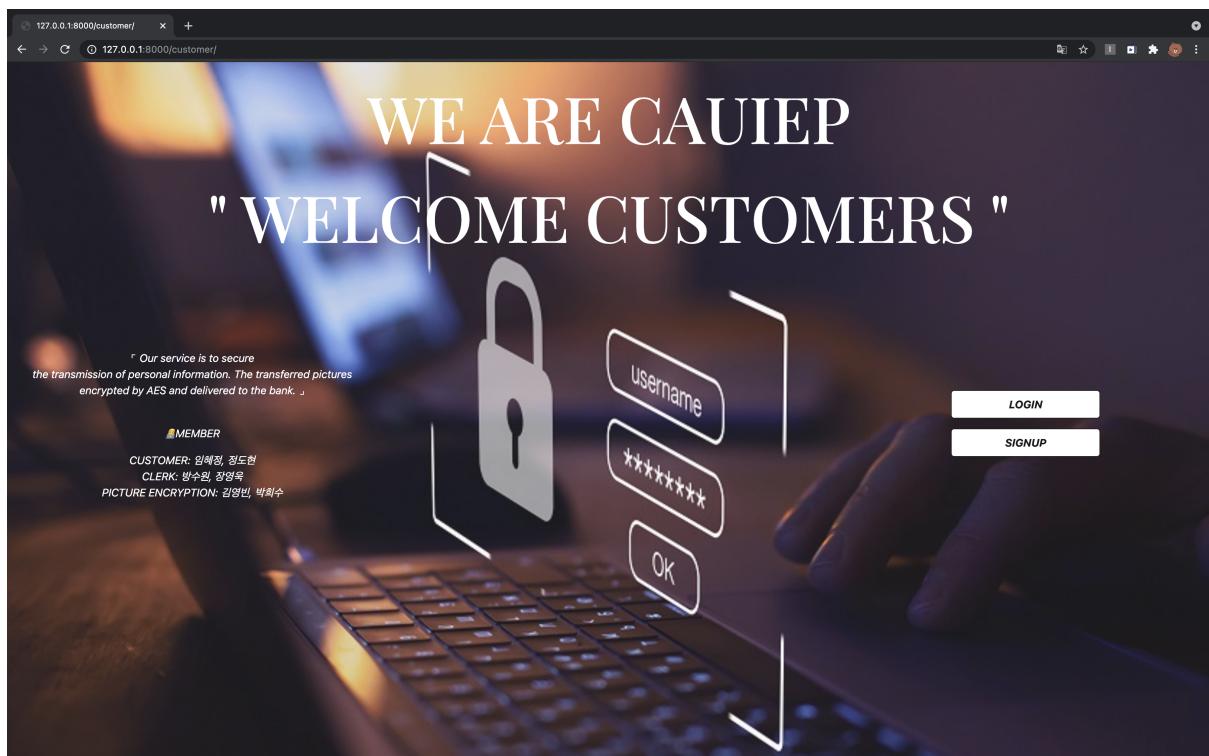
- /customer
- /customer/confirm
- /customer/detail/int:pk
- /customer/upload/int:pk
- /customer/signup

- /customer/login
- /customer/logout
- /customer/success
- /clerk
- /clerk/signup
- /clerk/login
- /clerk/logout
- /clerk/create
- /clerk/create/select/str:customer_name
- /clerk/rlist
- /clerk/download/int:pk
- /clerk/decryptor/int:pk
- /picturehandler/encrypt/int:pk
- /picturehandler/decrypt/int:pk
- /picturehandler/picturedelete/int:pk

Use Case

UC1 회원가입

- /customer 로그인, 회원가입



- /customer/signup 회원가입 : username, email, password, password confirmation 을 통해 회원가입을 할 수 있다. customer 값은 True

The screenshot shows a web browser window titled "Customer Home". The URL in the address bar is "127.0.0.1:8000/customer/signup/". Below the address bar, there are two buttons: "login" and "sign up". The "sign up" button is highlighted. The main content is a sign-up form with the following fields:

- Username**: An input field labeled "Username".
- Email**: An input field labeled "Email".
- Password**: An input field labeled "Password" with a note below it: "Your password can't be too similar to your other personal information. Your password must contain at least 8 characters. Your password can't be a commonly used password. Your password can't be entirely numeric.".
- Password confirmation**: An input field labeled "Password confirmation" with a note below it: "Enter the same password as before, for verification."
- Submit**: A dark blue "Submit" button.

- /clerk 회원가입 및 로그인 : Clerk가 회원가입과 로그인을 할 수 있는 홈 화면이다.



- /clerk/signup 회원가입 : username, email, password, password configuration 을 통해 회원가입을 할 수 있다. Clerk 계정이 생성된다.

| Home | Sign up Log in

Sign up page

Username	<input type="text"/>
Email	<input type="text"/>
Password	<input type="password"/>
Password confirmation	<input type="password"/>

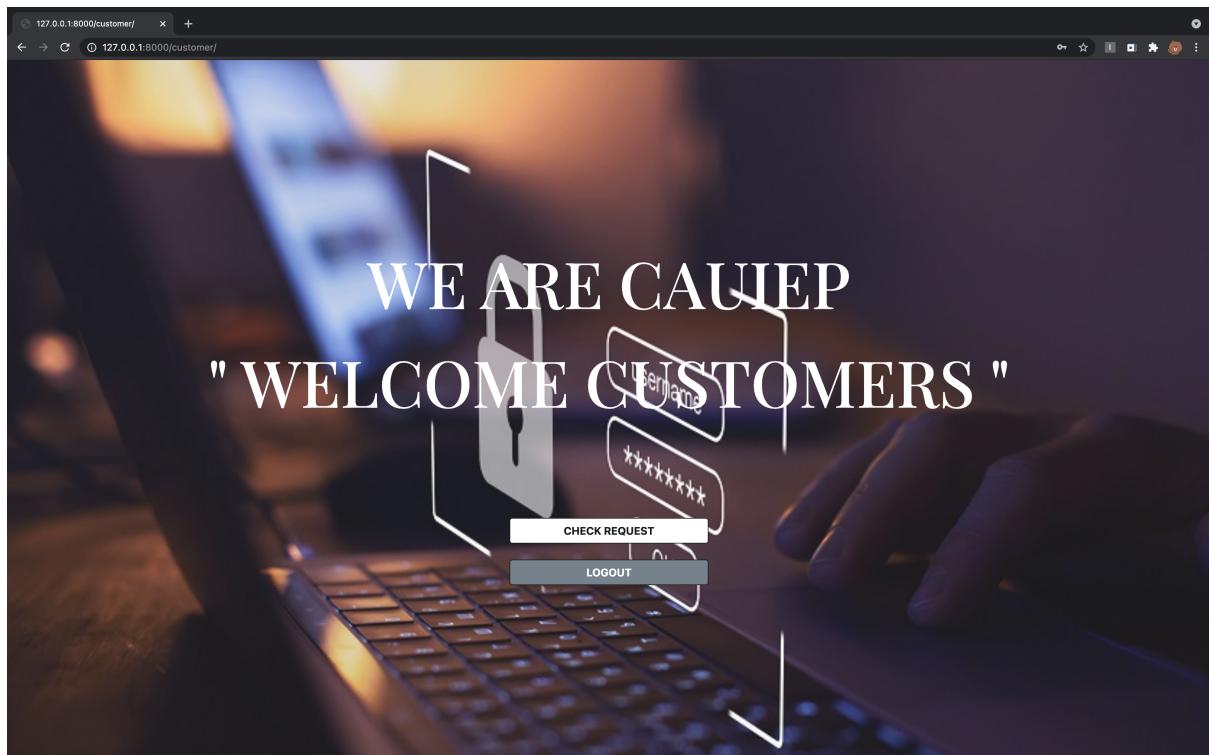
가입하기

UC2 로그인

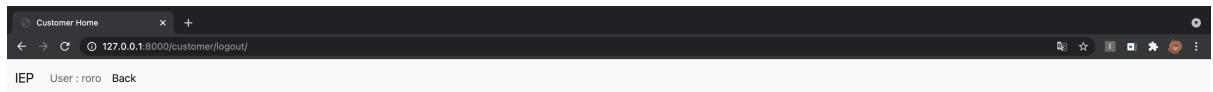
- /customer/login 로그인 : username, password 을 입력받아 비교하여 로그인을 실행 한다.

The screenshot shows a web browser window with the URL `127.0.0.1:8000/customer/login/`. The page title is "Customer Home". Below the title, there is a "Welcome" message and links for "login" and "sign up". The main content is a login form with fields for "Username" and "Password", and a "Login" button.

- 로그인 완료 : 로그인이 성공하였을 경우 요청확인 or logout 을 할 수 있다



- `/customer/logout` 로그아웃 재확인 : 로그아웃에 대한 재확인을 한다.



Do you want to logout ?

YES

- /clerk/login 로그인 : username, password 를 입력받아 비교하고 Clerk인지 여부를 확인하여 Clerk계정으로만 로그인을 실행할 수 있다.

| Home | Sign up Log in

Login page

Username

Password

로그인

- 로그인 완료 : 로그인이 성공하였을 경우 요청생성 및 사진 다운로드를 위해 생성된 요청을 조회 할 수 있다

| Home | Sign up Log out

Hello, 'Clerk'!

원하는 서비스를 선택하십시오.

고객에게 서류 사진 요청

요청된 서류 제출 확인

- /clerk/logout 로그아웃 재확인 : 로그아웃 여부를 재확인을 한다.

| Home | Sign up Log out

Log out page

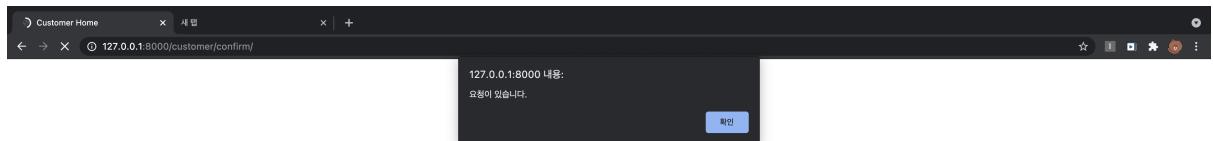
로그아웃 하시겠습니까?

네

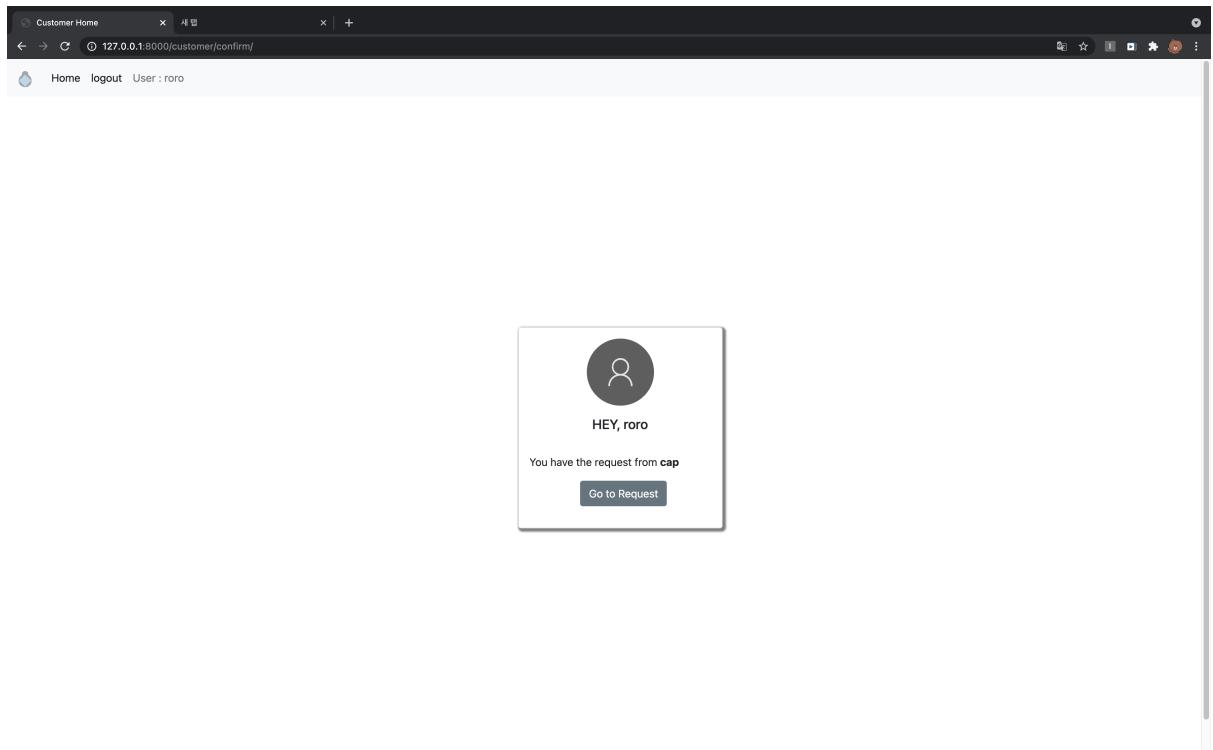
아니오

UC3 요청 확인

- /customer/confirm 요청확인 알람 : check request를 누른후 해당 요청이 있을경우 알람을 받을 수 있다. 요청 확인 : 어떤 clerk로 부터 요청을 받았는지 확인할 수 있다.

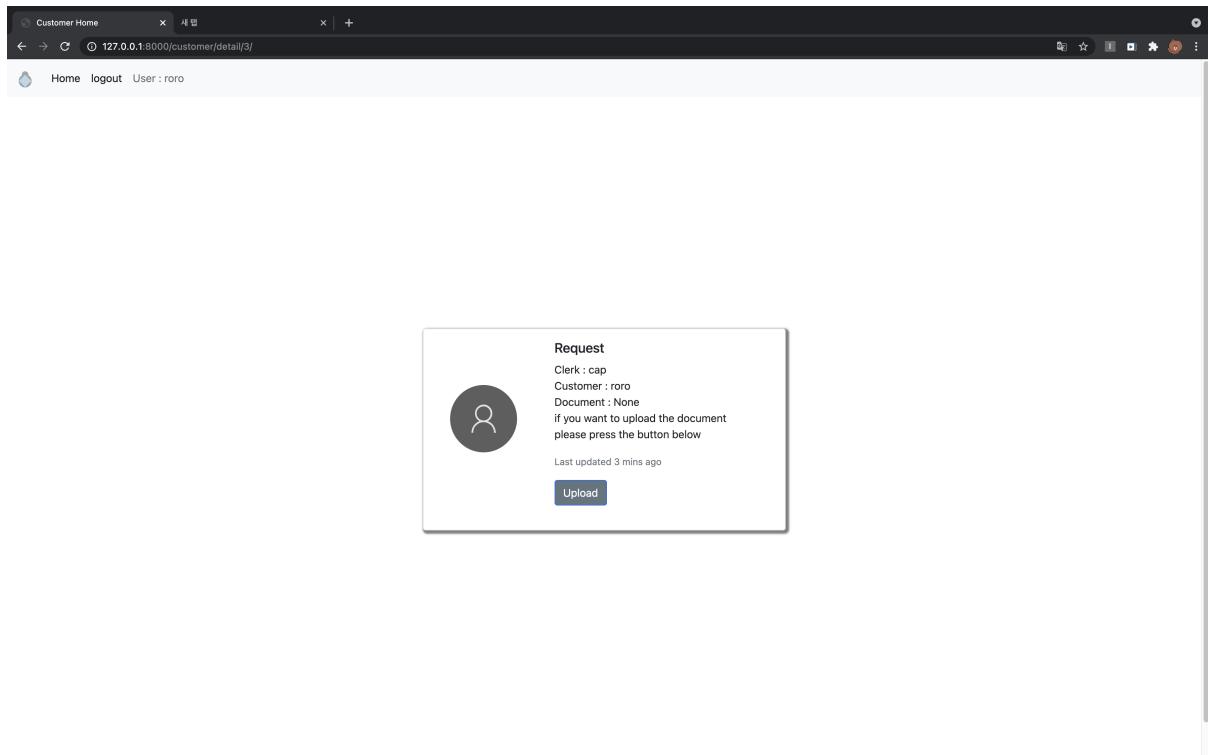


- /customer/detail/int:pk 생성된 요청내용 확인 : go to request 클릭 후 clear, customer, document 에 대한 값을 받는다.

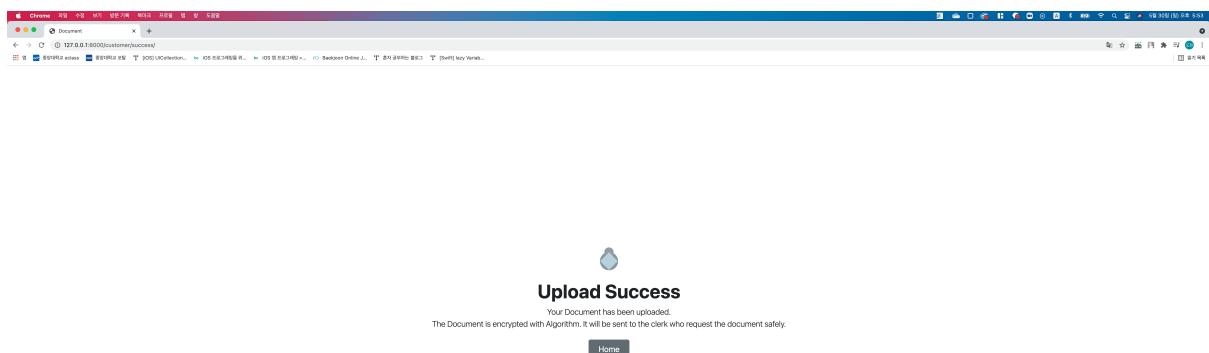
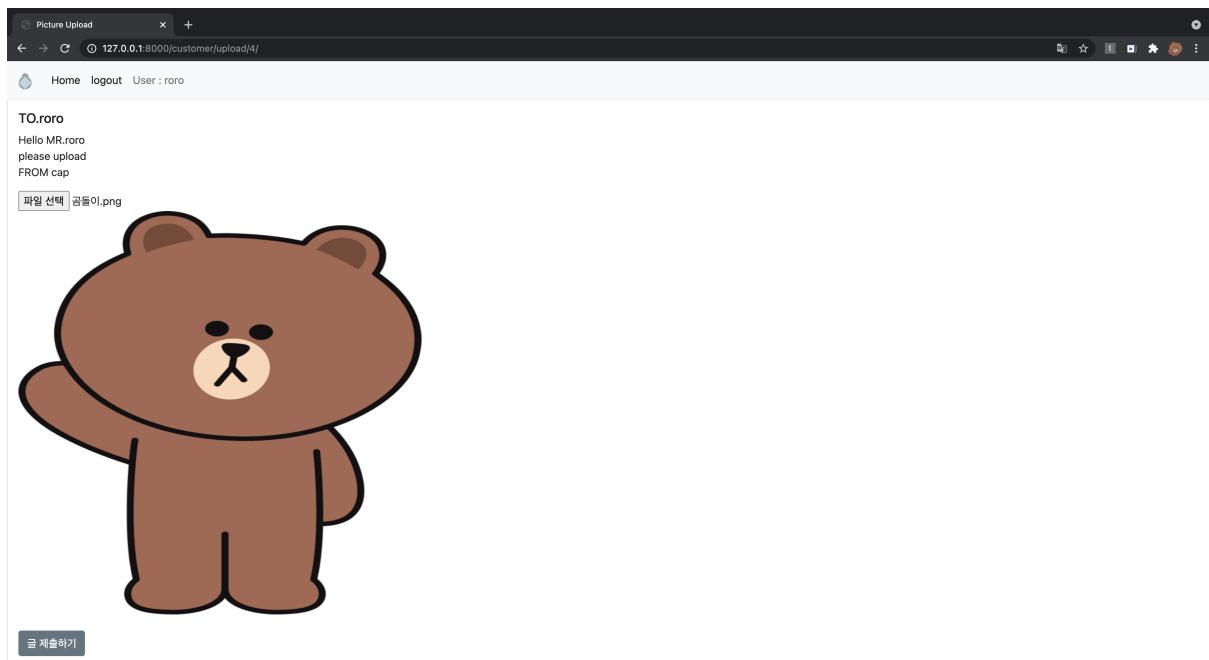


UC4 사진 업로드

- /customer/upload/int:pk 사진 업로드 : Upload 클릭 후 파일을 선택하여 해당 사진을 업로드할 수 있다. 성공적으로 업로드를 했을 경우, uploaded 는 True 값으로 바뀐다.



- /customer/success 사진 업로드 성공 : 성공적으로 업로드를 했을 경우, uploaded 는 True 값으로 바뀐다.



UC5 사진 암호화

- /picturehandler/encrypt/int:pk 사진 암호화 후 저장 : Clerk가 원하는 customer에 Request 를 생성하면 DB에는 다음과 같이 Request가 생성 된다. 아직 customer가 사진을 업로드 하지 않았으므로 Field는 비어있는 상태이다. 사진이 업로드 되지 않았기 때문에 Uploaded가 False이다.

Clerk:

aadmin



Customer:

kimkim



고객 사진:

선택된 파일 없음

Document:

주민등록등본



Uploaded



- Customer가 사진을 업로드하면 해당 사진파일은 내부 모듈에 의해서 AES 암호화가 진행되고 암호화된 파일 .enc 가 생성되어 저장된다. Customer가 사진을 업로드한 시점에 Uploaded는 True로 바뀌어 체크박스가 채워지고 Clerk가 사진을 다운받을 수 있도록 한다.

Clerk:

aadmin



Customer:

kimkim



고객 사진:

Currently: media/2021/05/30/ea/eab64179d1204cb2964acf6dcb1635f2.enc Clear

Change: 선택된 파일 없음

Document:

주민등록등본



Uploaded

UC6 사진 복호화

- /picturehandler/decrypt/int:pk 사진 복호화 : Customer가 등록한 사진이 암호화되어 저장되어 있고 Uploaded 가 True라면 Clerk는 사진 복호화 및 다운로드를 요청할 수 있다. Clerk가 사진 복호화 및 다운로드를 요청하기 직전에는 다음과 같은 내용이 DB에 들어간다.

Clerk:

▼

Customer:

▼

고객 사진:

Currently: [media/2021/05/30/ea/eab64179d1204cb2964acf6dc1635f2.enc](#) Clear

Change: 파일 선택 선택된 파일 없음

Document:

▼

Uploaded

- /picturehandler/picturedelete/int:pk 복호화된 사진 삭제 : Clerk가 사진을 다운받는 즉시 해당 레코드는 DB에서 삭제해서 기록을 없앤다.



Picture request with ID "2" doesn't exist. Perhaps it was deleted?

UC7 요청 생성

- /clerk/create Customer 선택 : Customer의 username을 검색하여 존재할 경우 문서 선택화면으로 이동한다. Customer이외의 계정을 대상으로 요청을 생성할 수 없다. : 일치하는 customer가 없다면 경고창이 띄워진다.

| Home | Sign up Log out

Request page

고객ID

search

127.0.0.1:8000 내용:

존재하지 않는 고객입니다.

확인

- /clerk/create/select/str:customer_name Document 선택 : 선택한 Customer에게 요청할 문서를 선택하여 요청을 생성한다. 문서를 선택하지 않고 생성을 완료할 수 없다.

| Home | Sign up Log out

Request page

| Customer | Customer
| Document | ----- ▾

요청

UC8 사진 다운로드

- /clerk/rlist 요청목록 조회 : 생성한 요청을 조회할 수 있고 사진이 업로드 되었다면 다운로드가 활성화 된다.

| Home | Sign up Log out

Request List

요청된 파일의 제출 현황입니다.
제출 상태를 확인하여 다운로드를 진행하십시오.

clerkID	customerID	Status
Clerk	Customer	Download Picture
Clerk	Customer	(unsubmitted)
Clerk	Customer	Download Picture

- /clerk/download/int:pk 사진 다운로드 : 업로드된 사진의 다운로드를 시도하거나 뒤로 돌아갈 수 있다.

| Home | Sign up Log out

Picture Download

ClerkID Clerk
CustomerID Customer

[DOWNLOAD 요청하기](#)

[↪ 리스트로 돌아가기](#)

- /clerk/decryptor/int:pk 복호화된 사진 다운로드 : 암호화된 파일로 부터 원본 사진을 얻어 다운로드 할 수 있으며 홈으로 돌아가는 즉시 해당 요청은 삭제된다.

| Home | Sign up Log out

Picture Download

