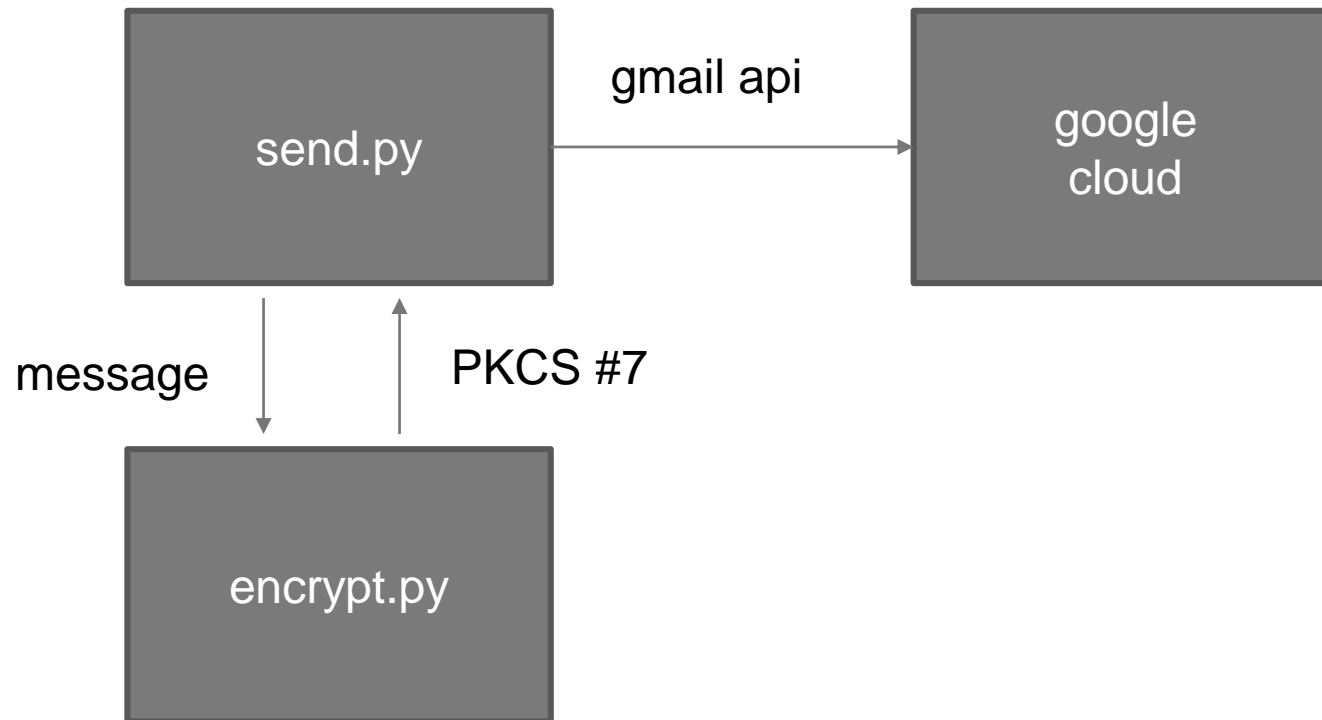


실습 : S/MIME 메일 보내기



순서

▶ Envelopedata 사용

1. 수신자 인증서 필요 -> 생성
2. S/MIME 객체 생성
3. e-mail로 보내기
4. 메일 수신하여 확인하기

수신자 인증서 생성

▶ 수신자 인증서 생성

▶ Openssl 로 실행

- easy rsa로 해도 무방

```
$ openssl req -x509 -newkey rsa:2048  
-nodes -days 365 -out recipient.pem
```

- 이메일 주소를 실제 자신의 것으로

👉 **privkey.pem, recipient.pem 생성**

S/MIME 객체 생성

▶ M2Crypto

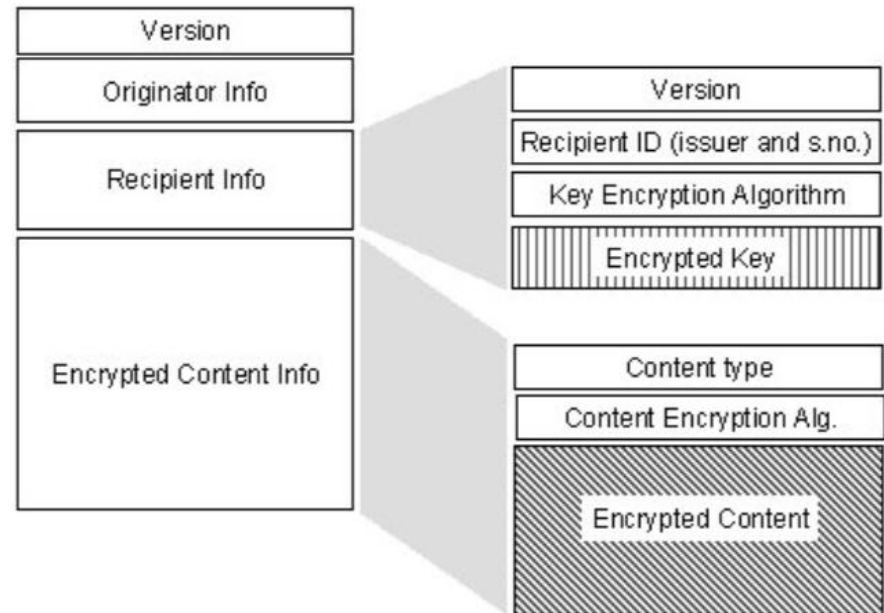
- Python wrapper for OpenSSL with MIME support
- 2.7 용이라 해야 할 작업
 - \$ sudo apt install libssl-dev swig python3-dev gcc
- 설치
 - \$ sudo pip3 install M2Crypto

▶ S/MIME 객체 생성 test : **encrypt.py**

- 파일 들은 class.ssu.ac.kr 에서 다운로드
- s/mime 메시지를 보여줌

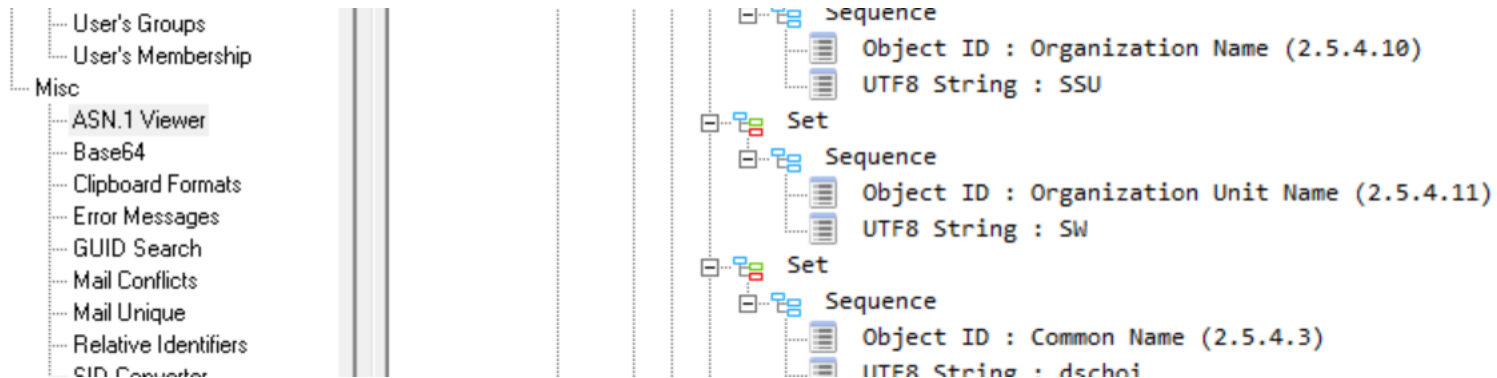
ENVELOPEDDATA 생성과정

1. Pseudo random 세션 키 생성
2. 각 수신자를 위해 수신자의 RSA 공개 키로 세션 키 암호화
3. 각 수신자를 위해 RecipientInfo 블록 준비
 - ✓ 수신자의 공개 키 인증서 식별자
 - ✓ 세션 키 암호에 사용된 알고리즘 식별자
 - ✓ 암호화된 세션 키 포함
4. 세션 키로 메시지 내용을 암호화



ASN.1 보기

- ▶ <https://nettools.net/asn1viewer/>
- ▶ Base64를 decoding하여
- ▶ asn.1 viewer 로 파일 읽기



메일 보내기

▶ Gmail api 시작


1. gmail api 등록

<https://console.cloud.google.com>

2. 새 프로젝트 만들기


 검색 **gmail**


문서 및 튜토리얼


Gmail 계정 정리 | ID 및 액세스 관리 - Google Cloud
 단계 순서는 Gmail 계정 소유자가 관리되는 사용자 계정으로 전...

의견 보내기


Google Cloud


 My Project 601



1



대선

검색

전체

문서 및 튜토리얼

MARKETPLACE 및 API

의견 보내기

필터링 기준

검색 결과

'gmail'의 검색결과 26개 중 26개가 표시됩니다.



Gmail API

View and manage Gmail mailbox data.



Google Cloud


 My Project 601



Gmail API

[Google](#)

View and manage Gmail mailbox data.

사용하기

관리

API 사용해 보기



API 사용 설정됨

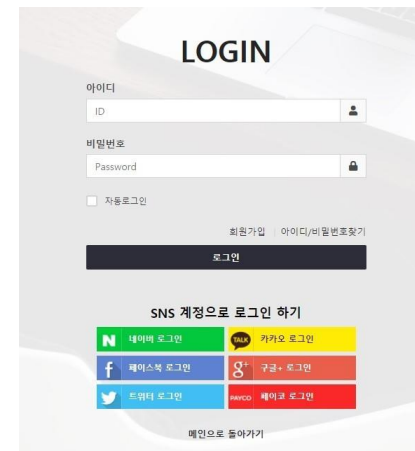
개요

문서

지원

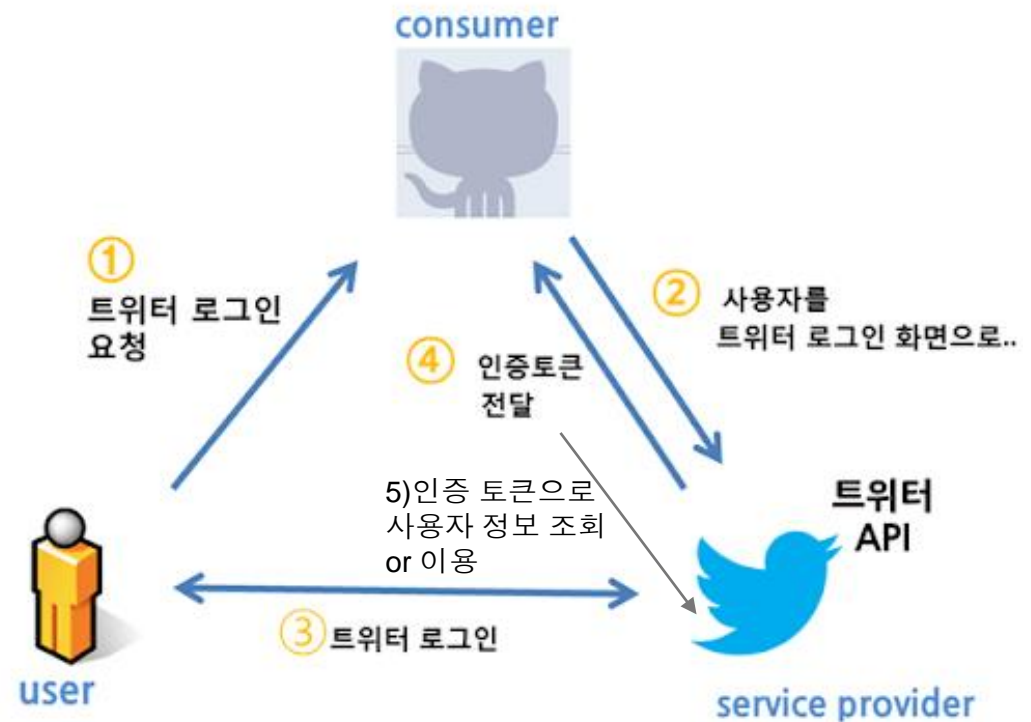
OAUTH

▶ 인증 프로토콜

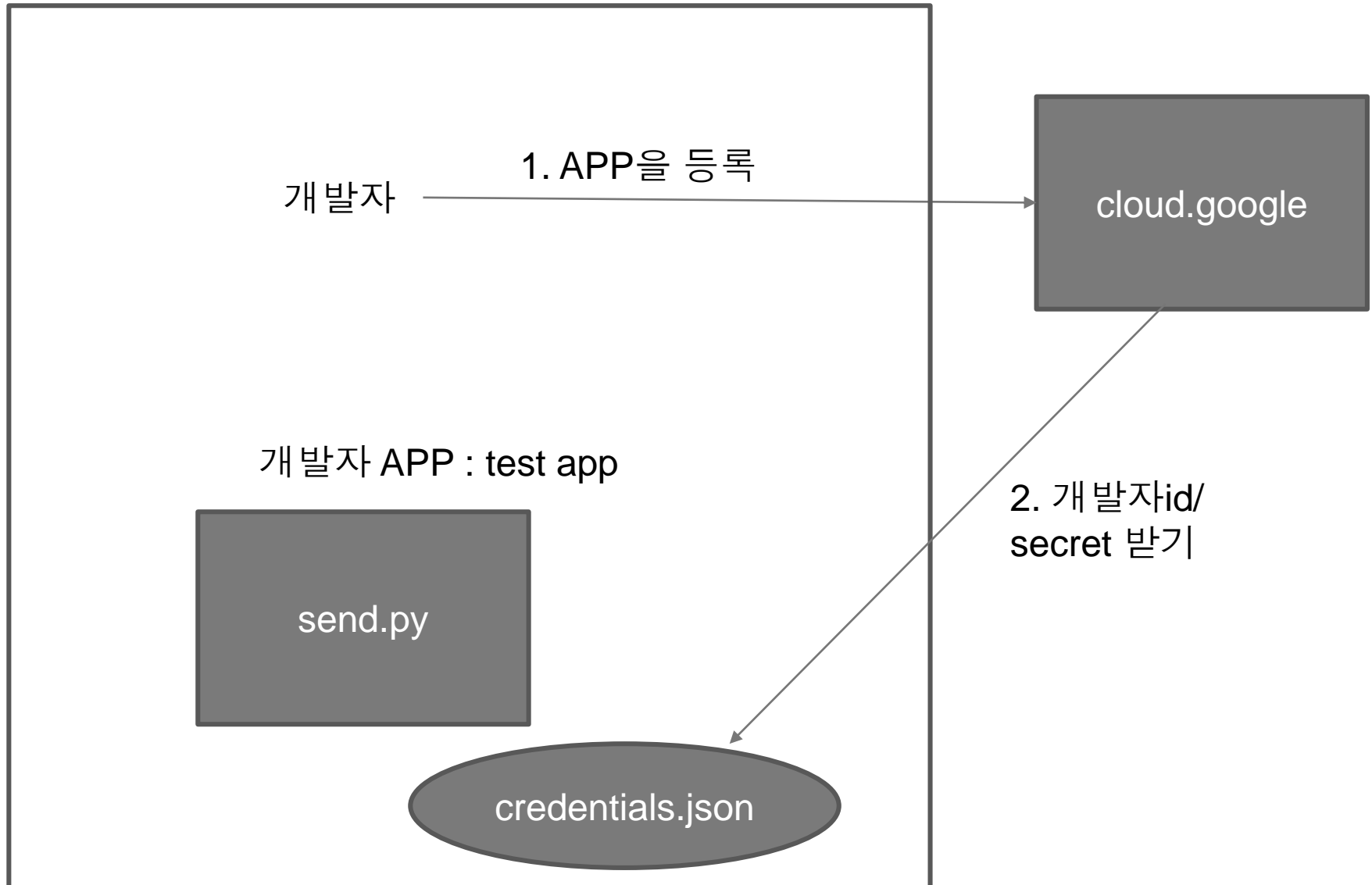


▶ 사이트 간 SSO (Single Sign On)

▶ Open API 정보조회



구글 API OAUTH



사용자 인증 정보 만들기

Project 601

1

검색

제품, 리소스, 문서(/)

사용자 인증 정보

+ 사용자 인증 정보 만들기

삭제

사용 설정한 API에 액세스하려면

API 키

이름

OAuth 클라이언트 ID 만들기

API 키

할당량과 액세스 권한을 확인하기 위해 간단한 API 키로 프로젝트를 확인합니다.

OAuth 클라이언트 ID

앱에서 사용자 데이터에 액세스할 수 있도록 사용자 동의를 요청합니다.

서비스 계정

크롬 계정을 사용하여 기본 키의 액세스를 인증을 사용 설정합니다.

제한사항

2

클라이언트 ID는 Google OAuth 서버에서 단일 앱을 식별하는 데 사용됩니다. 앱이 여러 플랫폼에서 실행되는 경우 각각 자체 클라이언트 ID가 있어야 합니다. 자세한 내용은 [OAuth 2.0 설정](#)을 참조하세요. OAuth 클라이언트 유형을 [자세히 알아보세요](#).

애플리케이션 유형 * 데스크톱 앱 ▼

이름 * 데스크톱 클라이언트 2

OAuth 2.0 클라이언트의 이름입니다. 이 이름은 콘솔에서 클라이언트를 식별하는 용도로만 사용되며 최종 사용자에게 표시되지 않습니다.

참고: 설정이 적용되는 데 5분에서 몇 시간이 걸릴 수 있습니다.

만들기 취소

3 OAuth 클라이언트 생성됨

API 및 서비스의 사용자 인증 정보에서 언제든지 클라이언트 ID와 보안 비밀에 액세스할 수 있습니다.

i OAuth 액세스는 OAuth 동의 화면에 나열된 테스트 사용자로 제한됩니다.

클라이언트 ID — 910764291268-61db9ta5r82oj18hnt8a17notvtfc15i.apps.googleusercontent.com

클라이언트 보안 비밀번호
G0CSPX-YyLH_Erbpwj_M2yyjCiutJ4YVyB1

↓ JSON 다운로드

확인

크리덴셜 이름 변경, 위치에 저장

\$ mv 받은 파일 credentials.json

OAUTH 동의 화면

API	API 및 서비스	OAuth 동의 화면
	사용 설정된 API 및 서비스	<p>대상 사용자를 비롯해 앱을 구성하고 등록하려는 방식을 선택하세요. 프로젝트에는 하나의 앱만 연결할 수 있습니다.</p> <p>User Type</p> <p><input type="radio"/> 내부 </p> <p>조직 내 사용자만 사용할 수 있습니다. 인증을 위해 앱을 제출할 필요는 없습니다. 사용자 유형 자세히 알아보기</p> <p><input checked="" type="radio"/> 외부 </p> <p>Google 계정이 있는 모든 테스트 사용자가 사용할 수 있습니다. 앱이 테스트 모드로 시작되고 테스트 사용자 목록에 추가된 사용자에게만 제공됩니다. 앱을 프로젝트에 푸시할 준비가 되면 앱을 인증해야 할 수도 있습니다. 사용자 유형 자세히 알아보기</p>
	라이브러리	
	사용자 인증 정보	
	OAuth 동의 화면	
	도메인 확인	
	페이지 사용 동의	

만들기

앱 등록 수정

1 OAuth 동의 화면

2 범위

3 테스트 사용자

4 요약

앱 정보

동의 화면에 표시되어 최종 사용자가 개발자를 확인하고 문의할 수 있습니다.

앱 이름 *

test app

동의를 요청하는 앱의 이름

사용자 지원 이메일 *

sunchoi@ssu.ac.kr

▼

사용자가 동의 관련 직무를 위해 무이한 때 이용합니다

사용자 추가

▶ 송신자 이메일

Project 601 ▼

검색
제품, 리소스, 문서(/)

앱 등록 수정

✓ OAuth 동의 화면

—

✓ 범위

—

3 테스트 사용자

—

4 요약

테스트 사용자

게시 상태가 '테스트 중'으로 설정된 동안에는 테스트 사용자만 앱에 액세스할 수 있습니다. 앱 인증 전에 허용되는 사용자 한도는 100명이며 앱의 전체 수명 주기에서 계산됩니다. [자세히 알아보기](#)

+ ADD USERS

✕ 사용자 추가



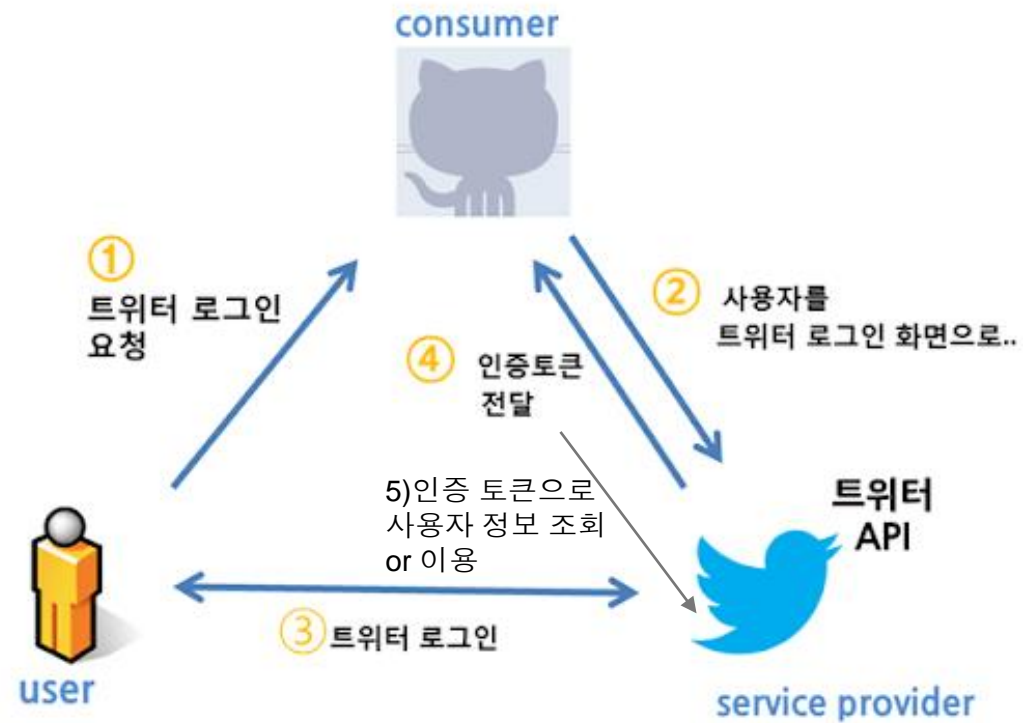
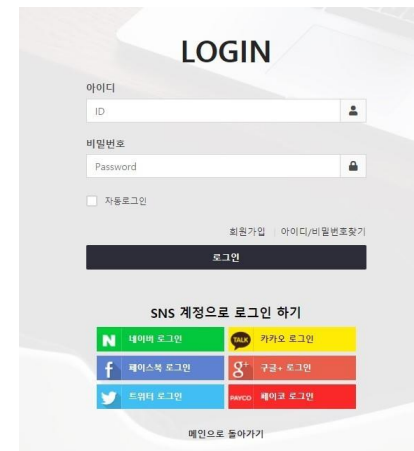
게시 상태가 '테스트 중'으로 설정된 동안에는 테스트 사용자만 앱에 액세스할 수 있는 사용자 한도는 100명이며 앱의 전체 수명 주기에서 계산됩니다.

[LEARN MORE](#)

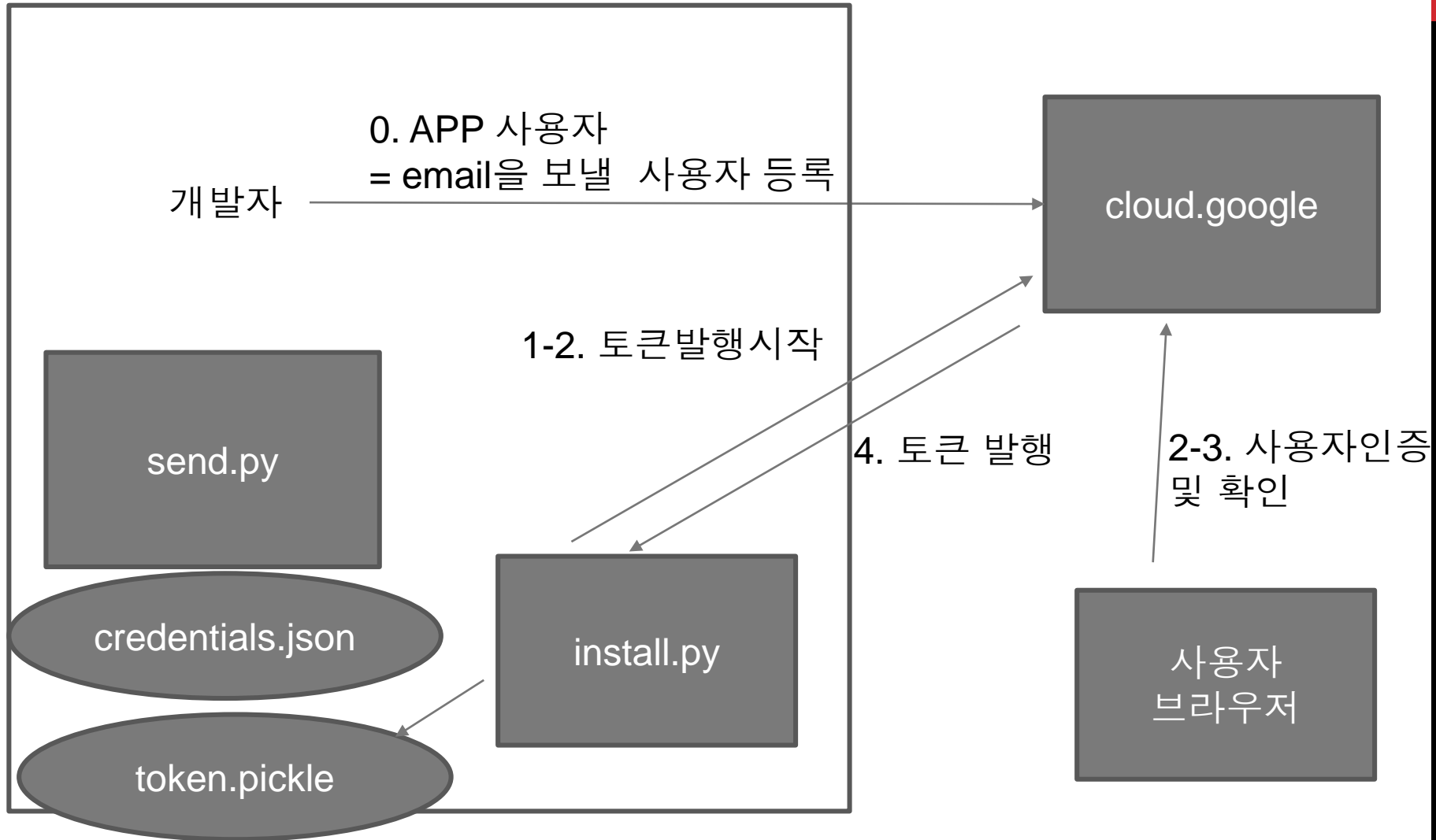
sunchoi@ssu.ac.kr ✕

추가

OAUTH



토큰 발행 구조



토큰 발행 시작


▶ Install google client library

```
$ pip3 install --upgrade google-api-python-client  
google-auth-httpplib2 google-auth-oauthlib
```


▶ 토큰 발행

```
$ python3 install.py
```



사용자 인증 및 동의

 Google 계정으로 로그인

test app에서 내 Google 계정에 액세스하려고 합니다


sunchoi@ssu.ac.kr

이렇게 하면 **test app**에서 다음 작업을 할 수 있습니다.

 Gmail 계정에서 이메일 읽기, 작성 및 전송
 

test app 앱을 신뢰할 수 있는지 확인

민감한 정보가 이 사이트 또는 앱과 공유될 수 있습니다. 언제든지 **Google 계정**에서 액세스 권한을 확인하고 삭제할 수 있습니다.

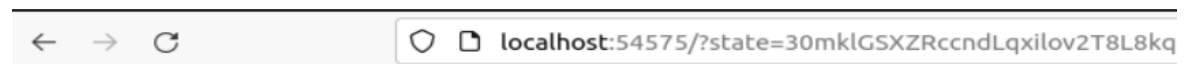
Google이 데이터를 **안전하게** 공유하는 방법을 알아보세요.

test app 의 개인정보처리방침 및 서비스 약관을 확인하세요.

취소

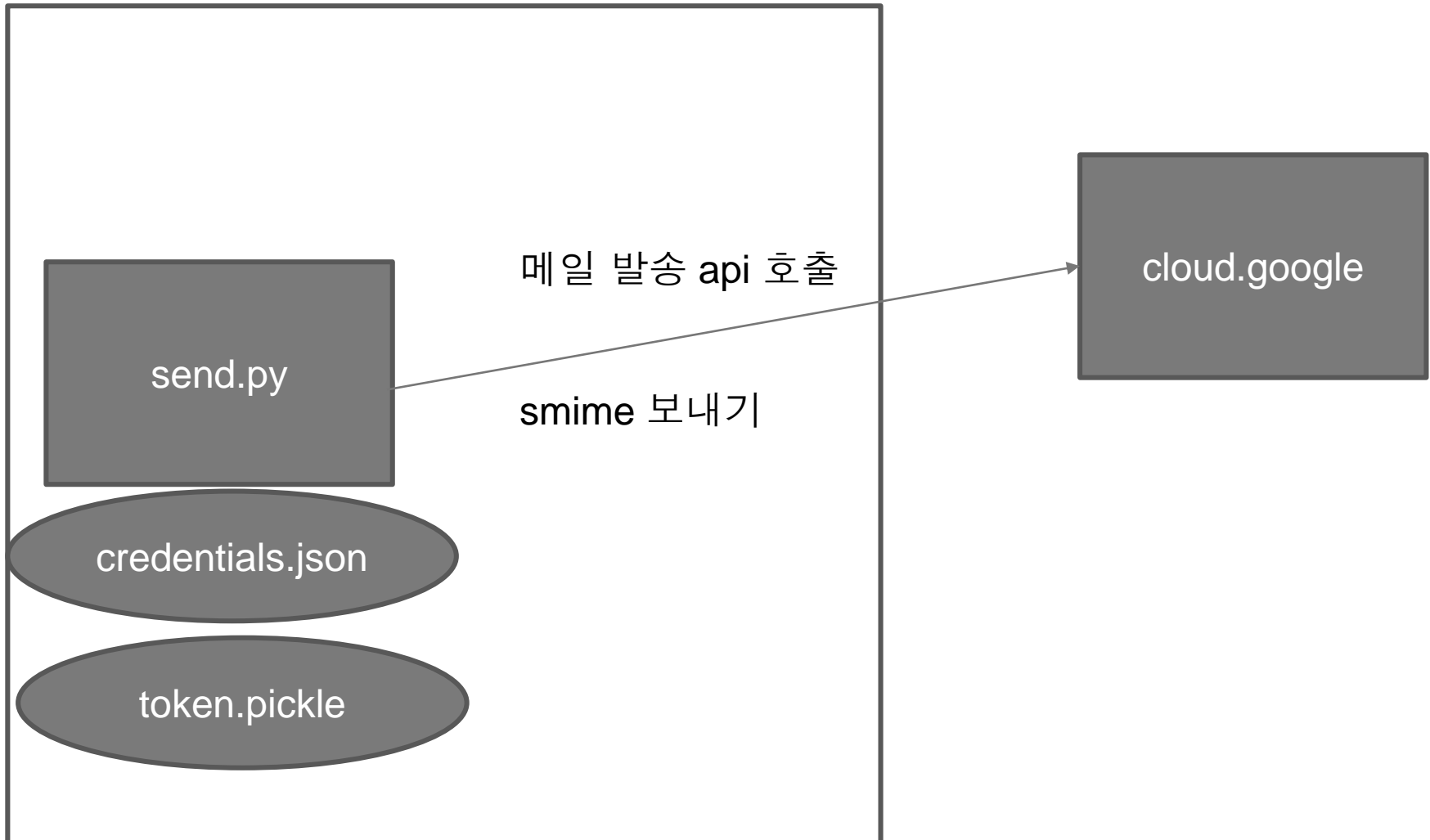
허용

▶ 토큰 발행됨



The authentication flow has completed. You may close this window.

API 호출

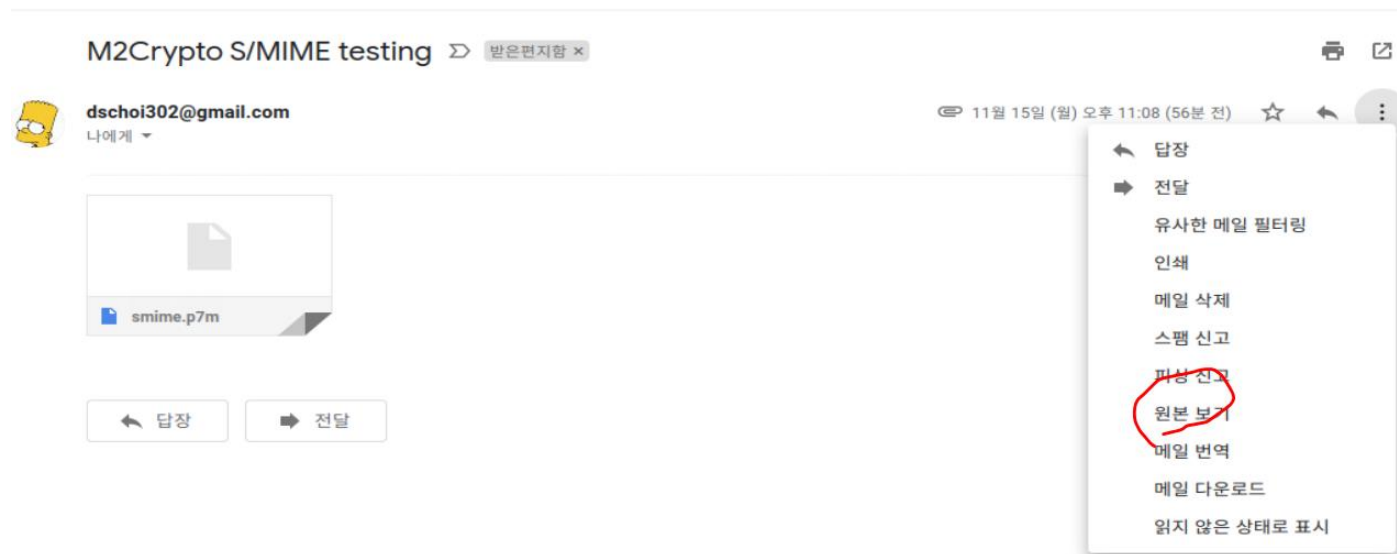


메일 보내기

▶ send.py

- 메시지
- 수신 주소 : 친구, 혹은 자신에게 보내기

▶ Gmail에서 보낸 메일 확인



과제1

▶ 아래 화면 캡처 : 1.jpg

원본 메일

메일 ID	<CAEZkUBqW5jk5Ur_4gOiKP0Gsz0uHdRZ+mzV=46qdD_TDZ9BU4A@mail.gmail.com>
생성 일시:	2021년 11월 15일 오후 11:08(0초 후 전송됨)
보낸사람:	dschoi302@gmail.com
받는사람:	dschoi302@gmail.com
제목:	M2Crypto S/MIME testing

원본 메일 다운로드

클립보드로 복사

```
Received: from 655323170175 named unknown by gmailapi.google.com with HTTPREST; Mon, 15 Nov 2021 15:08:15 +0100
From: dschoi302@gmail.com
To: dschoi302@gmail.com
Subject: M2Crypto S/MIME testing
MIME-Version: 1.0
Content-Disposition: attachment; filename="smime.p7m"
Content-Type: application/x-pkcs7-mime; smime-type=enveloped-data; name="smime.p7m"
Content-Transfer-Encoding: base64
Date: Mon, 15 Nov 2021 15:08:15 +0100
Message-Id: <CAEZkUBqW5jk5Ur_4gOiKP0Gsz0uHdRZ+mzV=46qdD_TDZ9BU4A@mail.gmail.com>
```

메일 내용 복호화 및 확인하기

▶ 인증서 설치

- P12 만들기 : 인증서 + 개인키

```
$ openssl pkcs12 -export -out my.p12 -in recipient.pem -inkey  
privkey.pem
```

- P12 파일을 PC로 가져와서 설치 하기

▶ 메일 확인

- p7mViewer
- <http://www.cryptigo.eu/p7mViewer/Download/>
- 메일을 길게 보내면 decrypt가 잘되므로, 메시지에 자기 이름을 넣고, decrypt 된 결과를 캡처한 것이 => **2.jpg 과제 2**