

Question 1)

i)

End-To-End Encryption

To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME. Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key. [Learn more](#)

OpenPGP

Thunderbird found 1 personal OpenPGP key associated with **cgrbyk9708@gmail.com**

✓ Your current configuration uses key ID **0xCDD3EC8C30EC0431** [Learn more](#) [Add Key...](#)

☐ None
Do not use OpenPGP for this identity.

☒ **0xCDD3EC8C30EC0431**
Expires on: 04.04.2026

Fingerprint 649D 7672 7DCB 5880 C6EF BD8D CDD3 EC8C 30EC 0431

Created 05.04.2023

[Key Properties](#) [More](#)

OpenPGP Key Manager

Key Properties

Claimed Key Owner Çağrı Büyük <cgrbyk9708@gmail.com>

Type key pair (secret key and public key)

Key ID 0xCDD3EC8C30EC0431

Fingerprint 649D 7672 7DCB 5880 C6EF BD8D CDD3 EC8C 30EC 0431

Created 05.04.2023

Expiry 04.04.2026

	Berker Avcı	Çağrı Büyük
Key ID	0x8FDE6166401D042A	0xCDD3EC8C30EC0431
Fingerprint	FFF3 9ED8 3E0A 09E2 8EEF 5EE2 8FDE 6166 401D 042A	649D 7672 7DCB 5880 C6EF BD8D CDD3 EC8C 30EC 0431
E-Mail	berkeravci41@gmail.com	cgrbyk9708@gmail.com

ii)

Search results for '0xCDD3EC8C30EC0431'

Type bits/keyID cr. time exp time key expir

```
pub rsa4096/649d7672dcb5880c6efbd8dcd3ec8c30ec0431 2023-04-05T19:35:58Z
    Hash=65189d75afeba87baef922cc44741698

uid Çağrı Büyük <cgrbyk9708@gmail.com>
sig sig cdd3ec8c30ec0431 2023-04-05T19:35:59Z 2026-04-04T19:35:58Z [selfsig]

sub rsa4096/fbe8a1fa6d0161231bd217666433df3520c45ad1 2023-04-05T19:36:00Z
sig sbind cdd3ec8c30ec0431 2023-04-05T19:36:01Z 2026-04-04T19:35:58Z []
```

Search results for '0x8FDE6166401D042A'

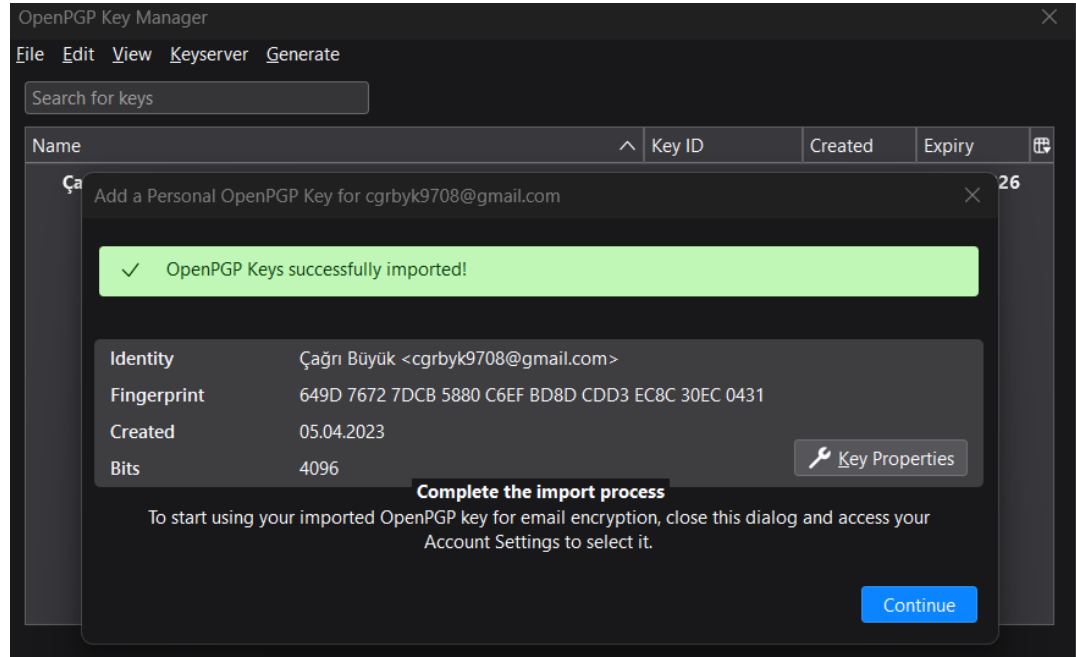
Type bits/keyID cr. time exp time key expir

```
pub rsa4096/fff39ed83e0a09e28eef5ee28fde6166401d042a 2023-04-05T20:33:15Z
    Hash=c8102bb6d928ac0598db9119850ce8f0

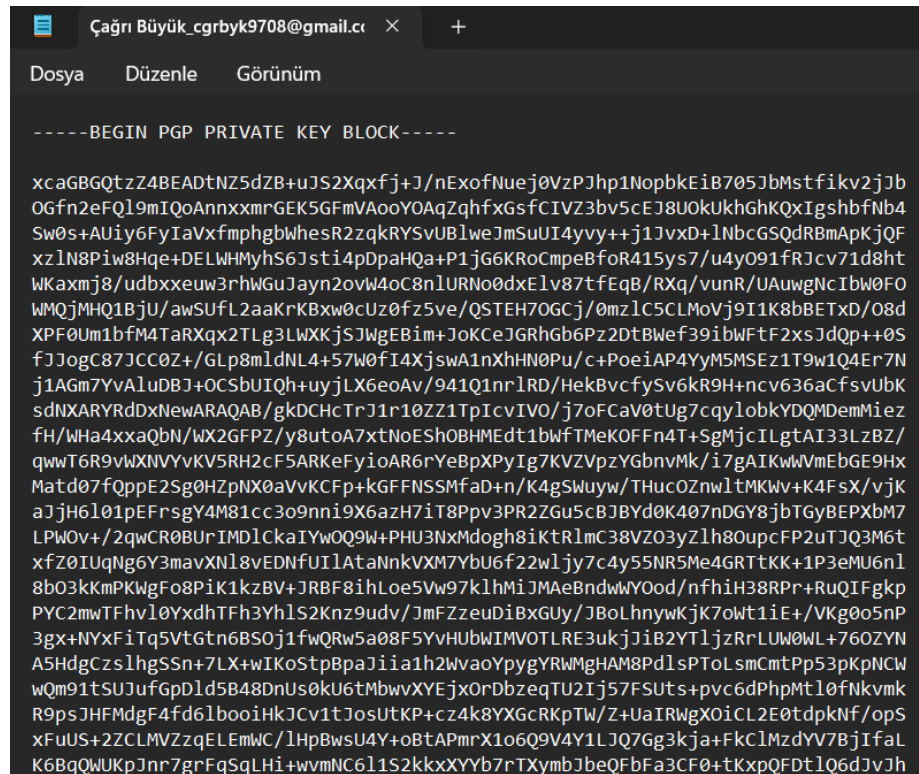
uid Berker Avcı <berkeravci41@gmail.com>
sig sig 8fde6166401d042a 2023-04-05T20:33:16Z 2026-04-04T20:33:15Z [selfsig]

sub rsa4096/97a3e97e801f054648c66043adb87e967e151557 2023-04-05T20:33:16Z
sig sbind 8fde6166401d042a 2023-04-05T20:33:18Z 2026-04-04T20:33:15Z []
```

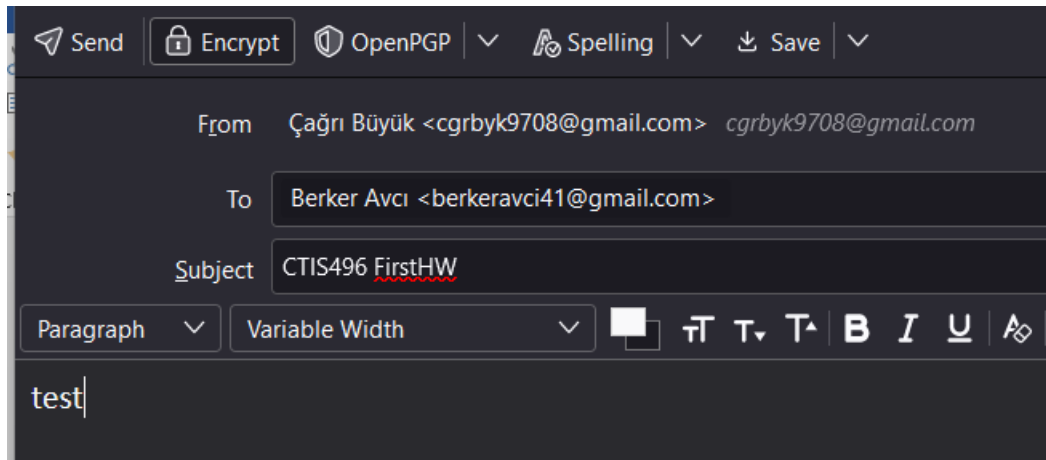
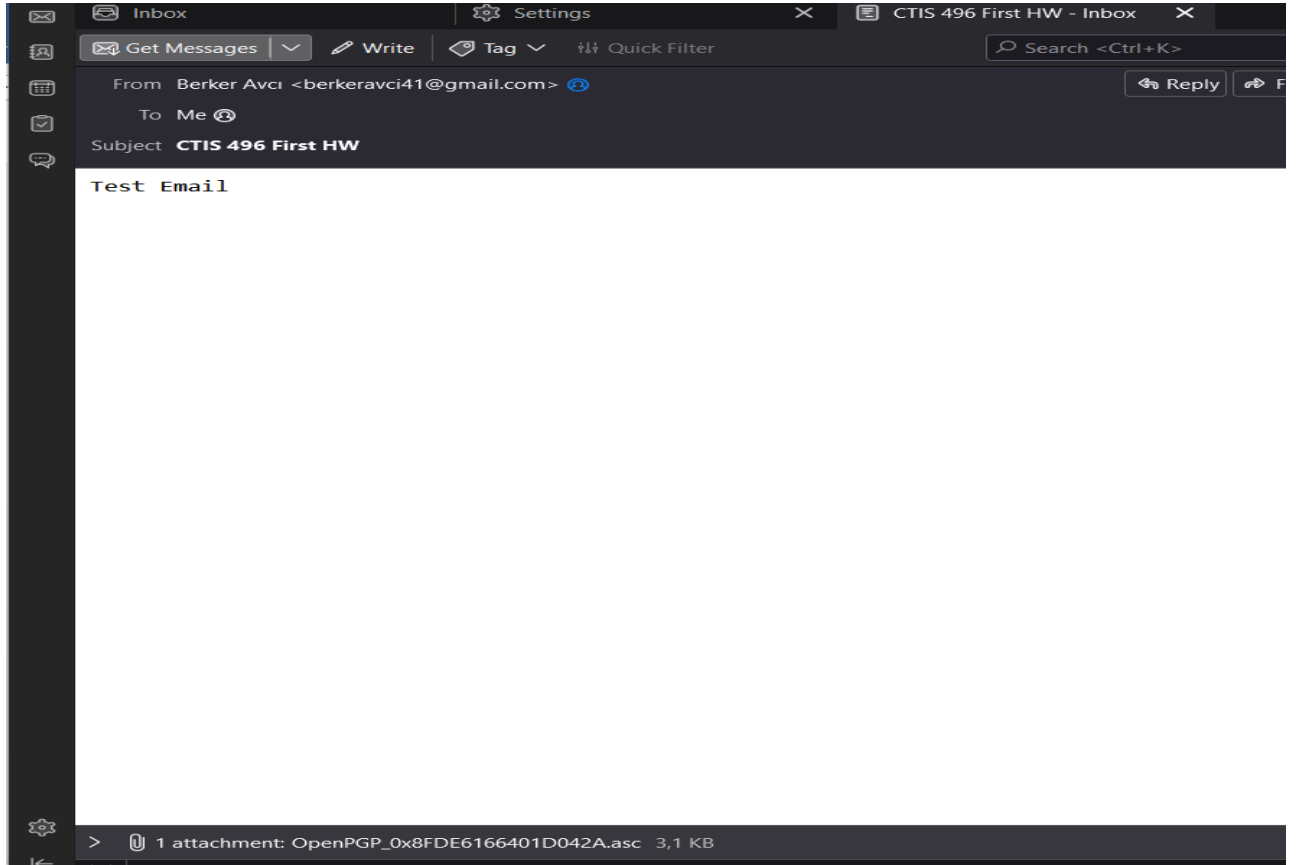
iii)



```
PS C:\Users\cagri> gpg --export-secret-keys --armor cgrbyk9708@gmail.com > cgrbyk-privkey.asc
```



iv)



- v) Confidentiality service used in part iv. Measures for maintaining confidentiality are intended to guard against unauthorized access to sensitive data. Data is frequently categorized based on the scope and nature of the harm that could result from it getting into the wrong hands. These categories can then be used to implement more or less strict measures.

vi)

Public key of Berker used to encrypt	Private key of Çağrı used to decrypt
0x8FDE6166401D042A	0xCDD3EC8C30EC0431

vii)

```
gpg -output encrypted_file.gpg -encrypt -recipient cgrbyk9708@gmail.com test_file.txt
```

```
PS C:\Users\cagri\Downloads> gpg --output encrypted_file.gpg --encrypt --recipient cgrbyk9708@gmail.com test_file.txt
```

viii)

```
gpg -decrypt encrypted_file.gpg
```

```
PS C:\Users\cagri\Downloads> gpg --decrypt encrypted_file.gpg
```

ix)

```
gpg -sign test.txt
```

```
PS C:\Users\cagri\Downloads> gpg --sign test.txt
```

x)

```
gpg -verify test_file.txt.gpg
```

```
PS C:\Users\cagri\Downloads> gpg --verify test_file.txt.gpg
```

xi)

```
gpg --edit-key cgrbyk9708@gmail.com
```

```
gpg (GnuPG/MacGPG2) 2.2.41; Copyright (C) 2022 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Gizli anahtar mevcut.

sec rsa4096/8FDE6166401D042A
  oluşturuldu: 2023-04-05   son kullanma tarihi: 2026-04-04   kullanımı: SC
  güvencesi: son derece   geçerliliği: son derece
ssb rsa4096/ADB87E967E151557
  oluşturuldu: 2023-04-05   son kullanma tarihi: 2026-04-04   kullanımı: E
[ son derece ] (1). Berker Avcı <berkeravci41@gmail.com>

gpg> trust
sec rsa4096/8FDE6166401D042A
  oluşturuldu: 2023-04-05   son kullanma tarihi: 2026-04-04   kullanımı: SC
  güvencesi: son derece   geçerliliği: son derece
ssb rsa4096/ADB87E967E151557
  oluşturuldu: 2023-04-05   son kullanma tarihi: 2026-04-04   kullanımı: E
[ son derece ] (1). Berker Avcı <berkeravci41@gmail.com>

Diğer kullanıcıların anahtarlarını doğrulayacak bu kullanıcının güven
derecesine lütfen karar verin. (pasportuna mı bakarsınız yoksa farklı
kaynaklardan parmakizlerini mi kontrol edersiniz...) kararınızı verin

1 = bilmiyorum, kem küm
2 = güvence vermem
3 = Şöyle böyle güveniyorum
4 = Tamamen güveniyorum
5 = Son derece güveniyorum
m = ana menüye dön

Kararınız? 5
Bu anahtarı gerçekten son derece güvenli yapmak istiyor musunuz? (e/H ya da y/N) e

sec rsa4096/8FDE6166401D042A
  oluşturuldu: 2023-04-05   son kullanma tarihi: 2026-04-04   kullanımı: SC
  güvencesi: son derece   geçerliliği: son derece
ssb rsa4096/ADB87E967E151557
  oluşturuldu: 2023-04-05   son kullanma tarihi: 2026-04-04   kullanımı: E
[ son derece ] (1). Berker Avcı <berkeravci41@gmail.com>

gpg> save
Güncelleme gereği olmadığından anahtar değişmedi.
berker@Berker-MacBook-Air desktop % gpg --verify test.txt.gpg
gpg: İmza Per 6 Nis 01:12:37 2023 +03 de
gpg: RSA kullanılarak anahtar 119190F4891C24D5793ADCBF31A2CB6F0AE4EBF1 ile yapılmış
gpg: güvence veritabanı denetleniyor
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: derinlik: 0 geçerli: 1 imzalı: 0 güvenilir: 0-, 0q, 0n, 0m, 0f, 1u
gpg: sonraki güvence veritabanı denetimi 2026-04-04 de
gpg: "Berker Avcı <berker.avci@ug.bilkent.edu.tr>" deki imza iyi [bilinmeyen]
gpg: UYARI: Bu anahtar güven dereceli bir imza ile sertifikalanmamış!
gpg: Bu imzanın sahibine ait olduğuna dair bir belirti yok.
Birincil anahtar parmak izi: 1191 90F4 891C 24D5 793A DCBF 31A2 CB6F 0AE4 EBF1
berker@Berker-MacBook-Air desktop %
```

```
PS C:\Users\cagri\Downloads> gpg --edit-key cgrbyk9708@gmail.com
gpg (GnuPG) 2.4.0; Copyright (C) 2021 g10 Code GmbH
This is free software: you are free to change and redistribute it.
```

xii)

```
gpg --sign berker_avci.asc
```

```
berker@Berker-MacBook-Air desktop % gpg --sign cagri_buyuk.asc
berker@Berker-MacBook-Air desktop %
```

Question 2)

```
PS C:\Users\cagri> wget https://www.tixati.com/tixati.key

StatusCode      : 200
StatusDescription : OK
Content         : {45, 45, 45, 45...}
RawContent      : HTTP/1.1 200 OK
                  Connection: keep-alive
                  Accept-Ranges: bytes
                  Content-Length: 1700
                  Content-Type: application/octet-stream
                  Date: Wed, 05 Apr 2023 22:10:44 GMT
                  ETag: "5c538bb2-6a4"
                  Last-Modified: T...
Headers         : {[Connection, keep-alive], [Accept-Ranges, bytes], [Content-Length, 1700], [Content-Type, applicat
                  on/octet-stream]...}
RawContentLength : 1700

PS C:\Users\cagri\OneDrive\Masaüstü> gpg --show-keys tixati.key
pub  rsa2048 2015-10-04 [SC]
    9DEA5E350F9D285E46D3B7E3CE737F191AF5DCFB
uid          Tixati Software Inc. (KH) <support@tixati.com>
sub  rsa2048 2015-10-04 [E]

PS C:\Users\cagri\OneDrive\Masaüstü> gpg --import tixati.key
gpg: CE737F191AF5DCFB anahtarı: Genel anahtar "Tixati Software Inc. (KH) <support@tixati.com>" içe aktarıldı
gpg: İşlenen toplam sayı: 1
gpg:           içe aktarılan: 1

PS C:\Users\cagri\OneDrive\Masaüstü> gpg --verify tixati_3.16-1_amd64.deb.asc tixati_3.16-1_amd64.deb.asc
gpg: İmza 11.02.2023 20:49:03 Türkiye Standart Saati içinde
gpg:           RSA kullanılarak 9DEA5E350F9D285E46D3B7E3CE737F191AF5DCFB anahtarı ile yapılmış
gpg: "Tixati Software Inc. (KH) <support@tixati.com>" konumundaki imza KÖTÜ [bilinmeyen]
```

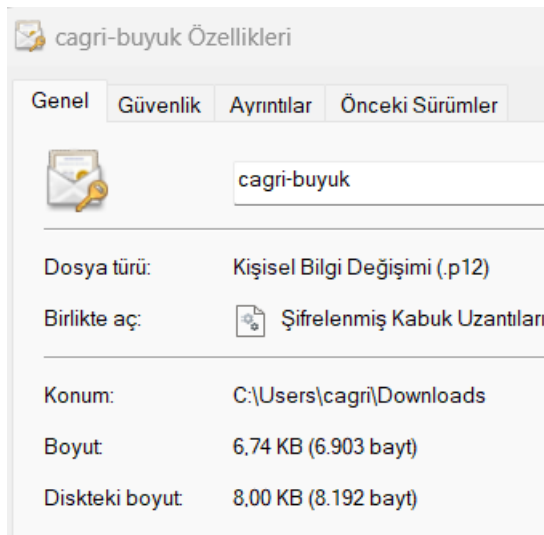
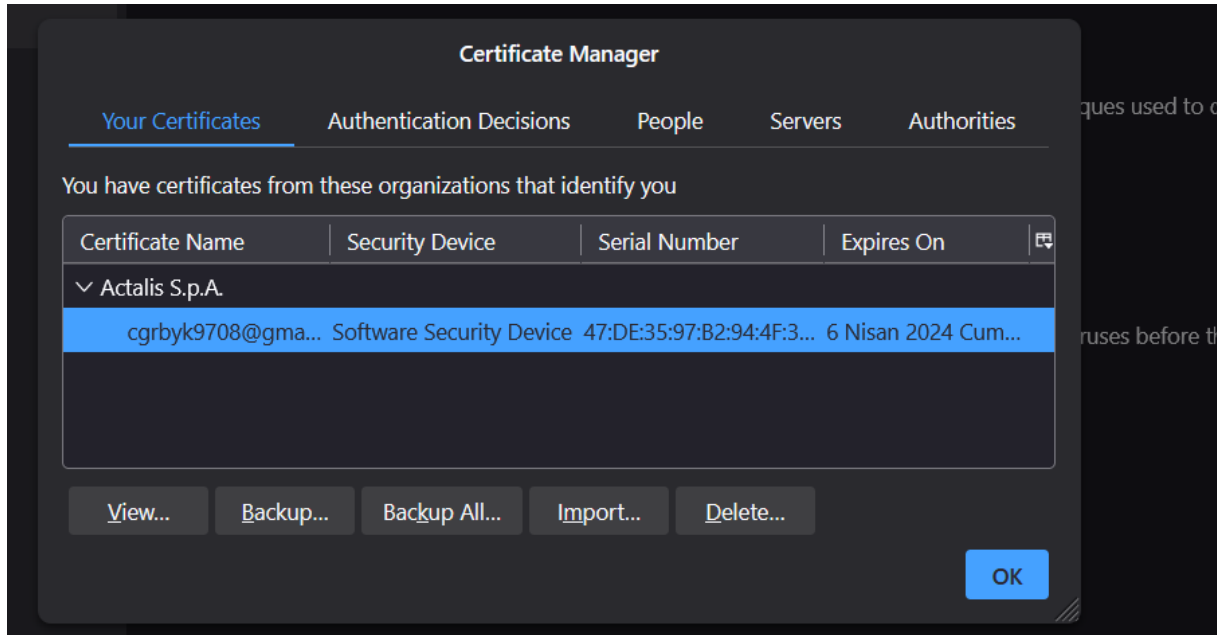
- ➔ gpg --show-keys tixati.key
- ➔ gpg --import tixati.key
- ➔ wget https://download2.tixati.com/download/tixati_2.84-1_amd64.deb.asc
- ➔ gpg --verify tixati_2.84-1_amd64.deb.asc tixati_2.84-1_amd64.deb

Question 3)

Certificate

cgrbyk9708@gmail.com	Actalis Client Authentication CA G3	Actalis Authentication Root CA
Subject Name		
Common Name	cgrbyk9708@gmail.com	
Issuer Name		
Country	IT	
State/Province	Bergamo	
Locality	Ponte San Pietro	
Organization	Actalis S.p.A.	
Common Name	Actalis Client Authentication CA G3	
Validity		
Not Before	Wed, 05 Apr 2023 22:18:33 GMT	
Not After	Fri, 05 Apr 2024 22:18:32 GMT	
Subject Alt Names		
Email Address	cgrbyk9708@gmail.com	

7



Note: It was a nice experience to see how to get a certificate and how to integrate it to system by using Mozilla. By using Thunderbird, one can view the specific details of issuer. In Thunderbird, there is a section for view certificates which includes details of certificates such as key lenght, id etc. Furthermore, there is a section for issuers which is authorities section. In that section, there are names of certificates such as TunTrust.


Question 4)


```
PS C:\Users\cagri> openssl pkcs 12 -in cagri-buyuk -nokeys -out cagri-buyuk.pem
```

```
berker-avci.pkcs12: No such file or directory
berker@Berker-MacBook-Air desktop % openssl pkcs12 -in berker-avci -clcerts -nokeys -out berker-avci.pem
Enter Import Password:
MAC verified OK
```


Using p12 file, which is created before, we are applied a conversion resulted as .pem file.


```
berker@Berker-MacBook-Air desktop % gpg --sign Çağrı Büyük_cgrbyk9708@gmail.com-0xCDD3EC8C30EC0431-pub
usage: gpg [options] --sign [filename]
berker@Berker-MacBook-Air desktop % gpg --sign Çağrı Büyük_cgrbyk9708@gmail.com-0xCDD3EC8C30EC0431-pub.asc
usage: gpg [options] --sign [filename]
berker@Berker-MacBook-Air desktop % gpg --sign cagri_buyuk.asc
```


From Berker Avcı <berkeravci41@gmail.com> 


To Çağrı Büyük 

Subject

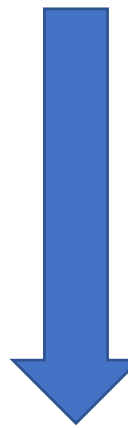



>  1 attachment: berker-avci.pem 2,3 KB

From Çağrı Büyük 

To berkeravci41@gmail.com 

Subject



>  1 attachment: cagri-buyuk.pem

*** Both mails, encrypted and signed by using Thunderbird.

