



Instruction –

## Installation of S/MIME certificate on MacOS and iOS

Installation of S/MIME certificate on MacOS and iOS

wersja 1.3

## Spis treści

1. Product description .....	3
2. Installation of S/MIME certificate on Mac OS.....	3
3. Installation of S/MIME certificate on iOS.....	5

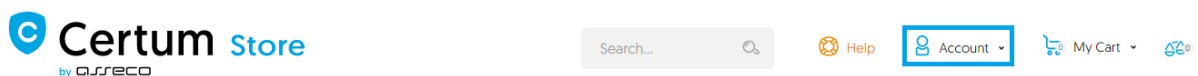
## 1. Product description

Protect your email privacy by signing and encrypting communication, using Certum S/MIME Certificates. Thanks to the unique signature function, you will be certain that emails sent by you are well protected against potential leaks or modification. You will also assure the recipient of your identity.

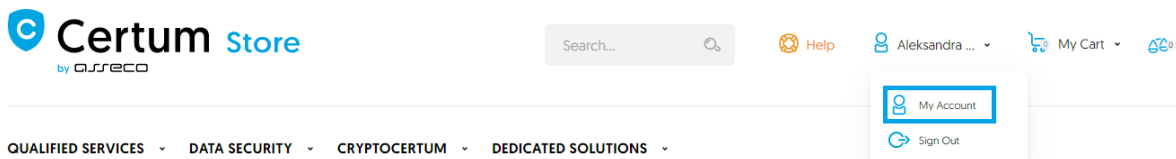
## 2. Installation of S/MIME certificate on Mac OS

To implement the certificate in an email program it is necessary to have access to the pfx/p12 file.

Log in to <https://certum.store/>



Click on [Your Account](#).



Once you are in the customer panel, select the [Manage Certificates/Certificate Management](#) section. Here you can see a list of issued certificates. Find your certificate and click on it.

Main page » My account » Certificates' management

- Electronic codes
- Activate Certificates
- Certificates' management
- Orders history
- Address details
- Tools
- Newsletter
- Domain verification
- Technical support
- Knowledge
- About Certum

### Certificates' management

Certificate profile:

Common name:

Email:

Serial number:

Validity starts after:

Validity ends before:

[Search](#)

Status

Obtain Valid

Valid

Not Valid

Revoked

In accordance with Article 13 sec. 1 and 2 of the General Data Protection Regulation (GDPR) of 27 April 2016 (hereinafter referred to as the "Regulation") I hereby inform that:

- The Administrator of your personal data is Asseco Data Systems S.A. seated in Gdynia, ul. Podolska 21, 81-321 Gdynia;
- The Data Protection Officer of Asseco Data Systems S.A. can be reached at the email address: [IOD@assecods.pl](mailto:IOD@assecods.pl), or phone number +48 42 675 63 60.
- Your personal data will be processed for the purpose necessary for the performance of the non-qualified certificate agreement pursuant to Article 6 sec. 1 letter b of the Regulation.
- Your personal data will be stored for a period of: 7 years from the date of revocation or expiration of the last certificate issued

Serial Number	Certificate profile	Email	Common name	Valid from	Expire date	Status
*****		*****@gmail.c	*****@gmail.co	October 30, 2020 6:13:19 PM	October 30, 2021 6:13:19 PM	Valid

Go to the certificate you purchased and select the [Save plain](#):



### 2.1.1. Creating a .pfx file

The .pfx file is needed to install the certificate. You can create the .pfx file after issuing the certificate.

a) After issuing the certificate download the certificate file (in the binary or text form) , from the Certificate Management Certum Store

### 2.1.2. Create from .cer file

a) Use the following command:

```
openssl pkcs12 -export -out certificate.pfx -inkey privatekey.key -in 1f1da80828adaae5d5ced0679e04657.cer
```

Bold values mean:

**certificate** - the name under which the .pfx file will be created

**privatekey** - name of the private key, generated together with the public key (must be exactly the same)

**1f1da80828adaae5d5ced0679e04657** - the name of the .cer file downloaded from Certum's store

After entering the command you will be asked to enter the password if you use a certificate with ECC keys. This is not required for RSA certificates.

After executing the request a .pfx file will be created under the specified name in the same folder.



certificate.pfx

### 2.1.3. Create file from .pem file

a) Use the following command:

```
openssl pkcs12 -export -inkey private-privatekey.key -in nameofpemfiles.pem -certfile intermediateca.pem -out pfxname.pfx
```

**privatekey** – name of .key file created during CSR generation.

**nameofpemfiles** – name of .pem downloaded from Certum Store (use exactly the same name)

**Intermediateca** – name of intermediate CA downloaded from Certum Store (use exactly the same name)

**Pfxname** – name of pfx file that you will created

NOTE: you need an intermediate file which you can also download from the Certum store. Use exactly the same file's name.

NOTE: If you want to encrypt the .pfx file add the attribute -aes256 to the request

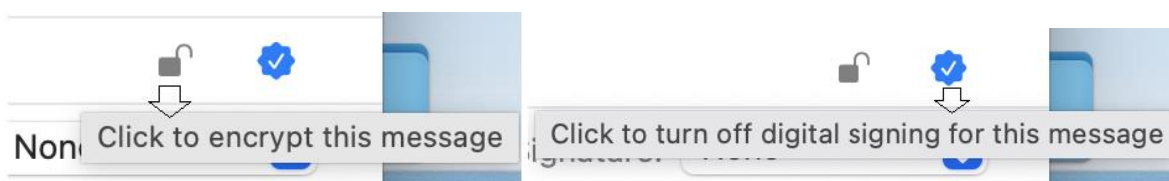
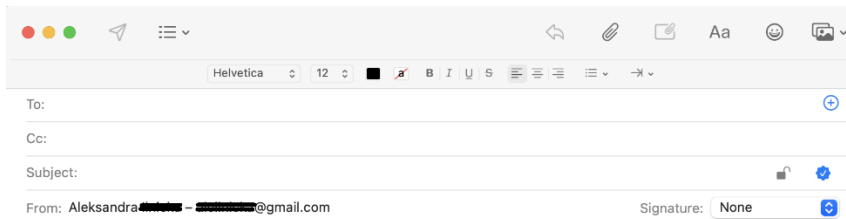
Additionally, if you want to decode your CSR, use the following command:

```
openssl req -newkey ec:ECC.pem -keyout keyprivate.key -out keypublic.csr -nodes
```

Once the pfx file is generated, double-click on it and install it in Login in the Keychain.

After installation the certificate will be visible in My certificates.

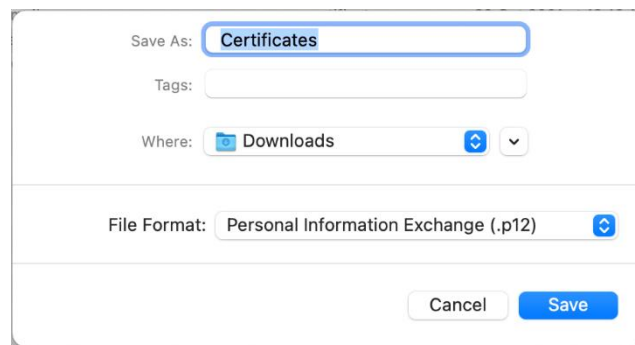
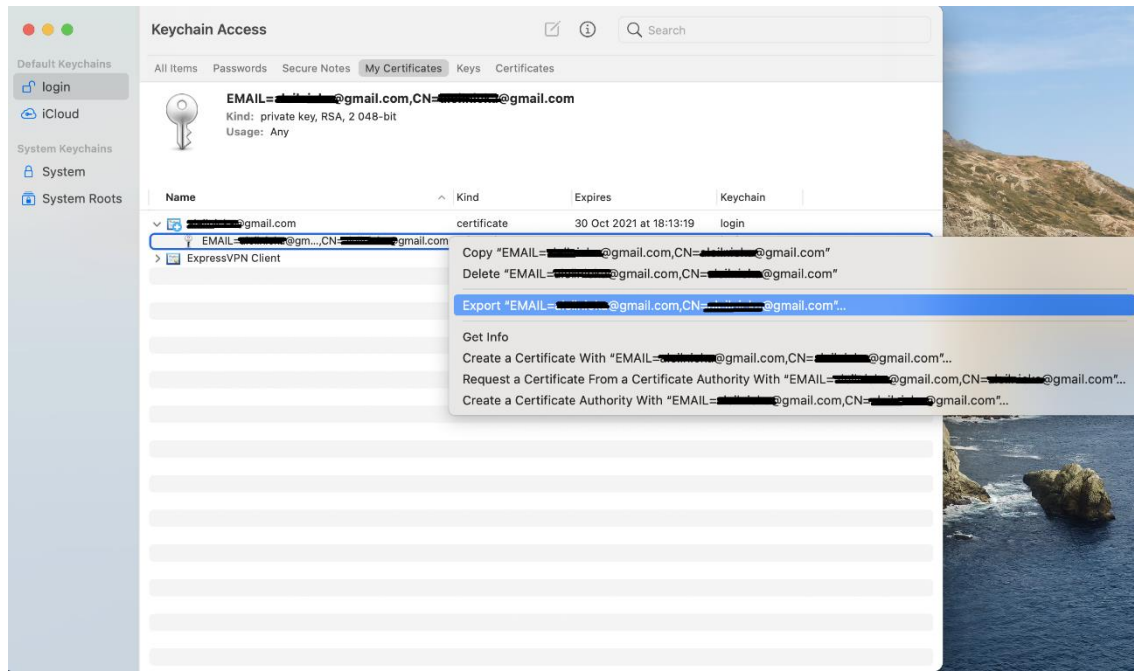
Open Mail. In a new message the certificate should load itself and you will see two new icons:



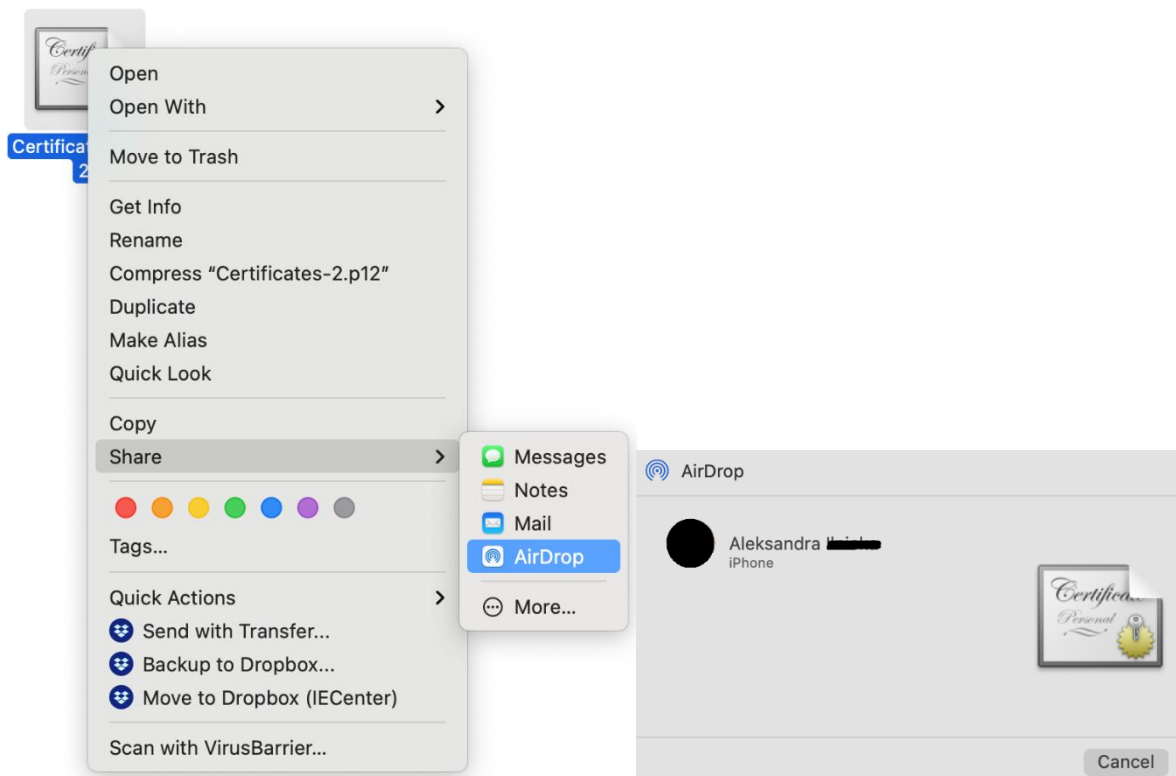
The certificate is installed correctly and is working.

### 3. Installation of S/MIME certificate on iOS

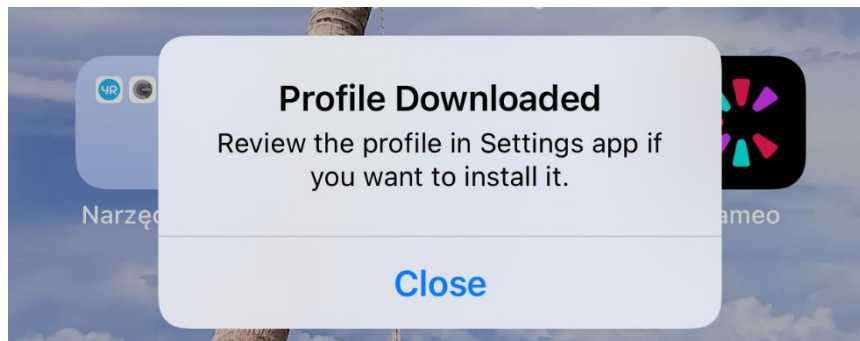
In the keychain, export the certificate to .p12, You will also be asked to password protect the exported file (the password is up to you)



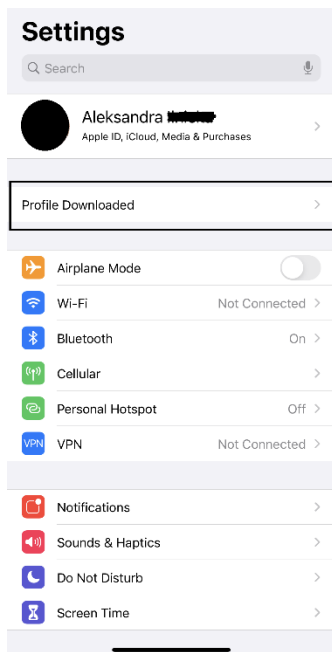
You can share the saved certificate with your Apple device (Iphone, Ipad) using AirDrop



After sharing the file to your device (Iphone, Ipad) you will see a window with information about downloading the profile and that it is available in the Settings

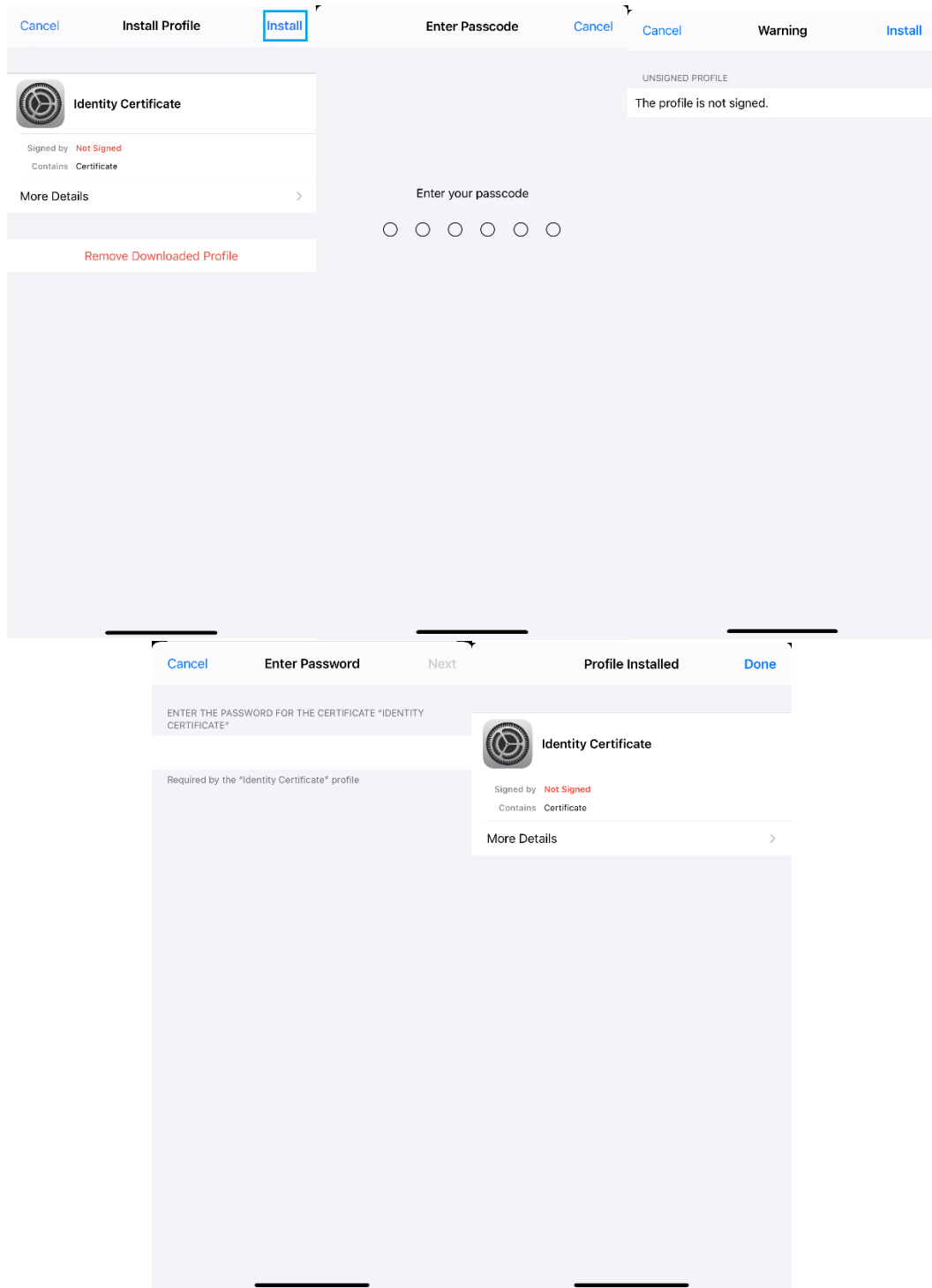


After entering the settings, enter the downloaded profile



Then in the identity certificate and click install -> enter passcode -> click install again -> enter password (the one you made when exporting the file) -> click Done





After installing the certificate you have to go to Settings -> Mail -> Accounts -> select the email for which you bought the certificate -> Account -> Advanced -> and at the very bottom you have the S/MIME section, select the sign and check yes, you can also select the option with default encryption -> exit the settings

Open the Mail application -> New message and you can see that certificate is installed (lock icon near the To: field)