

S/MIME certificate installation on MacOS and iOS

Ver. 1.5





Table of contents

1.	S/MIME certificate installation on Mac OS	.3
	Creating a .pfx file	3
	Create file from .pem file	3
2.	S/MIME certificate installation on iOS	.5

1. S/MIME certificate installation on Mac OS

To install the certificate you will need certificate file.

The issued certificate can be downloaded from the certificate creation e-mail or from the **Certificate details** view in the Data Security Products in your Certum store account in a convenient **PEM** encoding.

From the **Certificate details view** you can also download subordinate certificates for your certificate to install them in your system.

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 from the Certum store.

Create file from .pem file

a) Use the following command:

To obtain a pfx file from a .pem file, we have two working commands:

openssl pkcs12 -export -out certificate.pfx -inkey privatekey.key -in nameofpemfiles.pem

openssl pkcs12 -export -inkey privatekey.key -in nameofpemfiles.pem -certfile intermediate.pem -out certificate.pfx

To obtain a p12 file from a .pem file, we also have two working commands:

openssl pkcs12 -export -out certificate.p12 -inkey privatekey.key -in nameofpemfiles.pem

openssl pkcs12 -export -inkey privatekey.key -in nameofpemfiles.pem -certfile intermediate.pem -out certificate.p12

privatekey – name of .key file created during CSR generation. nameofpemfiles – name of .pem downloaded from Certum Store (use exactly the same name) Intermediate – name of intermediate CA downloaded from Certum Store (use exactly the same name) Certificate – name of pfx or p12 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.

2. S/MIME certificate installation 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)

•••	Keychain Access	I (j)	Q Search				
Default Keychains C login C loud System Keychains System	All Items Passwords Secure Notes My Certificates All Items Passwords Secure Notes My Certificates Image: Any Secure Notes EMAIL=at-the Lange genail.com,CN= Kind: private key, RSA, 2 048-bit Usage: Any Secure Notes Secure Notes Secure Notes	Keys Certificates					
System Roots	Name	Kind Expire certificate 30 Oc	es ct 2021 at 18:13:19	Keychain login			
	ExpressVPN Client	om Copy "EMAIL=======@gmail.com,CN======@gmail.com" Delete "EMAIL======@gmail.com,CN======@gmail.com"					
		Export TEMALE	■egmail.com,CN=	ogmail.com,CN=4	mt. L _dult egmail. L _dult egm	com" hail.com,CN=========== grail.com "	-⊋gmail.com*
	Save As:	Certificates					
	Tags:						
	Where:	🛅 Downloads	6				
	File Format:	Personal Inform	ation Exchang	e (.p12)	0		
			Cance	el Sav	/e		

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

Settings							
Q Search							
	Aleksandra Muleia Apple ID, iCloud, Media & Pu	rchases	>				
Profile	Downloaded	3	,				
۹ 🛃	irplane Mode						
🛜 V	Vi-Fi	Not Connected	>				
* E	lluetooth	On D	>				
(† ³⁾ C	Cellular	;					
ତ ଜ	ersonal Hotspot	Off	>				
VPN V	'PN	Not Connected	>				
	lotifications	;					
 S 	ounds & Haptics	;	>				
C c	00 Not Disturb	2	>				
X s	creen Time	3	>				

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

Cancel Ins	stall Profile	Install		Enter Pa	isscode	Cancel	Cancel	Warning	Install
							UNSIGNED PROFILE		
Identity Ce	rtificate						The profile is not	signed.	
Signed by Not Signed Contains Certificate									
More Details		>		Enter your	passcode				
Remove [Downloaded Profile		0	0 0	0 0	0			
	Cancel	Enter Passwo	ord	Next		Profile	installed	Done	
	ENTER THE PASSV CERTIFICATE"	VORD FOR THE CERTI	FICATE "IDENT	ITY					
						Identity Certifi	cate		
	Required by the "Ic	lentity Certificate" pro	file		Signed by Contains	Not Signed Certificate			
					More Det	ails		>	

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).