

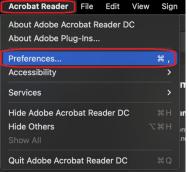
Manual for set up and signing with Adobe Acrobat DC for macOS

If there is not installed Adobe Acrobat DC on your device, you can download it from here.

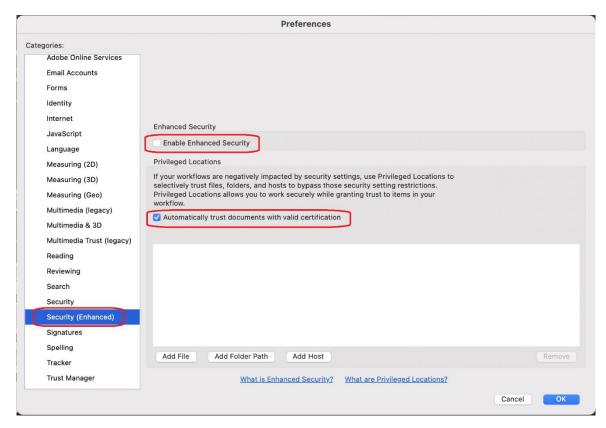
Note, you must load your electronic signature in your device and after that start Adobe Acrobat DC.

1. Settings:

From menu in Adobe Reader select Preferences...



Categories: Security (Enhanced)





	Creation	
Categories: Adobe Online Serv	Default Signing Method: Adobe Default Security	
Email Accounts	Default Signing Format: CAdES-Equivalent	
Forms	When Signing:	More
Identity	Show reasons	
Internet	Show location and contact information	
JavaScript	Include signature's revocation status	
Language	View documents in Preview Mode	More
Measuring (2D)	Enable Review of Document Warnings: When certifying a document	
Measuring (3D)	Prevent Signing Until Warnings Are Reviewed: When certifying a document	
Measuring (Geo)	Vuse modern user interface for signing and Digital ID configuration	
	Construction and any and any and any	More
Multimedia (legacy		
Multimedia (legacy Multimedia & 3D		
	Appearances	
Multimedia & 3D Multimedia Trust (I		
Multimedia & 3D Multimedia Trust (I Reading	Appearances	More
Multimedia & 3D Multimedia Trust (I Reading Reviewing		More
Multimedia & 3D Multimedia Trust (I Reading Reviewing Search	Appearances	More
Multimedia & 3D Multimedia Trust (I Reading Reviewing Search Security	Appearances	More
Multimedia & 3D Multimedia Trust (I Reading Reviewing Search Security Security (Enhancer	Appearances New Edit	More
Multimedia & 3D Multimedia Trust (I Reading Reviewing Search Security Security (Enhancer Signatures	Appearances New Edit Duplicate	More
Multimedia & 3D Multimedia Trust (I Reading Reviewing Search Security Security (Enhancer	Appearances New Edit Duplicate	More

Categories: Signatures \rightarrow Creation & Appearance select *More...*

Categories: Signatures \rightarrow Verification select *More*...

Signature Verification Preferences					
Verify signatures when the document is opened When document has valid but untrusted signatures	When document has valid but untrusted signatures, prompt to review and trust signers				
Verification Behavior When Verifying: Use the document-specified method; prompt if unavailable Use the document-specified method; if unavailable, use default method					
 Ose the document specified method; if diavailable, use default method Always use the default method: Adobe Default Security Require certificate revocation checking to succeed whenever possible during signature verification Use expired timestamps Ignore document validation information 					
Verification Time Verify Signatures Using: Time at which the signature was created Secure time (timestamp) embedded in the signature Current time	Verification Information Automatically add verification information when saving signed PDF: • Ask when verification information is too big • Always • Never				
Help	Cancel OK				



	Preferences	
ategories:		
Adobe Online Services	Digital Signatures	
Email Accounts	Creation & Appearance	
Forms	Control options for signature creation	More
Identity	Set the appearance of signatures within a document	
Internet	Verification	
JavaScript	Vernication	
Language	Control how and when signatures are verified	More
Measuring (2D)		
Measuring (3D)	Identities & Trusted Certificates	
Measuring (Geo)	Create and manage identities for signing	More
Multimedia (legacy)	Manage credentials used to trust documents	Wore
Multimedia & 3D		
Multimedia Trust (legacy)	Document Timestamping	
Reading	Configure timestamp server settings	More
Reviewing		
Search		
Security		
Security (Enhanced)		
Signatures		
o !!!		
		Cancel

Categories: Signatures → Identities & Trust Certificates select More...

At the left side of the menu select PKCS#11 Modules and Tokens:

	2	🦉 - 💽 Cei	rtificate Details	🊧 Export	C Refresh	Remove II
ID Accounts	Name	∧ Issuer	Storage Mech	ani Expires		
Files						
Digital IDs						
Modules and Tokens						
ficates						



Select Attach Module:

000	Digital ID and Trusted Certificate Settings
 Digital IDs 	Attach Module Detach Module 2 Refresh
Roaming ID Accounts	Module Manuf A Library Path
Digital ID Files	
Keychain Digital IDs	
PKCS#11 Modules and Tokens	
Trusted Certificates	
	(mmgi)
	Locate a PKCS#11 Module
	Library Path
	Cancel OK an load additional modules to gain access to

In the *Library Path* you should copy one of the following paths, depending on the type of smart card you use. For *Gemalto smart card you should copy:*

/Library/Frameworks/eToken.framework/Versions/A/libIDPrimePKCS11.dylib – for SAC Software

/Library/Gemalto/libidprimepkcs11.dylib – for Gemalto software

Any other smart cards models:

/Library/CV Cryptovision/libcvp11.dylib

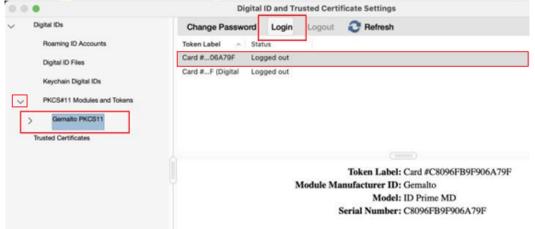
Once the path has been loaded you should see the following screen:

	•		Digital ID and	i Trusted (Certificate Settings
¥.	Dipital IDs	Attach Module	Detach	Module	C Refresh
	Roaming ID Accounts	Module Manufac	Library Path	n) -	
	Digital ID Files	Gemaito	Ulbrary11.dy	lb	
	Keychain Digital IDs				
\rightarrow	PKCS#11 Modules and Tokens				
	Trusted Certificates				
			Mod	lule Man	ufacturer ID: Gemalto
				Module	Description: Gemalto PKCS11
				Lib	rary Version: 2.3
				Cryp	toki Version: 2.20
				1	.ibrary Path: /Library/Gemalto/libidprimepkcs11.dylib



To import all needed certificates in Acrobat Reader, you should enter the PIN Code of your smart card electronic signature.

To visualize the smart card please, click on the left arrow next to **PKCS#11 Modules and Tokens**. Click on the left button of your mouse and select **Gemalto PKCS** then at the right side of the screen select **Login**, as shown:



Please, enter your PIN code in the dialog window:

Token Labe	1: Card #C805	96FB9F906A7	9F	
Password:	••••			
rassworu.				

After your PIN code has been entered and confirmed with OK, the screen should look like this:

000	D	igital ID and Tr	usted Certi	ficate Settings		
✓ Digital IDs	Change Passw	ord Login	Logout	C Refresh		
Roaming ID Accounts	Token Label 🗠	Status	. An			
Digital ID Files	Card #06A79F	Logged in				
Keychain Digital IDs	Card #F (Digital	Logged out				
V PKCS#11 Modules and Tokens						
Gernalto PKCS11						
Card #C8096FB9F906A79F						
Card #C8096FB9F906A79F (Digital						
Trusted Certificates	Token Label: Card #C8096FB9F906A79F					
	Module Manufacturer ID: Gemalto					
				Model: ID Prime MD		
			5	Serial Number: C8096FB9F906A79F		



You should consider the first token label, only. Its Status must be Logged in.

Please, press Close to close the window and then OK, to close the Preferences.

- 2. Document signing with integrated function in Acrobat Reader DC.
 - a. Open the document you wish to sign and click on *Tools* and then select *Certificates*: **Tools** → **Certificates**:

Home	Tools Инструкция з	за под			
Q Sear	rch tools				
		\wedge			
		len		l≟ <mark>⊜</mark> °	l≟ <mark>+</mark> °
	Comment	Fill & Sign	Edit PDF	Export PDF	Create PDF
	Open 👻	Open 👻	Open 🔻	Open 🔻	Open 💌
	┢╧ੑ ॒		යු	Luu	Ø9
	Combine Files	Share	Stamp	Measure	Certificates
	Add 🔻	Open 👻	Open 💌	Open 💌	Open 💌

b. Select option Digitally Sign:

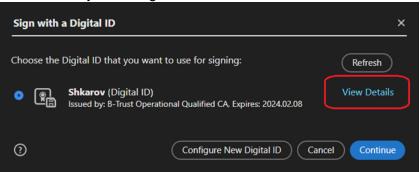


c. Make a square by holding the left button on your mouse and mark out the field where you wish to digitally sign.

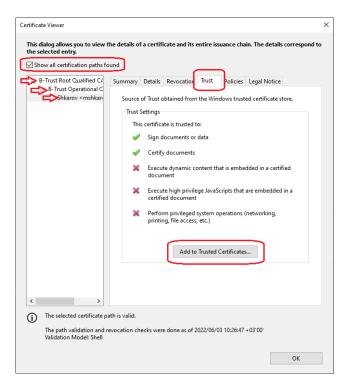




- a. After the signing field has been created you should see the following screen. It is recommended to add the certificate to trusted (only for new certificates, when signing for the very first time).
 - You can add it by choosing View Details



- Select "Show all certification paths found". From tabs select **Trust** and then **Add to Trusted Certificates...**, the following settings are the same for each one of the visible certificates on the left side of the screen. If the button **Trust** is not visible for some of the certificates, it means the setup had already been made.



- In the pop up window Acrobat Security, confirm with OK.

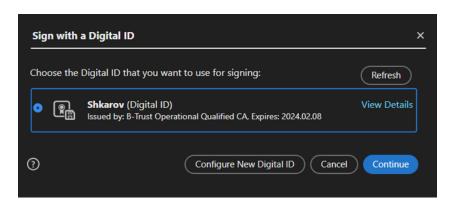
thange the trust settings, you will need to revalidate any signatures to see the ctly trusting the signer's identity you are overriding all inherited trust settings. sure you want to do this?

- В Import Contact Settings се маркират задължително посочените позиции:

Import Contact Settings	
Subject: Shkarov <mshkarov@borica.bg></mshkarov@borica.bg>	
Issuer: B-Trust Operational Qualified CA	
Usage: Digital Signature, Non-Repudiation, Encrypt Keys	
Expiration: 8.2.2024 r. 3:00:00	
Trust	
A certificate used to sign a document must either be designated as a trust anchor chain up to a trust anchor in order for signature validation to succeed. Revocatio checking is not performed on or above a trust anchor.	
Use this certificate as a trusted <u>r</u> oot	
If signature validation succeeds, trust this certificate for:	
Signed documents or data	
Certified documents	
Dynamic content	
Embedded high privilege JavaScript	
Privileged system operations (networking, printing, file access, etc.)	
Help	Cancel
Help OK O	cancel

- Confirm the closing of the windows twice with **OK** and then it returns to the previous screen.





- b. Mark the needed certificate and press Continue.
- *c.* The certificates are visualized and for signing you should press **Sign**. When entering the PIN the following screen might show:
 - Braegere fIMH 2 PW or Promoting Back Sign
- d. Then choose where to save the signed document and click Save.
- e. The signed document should look like this::

)	Signed and all signatures are valid.	Signature Panel
		Date: 2022.04.18 Shkarov '13:04:43 +03'00

At the top left side on your document, you should see that the document has been successfully signed and verified.

The settings are completed!

3. For validation of electronically signed documents, please follow the link: <u>B-TRUST | Qualified Signature Validation Service</u>

B-trust contact details: T: 0700 199 10 M: *9910 e-mail: <u>support@borica.bg</u>