DSCSigner Installation Manual for macOS

Contents

1.	DSO	CSigner installation in macOS	3
1.	1.	DSCSigner installation	3
2.	Bro	wser Configuration	6
2.	1.	Mozilla Firefox	6
2.	.2.	Google Chrome	9
2.	.3.	Apple Safari 1	0

1. DSCSigner installation in macOS

For MacOS operating system the following prerequisites are required:

- DSC token driver
- Oracle Java SE JDK 8 (<u>http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html</u>)
- 1.1. DSCSigner installation
 - 1. To install DSCSigner, double click on the DSCSigner.dmg file. The package will be extracted, and the application file is shown:



2. Copy the DSCSigner application to the applications folder



3. Search the application from Spotlight and launch the application.

2 DSCSigner	14 M
TOP HITS	
DSCSigner — DSCSigner	
SCSigner — iCloud Drive	
BSCSigner — Applications	
FOLDERS	
DSCSigner	
DSCSigner	
dsc-signer	
MAGES	DSCSigner
B DSCSigner.icns - DSCSigner	Version: 1.0
B DSCSigner.icns — macosx	
dscsigner.png	
OTHER	Kind Application
DSCSigner.dmg — DSCSigner	Size 13.6 MB
	Created 11/10/17
DSCSigner-1.0.dmg — bundles	Modified 11/10/17

4. Connect the DSC token and wait for few seconds for the application tray icon to appear with the status Running.



5. Right click on the tray icon to open the settings.



6. Select a predefined token driver e.g. ProxKey and then click on **Save** button.

•••	DSCSigner Settings								
If DSC token is not listed below, Select Custom and provide path to the driver									
	Select DSC token								
	PROXKey Proxkey								
Token Driver UsbKeyTool/libwdpkcs_Proxkey.dylib									
Save									

7. To use a custom DSC token, select the custom option and provide the path to the Token driver and then click on **Save** button.



2. Browser Configuration

The browser must be configured prior to the use of DSCSigner tool to configure the browser to trust the DSCSigner Client. The configuration for the browsers are given below.

2.1. Mozilla Firefox

1. Open Mozilla Firefox and type the following in the address bar and press enter.

2. Scroll down to view the Certificate section and click on the **View Certificates** button to open the certificate manager.



3. In the Certificate Manager popup, click on the Authorities tab and then click on Import button.

Certificate Manager									
Your Certificates People Servers Authorities Others									
You have certificates on file that identify these certificate authorities									
Certificate Nam	ne		Security De	evice					
AC Camerfirma S.	Α.								
Chambers of C	ommerce Root - 2008		Builtin Object To	ken					
Global Chambe	rsign Root - 2008		Builtin Object To	ken					
AC Camerfirma SA	CIF A82743287								
Camerfirma Ch	ambers of Commerce Root		Builtin Object To	ken					
Camerfirma Glo	obal Chambersign Root		Builtin Object To	ken					
ACCV									
ACCVRAIZ1			Builtin Object To	ken					
Actalis S.p.A./033	58520967								
Actalis Authent	ication Root CA		Builtin Object To	ken					
▼ AddTrust AB									
AddTrust Low-Value Services Root Builtin Object Token									
View Ed	dit Trust Import	Export	Delete or Distru	ust					
						OK			

4. Browse to DSCSigner/ssl folder and select the rootCA.crt file and click on the Open button.



National Informatics Centre, Kerala State Centre

5. Check the **Trust this CA to identify websites** and click on OK button to complete the root certificate export.

You have been asked to trust a new Certificate Authority (CA).								
Do you want to trust "DSCSigner Root CA" for the following purposes?								
Trust this CA to identify websites.								
Trust this CA to identify email users.								
Trust this CA to identify software developers.								
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).								
View Examine CA certificate								
Cancel								

6. The configuration is complete and now you can use Mozilla Firefox for digital signing using DSCSigner.

2.2. Google Chrome

1. Open Google Chrome browser and type the following in the address bar and press enter:

chrome://flags/#allow-insecure-localhost



2. Click on Enable link to allow Chrome to securely communicate with DSCSigner client. Now to apply the settings and restart Chrome browser click on Relaunch Now button at the bottom of the page

Your changes will take effect the next time you relaunch Google Chrome.

RELAUNCH NOW

3. The configuration is complete and now you can use Google Chrome for digital signing using DSCSigner.

2.3. Apple Safari

1. After installation of DSCSigner client, open Safari browser and type the following in the address bar and press enter:



2. Click on Continue button.



3. Check Always trust "localhost" when connecting to "localhost" and click on Continue button.

	Safari can't verify the identity of the website "localhost". The certificate for this website is invalid. You might be connecting to a website that is pretending to be "localhost", which could put your confidential information at risk. Would you like to connect to the website anyway?
Always trust	"localhost" when connecting to "localhost"
localhost	
Certificate Audicat Details	Iocalhost Issued by: DSCSigner Root CA Expires: Tuesday, October 29, 2154 at 4:21:44 PM India Standard Time This certificate was signed by an unknown authority
?	Hide Certificate Cancel Continue

4. Provide the current username and password and click on **Update Settings** button.

	You are making changes to your Certificate Trust Settings. Enter your password to allow this. User Name: xxxxxxxx						
	Password:						
		Cancel Update Settings					

n

5. The success message will be displayed in the browser as shown below:

Ś	Safari	File	Edit	View	History	Bookmarks	Window	Help		
••	• <						⊜ localho	st	Ċ	Ê 7 +
{"sta	tus":"s	ucces	₃"}							

6. The configuration is complete and now you can use Safari browser for digital signing using DSCSigner.