

Version 1.3



EuroCert Sp. z o.o. ul. Puławska 474 02-884 Warszawa KRS: 0000408592 NIP: 9512352379

Dział handlowy: +48 22 490 36 45 handlowy@eurocert.pl Dział techniczny: +48 22 490 49 86 wsparcie@eurocert.pl +48 22 390 59 95 biuro@eurocert.pl www.eurocert.pl



Table of contents

1.		Pro	gram	information
2.		Min	imur	n system requirements
3.		Inst	allati	on3
4.		Sign	ing	5
	4.	1	"Sig	nature parameters" section6
		4.1.	1	Signature variant
		4.1.	2	Signature type7
		4.1.	3	Digest algorithm
		4.1.	4	Commitment type9
	4.	2	"Dat	ta" section
	4.	3	Sign	ing process
	4.	4	Sign	ing a PDF file with graphical representation12
	4.	5	Add	ing signatures to a previously signed file13
5.		Ver	yfing	
	5.	1	Sign	ed file verification process14
6.		Sett	ings.	
	6.	1	Арр	lication settings
		6.1.	1	General settings
		6.1.	2	Signing settings
		6.1.	3	Timestamp settings
	6.	2	Sma	rt card management
		6.2.	1	Change token PIN
		6.2.	2	Unlock token PIN
		6.2.	3	Change token SO PIN
7.		Cert	ificat	te renewal 19
8.		Help	o	
9.		Abo	ut pr	ogram





1. Program information

SecureDoc v2.0 is an application designed to create and verify electronic signatures with the option of issuing a signature with a time stamp.

In the SecureDoc v2.0 application, an electronic signature may be submitted with the use of certificates issued by: EuroCert, CenCert (Enigma), KIR, PWPW, and Certum (Asseco).

Signature formats available in SecureDoc are PAdES-BES, PAdES-T, XAdES-BES, XAdES-T in internal and external types (Detached / Enveloping / Enveloped).

Cryptographic hash function (Digest algorithm): SHA-256

2. Minimum system requirements

- MacOS High Sierra (or newer) operating system
- Internet connection (required for using file verification and for using ECSigner cloud signature)

To use your qualified electronic signature issued by EuroCert in SecureDoc, second application must be installed:

- Cryptographic card management application Charismathics Smart Security Interface in case of electronic signature on a device
- ECSigner in case of ECSigner cloud signature

3. Installation

To install the application, go to <u>https://eurocert.pl/index.php/oprogramowanie</u> and download "SecureDoc 2 - application for signing and verification of qualified signatures". After running the downloaded installer, follow the dialogue boxes below:

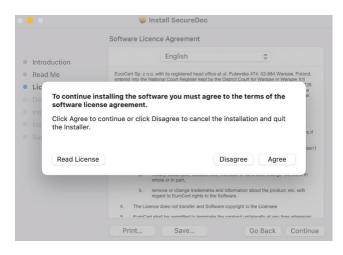
	Welcome to the SecureDoc Installer
Introduction	SecureDoc 2.0 is a modern application that allows you to sign document with an electronic signature as well as verify signed documents.
Read Me	
Licence	
Destination Select	
Installation Type	
Installation	
Summary	





		🥪 Install SecureDoc
		Important Information
0	Introduction	In order to use the electronic signature, the application for the cryptographic card management must be installed. This application could
•	Read Me	be found on our website https://eurocert.pl/en/oprogramowanie.
0	Licence	
0	Destination Select	
0	Installation Type	
0	Installation	
0	Summary	
		Print Save Go Back Continue

	Software Licence Agreement	
Introduction	English	
Read Me	EuroCert Sp. z o.o. with its registered head office at ul. Pulawska 474, 02-884 Warsaw, Pola	
Licence	entered into the National Court Register kept by the District Court for Warsaw in Warsaw XIII Commercial Division of the National Court Register, under No 000406392, Tax 10 No: 951 1 23 79, its share capital paid in full amounting to PLN 1.240.000, hereinafter EuroCort, grants licence to SecureDoc Software (hereinafter: Software) on terms and conditions set forth belo	235 a
Destination Select		w.
Installation Type	 The Software shall be used to submitting and verifying electronic signatures and electronic seals and to timestamping. 	
	2. EuroCert grants the Licensee a licence for an indefinite time period to:	
Summary	 use the whole Software free of charge on an unlimited number of compute the Licensee has a qualified certificate issued by EuroCert, or use only a verifying service of the Software free of charge if the License h 	
	a valid qualified certificate issued by EuroCert. 3. Licensee must not:	
	a. modify, decomplie, disassemble, translate or otherwise change. Software i whole or in part, b. remove or change trademarks and information about the product, etc. with regard to EuroCert rights to the Software.	
	The Licence does not transfer and Software copyright to the Licensee EuroCert shall be normitted to terminate the contract unilaterally at any time whene	





EuroCert Sp. z o.o. ul. Puławska 474 02-884 Warszawa KRS: 0000408592 NIP: 9512352379

Dział handlowy: +48 22 490 36 45 handlowy@eurocert.pl Dział techniczny: +48 22 490 49 86 wsparcie@eurocert.pl +48 22 390 59 95 biuro@eurocert.pl www.eurocert.pl

ź



Read Me Licence Destination Select Installation Type The installation was successful.	•	🥪 Install SecureDoc	
		Standard Install on "Macintosh HD) <i>"</i>
Go Back Install Install SecureDoc The installation was completed successfully. Introduction Read Me Licence Destination Select Installation Type Installation was successful. Installation The installation was successful. Installation The software was installed.	 Read Me Licence Destination Select Installation Type Installation 	Click Install to perform a standa	
 Install SecureDoc The installation was completed successfully. Introduction Read Me Licence Destination Select Installation Type Installation 			
 Introduction Read Me Licence Destination Select Installation Type Installation The installation was successful. The software was installed. 	• •		
 Read Me Licence Destination Select Installation Type Installation The installation was successful. The software was installed. 		The installation was completed su	ccessfully.
Installation The installation was successful. The software was installed.	Read MeLicenceDestination Select	The installation	D
	Installation		

After completing this step, the application is ready to use.

4. Signing

The "Signing" tab is dedicated to documents signing using electronic signatures. In the "Signature format" section there are two available signature formats:

- PAdES
- XAdES

		Secur	eDoc					
SecureDoc Sign	ing Veryfing Set	tings Certificate renewal	Help	About program	1			
	Signature variant:	PAdES-BES (without timestamp) Enveloped SHA-256					Show	
PAdES (only PDF)	Signature type:							0
XAdES	Digest algorithm:			Add Dele		Clear		Sign
	Commitment type:	None			,			
Signature format		Signature parameters	ure parameters			Data		
Inpu	ut data (0)	Output	data (0)			5	Status	



EuroCert Sp. z o.o. ul. Puławska 474 02-884 Warszawa KRS: 0000408592 NIP: 9512352379

Dział techniczny: +48 22 490 49 86 wsparcie@eurocert.pl



PAdES signature format is dedicated and exclusive for PDF files.

XAdES signature format can be used to sign any file format (.xml, .docx, .jpeg, .odt etc.). PDF files also can be signed using XAdES signature format, however it's always recommended to use PAdES.

4.1 "Signature parameters" section

This section contains all of the main parameters of the performed signature.

•••		Secur	eDoc						
SecureDoc Signi	ng Veryfing Sett	ings Certificate renewal	Help	About program	1				
	Signature variant: Signature type:	PAdES-BES (without timestamp) Enveloped				_			
PAdES (only PDF) XAdES	Digest algorithm:	SHA-256		Add Del		Clear	Show	B	
XAAES	Commitment type:	None	_	file fil		list	document	Sign files	
	communent type.	NOTE	_						
Signature format	S	ignature parameters				Data			
Inpu	it data (0)	Output	Output data (0)			Status			

4.1.1 Signature variant

Depending on the chosen Signature Format, the following Signature Variants are available: <u>PAdES-BES / PAdES-T</u> or <u>XAdES-BES / XAdES-T</u>.

			Secur	eDoc						
SecureDoc Sig	ning Veryfing	Settings	Certificate renewal	Help	About pr	ogram				
PAdES (only PDF)	Signature variant: Signature type: Digest algorithm: Commitment type:	the second se	S-BES (without limestamp) S-T (with timestamp)		Add file	Delete file	Add directory	Clear	Show document	Sign files
Signature format		Signature	parameters					Data		
Inp	ut data (0)		Output	data (0)	i.			-	Status	

Variant -BES means that during the signing process, electronic signature will be placed without a timestamp.

Variant -T means that during the signing process, electronic signature will be placed with a timestamp.

The Qualified Timestamp Service ("timestamp" mentioned above) is an additional service that allows to precisely determine the date and time of activities carried out in the electronic environment.

Timestamping makes it possible to confirm the time and date when the electronic signature was placed on the file or to determine if a given document existed at a specific time and





has not been changed since. Under the provisions of applicable law, this has effects of a *date certain*.

By using a timestamp issued by a qualified entity, you get a guarantee that the deadline for signing the document will not be challenged in relation to courts, institutions, companies, individual clients, etc.

It is also worth noting that the timestamp does not retrieve the current time from the computer on which the signature is issued, but asks a dedicated server to obtain information about the time.

4.1.2 Signature type

000			SecureDoc						
SecureDoc Sign	ing Veryfing Signature variant: Signature type:	Settings Certificate renewal Help Ostached Enveloping ✓ Enveloped		About pr		Add directory	Clear	Show	
XAdES	Digest algorithm: Commitment type:	SHA-256 None	Add	Delete	Sign files				
Signature format	communen (ypc.	Signature parameters					Data		
Inp	ut data (0)		Output data (0)	8			5	Status	

4.1.2.1 Detached

When signing a document with a detached signature type, the signature itself will be created in a separate file and saved in the same folder as the original file. The file which is being created after signing the document with a detached signature type, has a XAdES format.

Detached signature type can be used to sign files of any format or size.

It should be noted, that when verifying a file signed with a detached signature - you must have access to a source file (original file, which contains contents of a document) + file with a signature (file created during the signing process, which contains only the signature). Also, when sending a file signed using a detached signature type - it is necessary to send both files (the original one and the one containing the signature).

It is important not to change in any way (including the name of the files) the original file or the file which was created, as any changes will result in negative verification of the signature.





4.1.2.2 Enveloping

Enveloping signature type should be used for any files being signed in XAdES format, where we need the signature to be included in the signed file. So the signature issued using Enveloping signature type will contain both – the content of the document and the signature itself (2 in 1).

It is worth remembering that the file signed using the Enveloping signature type will be saved in XAdES format.

So, if for example, we sign a file "document.txt", the resulting file (containing the signature) will be named "document.txt.XAdES".

4.1.2.3 Enveloped

This signature type is equivalent to the Enveloping signature type and is used only for XML files. File signed using this signature type will contain both the contents of a document as well as a signature as well.

So if we want to sign an XML file so it contains the signature with the content of the document – Enveloped signature type should be selected. This signature type applies only to XML files.

... SecureDoc SecureDoc Signing Veryfing Settings Certificate renewal Help About program Signature variant: XAdES-BES (without timestamp) Signature type: PAdES (only PDF) Enveloped Digest algorithm: XAdES Add Clea Commitment type: None Signature format Signature parameters Data Input data (0) Output data (0) Status

4.1.3 Digest algorithm

SHA-256 is a type of cryptographic hash function. Higher hash value provides higher security.



EuroCert Sp. z o.o. ul. Puławska 474 02-884 Warszawa KRS: 0000408592 NIP: 9512352379

Dział handlowy: +48 22 490 36 45 handlowy@eurocert.pl Dział techniczny: +48 22 490 49 86 wsparcie@eurocert.pl



4.1.4 Commitment type

				Secu	reDoc								
SecureDoc	Signir	veryfing	Settings	Certificate renewal	Help	About pr	ogram						
		Signature variant:	XAdES	-BES (without timestamp)									
PAdES (only PDF)		Signature type:	Enveloped					Do					
XAdES		Digest algorithm:	SHA-256			Add	Delete	Add directory	Clear	Show document	Sign files		
		Commitment type:	V Non	A CONTRACTOR OF		1.12	100		1970	1.00000000			
Signature forma	Signature format			Proof of origin Proof of recipt			Data						
il.	Inpu	t data (0)	Pros	of of delivery	D)	l.			5	Status			
			Proc	of of sender of of approval of of creation									

This field is optional and contains additional information about the signing reason. There are 6 types of commitments to choose from:

- Proof of origin
- Proof of receipt
- Proof of delivery
- Proof of sender
- Proof of approval
- Proof of creation

4.2 "Data" section

• • •			Secur	eDoc						
SecureDoc Sig	ning Veryfing	Settings	Certificate renewal	Help	About program	1				
	Signature variant:	PAdES	S-BES (without timestamp)							
PAdES (only PDF)	Signature type:	Envelo	oped							
XAdES	Digest algorithm:	SHA-2	256			lie Add directory	Clear	Show document	Sign files	
	Commitment type:	None				,				
Signature format	Signature format Signatu			ature parameters Data						
Ing	out data (0)		Output data (0)			Status				

After clicking <u>"Add file</u>" button, the file explorer window will appear, from which user can indicate files for signing. Alternatively, files can be added to the list by drag&drop feature.

<u>"Add directory</u>" – with this button, from the selected folder we can add all files that meet the criteria in the signature settings, e.g. if we have chosen the PAdES signature format - all PDF files will be uploaded from the chosen catalog, and with the selected XAdES signature format all file formats will be uploaded.

We can also delete files that we have selected for signing using the "Delete file" button – for single file delete (the selected file (the highlighted one) will be deleted from the signing list), or "Clear list" – to delete all files from the list.

After clicking <u>"Show document</u>" button, file preview will be displayed in a new window.





"<u>Sign files</u>" – after pressing this button, all files from the list will be queued to the process of signing.

4.3 Signing process

To sign a file using a qualified signature, the device with a cryptographic card must be plugged into your PC. In case of using the ECSigner cloud signature, ECSigner application must be running in the background with your account logged in.

1. Specify the signature format with which the document should be signed (in the "Signature format" section).

• • •			Secu	reDoc						
SecureDoc Signi	ng Veryfing S	ettings	Certificate renewal	Help	About pr	ogram				
	Signature variant:	PAdES	PAdES-BES (without timestamp)							
PAdES (only PDF)	Signature type:	Envelop					C3	•		6
XAdES	Digest algorithm:	SHA-2	SHA-256 None			Delete	Add directory	Clear	Show document	Sign
	Commitment type:	None					urecusy	194	ocoment	
Signature format	Signature parameters							Data		
Inpu	t data (0)		Output data (0)			Status				

2. Select the required signature parameters in the "Signature parameters" section.

• • •			Secur	eDoc						
SecureDoc Signi	ng Veryfing	Settings	Certificate renewal	Help	About pr	ogram				
PAdES (only PDF)	Signature variant: Signature type: Digest algorithm:	Envelop SHA-25			Add file	Delete file	Add directory	Clear	Show document	Sign files
Signature format	Commitment type:	None	parameters					Data		
Inpu	ıt data (0)		Output	data (0)				5	Status	

- 3. Add files you would like to sign.
- 4. Click "Sign files". It is worth noting that all of the documents from the selected files list will be signed using the same signature parameters.
- 5. After clicking on "Sign files", the certificate selection window will appear. Select the "<u>Cryptographic device</u>" tab, and select a particular certificate from the list. Then click "OK". Certificates from the currently connected device and ECSigner cloud signature certificates are displayed in this tab.

In the <u>"Personal Certificates</u>" tab all of the registered in Windows certificates are displayed (including non-qualified certificates which are not placed on the cryptographic device).

It is recommended to use the <u>"Cryptographic device</u>" tab, as in such a case the application refers directly to the certificate from the connected cryptographic device.





PAdES (only PDF) XAdES	ng Veryfing Si Signature variant: Signature type: Digest algorithm: Commitment type:	nttings Certificate renewal Help PAdES-BES (without timestamp) Enveloped SHA-256 None	About program	Add Clear directory list	Dow Sign Sea
Signature format		Signature parameters		Data	
Inpu	it data (1)	Output data (1))	Stat	us
Cryptograph Issued for	ic device	issued by		Valid from	Valid to
Lukasz		Centrum Kwalifikowane Euro	Cert	02/10/2021 10:03:21	02/10/2024 10:03:2

6. After selecting the certificate and clicking "OK", a pop-up window with relevant information will appear. After reading the message click "OK".



7. In case of electronic signature on a USB device, PIN code has to be entered. If the PIN is correct, signature will be made.



EuroCert Sp. z o.o. ul. Puławska 474 02-884 Warszawa KRS: 0000408592 NIP: 9512352379

Dział handlowy: +48 22 490 36 45 handlowy@eurocert.pl •



• • •	SecureDoc
000	N code ter the PIN code
- The sele	OK Cancel
10 2	Issued for: Łukasz Issued by: Centrum Kwalifikowane EuroCert Valid from: 05/05/2021 11:02:31 Valid to: 05/05/2023 11:02:31
₽	Smart card reader: Gemalto USB Shell Token V2 Token: CardOS V5.3 EC0052355

In case of ECSigner cloud signature, user has to log in using his email address and password and then enter the authorization code (OTP code) from the mobile ECSigner application.

 The last step is to check the signature status. If the document has been successfully signed – the status in the window next to the signed file will be <u>"Signed</u>". If an error has occurred during the process – the status will be <u>"Unsigned</u>".

• • •		Secu	reDoc					
SecureDoc Signi	ng Veryfing Setti	ngs Certificate renewal	Help	About program	1			
	Signature variant:	PAdES-BES (without timestamp)						
PAdES (only PDF)	Signature type:	Enveloped			5 03			
XAdES	Digest algorithm:	SHA-256		Add Dele		Clear	Show document	Sign
	Commitment type:	None					0000011011	
Signature format	Si	nature parameters				Data		
Input data (2) Output data (2)					5	Status		
📃 /Users/reboot/Documents/demoi 📄 /Users/reboot/Documents/demoi 🔊 Signed								
/Applications	/Charismathics/CSSI	🛃 /Applications/C	harismat	thics/CSSI	💋 Unsig	ned		

4.4 Signing a PDF file with graphical representation

To sign PDF files with graphical representation, "Perform graphic signature when creating a signature in PAdES format" option must be enabled in "Settings" tab. Then the signature process will contain an additional step, in which the PDF file preview is displayed. After clicking the rubberstamp icon and clicking on a particular place in the file, the graphical representation will be placed.





• • •	/Users/eurocert/Desktop/example.pdf
205% ~ 🗇 🕂	 Apply to all files in the queue Sign
	≗
	OVIDER

After clicking <u>"Sign</u>" button, the signature will be created. If there are more files in the queue for signing, these steps must be repeated. During the signature process only one graphical representation can be added on a given file.



When signing a lot of PDF files, user can add a graphical representation on the first file, then enable the <u>"Apply to all files in the que</u>" option and then click "<u>Sign</u>" button. This way all files will be signed with the graphical representation in the same place.

4.5 Adding signatures to a previously signed file

To add a signature to a file that was previously signed – add the file and proceed in the same way as you would normally sign any file. When the <u>"Choose an action</u>" window will appear – click the <u>"Add signature</u>" button.





EuroCert Sp. z o.o. ul. Puławska 474 02-884 Warszawa KRS: 0000408592 NIP: 9512352379

Dział handlowy: +48 22 490 36 45 handlowy@eurocert.pl Dział techniczny: +48 22 490 49 86 wsparcie@eurocert.pl



5. Veryfing

In this tab user can verify already signed files and generate a verification report.

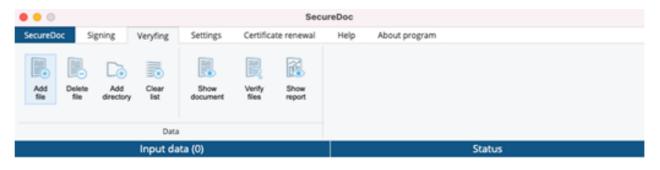
The functionality of the <u>"Add file</u>", <u>"Delete file</u>", <u>"Add directory</u>", <u>"Clear list</u>" and <u>"Show document</u>" is exactly the same as the functionality of the corresponding buttons in the <u>"Signing</u>" tab. Files signed using different signature configuration can be added to the list at the same time.

If file was signed using the "Detached" signature type – only the file containing the signature should be added to the list (without the original file). Remember that both the signature file and the signed file should be in the same folder. Otherwise, the application will not be able to refer to the source file (signed with detached signature type).

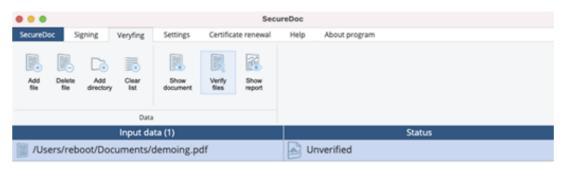
In the case of an internal signature (Enveloping / Enveloped), signed file has to be added to the list.

5.1 Signed file verification process

1. Add files that you want to verify by clicking <u>"Add file</u>" button or by using drag&drop.



2. Click "Verify files" (Internet connection is required).







3. Wait for the verification process to finish.

•••					reDoc				
SecureDoc	Signing	Veryfing	Settings	Certifica	ate renewal	Help	About program		
Add D	Relete Add	Clear	Show document	Verity files	Show report				
		Data	1						
	Input data (1)							Status	
/Users	/Users/reboot/Documents/demoing.pdf					💋 Co	rrectly verified		

Depending on the result of the verification "Correctly verified" or "Negatively verified" status will appear.

For more information about the verification result click "Show report".

There is also an option to open a verified document by clicking on <u>"Show document</u>".

6. Settings

6.1 Application settings

6.1.1 General settings

•	• •					Se	cureDoc	
5	iecureDoc	Signing	Veryfing	Settings	Certific	ate renewal	Help	About program
ſ	00	Ø	4	<u>5</u>)	0	(Ø)	1	
	General settings	Signing settings		stamp ings	Change token PIN	Unlock token PIN	Unlock token PIN	
		Application se	ettings		Sm	art card mana	gment	

6.1.1.1**Language**

In order to change the language in General settings, select one of the available languages from the drop-down list in the "Language" section.

6.1.1.2 **Updates**

During application startup, SecureDoc 2.0 will search for available updates and will display a notification upon finding a newer version. In order to install the newest update, accept the notification and proceed with the installation.

You may also find information about the installed and available versions of the application in this section.





6.1.1.3**Proxy**

In this section proxy server can be configured for SecureDoc. In order to configure a proxy, the "<u>Turn on proxy</u>" option has to be enabled. Fill in all the necessary information and click "<u>Save</u>".

Alternatively, system settings can be used for the proxy configuration. To do that, enable both options <u>"Turn on proxy</u>" and <u>"Use system credentials</u>".

Before signing files, it's advised to test the connection by clicking <u>"Check connection to proxy server</u>".

6.1.2 Signing settings

In the Signing settings tab, we can adjust the default settings at the application start-up. Newly set default settings of the signature parameters will be available after application restart.

The following default setting options are available in the application (Each of the available options is explained shortly within SecureDoc v2.0):

- Default signature format
- Default signature variant
- Default signature type
- Default digest algorithm
- Default type of commitment

6.1.2.1 Additional signing options

In this section, we can configure the following options:

"Overwrite a PDF document when a PAdES format signature is created" – Unchecking this option will result in the creation of a signed copy of the file with -sig suffix within the source directory.

With this option checked, the signature will be created within the source file and will overwrite the original document.

"Perform graphic signature when creating a signature in PAdES format" - Selecting this option will allow to add a graphic signature when signing with the PAdES signature format (on .pdf documents).

"Do not encode XML data to Base64 when using the Enveloping type in XAdES signature format" – Unchecking this option will allow us to sign the XML files encoded as Base64. Checking this option will allow us to sign XML files normally, using the standard UTF-8 encoding.





"Overwrite the XML document when using the Enveloping type in XAdES signature format"

- If the signed file is in XML format, and we need to sign it keeping the original file extension - **check** this option.

If we need to create the XAdES file out of XML file - **uncheck** this option.

"Create the Enveloped signature type in standard version" – A signature created with this option checked will disallow adding next signatures to the document.

6.1.3 Timestamp settings

To sign files using timestamps, the timestamp configuration has to be done beforehand. The client will obtain the required configuration data via email upon purchasing the optional Timestamp service product. This data has to be entered here and saved.

- Timestamp server address personalized access link to the timestamp server
- Username personalized login
- Password personalized password (cannot be changed)

After saving the data, it's advised to test the connection with the server by clicking "Check timestamp configuration" button.

6.2 Smart card management

Warning! If the PIN was entered incorrectly three times, it will get locked. In order to unlock the PIN code, follow the instructions in the "Unlock token PIN" section.

6.2.1 Change token PIN

To change your PIN code, click "Change token PIN" button. The following window will appear:

	SecureDoc	
Old PIN:	hange your card PIN here.	
New PIN:		
Confirm new PIN:		_
	Change PIN Cancel	
	d reader: Gemalto US8 Shell Token V2 rdOS V5.3 EC0052355	

First enter your current PIN code in the "Old PIN" field, then enter the new PIN code twice.





The minimal PIN length is 4 characters. The maximum PIN length is 8-10 characters. New PIN can contain any characters: numbers, letters (lowercase, uppercase), symbols, and other.

6.2.2 Unlock token PIN

Entering the incorrect PIN code three times will lock it. In order to unlock the PIN code, press "Unlock token PIN", then the following window will appear:

SO PIN	:	-		
New P	N:			
Confir	n new PIN:			
			Unlock PIN	Cancel
	Smart card reader Token: CardOS V5			

Enter your SO PIN code, then enter new PIN code twice.

WARNING! If incorrect SO PIN was entered three times, the cryptographic card will be irreversibly locked. In such a case, a new cryptographic card with a new certificate will have to be purchased.

6.2.3 Change token SO PIN

To change your SOPIN code, click "Change token SO PIN" button. The following window will appear:

	SecureDoc
****	Here you can change the SO PIN of your card.
SO PIN	2
New S	D PIN:
Confirm	m new SO PIN:
	Change SO Cancel
8	Smart card reader: Gemalto US8 Shell Token V2 Token: CardOS V5.3 EC0052355

Enter your current SO PIN, then enter new SO PIN twice.

New SO PIN can contain any characters: numbers, letters (lowercase, uppercase), symbols,





and other characters. Minimal SO PIN length is 4 characters, the maximum length depends on cryptographic card modes, and normally is 8-10 characters.

WARNING! If incorrect SO PIN was entered three times, the cryptographic card will be irreversibly locked. In such a case, a new cryptographic card with a new certificate will have to be purchased.

Additional information:

During the PIN / SO PIN code change procedure, only one cryptographic card can be connected. Connecting more devices can cause locking the card. EuroCert does not take responsibility for the causes of not following the aforementioned procedure.

7. Certificate renewal

Purchase renewal

To buy the certificate renewal, go to our website (<u>sklep.eurocert.pl</u>) or contact with our sales department (sales@eurocert.pl).

Certificate renewal

We suggest starting the renewal procedure at least 7 days before the expiration date of the current certificate. If the procedure had been started less than 72 hours prior to the expiration date, we do not guarantee a successful renewal.

After purchasing the renewal code, go to the "Certificate renewal" tab in SecureDoc and click the "<u>Certificate renewal</u>" button.

Enter your renewal code in the new window. Fill in the form and sign the newly generated agreement with your valid signature.

Please notice that <u>purchasing the renewal code does not result in renewing the certificate</u>. The Certificate will be renewed only after finishing the Certificate renewal procedure.

After the agreement had been accepted by EuroCert, enter the renewal code in SecureDoc application in the Certificate renewal tab again. Entering the renewal code after the agreement acceptation will result in activating the renewed certificate.

8. Help

This tab contains our Technical Department's contact details along with a download link leading to AnyDesk remote access application.

9. About program

This tab contains SecureDoc 2 licence terms.

