18, Suschevsky val, Moscow, Russia, 127018 tel. +7 (495) 995-48-20 http://www.cryptopro.ru E-mail: info@cryptopro.ru



 $\begin{array}{l} \mathbf{C} \mathbf{r} \mathbf{y} \mathbf{p} \mathbf{t} \mathbf{o} \mathbf{g} \mathbf{r} \mathbf{o} \mathbf{s} \mathbf{s} \mathbf{s} \mathbf{r} \mathbf{v} \mathbf{t} \mathbf{c} \mathbf{s} \\ \mathbf{P} \mathbf{r} \mathbf{o} \mathbf{v} \mathbf{i} \mathbf{d} \mathbf{r} \end{array}$

CryptoPro CSP version 4.0 1-Lic User guide for Microsoft Windows

Pages 109

Table of contents

1	Cry	ptoPro CSP installation	4				
2 CryptoPro CSP interface							
	2.1	CSP control panel	11				
	2.2	General settings	12				
	2.3	Entering the CSP license serial number	12				
	2.4	CSP Hardware configuration	14				
		2.4.1 Key readers configuration	14				
		2.4.2 Key carrier types configuration	19				
		2.4.3 Random number generators (RNG) configuration	$\overline{23}$				
	2.5	Certificates and containers	$\frac{-0}{27}$				
	2.0	2.5.1 Checking a private key container	$\frac{-1}{28}$				
		2.5.2 Copying a private key container	20 31				
		2.5.2 Copying a private key container	33				
		2.5.4 Viewing certificates in a private key container	$35 \\ 35$				
			$\frac{33}{38}$				
			$\frac{30}{39}$				
		2.5.7 Changing the password for a private key container	42				
	0.0	2.5.8 Deleting saved passwords	43				
	2.6	Security parameters	44				
	2.7	Advanced settings	45				
	2.8	Algorithms parameters	47				
	2.9	Winlogon settings	48				
	2.10	TLS settings	49				
3	Kor	y generation interface	51				
3							
	$3.1 \\ 3.2$	Crypto-Pro LLC Test Certificate Authority	51				
	3.2	Creating a key container	52				
			52				
		3.2.2 Generating RNG initial sequence	53				
		3.2.3 Setting the key container password	53				
		3.2.4 Selecting a way of private key access protection	54				
	3.3	Installing certificate in the store	56				
4	Cry	ptoPro TLS network authentication module	59				
	4.1	Enabling IIS on the server	59				
	4.2	Installing CryptoPro CSP	60				
	4.3	Installing root certificate in the computer store	61				
	4.4	Installing IIS certificate	65				
		4.4.1 Issuing IIS certificate	65				
		4.4.2 Configuring IIS	67				
		4.4.3 Testing HTTPS connection	69				
	4.5	Installing personal user certificate	09 73				
	4.5 4.6	Testing two-way client-server authentication	73				
	4.0	results two-way chemeser ver authentication	10				

5	Cry	ptoPro Winlogon	75
	5.1	Installing and configuring Active Directory CA	75
	5.2	Adding certificate templates on the server	80
		5.2.1 Configuring certificate templates	82
	5.3	Issuing a DC certificate	85
	5.4	Issuing an Enrollment Agent certificate	89
	5.5	Issuing a Smartcard User certificate	92
6	Usi	ng CryptoPro CSP with Microsoft Outlook 2016	96
6		ng CryptoPro CSP with Microsoft Outlook 2016 Configuring Microsoft Outlook 2016	00
6			96
6	6.1	Configuring Microsoft Outlook 2016	96 99
6	$\begin{array}{c} 6.1 \\ 6.2 \end{array}$	Configuring Microsoft Outlook 2016	96 99 100
6	$6.1 \\ 6.2 \\ 6.3 \\ 6.4$	Configuring Microsoft Outlook 2016	96 99 100 104

1 CryptoPro CSP installation

The CryptoPro CSP installation must be performed by a user with administrator privileges. To install the software insert the CD in the CD-ROM drive. If installation doesn't start automatically, browse the disc to find the program setup file called CSPSetup.exe. Run the file to start installation (Figure 1).

CryptoPro CSP 4.0 (Disk 1 of 1)	Start
	Language Switch to russian Install x86/x64-based operating systems Other Information Read the release notes Browse documentation Browse this CD Visit Crypto-Pro Corp. website
Crypto <mark>Pro</mark> CSP 4.0 R3	E <u>x</u> it

Figure 1. Installation CSP from CD

Note. Installation can also be made from the distribution obtained from the CRYPTO-PRO LLC site. Run the file CSPSetup.exe to start installation.

	confirmation» window op	on of CryptoPro CSP is already ins pens: ^{Update}	stalled on your comp	uter, the «CSP update
	Cŋ	yptoPro CSP 4.0.9842 will be updated to version 4.0.994	4. Continue?	
-		Install Root Certificates	Yes No	
	•	evel updating, the base program fer rity level you should previously rer		0

Before running the Setup Wizard you will see a welcome window (Figure 2). Select Install to start installation immediately with recommended options. Select Additional options to choose the security level (KC) and installation language.

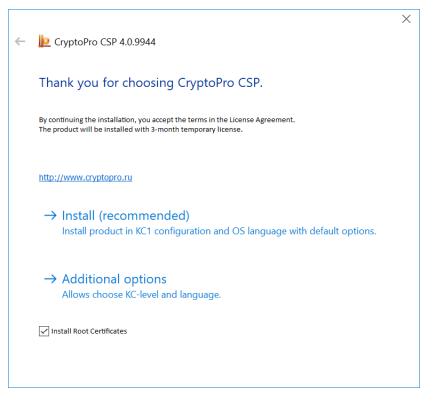


Figure 2. CSP welcome window

According to the Russian Federal Security Service requirements, CryptoPro CSP provides three types of security levels - KC1 and KC2. After choosing the required security level and installation language select **Install** to run the Setup Wizard (Figure 3).

		\times
←	CryptoPro CSP 4.0.9944	
	Thank you for choosing CryptoPro CSP.	
	Installation language:	
	◯ Russian	
	English	
	Security level:	
	● KC1	
	⊖ кс2	
	() КСЗ	
	\rightarrow Install	
	Install with chosen KC-level and language.	
	✓ Install Root Certificates	

Figure 3. Installation options

The Setup Wizard (Figure 4) will install CryptoPro CSP on your computer. To begin the installation click **Next**.



Figure 4. Setup Wizard welcome window

For the next steps of installation follow the messages in the «Setup Wizard» window. You should read and accept the license agreement and enter the serial number. If no serial number is entered, the 3 months

evaluation version of CryptoPro CSP will be installed.

Note. You can enter the product license number after installation using the CSP control panel. See Entering the CSP license serial number for details.

During the installation process the following settings can be configured:

- additional key readers
- use of the cryptographic key services

All these settings can be made during the installation process or at any time after installation using the CryptoPro CSP control panel.

At the next step choose the type of installation - typical or custom (Figure 5).

뤻 CryptoPro CSP	4.0.9944 Setup				\times			
Setup Type								
Choose the set	Choose the setup type that best suits your needs.							
Please select a	setup type.							
Typical Typical components will be installed.								
Custom Choose which program features you want to install and where they will be installed. Recommended for advanced users.								
		< Back	Next >	Cancel				

Figure 5. The installation type selection window

By default (type of installation «Typical»), only the base program features for CSP are installed (for Windows Server 2008 the «Driver Library CSP» is also installed by default). Using the «Custom» installation type you can install the following additional components (Figure 6):

• Advanced compatibility with Microsoft products option provides compatibility with applications such as Microsoft Office, Outlook Express. This option is required for smart card logon process.

• Key storage service provides storage, use and caching of keys in a separate OS service.

• **Revocation Provider** is a verification mechanism of a certificate status with the help of OCSP. It is complementary to the standard Windows mechanism of the certificate status verification based on Certificate Revocation List (CRL). In addition, there is an option to use CRL produced in accordance to RFC 3280.

• Kernel mode CSP is required for the TLS protocol support in Windows OS.

• CryptoPro CSP 3.0 (3.6) compatibility component registers the names of providers that are compatible with CryptoPro CSP 3.0 (3.6). It is necessary only if there are certificates installed by CryptoPro CSP 3.0 (3.6) in the certificate storage «Personal».

🕼 CryptoPro CSP 4.0.9944 Setup			×
Custom Setup			
Select the program features you want instal	ed.		
Click on an icon in the list below to change ho Base files Advanced compatibility with Micros		alled. Feature Descriptio Necessary files.	n
Kernel mode CSP CryptoPro CSP 3.0 compatibility	on produces		
Install to:			
C:\Program Files (x86)\Crypto Pro\CSP\			Change
Tips	< Back	Next >	Cancel

Figure 6. Custom Setup window

The last Setup wizard window contains the list of additional CSP libraries which should be configured and some security settings (Figure 7).

Before starting the installation, it is necessary to enable the **Strengthened key usage control** mode. This mode allows to monitor the validity period of long-term keys of electronic signature and key exchange, control the trust of the keys for checking the electronic signature and control the correct use of the software random number generator (RNG).

Note. CryptoPro CSP 4.0 without enabling the strengthened control of key usage can only be used for test purposes.

Choose the required options and select Install to start the installation process.

🕼 CryptoPro CSP 4.0.9944 Setup			×
The last step before install program			
The wizard is ready to begin installation.			
Choose needed support libraries (can be c	onfigured later):		
Register "Registry" reader			
Register smart card reader			
Register removable media reader			
Do not save removable media inforr Do not disable Microsoft Windows te Strengthened key usage control Click Install to begin the installation.			
If you want to review or change any of you the wizard.	ur installation setti	ngs, click Back. Click (Cancel to exit
	< Back	Install	Cancel

Figure 7. The supported libraries and security settings window

If the strengthened key usage control mode was enabled, data from the RNG will be requested during the CryptoPro CSP installation. In case of using a biological RNG a corresponding window opens (Figure 8). Press the keys on the keyboard or move the mouse pointer to generate the random sequence.

📆 Crypt	oPro CSP	Х
	Press keys or move mouse pointer to generate a random sequence	0:09:52 ce.
		ncel
	Car	ICEI

Figure 8. Biological RNG window

If an error occurs during the random data acquisition process, the Wizard displays a corresponding message (Figure 9).



Figure 9. Random data acquisition error message

In this case check that at least one physical RNG (for example, biological RNG, external gamma or hardware RNG) is registered and execute the command:

csptest.exe -keyset -verifycontext -hard_rng

After CryptoPro CSP installation with enabled strengthened key usage control mode you must install the trusted root certificates into the CryptoProTrustedStore certificate store of the Local Computer («CryptoPro CSP Trusted Roots») using the Certificates snap-in or the certmgr.exe utility:

certmgr.exe -inst -cert -silent -store mCryptoProTrustedStore -file ca.cer

Once installation is completed close the Setup Wizard and reboot your computer.



Figure 10. Final Wizard window

Now CryptoPro CSP 4.0 is ready for use.



Note. CryptoPro CSP SDK includes a description of the Windows Installer command line parameters (\CHM\msi-readme.txt) that can be useful during the installation.

2 CryptoPro CSP interface

The following section includes information on how to use the CryptoPro CSP control panel (Settings panel).

2.1 CSP control panel

The CryptoPro CSP Settings panel is available as a separate item in the program group «Crypto-Pro» (Start menu \Rightarrow All Programs \Rightarrow Crypto-Pro \Rightarrow CryptoPro CSP) (Figure 11).

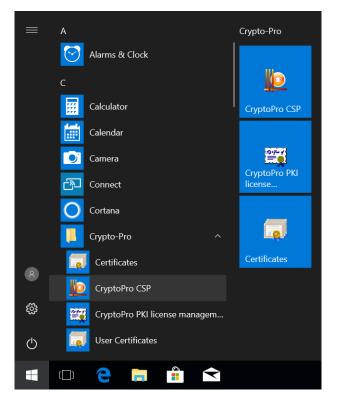


Figure 11. Access to the CSP control panel

The CryptoPro CSP control panel provides the ability to view and change CSP settings using the following 7 tabs:

- General
- Hardware
- Service
- Algorithms
- Security
- Winlogon
- TLS Settings
- Advanced

2.2 General settings

The General tab (Figure 12) of the CryptoPro CSP control panel is used to view information about the program version and license, to set the CSP license serial number (see Entering the CSP license serial number for details) and to select the CryptoPro CSP display language.

Securi	v		Winlogon		TL	S Settings
General	Hardv	vare	Service	A	dvanced	Algorithms
CryptoPro CSP Product version:4.0.9944 CSP core version:4.0.9017 KC1 © Crypto-Pro LLC. All rights reserved.						
	dministra	<u>tor</u>				
License Serial num Owner: Organizati License va License tyj First instal	on: lidity: pe:		/2018 rr	C6K4		ense
Language Select lanc	uage to g	lisplay	CSP windows		<system de<="" td=""><td>afaults v</td></system>	afaults v
for your u			co. mildons	l	< system De	adult?
Select language to display CSP windows for users who did not set language (system default):						
						_

Figure 12. General tab

2.3 Entering the CSP license serial number

During the CryptoPro CSP installation you will be asked to enter the CSP license serial number. If you do not do this, you will be provided with a trial license with a limited 3 month validity period. After the end of this period you must enter the serial number from the License form obtained from the CSP developer or distributor.

To enter the CSP license serial number open the CSP control panel General tab and click **Set license** button. The «Customer information» window opens (Figure 13). Input the 25-digit serial number from the License form into the corresponding field.

🕼 CryptoPro CSP 4.0.9944		×
Customer Information		
Please enter your personal information.		
User Name:		
Windows User		
Organization:		
Acme		
<u>S</u> erial Number:		
XXXXX-XXXXX-XXXXX-XXXXX		
Input serial number from the license agreement.		
	ОК	Cancel

Figure 13. Customer information window

You can also enter the license number using the CryptoPro PKI license management snap-in (Start menu \Rightarrow All Programs \Rightarrow Crypto-Pro \Rightarrow CryptoPro PKI license management). Open the snap-in and choose the CryptoPro product for which you want to enter a license. Select Action — All Tasks — Enter serial number in the context menu (Figure 14) or use the button on the toolbar.

🖼 CryptoPro PKI license	management		- 🗆 X
🖼 File Action View	Window Help		_ 8 ×
🗢 🔿 🙍 🖬 🛛	T 🖼 P		
License management			Actions
CryptoPro CSP	Crumto Dro CSE		CryptoPro CSP
🗞 CryptoPro Win	All Tasks	Enter serial number	More Actions
	View >	Buy product	
	New Window from Here	8	
	button on the toolbar o	n: KC2 4.0.9017 erial number by using corresponding r context menu of this item.) file use "License managment".	g
Enter a new license serial nu	umber		

Figure 14. «CryptoPro PKI license management» snap-in

2.4 CSP Hardware configuration

The Hardware tab (Figure 15) allows you to add or remove key carriers, key readers and random number generators (RNG). All smart card readers (and their corresponding media types) and all removable disk drives including flash-media are supported by default.

In case of KC1 security level, a biological RNG is preinstalled. During the CryptoPro CSP installation process you can also add a «Registry» reader (Figure 7)

Properto Pro	CSP			×	
Securi	ty	Winlogon	Т	LS Settings	
General	Hardware	Service	Advanced	Algorithms	
Private key readers Allows to add or remove private key readers.					
Random nu	100100 Allows to add or remove random number generators.				
Key carrier	Key carrier types Allows to add or remove key carrier types. Configure key carrier types				
		ОК	Cancel	Apply	

Figure 15. Hardware tab

2.4.1 Key readers configuration

2.4.1.1 Adding a reader

To add a new key reader the CSP control panel must be run with administrator privileges. To do this, open the CSP control panel General tab and click **Run as administrator**. Then open the Hardware tab and click **Configure readers** button. The «Readers' control» window opens (Figure 16).

녩 Readers' control		×
Readers		
The following readers are insta	lled:	
▲ All SmartCard readers All removable media 답 Registry		
Add	Remove	Properties
	ОК	Cancel

Figure 16. Readers' control window

To make a new reader available for CryptoPro CSP click **Add** button. The «Reader Installation Wizard» window opens (Figure 17). For further steps click **Next**.

Preader Installation wizard		×
	Reader Installation wizard.	
	This wizard will help you to install reader and support library.	
	To begin installation, click "Next".	
	To begin installation, cick next .	
	< Back Next > Cancel	

Figure 17. Reader Installation Wizard

In the next Wizard window choose the reader that you want to add and click Next (Figure 18).

Reader Installation wizard		×
Which reader do you want to	o instan <i>r</i>	
Select support libraries of you	ir reader and then click Next.	
Manufacturers:	Available readers	
(All manufacturers)	Accord	
Crypto-Pro LLC	Dallas (DS1410E)	
	🚺 Dallas (DS9097E)	
	🚺 Dallas (DS9097U)	
	Sable	
	< Back Next > Ca	ncel

Figure 18. Choosing a reader

Depending on the type of selected reader the choice of reader connection can be required. Select the connection for the reader and click **Next** (Figure 19).

Reader Installation wizar Select the connection. You must choose the conn	rd nection type for this device.	×
	the connection to use for this device. To continue on after it, click "Next".	
	Available connections: LPT1 LPT2	
	< Back Next > Cancel	

Figure 19. Choosing the reader connection

Assign a name for the installed reader and then click Next (Figure 20).

Peader Install Reader name You can assig	ation wizard	
	You can type a name for this reader, or you can use the name supplied below. When you finished, click Next.	
	Reader name	
	Dallas (DS1410E), LPT1	
	< Back Next > Cancel	

Figure 20. Setting the reader name

Read the text in the final wizard window and click Finish to complete the reader installation (Figure 21). After the reader installation is completed it is recommended to reboot your computer.

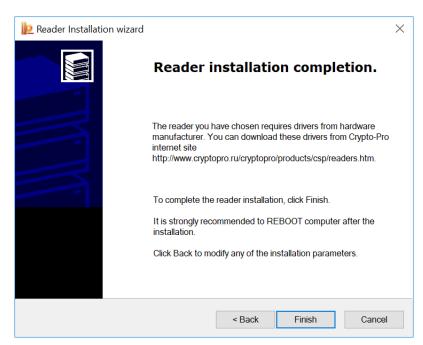


Figure 21. Reader installation completion



Note. Some drivers that enable the interaction of CryptoPro CSP with readers are not included in the setup package. In this case you should use the installation program supplied by the manufacturers of such devices. Also, if CryptoPro CSP is already installed and you need to use new devices, you should install support drivers and other modules from the manufacturers of these devices.

2.4.1.2 Removing a reader

To remove a key reader the CSP control panel must be run with administrator privileges. To do this, open the CSP control panel General tab and click **Run as administrator**. Then open the Hardware tab and click **Configure readers** button. The «Readers' control» window opens (Figure 16).

Select the reader you want to remove and click the **Remove** button. Confirm deletion of the reader (Figure 22).

Delete reader confirmation	×
Confirm the deletion of	the reader: Dallas (DS1410E), LPT1
	OK Cancel

Figure 22. The reader deletion confirmation window

2.4.1.3 Displaying reader properties

To view the reader properties open the Hardware tab and click **Configure readers** button. The «Readers' control» window opens (Figure 16).

Select the reader which properties you want to view and click the **Properties** button. The «Reader properties» window opens (Figure 23).

<u> D</u> allas (DS1	녣 Dallas (DS1410E), LPT1			
General				
1	Touch-mo LPT.	emory reader DS1410E, connected to		
Connect:		LPT1		
Reader:				
Status:		Failed		
Manufacture	er:	Dallas Semiconductor		
Version:		Unknown		
-Support Libr	ary:			
Status:		Installed		
Manufacture	er:	Crypto-Pro LLC		
Version:		4.0.4737.0		
		OK Cance	I	

Figure 23. The reader properties window

2.4.2 Key carrier types configuration

2.4.2.1 Adding a carrier type

To add a new key carrier type the CSP control panel must be run with administrator privileges. To do this, open the CSP control panel General tab and click **Run as administrator**. Then open the Hardware tab and click **Configure key carrier types** button. The «Key carriers' control» window opens (Figure 24).

腔 Key carriers' control	\times
Key Carriers	
3	
The following key carriers are installed:	
ALIOTH, SCOne J3H081	~
Reg ALIOTH, SCOne Series	
MIALIOTH, SCOne V3	
RUI ALIOTH, SCOne V4	
Athena IDProtect (F)	
ESMART Token 32K	
ESMART Token 64K	
ESMART Token GOST	~
ESMART Token GOST	•
Add Remove Pro	perties
Aud Relilove Flo	perties
ок	Cancel

Figure 24. Key carriers' control window

To make a new key carrier type available for CryptoPro CSP click Add button. The «Key carrier Installation Wizard» window opens (Figure 25). For further steps click Next.

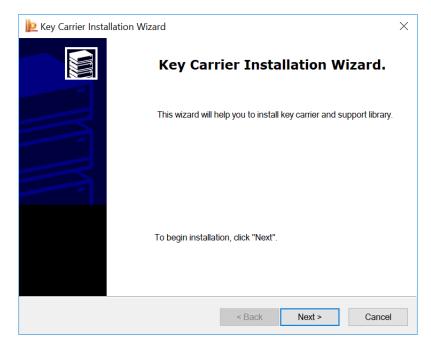


Figure 25. Key Carrier Installation Wizard

In the next Wizard window choose the key carrier type that you want to add and click Next (Figure 26).

De Key Carrier Installation Wiz Select key carrier Which key carrier do you war			×
Select support libraries of your	key carrier and then click Next.		
Manufacturers:	Available key carriers		
(All manufacturers)	① DS199x		~
(Unknown manufacturer)	ESMARTToken		
Crypto-Pro LLC	ESMARTTokenGOST		
ProgramPark Ltd.	ISBC_JavaCard		
SafeNet, Inc	Jcard		
	MPCOS-GEMALTO		
	MPCOSEMV		~
	< Back	Next >	Cancel

Figure 26. Choosing a carrier type

Assign a name for the installed key carrier type and then click Next (Figure 27).

Le Key Carrier Installation Wizard			×
Key carrier name You can assign a name for this key carrier			
You can type a name for this the name supplied below. Whe			
Key carrier name DS199x			
	< Back	Next >	Cancel

Figure 27. Setting the carrier name

Depending on the type of selected key carrier type some special key carrier settings can be required, for example, card format attributes (ATR, MASK), file system settings or the possibility of using a smart card to logon (Figure 28). After specifying key carrier settings click **Next** to continue.

Vey Carrier What file system Set file system			×
Туре	Start	Quantity	
DS1993	0	512	
DS1994	0	512	
DS1995	0	2048	
DS1996	0	8192	
		< Back	Next > Cancel

Figure 28. The carrier parameters setting

Click Finish to complete the key carrier installation (Figure 29). After the installation is completed it is recommended to reboot your computer.

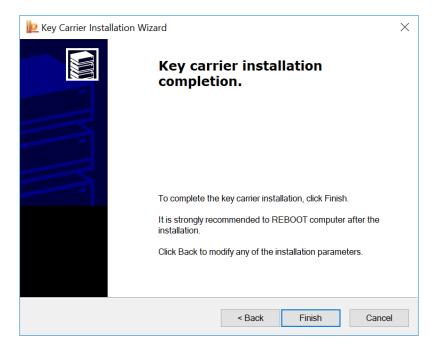


Figure 29. Key carrier installation completion

2.4.2.2 Removing a carrier type

To remove a key carrier type the CSP control panel must be run with administrator privileges. To do this, open the CSP control panel General tab and click **Run as administrator**. Then open the Hardware tab and click **Configure key carrier types** button. The «Key carriers' control» window opens (Figure 24).

Select the key carrier type you want to remove and click the **Remove** button. Confirm deletion of the carrier (Figure 30).

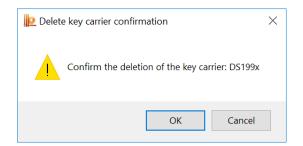


Figure 30. The carrier deletion confirmation window

2.4.2.3 Displaying carrier type properties

To view the key carrier properties open the Hardware tab and click **Configure key carrier types** button. The «Key carriers' control» window opens (Figure 24).

Select the key carrier which properties you want to view and click the **Properties** button. The «Key carrier properties» window opens (Figure 31). Depending on the selected key carrier type this window can contain more than one tab with carrier properties.

DS199x	×	DS199x		×
General File System		General File Syste	em	
DS199x		Type DS1993 DS1994 DS1995 DS1996	Start 0 0 0 0 0 0	Quantity 512 512 2048 8192
Support Library: Status: Active Manufacturer: Crypto-Pro LLC Version: 4.0.4733.0				
ОК	Cancel			OK Cancel

Figure 31. The carrier properties window

2.4.3 Random number generators (RNG) configuration

2.4.3.1 Adding a RNG

Note. Before configuring the RNG and loading the dynamic libraries, make sure the software of the selected generator is installed.

Note. If there are more than one RNG are configured, the initial key information will be generated by the RNG which is located at the top of the installed RNG list. If the first RNG is not available, the next one on the list will be used, and so on. For example, if Biological RNG and Accord are installed (see Figure 32) and both of them have «Connected» status, the first RNG on the list will be used, that is Accord. In order to use a Biological RNG to generate initial information, put the Biological RNG on top of the list using the buttons in the first RNG of the list using the buttons is and information.

To add a new RNG the CSP control panel must be run with administrator privileges. To do this, open the CSP control panel General tab and click **Run as administrator**. Then open the Hardware tab and click **Configure RNGs** button. The «Random number generator control» window opens (Figure 32).

Derived Random number generators control $ imes$
RNG
The following random number generators are installed:
Record Biological random number generator
4
Add Remove Properties
OK Cancel Apply

Figure 32. Random number generator control window

To make a new RNG available for CryptoPro CSP click Add button. The «RNG Installation Wizard» window opens (Figure 33). For further steps click Next.

PRNG Installation wizard		×
	RNG Installation wizard.	
	This wizard will help you to install random number generator (RNG) and support library.	
M.		
	To begin installation, click "Next".	
	< Back Next > Cancel	

Figure 33. RNG Installation Wizard

In the next Wizard window choose the RNG type that you want to add and click Next (Figure 34).

RNG Installation wizard Select RNG Which RNG do you want to ins	stall?
Select support libraries of your F	
Manufacturers: (All manufacturers) Ancud Ltd. Crypto-Pro LLC	Available RNGs APMDZ random-number generator CryptoPro Source Data Maxim RNG Sable
	< Back Next > Cancel

Figure 34. Choosing a RNG type

Assign a name for the installed RNG and then click Next (Figure 35).

RNG Installation wizard RNG name You can assign a name for this RNG	×
You can type a name for this RNG, or you can use the name supplied below. When you have finished, click Next.	
RNG name APMDZ random-number generator	
< Back Next >	Cancel

Figure 35. Setting the RNG name

Click Finish to complete the key carrier installation (Figure 29). After the installation is completed it is recommended to reboot your computer.

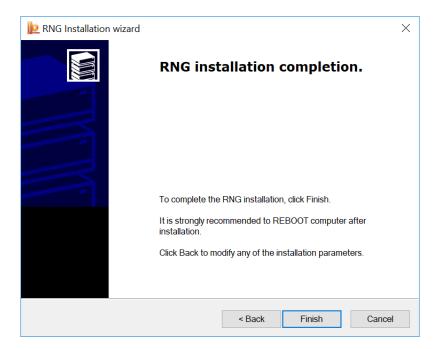


Figure 36. RNG installation completion

2.4.3.2 Removing a RNG

To remove a RNG the CSP control panel must be run with administrator privileges. To do this, open the CSP control panel General tab and click **Run as administrator**. Then open the Hardware tab and click **Configure RNGs** button. The «Random number generator control» window opens (Figure 32).

Select the RNG you want to remove and click the **Remove** button. Confirm deletion of the RNG (Figure 37).

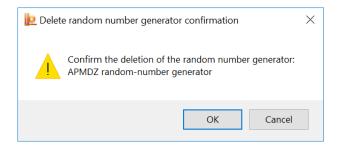


Figure 37. RNG deletion confirmation window

2.4.3.3 Displaying RNG properties

To view the RNG properties open the Hardware tab and click **Configure RNGs** button. The «Random number generator control» window opens (Figure 32).

Select the RNG which properties you want to view and click the **Properties** button. The «Random number generator properties» window opens (Figure 38).

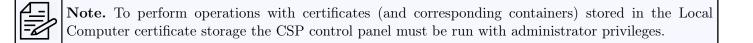
PMDZ random	-number generator	\times
General		
Certi	fied APMDZ random-number generator	
Random Number C		
Status:	Failed	
Manufacturer:	Ancud Ltd.	
Version:	1.0.0.19	
Support Library:		
Status:	Installed	
Manufacturer:	Ancud Ltd.	
Version:	1.0.0.19	
	OK Ca	ncel

Figure 38. RNG properties window

2.5 Certificates and containers

The Service tab of CryptoPro CSP control panel (Figure 39) is used to perform the following operations:

- copying and deleting a private key container;
- testing (functional check) and displaying the properties of the key(s) and certificate(s) in the container;
- viewing certificates in a private key container and installing them into the certificate store;
- linking certificate from a file with a private key container;
- changing and removing saved passwords (PIN-codes) for accessing private key container;
- removing information about previously used removable carriers.



Securi	ty	Winlog	jon		TL	S Settings
General	Hardware	Serv	ice	A	dvanced	Algorithms
a carrier.	ds allow to chee	k, copy or	delete	e a pri	ivate key co	ontainer from
Ch	eck	Co	ру		D	elete
Certificates	in private key o	ontainer				
	d allows to view them into a cer			ted in	a private k	ey container
		1/1				
		view	certific	ates i	n container	
Private cert	ificate	view	certific	ates i	n container	
This wizard	ificate d allows to link by installing it ir	certificate	from a	a file v		
This wizard	d allows to link	certificate nto a certif	from a icate s	a file v tore.		
This wizard container b	d allows to link by installing it ir	certificate nto a certif Ir	from a icate s	a file v tore.	with a priva	
This wizard container b Passwords This wizard	d allows to link	certificate nto a certif Ir nge passw	from a icate s istall n ords (F	a file v tore. ny cer	with a priva tificate	ite key

Figure 39. Service tab

2.5.1 Checking a private key container

To perform a functional container check, open the CSP control panel Service tab and click **Check** button. The «Check private key container» window opens (Figure 40).

P Check private key container			×
Private key container Type or choose private key container to check			
Key container name:			
			Browse
This name specifies key container for:			By certificate
User Computer			
Choose CSP for key containers search:			
Choose CSP for key containers search: Crypto-Pro GOST R 34.10-2001 Cryptographic Se	ervice Provider	~	
	ervice Provider	~	

Figure 40. Check private key container window

2.5.1.1 Choosing a key container

Choose the container you want to test by filling in the Key container name field. It can be entered using the keyboard or selected from the container list (Figure 41) by clicking the **Browse** button or from the certificate list (Figure 42) using the button **By Certificate**.

🖢 CryptoPro CSP	X
Select key container	0:09:34
View:	
Friendly names OUnique names	mes
User key container list:	
Reader Name	
Regis te-92ebe593-3e03-4ee5-98aa-a3f17780	f672
Regis te-8954b882-e540-4c92-b586-1b10fcb0	5896
ОК	Cancel

Figure 41. Selecting a key container

Windows	Security		×		
Select a Certificate					
Choose	a certificate from "Pers	onal" store of the current us	er.		
	usertest				
لس	Issuer: CRYPTO-PRO T	est Center 2			
	Valid From: 23/08/201	8 to 23/11/2018			
	Click here to view cert	tificate properties			
More ch	oices				
	usertest2 Issuer: CRYPTO-PRO Valid From: 23/08/20				
	usertest Issuer: CRYPTO-PRO Valid From: 23/08/20				
	OK	Cancel			

Figure 42. Selecting a certificate

There are two options for searching a key container:

• This name specifies key container for — option specifies in which type of certificate store (Current User or Local Computer) certificate is located.

• Choose CSP for key containers search – option specifies the CSP used in the key container.

After filling in the form (Figure 43) click Next.

녣 Check private key container	×
Private key container Type or choose private key container to check	
Key container name:	
te-92ebe593-3e03-4ee5-98aa-a3f17780f672	Browse
This name specifies key container for: • User Computer	By certificate
Choose CSP for key containers search: Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider	
,, <u>9</u> p	
< Back Next :	> Cancel

Figure 43. Filing in Check private key container form

If a password is set for the selected container, it will be requested in the password input window (Figure 44). Enter the password and click **OK** to continue.



Figure 44. Entering a container password

A window with the test result opens. It contains information on the results of the container functional check, the parameters of the container.

腔 Check private ke	ey container	2
	The private ke wizard comple	ey container check eted
	Check container succeed Private key container name unique name FQCN container integrity check Exchange key Public key length public key compute public key compute public key import signing verifying	no errors were detected user's te-92ebe593-3e03-4ee5-98aa-a: REGISTRY\\te-92ebe593-3e03-4 \\.\REGISTRY\te-92ebe593-3e03 c succeed available 512 bits succeed succeed succeed succeed succeed
	<	
		Copy to clipboard
	< Ba	ck Finish Cancel

Figure 45. Key container check results

2.5.2 Copying a private key container

To copy a key container, open the CSP control panel Service tab and click **Copy** button. The «Copy private key container» window opens (Figure 46).

Choose the key container you want to copy by filling in the **Key container name field** (see Choosing a key container for more information) and click **Next**.

腔 Copy private key container	×
Private key container Type or choose private key container to copy	
Key container name:	
te-4956da70-c243-488e-a164-bc89f6b2bddb	Browse
This name specifies key container for:	By certificate
User Computer	
Compater	
Choose CSP for key containers search:	
Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider $\qquad \qquad \qquad$	
< Back Next >	> Cancel

Figure 46. Copy private key container window

If a password is set for the selected container, it will be requested in the password input window. Enter the password and click \mathbf{OK} to continue.

In the next window enter a name for the new key container and check the box to to indicate which type of certificate store (Current User or Local Computer) key container is specified for (Figure 47). Click **Finish** to start the key container copying.

Dopy private key container	\times
Private key container Type private key container name to copy to	
New key container name:	
te-4956da70-c243-488e-a164-bc89f6b2bddb - Copy	
This name specifies key container for:	
● <u>U</u> ser	
<u>C</u> omputer	
Choose CSP for key containers search:	
Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider	
< <u>B</u> ack Finish Cancel	

Figure 47. Setting a name for the new key container

Choose the carrier for the copied key container and click OK (Figure 48).

EryptoPro CSP	<	
0:09:45 Insert and select carrier media for storing private key container "te- 4956da70-c243-488e-a164-bc89f6b2bddb - Copy".		
Details		
Readers: Carrier media inserted:		
Registry		
Aktiv Rutoken		
OK Cancel Details <<		

Figure 48. Choosing the carrier for the new key container

Set the password for the produced container (Figure 49) and click OK to finish the container copying. If successful, a window with an appropriate message opens (Figure 50).

🖢 CryptoPro CSP	×
Set password on produced container "te 488e-a164-bc89f6b2bddb - Copy".	0:09:52 a-4956da70-c243-
• Set new password	EN
New password:	
Confirmation:	
OK Cancel	Details >>

Figure 49. Setting a password for the produced container



Figure 50. Successful container copy completion

To be able to copy the private key container, the key must be mark as exportable during its creation. If not, an attempt to copy the container fail and a window with corresponding error message opens (Figure 51).

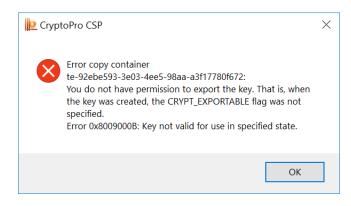


Figure 51. Container copy error message

2.5.3 Deleting a private key container

To delete a key container, open the CSP control panel Service tab and click **Delete** button. The «Delete private key container» window opens (Figure 52).

Choose the key container you want to delete by filling in the **Key container name field** (see Choosing a key container for more information) and click **Next**.

녣 Delete private key container		Х
Private key container Type or choose private key container to delete		
Key container name:		
te-4956da70-c243-488e-a164-bc89f6b2bddb - Copy		Browse
This name specifies key container for:		By certificate
● User		
O Computer		
Choose CSP for key containers search:		
Crypto-Pro GOST R 34.10-2012 Cryptographic Service Pro	ovider 🗸	
	Widel	
< E	Back Finis	h Cancel

Figure 52. Delete private key container window

Confirm deletion of the key container in the window (Figure 53). After a successful completion the following window opens (Figure 54).

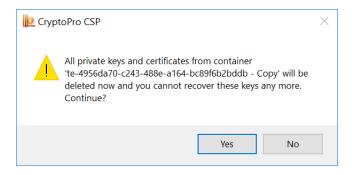


Figure 53. The key container deletion confirmation window

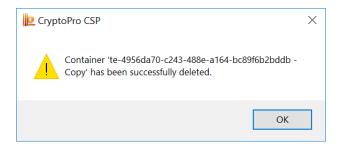


Figure 54. Successful container delete completion

If the selected container is stored on the removable media that is not currently connected to the computer, you will be asked to insert this carrier (Figure 55).

崖 CryptoPro CSP	×
Insert key carrier m "rutoken_ecp_346ft	
Details	
Readers: Aktiv Rutoken ECP 0	Carrier media inserted: Status: Another carrier media.
	Cancel Details <<

Figure 55. Key carrier media request

Once the carrier is connected the container will be deleted automatically. If successful, a window with an appropriate message opens (Figure 54). You can also choose whether to delete the corresponding certificates from system certificate stores or not.

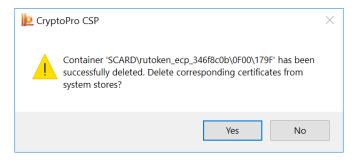


Figure 56. Successful container delete completion

2.5.4 Viewing certificates in a private key container

To view certificates in a key container and install them into the system certificate store, open the CSP control panel Service tab and click **View certificates in container** button. The «Certificates in private key container» window opens (Figure 57).

Choose the key container which contains the certificate you want to view by filling in the **Key container name field** (see Choosing a key container for more information) and click **Next**.

P Certificates in private key container	×
Private key container Type or choose private key container for view certificates in this container	
Key container name:	
te-4956da70-c243-488e-a164-bc89f6b2bddb	Browse
This name specifies key container for:	By certificate
User Computer	
Choose CSP for key containers search:	
Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider	

Figure 57. Certificates in private key container window

If there is no certificate in private key container, the corresponding message opens (Figure 58).

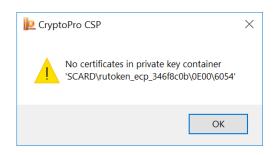


Figure 58. No certificates in private key container

If there are certificates in the selected container, the «Certificate to view» window opens (Figure 59).

Dertificates in priv	vate key container X
Certificate to view View and choose c	ertificate
Certificate:	usertest3
Subject:	CN=usertest3, C=RU
Issuer:	E=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN=C
Valid from:	Friday, August 24, 2018 2:17:30 PM
Valid to:	Saturday, November 24, 2018 2:27:30 PM
Serial number:	1200 2C4C 43DC 4A55 8CE5 B689 3900 0000 2C4C 43
	Install Properties
	Browse
	Donsen
	< Back Finish Cancel

Figure 59. Certificates in the private key container

To view the properties of the certificate in a key container, click **Properties** button. The «Certificate» window opens (Figure 60). Use **Install Certificate** button on the General tab to install the certificate into the store you selected. On the Certification Path tab you can view all certificates to the root CA if they are contained in the selected container.

Certificate	\times
General Details Certification Path	
Certificate Information This certificate is intended for the following purpose(s): • Proves your identity to a remote computer	-
Issued to: usertest3 Issued by: CRYPTO-PRO Test Center 2	-
Valid from 24/08/2018 to 24/11/2018 ⁹ You have a private key that corresponds to this certificate.	
Install Certificate Issuer Stateme	nt
O	K

Figure 60. Certificate properties

2.5.5 Installing a personal certificate stored in a private key container

Note. In this section, personal certificate installation is understood as an installation of the certificate into the Personal store with the corresponding private key linking.

CryptoPro CSP allows you to store personal user certificates both in the Local Computer certificate store and together with the user's personal keys on a key carrier. Keeping a certificate on a key carrier allows the user to transfer all the necessary key information from the computer where the user's key was generated to other workstations.

To install a personal certificate, open it for viewing by following the actions specified in Viewing certificates in a private key container section.

In the «Certificate to view» window click **Install**. The certificate will be installed into the **Personal** Current User or Local Computer certificate store depending on the option selected when searching for the container (Figure 61).

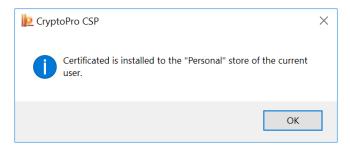


Figure 61. Successful certificate installation completion

If the selected certificate is already present in the store, you can replace the existing certificate with a new one and link it to a private key (Figure 62).

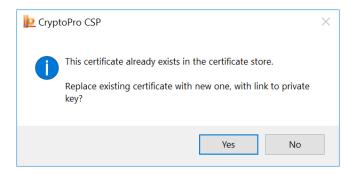


Figure 62. Replace the certificate in the store

Using this installation method root and intermediate CA certificates are also installed into the corresponding stores, if they are contained in the private key container.

2.5.6 Installing a certificate stored in a file

Note. In this section, personal certificate installation is understood as an installation of the certificate into the Personal store with the corresponding private key linking.

To install a personal certificate stored in a file, open the CSP control panel Service tab and click Install my certificate button. The Private certificate installation wizard opens (Figure 63).

Choose the certificate file you want to install by filling in the **Certificate file name** field. It can be entered using the keyboard or selected from the list by clicking the **Browse** button. Click **Next** to continue.

Private certificate installation wizard			×
Certificate file location Type or choose installing certificate file location	I		
Certificate file name:			
C:\cert_usertest.cer			Browse
Certificate file format can be one of the following: Certificate file - X.509 (.CER,.CRT) Message in PKCS #7 standard (.P7B,.P7M,.DEF Microsoft serialized certificate store (.SST) Note: More than one certificate can be stored in a single formats.			
	< Back	Next >	Cancel

Figure 63. Private certificate installation wizard

The window with the main certificate information opens (Figure 64). Use **Properties** button to see the selected certificate properties.

녩 Private certifica	te installation wizard $ imes$
Certificate to ins View and choos	tall e certificate to install
Certificate:	usertest
Subject:	CN=usertest, C=RU
Issuer:	E=support@cryptopro.ru, C=RU, L=Moscow, O=CRYPTO-PRO LLC, CN=CR
Valid from:	Thursday, August 30, 2018 2:37:26 PM
Valid to:	Friday, November 30, 2018 2:47:26 PM
Serial number:	1200 2C88 7AEF 7F4A 6CB1 CBE7 1B00 0000 2C88 7A
	Properties
	Browse
	< Back Next > Cancel

Figure 64. Choosing a certificate for installation

At the next step choose a private key container corresponded to the selected certificate by filling in the **Key container name field** (see Choosing a key container for more information) and click **Next** (Figure 65).

Private certificate installation wizard		Х
Private key container Type or choose private key container, correspo	nded to selected certificate	
Find container automatically		
Key container name:		
te-d2b7d376-c1d3-4f62-929a-a0ae58d2d7b7		Browse
This name specifies key container for:		
• User		
Computer		
Choose CSP for key containers search:		
Crypto-Pro GOST R 34.10-2012 Cryptographic Se	rvice Provider	
7 7 7 5 1		
	< Back Next	> Cancel

Figure 65. Choosing a private key container

Choose the certificate store to which you want to install the certificate (Figure 66). The certificate will be installed into the **Personal** Current User or Local Computer certificate store depending on the option selected when searching for the container. You cannot change the «Using certificate store» field value — it is determined by the private key container location.

You can also install the certificate into the key container for easy search for a certificate when you move the container to another computer. Mark the field «Install certificate (certificate chain) to container» with a square to install into the container only the certificate or set a check mark to install all the certificate chain.

腔 Private certificate installation wizard	×
Certificate store Choose certificate store to install certificate	
Selection of certificate store constraints flag value selected earlier (use use	er's or machine's key)
Personal	Browse
Using certificate store:	
User Computer	
Computer	
Install ceritificate (certificate chain) to container	
< Back Ne	ext > Cancel

Figure 66. Choosing a certificate store

In the last wizard window check the specified installation parameters and click Finish to perform the certificate installation (Figure 65).

Private certificate insta		g the private certificat n wizard	×
	You have specified t	the following settings:	
	Get certificate from file certificate name subject issuer valid from valid to serial number Make link <	C:\cert_usertest.cer CN=usertest, C=RU CN=usertest, C=RU E=support@cryptopro.ru, C=RU, L=Mos Thursday, August 30, 2018 2:37:26 PM Friday, November 30, 2018 2:47:26 PM 1200 2C88 7AEF 7F4A 6CB1 CBE7 1B	~
	Make sure you spec perform installation.	ify the correct parameters and click Finish	to
		< Back Finish Cance	el

Figure 67. Private certificate installation wizard completion

In case of installation the certificate into the key container if a password is set for the container, it will be

requested in the password input window.

2.5.7 Changing the password for a private key container

To change the private key container password, open the CSP control panel Service tab and click **Change password** button. The «Change password for private key container» window opens (Figure 68).

Choose the private key container for which you want to change password by filling in the **Key container name field** (see Choosing a key container for more information) and click **Next**.

녩 Change password for private key container	×
Private key container Type or choose private key container to change password on	
Key container name:	
te-4956da70-c243-488e-a164-bc89f6b2bddb	Browse
This name specifies key container for: • User Computer	By certificate
Choose CSP for key containers search: Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider	
< Back Finis	Cancel

Figure 68. Change password for private key container

If a password is set for the selected container, it will be requested in the password input window (Figure 69). Enter the password and click **OK** to continue.

🖢 Crypt	toPro CSP	×
ł	Type password for container "te-4956da70-c a164-bc89f6b2bddb"	0:09:48 243-488e-
		EN
	Password:	
Save	password	
	OK	

Figure 69. Entering the password

If the entered password is correct the new password setting window opens (Figure 70). Enter the new password twice and click **OK**. The new password will be installed on the container.

🖢 CryptoPro CSP		×
Type new pass a164-bc89f6b2	word for container "te-4956da70-c243 bddb" twice	0:09:45 8-488e-
Set new password		EN
New password:		
Confirmation:		
ОК	Cancel Deta	ils >>

Figure 70. Setting the new password

Note. Instead of using a private key container password, you can set a master key for access to the private key or split the key into several key carriers. See Selecting a way of private key access protection for details.

2.5.8 Deleting saved passwords

CryptoPro CSP allows you to save a key container password in a special Local Computer store. To do that, check the **Save password** box (Figure 69). If the password is saved, it is not requested when accessing the private key.

To delete saved passwords, open the CSP control panel Service tab and click **Delete saved passwords** button. The «Delete saved passwords» window opens (Figure 71).

P Delete saved passwords	×
Delete all saved passwords to private keys of: User Computer	
Delete removable media information: User Computer	
OK Cancel	

Figure 71. Delete saved passwords

Set the User / Computer flags to delete the passwords stored on the local computer and click OK. If there are no saved passwords, the corresponding fields will not be available.

Note. Saved passwords will be deleted only from the special Local Computer store. The password for accessing the private key container is not deleted.

You can also use this window to delete the removable media information. This is useful if the key container on the new media has the same name as one of the previously used on this computer containers.

2.6 Security parameters

The Security tab of the CryptoPro CSP control panel is used to select CryptoPro CSP security settings.

To set CryptoPro CSP security parameters the CSP control panel must be run with administrator privileges. To do this, open the CSP control panel General tab and click **Run as administrator**. Then open the **Security tab** (Figure 72).

CryptoPro CSP			×	
General Hardwa	re Service	Advanced	Algorithms	
Security	Winlogon	Т	LS Settings	
Default CSPs for specified types GOST R 34.10-2001 Signature with Diffie-Hellman Key Exchange: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider GOST R 34.10-2012 (256) Signature with Diffie-Hellman Key Exchange:				
Crypto-Pro GOST R		•		
GOST R 34.10-2012 Crypto-Pro GOST R 3	. , 5		, ,	
Save removable n Strengthened key Choose CSP to config	usage control			
All supported cryptop	roviders		\sim	
 Store keys in appl Use keys storage s Enable caching 		Cache size:	8	
	ОК	Cancel	Apply	

Figure 72. Security tab

The following options are available for setting using the **Security tab**:

- default CSPs for specified types;
- saving removable media information;
- strengthened key usage control;
- key storage location;
- caching key containers.

Using the **Security tab** you can enable the strengthened key usage control if it was not enabled when installing CSP. After enabling the strengthened key usage control using the control panel you must perform the following operations:

1) run the csptest.exe command: csptest.exe -keyset -verifycontext -hard_rng

2) install the trusted root certificates into the CryptoProTrustedStore certificate store of the Local Computer («CryptoPro CSP Trusted Roots») using the Certificates snap-in or the certmgr.exe utility:

certmgr.exe -inst -cert -silent -store mCryptoProTrustedStore -file ca.cer

3) reboot computer.

There are two key storage modes available in CryptoPro CSP — storing keys in applications' memory and using the keys storage service. In case of using the key storage service all operations with a private key are performed inside the service, the external application receives only the result of these operations, that is more secure than storing keys directly in application memory.

In case of KC1 security level the key storage service is not installed by default. If you want to use it, click **Install** button on the **Security tab**, wait until the installation is complete and select the corresponding field.

When storing keys in the key storage service, you can use the caching of the private key containers, which means that the keys obtained from key carriers are then temporarily stored in the service memory space.

The key from the cache is available even after the key carrier is removed from the reader, and after completion of the application that downloaded the key. Each key from the cache is available to any application that works under the same account as the application that placed this key in the cache. All keys from the cache are available before shutting down the key storage service. When the cache is overflow, the next key is written instead of the earliest key in the cache.

Key containers caching can increase application performance due to faster access to the private key, because the key is read only once.

To enable the key container caching mode, check the **Enable caching** box on the **Security tab** and set the cache size. The cache size specifies the number of keys that can simultaneously stored in memory.

Note. If the key container has a password, the password was not saved on the local computer and the private key stores in the cache, the access to this private key will perform without a password request and the key will automatically be read from the cache.

Note. CSP caches private keys associated with certificates, installed in the Local Machine certificate store (for example, Certification Authority or Web-server private keys), only for a specific user.

2.7 Advanced settings

The Advanced tab of the CryptoPro CSP control panel allows to:

- view versions and paths of the files that are used by CryptoPro CSP;
- set the time-out for entering information from the user.

To view versions and paths of the files that are used by CryptoPro CSP, open the CSP control panel Advanced tab (Figure 73).

Security		Winlogon			TLS Settings	
eneral Ha	rdware	Servic	e	٨d	/anced	Algorithn
e versions						
Name ^	Versio	n	т	S	Path	•
accord.dll	4.0.47			OK		ram Files\(
accord.dll	4.0.47					ram Files (
apmdz.dll	1.0.0.1					aram Files\(
apmdz.dll	1.0.0.1					ram Files (
bio.dll	4.0.48					ram Files\(
bio.dll	4.0.48	52.0				ram Files (
certenroll.dll	10.0.1	7134.1	x64	OK	C:\WIN	DOWS\syst ❤
<						>
				_		
Recalculate	hashes		(Copy	to clipbo	ard
ser input timeou	ł					
During use of CS	P IL Mdy Sh	ow ulaio	y wind	ows v	valung ic	or user input.
imeout can be s	et here that	allows to	o close	these	window	/s after a
pecified time per						
			Set	user	input tir	neout

Figure 73. Advanced tab

In the **File versions** section there is a table that contains information about versions and paths of the files used by CryptoPro CSP. If you want to copy this information, click **Copy to clipboard** button.

While the CSP is working, dialog boxes may appear on the screen, requiring the user to enter certain data (for example, a password for accessing the private key). To set the time interval after which these windows will be automatically closed (an action equivalent to clicking the **Cancel** button), open the CSP control panel **Advanced tab** (Figure 73) and click **Set user input** timeout button. The User input timeout window opens (Figure 74).

녣 User input timeout	\times
Choose timeout of user input for CryptoPro CSP dialo windows (in seconds):	og
User value:	
• Use system default value	
◯ Set infinite timeout	
◯ Set timeout: 600 💂 seconds	
System default value:	
◯ Set infinite timeout	
● Set timeout: 600 ← seconds	
OK Cancel	

Figure 74. User input timeout

Check the User value radio button to choose one of the following values:

- use system default value sets the default value defined by the field **System default value**;
- set infinite timeout sets infinite waiting for user input;
- set timeout specifies the time interval (in seconds) during which the user must enter data.

The **System default value** field can take the same values. Only the administrator of the local computer can change the **System default value** field value. To do this, run CSP control panel as administrator by clicking **Run as administrator button** on the General tab.

The default time-out value is 600 seconds.

Note. The User value field has a higher priority than the System default value field. For example, if the System default value field value is set to «Set timeout 600 seconds» and the User value field value is set to «Set infinite timeout», then the value «Set infinite timeout» will be valid.

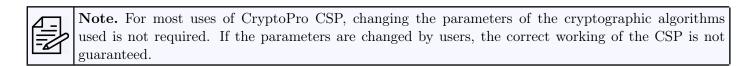
2.8 Algorithms parameters

The Algorithms tab of the CryptoPro CSP control panel is used to set various parameters of the cryptographic algorithms implemented in the CSP.

To set the parameters of cryptographic algorithms the CSP control panel must be run with administrator privileges. To do this, open the CSP control panel General tab and click **Run as administrator**. Then open the **Algorithms tab** (Figure 75).

Securit	/	Winlogon	TL	S Settings
General	Hardware	Service	Advanced	Algorithms
Algorithm p	arameters			
Choose CS	P type:			
		ature with Diffie	-Hellman Key Ex	change 🖂
Eng	ryption algorith	n parameters:		
		lefault paramete	rs	×~:
	ature algorithm			
-		1, default paran	neters	~
Diffi	ie-Hellman algo	rithm parameter	s:	
GO	ST R 34.10-200	1, default excha	inge parameters	2002

Figure 75. Algorithms tab



To set the parameters of cryptographic algorithms, you need to select the type of CSP which you want to configure. You can set the parameters for the following types of the cryptographic algorithms:

- encryption algorithm;
- signature algorithm;
- Diffie-Hellman algorithm.

2.9 Winlogon settings

The Winlogon tab of the CryptoPro CSP control panel allows to set up domain authentication using GOST algorithms.

To configure Winlogon authentication parameters, open the CSP control panel Winlogon tab (Figure 76).

	Hardware	Service	Advand	ced	Algorithms
Security	/	Winlogon		TLS	Settings
Default key i	reader				
Choose CS	P to configure:				
Crypto-Pro	GOST R 34.10)-2001 Cryptogr	aphic Serv	vice Pro	vider 🗸 🗸
Choose rea	der:				
Not set					\sim
Parameters -					
Disphie					
	CryptoPro Winl	ogon			
		l <mark>ogon</mark> orithms on KDC			
		-			
		-			
Use Cry	ptoPro CSP alg	orithms on KDC			
Use Cry	ptoPro CSP alg	orithms on KDC			
Use Cry	ptoPro CSP alg	orithms on KDC			
Use Cry	ptoPro CSP alg	orithms on KDC	~	E	Export
Identifiers of Domain cor	ptoPro CSP alg	orithms on KDC	~	E	xport
Identifiers of Domain cor	f domain contro	orithms on KDC	~		Export

Figure 76. Winlogon tab

When CSP is installed on the domain controller, the option Use CryptoPro CSP algorithms on KDC will be available and Domain controller and Identifier of the domain controller will be automatically filled. For more information about configuring Winlogon, see section 5.

You can disable the GOST algorithms in domain authentication by checking the **Disable CryptoPro Winlogon** box.

2.10 TLS settings

The TLS Settings tab of the CryptoPro CSP control panel is used to configure the TLS protocol, which provides authentication of the communicating parties, the confidentiality and integrity of the forwarded information.

To configure TLS protocol, open the CSP control panel TLS Settings tab (Figure 77).

🧕 CryptoPro	CSP					×
General	Hardware	Service	Advance	d	Algorithms	
Security	y	Winlogon		TLS S	Settings	
Client						
Use OC	SP protocol					
Disable	Disable server certificate revocation check					
Disable	self certificate E	KU check				
🗸 Do not	use legacy ciphe	er suites				
Server						
Use OC	SP protocol					
Disable	Disable client certificate revocation check					
Disable	self certificate E	KU check				
Do not use legacy cipher suites						
🗸 Enable	RFC 5746 suppo	ort (Renegotiati	on Indicatio	n)		
Require	e RFC 5746 supp	oort (Renegotiat	ion Indicati	on)		
Use def	fault machine cro	edential				
Session	is cache size:				64 👻	
Maximum certificate request CA count: 100						
		ОК	Cano	el	Apply	

Figure 77. TLS settings tab

The following options can be configured in the **Client** settings:

• Use OCSP protocol (if you have OCSP-client) — client performs certificate verification protocol on the OCSP Responder server database;

• Disable server certificate revocation check — client does not check whether the server certificate is in Certificate Revocation List;

- Disable self certificate EKU check client does not check the assignment of its certificate;
- Do not use legacy cipher suites client does not use cipher suites in which vulnerabilities were found.

The following options can be configured in the **Server** settings:

• Use OCSP protocol (if you have OCSP-client) — server performs certificate verification protocol on the OCSP Responder server database;

• Disable client certificate revocation check — server does not check whether the server certificate is in Certificate Revocation List;

• Disable self certificate EKU check — server does not check the assignment of its certificate;

• Do not use legacy cipher suites — server does not use cipher suites in which vulnerabilities were found;

 \bullet Enable RFC 5746 support (Renegotiation Indication) — server supports the TLS Renegotiation Indication Extension (see RFC 5746 for details);

• Require RFC 5746 support (Renegotiation Indication) — server requires the TLS Renegotiation Indication Extension support by client (see RFC 5746 for details);

- $\bullet\,$ Use default machine credential server uses the default computer certificate;
- Set a session cache size and maximum certificate request CA count.

3 Key generation interface

CryptoPro CSP can be used by various applications to create key containers on a Windows platform using the Windows Server Certificate Services.

3.1 Crypto-Pro LLC Test Certificate Authority

In order to test the key generation interface, you can use Crypto-Pro LLC Test Certificate Authority https://www.cryptopro.ru/certsrv/en/ to generate private keys and obtain public key certificates.

To generate a certificate request, open the Crypto-Pro LLC Test CA home page and click **Generate the** keys and send the certificate request button. The «Advanced Certificate Request» form opens (Figure 78).

dentifying Inform	nation:
Name:	
E-Mail:	
Company:	
Department:	
City:	
State:	
Country/Region:	
Type of Certifica	te Needed:
	Client Authentication Certificate V
Key Options:	
	Create new key set O Use existing key set
CSP:	Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
Key Usage:	◯ Exchange ◯ Signature
Key Size:	512 Min:512 (common key sizes: 512) Max:512 (common key sizes: 512)
	\textcircled{O} Automatic key container name \bigcirc User specified key container name
	☐ Mark keys as exportable
	Use Local Computer Store for certificate It saves certificate at Local Store except Current User Store. It does not install CA certificate. It needs to be Administrator to create Local Store.
Additional Optio	ns:
Request Format:	○CMC ●PKCS10
Hash Algorithm:	FOCT P 34.11-94 ∨ Only used to sign request.
	☐ Save request
Attributes:	
Friendly Name:	

Figure 78. Advanced Certificate Request form

To complete the certificate request, fill in the following fields:

- **Name** name of the certificate owner;
- E-mail email address may use the characters A-Z, a-z, 0-9 and some special characters;
- Company, Department, City, State optional fields;
- Country/Region two-letter country code according to ISO 3166 (for example, RU for Russia);

• Type of certificate — selected from the list. If the requested certificate is intended to be used in e-mail, choose E-Mail Protection Certificate. If the requested certificate is intended to be used in TLS protocol, choose Client Authentication Certificate.

• Key options:

- key container name - select **User specified key container name** to use a container name specified in the **Container Name** field.

- create exportable keys - check the \mathbf{Mark} keys as exportable box to be able to export keys in the future.

- use Local Computer certificate store - choose Use Local Computer Store for certificate to install the certificate in the Local Computer store instead of Current User. You need to have administrative rights to perform this operation.

Note. If the entered e-mail address does not match the address registered in Microsoft Outlook Express (Microsoft Outlook), the cryptographic functions in the e-mail will not be available.

If you do not need to install a certificate immediately, you can save the certificate request in a file for later installation. To do this, check the **Save request** box. In this case, the certificate will not be installed, and the request result will be saved as a PKCS#10 file.

Click the ${\bf Submit}$ button to start the certificate issuance procedure.

3.2 Creating a key container

3.2.1 Selecting a key carrier

During the creation of the key container, if there are several available key carriers, the key carrier selection window opens (Figure 79).

CryptoPro CSP	×
Insert and select carrier me "te-659dd422-7bd6-4674-	0:09:37 edia for storing private key container af2a-53827e99349e".
Details	
Readers: Carr	ier media inserted:
Registry Stat	us:
Aktiv Rutaken	
ОК	Cancel Details <<

Figure 79. Choosing a key carrier

If there is only one available key carrier, it is automatically selected for storing the private key container and this window is not displayed.

Click **OK** to confirm the key carrier selection.

3.2.2 Generating RNG initial sequence

After selecting a key carrier, if there are no installed hardware RNGs, the Biological RNG window opens (Figure 80).

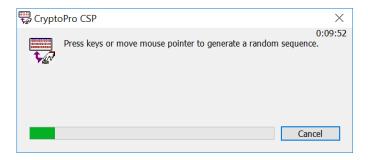


Figure 80. Biological RNG window

The Biological RNG is intended for initial sequence generation. Press the keys on the keyboard or move the mouse pointer to generate the random sequence.

3.2.3 Setting the key container password

After the Biological RNG finishes working, a window for entering the password for accessing the private key of the created container opens (Figure 81).

CryptoPro CSP	×
Set password 4674-af2a-538	0:09:54 on produced container "te-659dd422-7bd6- 827e99349e".
Set new password New password:	EN [
Confirmation:	
ОК	Cancel Details >>

Figure 81. Setting the key container password

Set the password for the produced container in the **New password** field and confirm it in the **Confirmation** field. Click OK to finish.

If the key is generated on a carrier that supports a hardware password or PIN, you should enter the password (PIN) that is set for this key carrier.

3.2.4 Selecting a way of private key access protection

In addition to key container password, there are other ways of private key access protection. To select the appropriate one, click the **Details** button in the password input window. The window for selecting the authentication method for the key container opens (Figure 82).

🔠 CryptoPro CSP	×
Set password on produced container 4674-af2a-53827e99349e*.	0:09:36 "te-659dd422-7bd6-
◯ Set new password	EN
New password:	
Confirmation:	
● Set master key	
Container name:	Browse
Create new container	
O Split key to a few carriers	
Number of carriers to restore key;	3
Total amount of carriers:	5
OK Cancel	Details <<

Figure 82. Selecting a key container authentication method

The following options are available:

- Set new password text password is used to access the private key;
- Set master key private key is encrypted using the other key (from the other container);
- Split key to a few carriers private key is split into a few carriers.

If the **Set master key** authentication method is selected, choose the container you want to use to access the generated key. It can be entered using the keyboard or selected from the container list using the **Browse** button (Figure 83). The generated private key will be encrypted with a private key from the selected container.

Select key container View:	×			CryptoPro CSP
View: Ounique names Iser key container list: Iser key container list: Reader Name Aktiv Rutoken ECP 0 te-0fe 134fa-0c4f-44cb-98bf-fa0d38 17dfa6 Aktiv Rutoken ECP 0 te-0fe 134fa-0c4f-44cb-98bf-fa0d38 17dfa6 Aktiv Rutoken ECP 0 te-1d5c71e6-05b7-4c1f-8fe4-6d058d00f9ee Registry te-4956da70-c243-488e-a164-bc89f6b2bddb Registry te-4956da70-c243-488e-a164-bc89f6b2bddb Registry te-8954b882-e540-4c92-b586-1b10fcb05896 Registry te-92ebe593-3e03-4ee5-98aa-a3f17780f672 Registry te-a068928e-908f-4347-ad3e-1e23615cd3fa	0:08:19			
Image: Ser Key container list: Image: Output of the series o				elect key container
Iser key container list: Reader Name Aktiv Rutoken ECP 0 te-0fe134fa-0c4f-44cb-98bf-fa0d3817dfa6 Aktiv Rutoken ECP 0 te-1d5c71e6-05b7-4c1f-8fe4-6d058d00f9ee Registry te-4956da70-c243-488e-a164-bc89f6b2bddb Registry te-4956da70-c243-488e-a164-bc89f6b2bddb Registry te-8954b882-e540-4c92-b586-1b10fcb05896 Registry te-92eb593-3e03-4ee5-98aa-a3f17780f672 Registry te-a068928e-908f-4347-ad3e-1e23615cd3fa				View:
Reader Name Aktiv Rutoken ECP 0 te-0fe134fa-0c4f-44cb-98bf-fa0d3817dfa6 Aktiv Rutoken ECP 0 te-1d5c71e6-05b7-4c1f-8fe4-6d058d00f9ee Registry te-4956da70-c243-488e-a164-bc89f6b2bddb Registry te-4956da70-c243-488e-a164-bc89f6b2bddb Registry te-8954b882-e540-4c92-b586-1b10fcb05896 Registry te-92eb593-3e03-4ee5-98aa-a3f17780f672 Registry te-a068928e-908f-4347-ad3e-1e23615cd3fa			O Unique names	Friendly names
Aktiv Rutoken ECP 0 te-0fe 134fa-0c4f-44cb-98bf-fa0d3817dfa6 Aktiv Rutoken ECP 0 te-1d5c71e6-05b7-4c1f-8fe4-6d058d00f9ee Registry te-4956da70-c243-488e-a164-bc89f6b2bddb Registry te-4956da70-c243-488e-a164-bc89f6b2bddb Registry te-8954b882-e540-4c92-b586-1b10fcb05896 Registry te-92eb593-3e03-4ee5-98aa-a3f17780f672 Registry te-a068928e-908f-4347-ad3e-1e23615cd3fa				ser key container list:
Aktiv Rutoken ECP 0 te-1d5c71e6-05b7-4c1f-8fe4-6d058d00f9ee Registry te-4956da70-c243-488e-a164-bc89f6b2bddb Registry te-4956da70-c243-488e-a164-bc89f6b2bddb - Copy1 Registry te-8954b882-e540-4c92-b586-1b10fcb05896 Registry te-92ebe593-3e03-4ee5-98aa-a3f17780f672 Registry te-a068928e-908f-4347-ad3e-1e23615cd3fa			Name	Reader
Registry te-4956da70-c243-488e-a164-bc89f6b2bddb Registry te-4956da70-c243-488e-a164-bc89f6b2bddb - Copy1 Registry te-8954b882-e540-4c92-b586-1b10fcb05896 Registry te-92ebe593-3e03-4ee5-98aa-a3f17780f672 Registry te-a068928e-908f-4347-ad3e-1e23615cd3fa			te-0fe134fa-0c4f-44cb-98bf-fa0d3817dfa6	Aktiv Rutoken ECP 0
Registry te-4956da70-c243-488e-a164-bc89f6b2bddb - Copy1 Registry te-8954b882-e540-4c92-b586-1b10fcb05896 Registry te-92ebe593-3e03-4ee5-98aa-a3f17780f672 Registry te-a068928e-908f-4347-ad3e-1e23615cd3fa			te-1d5c71e6-05b7-4c1f-8fe4-6d058d00f9ee	Aktiv Rutoken ECP 0
Registry te-8954b882-e540-4c92-b586-1b10fcb05896 Registry te-92ebe593-3e03-4ee5-98aa-a3f17780f672 Registry te-a068928e-908f-4347-ad3e-1e23615cd3fa			te-4956da70-c243-488e-a164-bc89f6b2bddb	Registry
Registry te-92ebe593-3e03-4ee5-98aa-a3f17780f672 Registry te-a068928e-908f-4347-ad3e-1e23615cd3fa		Copy1	te-4956da70-c243-488e-a164-bc89f6b2bddb ·	Registry
Registry te-a068928e-908f-4347-ad3e-1e23615cd3fa			te-8954b882-e540-4c92-b586-1b10fcb05896	Registry
			te-92ebe593-3e03-4ee5-98aa-a3f17780f672	Registry
Registry te-d2b7d376-c1d3-4f62-929a-a0ae58d2d7b7			te-a068928e-908f-4347-ad3e-1e23615cd3fa	Registry
			te-d2b7d376-c1d3-4f62-929a-a0ae58d2d7b7	Registry
OK Ca	ancel	OK Can		

Figure 83. Selecting a key container for the master key

CryptoPro CSP allows to encrypt a key not only with a private key from the existing container, but also from the new one. Check **Create a new container** box to create a new container with private key that is used to encrypt the generated key.

If the **Split key to a few carriers** authentication method is selected (Figure 84), the private key will be split into a few independent carriers each of which has its own password.

崖 CryptoPro CSP	×
Set password on produced container "te- 4674-af2a-53827e99349e".	0:09:18 -659dd422-7bd6-
◯ Set new password	EN
New password:	
Confirmation:	
○ Set master key	
Container name:	Browse
Create new container	
• Split key to a few carriers	
Number of carriers to restore key:	3
Total amount of carriers:	5
OK Cancel	Details <<

Figure 84. Splitting a key into a few carriers

Fill in the following fields in the window:

- Number of carriers to restore key the number of carriers required to access the private key;
- Total amount of carriers the total number of carriers between which the key will be split.

After filling these fields, the process of splitting the key starts:

• several key containers will be created, which number is equal to the **Total amount of carriers** field value;

• for each created container the key carrier selection window opens (Figure 79) - select the carrier you want to use to store the container;

• after selecting the carrier for each container the Biological RNG window opens (Figure 80);

• after generating the initial random sequence a password entry window opens for each created container (Figure 81) — set the password or choose the other authentication method for each container.

After all of the containers are created, the key split process is completed.

3.3 Installing certificate in the store

After creating the container, the page with a link to install the issued certificate opens in the Crypto-Pro LLC Test CA web interface (Figure 85). To install the certificate, click **Install this certificate** button.

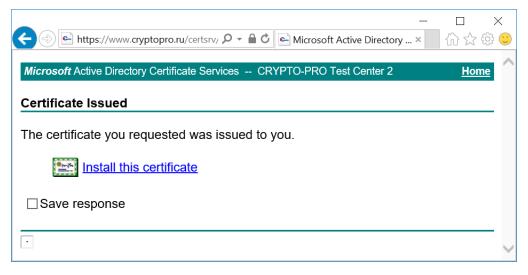


Figure 85. Installing a certificate

If a password is set for the corresponding container, it will be requested in the password input window during the certificate installation process. If the certificate is successfully installed, a corresponding message appears in CA web interface (Figure 86).

□ × ☆ ☆ ♡
Home
_
~

Figure 86. Successful certificate installation completion

To verify that the certificate is installed correctly, use the CryptoPro **Certificate** snap-in. Open **Start** menu \Rightarrow **All Programs** \Rightarrow **Crypto-Pro** \Rightarrow **Certificates** and find the certificate in the Current User or Local Computer Personal certificate store (Figure 87).

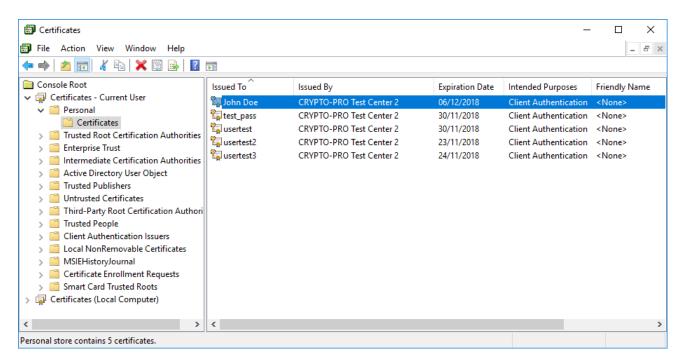


Figure 87. Certificates snap-in

4 CryptoPro TLS network authentication module

To configure a two-way connection (client-server) using TLS protocol, the user with administrator rights must perform the following actions:

- install IIS on Windows Server;
- install CryptoPro CSP;
- install a root CA certificate;
- install IIS certificate and configure a two-way authentication;
- install user certificate;
- test a two-way authentication.

In this section Crypto-Pro LLC Test Certificate Authority is used to demonstrate the CryptoPro CSP operation and issue test certificates.

4.1 Enabling IIS on the server

If Internet Information Services (IIS) is not installed on the server by default, you are need to enable it using Window Server Control Panel. To do this, open **Control Panel** \Rightarrow **Programs** \Rightarrow **Programs and Features** \Rightarrow **Turn Windows features on or off**. Add Roles and Features Wizard opens. Fill in the Installation type and Server Selection tabs following the instructions in the wizard. On the Server Roles tab (Figure 88) check **Web Server (IIS)** box and click **Next**.

📥 Add Roles and Features Wizard				-		\times
Select server roles Before You Begin	Select one or more roles to install on the selected server.				ATION SER\ -CAJVJECNJ	
Installation Type	Roles		Description			
Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	 Active Directory Federation Services Active Directory Lightweight Directory Services Device Health Attestation DHCP Server DNS Server Fax Server File and Storage Services (1 of 12 installed) Host Guardian Service Hyper-V MultiPoint Services Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Windows Deployment Services Windows Server Essentials Experience Windows Server Update Services 	~	Web Server (II manageable, a application inf	ind scalab	le Web	e,
	< Previous	Next	:> In	stall	Cance	ł

Figure 88. Selecting server roles

On the Select role services tab (Figure 89) select the required role services for IIS. For TLS protocol

📥 Add Roles and Features Wizard		- 🗆 X
Select role service	25	DESTINATION SERVER WIN-CAJVJECNJUA
Before You Begin	Select the role services to install for Web Server (IIS)	
Installation Type	Role services	Description
Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	 ✓ Web Server ▷ ✓ Common HTTP Features ▷ ✓ Health and Diagnostics ▷ ✓ Performance ▷ ✓ Security ▷ ✓ Application Development ▷ FTP Server ▷ ✓ Management Tools 	Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
	< Previous Next	> Install Cancel

functioning Web Server and Management Tools role services must be enabled.

Figure 89. Selecting the role services

Confirm the list of installed roles and role services in the next window and click **Install**. Wait until installation procedure is completed.

4.2 Installing CryptoPro CSP

To install CryptoPro CSP follow the instructions in CryptoPro CSP installation section. In the «Setup type» wizard window choose **Custom** setup type to be able to enable components that are not included in CSP by default.

In the «Custom setup» wizard window specify that the application will be used as a kernel mode CSP (Figure 90).

🕼 CryptoPro CSP 4.0.9950 Setup	×
Custom Setup	
Select program features you want to install.	
Click on an icon in the list below to change how a feature w	ill be installed.
Base files	Feature Description
Base files (x64)	Required for services and Windows
Advanced compatibility with Microsoft products	kernel (TLS server, IPsec, EFS).
Kernel mode CSP	
This feature will be installed on local hard dr	ive
☐ This feature, and all subfeatures, will be insta	
This feature will be installed to run from net	work.
Instal 🕮 This feature, and all subfeatures, will be insta	alled to run from the network.
× This feature will not be available.	
Tips < Back	Next > Cancel

Figure 90. Selecting server roles

The further installation is performed with the recommended default settings. When the installation is complete, restart the computer.

To enter a license for TLS or check its availability, use the CryptoPro PKI license management snap-in (Start menu \Rightarrow All Programs \Rightarrow Crypto-Pro \Rightarrow CryptoPro PKI license management).

4.3 Installing root certificate in the computer store

A root certificate authority certificate must be installed in the certificate store for the correct operation of the server. You can use the test CryptoPro CA to obtain certificates.

The browser through which you access the web interface of the CA must be opened by administrator. Add the CA web address to the trusted sites list in your browser settings to ensure its correct operation. To do this, select Security settings tab and add the https://www.cryptopro.ru/ to the trusted sites list.

Open the CA welcome page and click Obtain the Crypto-Pro LLC Test CA certificate or the certificate revocation list button (Figure 91).

КРИПТОПРО Crypto-Pro LLC Test Certificate Authority
Welcome to the website of the Crypto-Pro LLC Test Certificate Authority (CA).
 You can use the test CA to obtain a public key certificate for a digital signature verification. To obtain a certificate you should generate the private and public keys and input the data that is used to associate a public key and the certificate's owner.
Requirements
 For the test CA signature verification you need to have CSP that supports Russian cryptographic algorithms - CryptoPro CSP and others. You can download CSP <u>here</u>. The Crypto-Pro LLC Test CA is based on the certification service, which is a part of Microsoft Windows Server 2012 R2 operating system. If you use a web browser different from Microsoft Internet Explorer, you need to install <u>CryptoPro Digital Signature Browser Plug-in</u> to obtain the certificate.
The Crypto-Pro LLC Test CA is intended only for testing purposes and should not be used for other purposes. The Crypto-Pro LLC Test CA does not verify the certificate request information. Do not trust the certificates issued by the test CA . You can learn more about available services of the existing Crypto-Pro LLC Certificate Authority <u>here</u> .
Get certificate
Select the necessary action:
Generate the keys and send the certificate request
 Send the Base64 encoded PKCS#10 or PKCS#7 request Obtain the Crypto-Pro LLC Test CA certificate or the certificate revocation list
© "Crypto-Pro" LLC, 2000-2016
+7 (495) 995-48-20

Figure 91. Obtaining the CryptoPro LLC Test CA certificate

On the next page choose the certificate encoding method and click **Download CA certificate** button (Figure 92).

Microsoft Active Directory Certificate Services CRYPTO-PRO Test Center 2				
Download a CA Certificate, Certificate Chain, or CRL				
o trust certificates issued from this certification authority, install this CA certificate chain.				
o download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.				
CA certificate:				
Current [CRYPTO-PRO Test Center 2]				
Incoding method:				
● DER ○ Base 64				
Download CA certificate Download CA certificate chain Download latest base CRL				

Figure 92. Downloading the CryptoPro LLC Test CA certificate

Once the certificate is downloaded, choose **Open certificate**. Install this certificate to the Trusted Root Certification Authorities store of the Local Computer if it has not been installed before.

To install the CA certificate, click Install button in the «Certificate Information» window (Figure 93).

🖬 Certificate	×
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s): • All issuance policies • All application policies	
	_
Issued to: CRYPTO-PRO Test Center 2	
Issued by: CRYPTO-PRO Test Center 2	
Valid from 8/5/2014 to 8/5/2019	
Install Certificate Issuer Stateme	nt
0	<

Figure 93. Installing the CryptoPro LLC Test CA certificate

The Certificate Import Wizard opens (Figure 94). Choose Local Machine store location and click Next.



Figure 94. Certificate Import Wizard

In the next wizard window select Place all certificates in the following store and choose Trusted Root Certification Authorities store (Figure 95).

4	Sertificate Import Wizard	×	
	Certificate Store Certificate stores are system areas where certificates are kept.	_	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.		
	Place all certificates in the following store Certificate store: Browse		
	Select Certificate Store Select the certificate store you want to use		×
	Personal Trusted Root Certification Author Enterprise Trust Intermediate Certification Authori Trusted Publishers	ities	^
	Intrusted Certificates Show physical stores	>	~
		Cancel	I

Figure 95. Specifying the CA certificate location

For the next steps of installation, follow the messages in the «Certificate Import Wizard» window.

In order to verify the correct certificate installation open the Certificates snap-in (Start menu \Rightarrow All **Programs** \Rightarrow Crypto-Pro \Rightarrow Certificates). If the certificate is properly installed, you will find it in the Local Computer Trusted Root Certificate Authorities store (Figure 96).

 Console Root Certificates - Current User Certificates (Local Computer) Personal Trusted Root Certification Authorities Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Trusted Publishers Trusted Publishers Cient Authentication Issuers Trusted Pople Client Authentication Issuers Preview Build Roots Cient Authentication Authorities Client Authentication Authorities Client Authentication Authorities Client Authentication Authorities Microsoft CA X3 ST Root CA X3 ST Root CA X3 So Copyright Certificates MistEhistoryJournal Certificate Encollment Requests Microsoft Authenticode(tm) Requests Microsoft Authenticode(tm) Requests Microsoft Authenticode(tm) Requests Microsoft Authenticode(tm) Requests 	Certificates				- 🗆 ×
Console Root issued To issued To issued By Expiration Date Intended Purpo Console Root Certificates - Current User Certificates (Local Computer) AddTrust External CA Root 30/05/2020 Server Authenti Console Root Personal Certificates (Local Computer) Baltimore CyberTrust Root Baltimore CyberTrust Root 30/05/2020 Server Authenti Certificates Certificates Certificates 11/06/2027 Server Authenti Certificates Certificates Certum Trusted Network CA 11/106/2027 Server Authenti Certum Trusted Network CA Certum Trusted Network CA 11/106/2027 Server Authenti Copyright (c) 1997 Microsoft C Copyright (c) 1997 Microsoft Corp. 11/12/1999 Time Stamping Copyright (c) 1997 Microsoft C Copyright (c) 1997 Microsoft Corp. 11/12/1999 Time Stamping Copyright (c) 1997 Microsoft C. DigiCert High Assurance EV Root 10/11/2031 Server Authenti DigiCert High Assurance EV Root DigiCert High Assurance EV Root 10/11/2031 Server Authenti DST Root CA X3 DST Root CA X3 30/09/2021 Secure Email, Se Cipyto Pro CSP Trusted Root	File Action View Window Help				- 8
Intervention Intervention <tdinterventin< td=""> Interventin In</tdinterventin<>	Þ 🔿 🚈 💼 🔏 🖹 🗎 🗩 🗐				
> 📋 Trusted Devices	 Gertificates - Current User Certificates (Local Computer) Personal Trusted Root Certification Authorities Certificates Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Third-Party Root Certification Authorities Trusted People Client Authentication Issuers CryptoPro CSP Trusted Roots Sim CryptoPro CSP Trusted Roots Monegroup Machine Certificates Local NonRemovable Certificates Sim StEHistoryJournal Smart Card Trusted Roots 	AddTrust External CA Root Baltimore CyberTrust Root Certum CA Certum Trusted Network CA Class 3 Public Primary Certificat Copyright (c) 1997 Microsoft C Copyright (c) 1997 Microsoft Authenticode(tm) Ro Copyright (c) 1997 Microsoft Root Authority	AddTrust External CA Root Baltimore CyberTrust Root Certum CA Certum Trusted Network CA Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. CRYPTO-PRO Test Center 2 DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Root DST Root CA X3 GeoTrust Global CA GlobalSign GlobalSign Root CA Go Daddy Class 2 Certification Au Go Daddy Root Certificate Author Hotspot 2.0 Trust Root CA - 03 Microsoft Authenticode(tm) Root	30/05/2020 13/05/2025 11/06/2027 31/12/2029 02/08/2028 31/12/1999 05/08/2019 10/11/2031 10/11/2031 10/11/2031 10/11/2031 30/09/2021 21/05/2022 15/12/2021 28/01/2028 29/06/2034 01/01/2038 08/12/2043 01/01/2000 31/12/2020	Server Authentica Server Authentica Secure Email, Ser Server Authentica Server Authentica Server Authentica Server Authentica Server Authentica Server Authentica Secure Email, Coi <all></all>

Figure 96. Certificates snap-in

4.4 Installing IIS certificate

The following steps are required to configure TLS connection with server:

- issue an IIS certificate (if it was not issued earlier) and install it in the appropriate store;
- configure IIS with the indication of the certificate;
- test HTTPS connection.

4.4.1 Issuing IIS certificate

The test CryptoPro CA is used to obtain IIS certificate. The browser through which you access the web interface of the CA must be opened by administrator.

To issue the IIS certificate follow the steps in Key generation interface section in accordance with the recommendations below:

1) In the **Name** field specify the name of the certificate. It must match the name of the domain served by the IIS server for which the certificate is issued.

2) In the **Type of Certificate Needed** select «Server Authentication Certificate».

3) In Key Options section select «Create new key set» and choose the CSP below.

4) If you plan to use the key in future, check the «Mark keys as exportable» box and specify the friendly name in additional parameters.

5) Check the Use Local Computer Store for certificate box to install the obtained certificate in the certificate store of the local computer.

6) Leave the rest of the request parameters as default.

7) Do not the password for the created container. To do this, leave fields in the password input window empty and click **OK**.

Microsoft Active	Directory Certificate Services CRYPTO-PRO Test Center 2
Advanced Ce	rtificate Request
Identifying Inforr	nation:
Name:	test-srv.local
E-Mail:	
Company:	
Department:	
City:	
State:	
Country/Region:	
Type of Certifica	te Needed:
	Server Authentication Certificate 🗸
Key Options:	
	Create new key set O Use existing key set
CSP:	Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider
Key Usage:	○ Exchange ○ Signature
Key Size:	512 Min:512 (common key sizes: <u>512</u>)
	\bigcirc Automatic key container name $\qquad \textcircled{\sc 0}$ User specified key container name
Container Name:	test-srv.local
	✓ Mark keys as exportable
	✓ Use Local Computer Store for certificate It saves certificate at Local Store except Current User Store. It does not install CA certificate. It needs to be Administrator to create Local Store.
Additional Option	ns:
Request Format:	CMC
Hash Algorithm:	GOST R 34.11-2012 256 bit 🗸
	Only used to sign request.
	Save request
Attributes:	
Friendly Name:	
	Submit >

Figure 97. IIS certificate request

In order to verify the correct certificate installation open the Certificates snap-in (Start menu \Rightarrow All **Programs** \Rightarrow Crypto-Pro \Rightarrow Certificates). If the certificate is properly installed, you will find it in the Local Computer Personal store (Figure 98).

🗐 Certificates				-	- 🗆 X
छ File Action View Window Help)				_ & ×
🗢 🔿 🞽 📅 🖌 🖬 🔀 📾	?				
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
> 🔂 Certificates - Current User	test-srv.local	CRYPTO-PRO Test Center 2	07/12/2018	Server Authenticati	<none></none>
✓ ☐ Certificates (Local Computer)					
V Personal					
Certificates					
> Trusted Root Certification Au					
> 🦰 Enterprise Trust					
> 🧮 Intermediate Certification Au					
> Trusted Publishers					
> Untrusted Certificates					
> Third-Party Root Certification					
> Trusted People					
> Client Authentication Issuers					
> Preview Build Roots					
> CryptoPro CSP Trusted Roots					
> 📔 eSIM Certification Authorities					
> 📔 Homegroup Machine Certific					
> 📔 Local NonRemovable Certific					
> MSIEHistoryJournal					
> 📔 Certificate Enrollment Reque:					
Smart Card Trusted Roots					
> Trusted Devices					
Vindows Live ID Token Issuer					
< >	<				>
Personal store contains 1 certificate.					

Figure 98. Certificates snap-in

If the certificate does not appear in the Personal Local Computer store, find it in the Personal Current User store through the Certificates snap-in and transfer it to the specified repository.

4.4.2 Configuring IIS

To configure IIS, open IIS Manager using one of the following ways:

- open Server Manager \Rightarrow Tools \Rightarrow Internet Information Services (IIS) Manager;
- open the Run window using Win+R keyboard shortcut and execute the **inetmgr** command.

In IIS Manager right-click **Default Web Site**, and then in the context menu click **Edit Bindings...** (Figure 99).

🕞 Internet Information Services (IIS) Manager		– 🗆 X
← → WIN-CAJVJECNJUA → Sites → Default Web	Site >	🔤 🖂 👔 😨 🗝
File View Help		
Connections Start Page WIN-CAJVJECNJUA (WIN-CAJVJECNJUA\Administrator) Application Pools Sites Connections Sites Connections Connections Connections Connection Con	Fitter: Image: Configurate content view Is Image: Configurate content view Authentic Compression Default Directory Error Pages Handler Handler HTTP Mappings Respon Image: Configurate configurate content view Output Configurate configurate content view From View	Actions
Ready		4 .:

Figure 99. IIS Manager

The «Site Bindings» window opens. Click Add button to add site binding. In the opened window (Figure 100) select https in the Type field and choose the IIS certificate in the SSL certificate field. Click OK to save the settings.

Internet Information Services (IIS) Manager		- 🗆 X
← →	fault Web Site 🔸	🔯 🖂 🔞 🕡 🗸
File View Help		
v - i Sites >	Default Web Site Home Filter: Bindings ? Yope Host Name Port IP address: Port: Add Site Binding ? Yope: IP address: Port: https:// All Unassigned View Beloction Stl certificate: test-srv.local Select View OK Cancel Image: OK Cancel	Actions Explore Edit Permissions Edit Site Bindings Basic Settings View Applications View Virtual Directories Manage Website © Restart > Stop Browse Website © Browse *:80 (http) Advanced Settings Configure Limits Add FTP Publishing @ Help
Ready		• <u>1</u> .:

Figure 100. Adding a site binding

Close the «Site Bindings» window and restart IIS by clicking the ${\bf Restart}$ button in the Manage Website section.

4.4.3 Testing HTTPS connection

For a local connection check, use the **Browse *: 443 (https)** link on the right panel of the IIS Manager window (Figure 101) or use the browser to open https://<domainname>/, where <domainname> is the site domain name (DNS must be previously configured).

💐 Internet Information Services (IIS) Manager		– 🗆 X
← → 😔 ► WIN-CAJVJECNJUA ► Sites ► Default W	′eb Site →	📴 🖂 🔐 😨 🗸
File View Help		
Connections Image: Start Page Image: Start Page	Operative Default Web Site Home Fitter • • •	Actions Explore Edit Permissions Edit Site Bindings Basic Settings View Applications View Virtual Directories Manage Website © Restart Start Start Start Browse ":80 (http) Ø Browse ":80 (http) Ø Browse ":433 (https) Advanced Settings Configure Limits Add FTP Publishing @ Help

Figure 101. Testing HTTPS connection

Note. CryptoPro CSP, which runs on Windows 10, also supports HTTP/2 work with Internet Explorer/Edge and Internet Information Services (IIS). To maintain backward compatibility with the HTTP protocol in case of problems related to the lack of support for HTTP/2 on the client/server, disable HTTP/2 support in Internet Explorer/Edge/IIS settings (on the server it is disabled by the registry parameter HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters\EnableHttp2Tls)

If IIS is configured correctly, the browser displays the appropriate page (Figure 102).

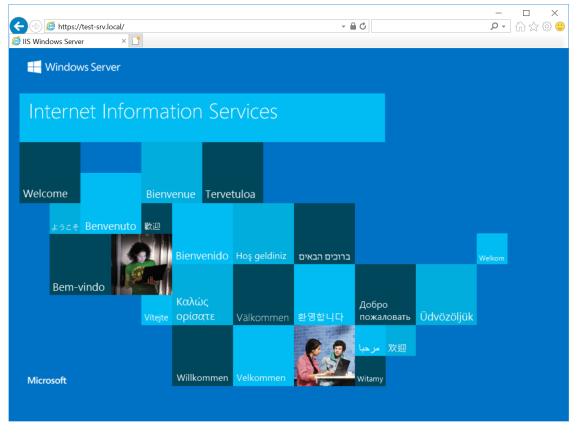


Figure 102. IIS welcome page

To provide two-way authentication between user browser and IIS server, set the appropriate requirements in the IIS settings. To do this, select **Default Web Site** in the left panel and choose **SSL settings** in the panel Features View (Figure 103).

📲 Internet Information Services (IIS) Manager — 🗆 🔿	×
🤆 -> 🚱 > WIN-CAJV/ECNUUA > Sites > Default Web Site >	• 0
File View Help	
Logging MIME Types Modules Output Request Caching Filtering SSL Settings Management Editor Configurat Editor Configurat Editor Editor Editor Configurat Editor Ed	

Figure 103. IIS manager Features view

In the «SSL settings» window (Figure 104) check the **Require SSL** box and select **Require** in the Client certificates field. Click **Apply** button to save the changes and restart IIS.

💐 Internet Information Services (IIS) Manager -				×		
← → ④ → WIN-CAJVJECNJUA → Sites → Default Web Site →			🕶 🖂 🟠	• 🕥		
File View Help						
Confections	This page lets you modify the SSL settings for the content of a website or application.	Actions		63		
Configuration: 'localhost' applicationHost.config, <location path="Default Web Site"></location>				•		

Figure 104. SSL settings

4.5 Installing personal user certificate

The user should do the following steps to support correct TLS connection with server:

• install CryptoPro CSP on the user machine (use default parameters);

• issue user certificate and install it in the Personal Current User store or other carrier type, which is available on the computer;

• test the connection with server.

To issue the IIS certificate follow the steps in Key generation interface section in accordance with the recommendations below:

1) In the **Name** field specify the name of the certificate user.

2) In the **Type of Certificate Needed** select «Client Authentication Certificate».

3) In Key Options section select «Create new key set» and choose the CSP below.

4) If you plan to use the key in future, check the «Mark keys as exportable» box and specify the friendly name in additional parameters.

5) Leave the rest of the request parameters as default.

A user certificate as a part of a private key container can also be stored on different types of key carriers.

In order to verify the correct certificate installation open the Certificates snap-in (Start menu \Rightarrow All **Programs** \Rightarrow Crypto-Pro \Rightarrow Certificates). If the certificate is properly installed, you will find it in the Current User Personal store.

4.6 Testing two-way client-server authentication

To verify TLS connection with server, browse https:/<domainname>//, where <domainname> is a server domain name.

If the connection is configured correctly, the certificate selection window opens when you open the page (Figure 105).



Figure 105. Selecting a user certificate

After selecting the certificate, the password to the user certificate container will be requested. If the user

enter the correct password, he will be granted access to the site.

Note. Make sure that the following fields on the Details tab of the user certificate have the specified values:
Enhanced Key Usage - «Client Authentication (1.3.6.1.5.5.7.3.2)»;

• **Key Usage** – «Digital Signature, Non-Repudiation, Key Enchipherment, Data Enchipherment (f0)». If one of these values is absent, two-way client-server authentication may not be possible.

5 CryptoPro Winlogon

To implement the initial authentication of the Kerberos V5 protocol user using the certificate and key carrier (issued in accordance with GOST R 34.10-2001 or GOST R 34.10-2012 algorithms using the certified CryptoPro CSP), perform the following actions:

1) Install and configure the domain controller (DC) on the server (Active Directory Domain Services is configured according to the standard Windows documentation).

2) Install CryptoPro CSP on the DC server, CA server (in case the CA service is located on a separate server) and on the domain users computers.

3) Install and configure the Active Directory CA.

- 4) Issue a DC certificate.
- 5) Issue a Registration Agent certificate.
- 6) Issue a smart card for the domain user.

For CryptoPro Winlogon operation, a special license is required (for the server and the client PC). This license may be included in the CryptoPro CSP license, or be issued separately. You can enter the license serial number using the **CryptoPro PKI License Management** snap-in (see subsection 2.3 for details).

5.1 Installing and configuring Active Directory CA

Domain and domain user certificates are requested through the Certificates snap-in on the server with configured Enterprise CA or via the Certification Authority web interface by a person authorized to issue certificates.

Before installing and configuring the Enterprise CA, install CryptoPro CSP on the server. You also should have the Enterprise Administrators rights.

To install the Enterprise CA, you need to add the Certification Authority role on the server. To do this, open **Server Manager** \Rightarrow **Add roles and features**. The Add Roles and Features Wizard opens. On the Server Roles tab (Figure 106) check **Active Directory Certificate Services** box and click **Next**.

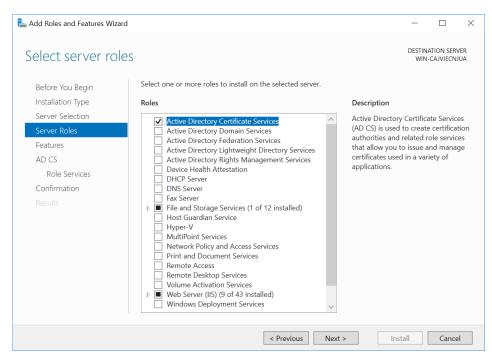


Figure 106. Selecting server roles

On the Select role services tab (Figure 107) select «Certification Authority» role service and click Next.

Science conceses Destination Spread With CADRECTURE Before You Begin Installation Type Installation Type Second Secon	×			
Select role service	S			
Before You Begin	Select the role services to install for Active Directory Certificate Services			
Installation Type	Role services Description			
Server Roles Features AD CS Role Services Confirmation	Certificate Enrollment Policy Web Service to issue and m Certificate Enrollment Web Service Multiple CAs of public key infr Certification Authority Web Enrollment public key infr Network Device Enrollment Service Public key infr	anage cer an be link	tificates. ed to forr	
	< Previous Next > In	stall	Cance	1

Figure 107. Selecting AD CS roles

Confirm the installation of the selected components in the next window. After installing the components required for the Certification Authority role, you should configure Certificate Services. To do this, in the Installation progress window click Configure Active Directory Certificate Services on the destination server (Figure 108).

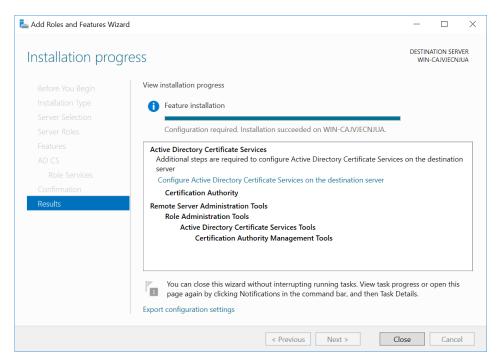


Figure 108. AD CS installation progress

The AD CS Configuration wizard opens. Specify credentials to configure role services and click **Next**. On the Role Services tab (Figure 109) select Certification Authority role service and click **Next**.

L AD CS Configuration	Destination server win-calviechilda s Select Role Services to configure s Select Role Services to configure certification Authority Certification Authority certification Authority Certification Authority certificate Enrollment Service Network Device Enrollment Service graphy Certificate Enrollment Web Service Period Certificate Enrollment Policy Web Service on Network Device Enrollment Policy Web Service			
Role Services	Role Services WIN-CAJV.			
Credentials Role Services	Select Role Services to configure			
Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service			
	More about AD CS Server Roles			
	< Previous Next >	Configure	Cance	:I

Figure 109. Selecting role services

On the Setup Type tab select the appropriate CA setup type and click **Next**. On the CA Type tab specify the type of the CA.

On the Private Key tab (Figure 110) choose Create a new private key and click Next.

AD CS Configuration	- 🗆 X
Private Key	DESTINATION SERVER WIN-CAJVJECNJUA
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 Specify the type of the private key To generate and issue certificates to clients, a certification authority (CA) must have a private key. Create a new private key Use this option if you do not have a private key or want to create a new private key. Use existing private key Use this option to ensure continuity with previously issued certificates when reinstalling a CA. Select a certificate and use its associated private key. Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key. Select an existing private key on this computer Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
	More about Private Key < Previous

Figure 110. Creating a new private key

On the Cryptography for CA tab (Figure 111) select a cryptographic provider and check the Allow administrator interaction when the private key is accessed by the CA box. Click Next to continue.

📥 AD CS Configuration		- 🗆 X
Cryptography for	CA	DESTINATION SERVER WIN-CAJVJECNJUA
Credentials Role Services	Specify the cryptographic options	
Setup Type	Select a cryptographic provider:	Key length:
СА Туре	Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Pr	1024 ~
Private Key Cryptography CA Name	Select the hash algorithm for signing certificates issued by this CA: GOST R 34.11-2012 512 bit	
Validity Period Certificate Database Confirmation		
Progress Results	\checkmark Allow administrator interaction when the private key is accessed l	by the CA.
	More about Cryptography	
	< Previous Next >	Configure Cancel

Figure 111. Specifying the cryptographic options

On the CA Name tab (Figure 112) specify the CA common name and distinguished name suffix and click

Next.

AD CS Configuration		-		×
CA Name		DESTINA WIN-C	TION SER	
Credentials Role Services Setup Type CA Type Private Key Cryptography <u>CA Name</u> Validity Period Certificate Database Confirmation Progress Results	Specify the name of the CA Type a common name to identify this certification authority (CA). This n certificates issued by the CA. Distinguished name suffix values are auto be modified. Common name for this CA: test-DC-CA Distinguished name suffix: DC=test, DC=local Preview of distinguished name: CN=test-DC-CA,DC=test, DC=local			can
	More about CA Name			
	< Previous Next >	Configure	Cance	el

Figure 112. Specifying the CA name

In the next windows specify the validity period for the certificate and certificate database location.

All the above parameters are displayed once again in the «Confirmation» window. Click **Configure** to configure the services according to the specified parameters.

During the CA key generation you might be asked to select key carrier (choose **Registry**), generate the initial random sequence using Biological RNG and set the password for the produced container. Select **Registry** as a key carrier and **do not set the password**.

After issuing the CA certificate open the Certificates snap-in (Start menu \Rightarrow All Programs \Rightarrow Crypto-Pro \Rightarrow Certificates) to check for a certificate in the Trusted Root Certification Authorities store of the Local Computer (Figure 113).

File Action View Window Help				_ 8
• 🔿 🙍 📰 🦸 🛍 🗙 🗐 🗟 🔢 🖬	9			
 Console Root Certificates - Current User Certificates (Local Computer) Personal Trusted Root Certification Authorities Certificates Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Third-Party Root Certification Authoriti Trusted People Client Authentication Issuers Preview Build Roots CryptoPro CSP Trusted Roots ESIM Certificates Cosal NonRemovable Certificates MSIEHistoryJournal Certificate Enrollment Requests 	 Issued To GeoTrust Global CA GlobalSign GlobalSign Root CA Go Daddy Class 2 Certification Go Daddy Class 2 Certificate Auth Hotspot 2.0 Trust Root CA - 03 Microsoft Authenticode(tm) Ro Microsoft Root Certificate Auth Starfield Class 2 Certification A Symantec Enterprise Mobile Ro test-DC-CA thawte Primary Root CA Thawte Timestamping CA VeriSign Class 3 Public Primary 	Microsoft Root Authority Microsoft Root Certificate Authori Microsoft Root Certificate Authori Microsoft Root Certificate Authori NO LIABILITY ACCEPTED, (c)97 Ve Starfield Class 2 Certification Auth	Expiration Date 21/05/2022 15/12/2021 28/01/2028 29/06/2034 01/01/2038 08/12/2043 01/01/2030 31/12/2020 10/05/2021 24/06/2035 23/03/2036 08/01/2004 29/06/2034 15/03/2032 07/09/2023 17/07/2036	Intended Purposes Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Secure Email, Code <all> <all> <all> Time Stamping Server Authenticati Code Signing <all> Server Authenticati Time Stamping Server Authenticati Time Stamping Server Authenticati</all></all></all></all>
Smart Card Trusted Roots Trusted Devices Mindows Live ID Token Issuer	VeriSign Class 3 Public Primary Головной удостоверяющий ц	· · ·	17/07/2036 17/07/2027	Server Authenticati <all></all>

Figure 113. Certificates snap-in

5.2 Adding certificate templates on the server

To ensure that the DC supports Winlogon, the DC certificate must be issued. In order for a user with the Registration Agent role to be able to issue certificates for other users, you must issue the Certificate of the Registration Agent and the Smart Card Login.

Templates for the above certificates by default can be disabled, so you need to check them in the list of certificate templates and include the missing ones. To do this, on the server with installed CA services open CA snap-in (Control Panel \Rightarrow System and Security \Rightarrow Administrative Tools \Rightarrow Certification Authority.

The following templates should be included in the list of certificate templates:

- Domain Controller;
- Enrollment Agent;
- Smartcard User.

To do this, select Certificate Templates, then from the context menu choose New - CertificateTemplate to Issue (Figure 114).

File Action View Help	×
Certification Authority (Local) Etest-DC-CA Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates Manage New > Certificate Template to Issue Refresh	
 test-DC-CA Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates Manage New Certificate Template to Issue Refresh Refresh	
New Certificate Template to Issue Refresh Image: Certificate Template to Issue	
Refresh	
Help	
Enable additional Certificate Templates on this Certification Authority	

Figure 114. Adding certificate templates

In the «Enable Certificate Templates» window (Figure 115) select the required templates and click OK.

Enable Certificate Templates		×
Select one Certificate Template to enable on this (Note: If a certificate template that was recently cre information about this template has been replicate All of the certificate templates in the organization n For more information, see <u>Certificate Templa</u>	eated does not appear on this list, you may need to wait unt d to all domain controllers. nay not be available to your CA.	il
Name	Intended Purpose	^
R Authenticated Session	Client Authentication	
🗷 CA Exchange	Private Key Archival	
R CEP Encryption	Certificate Request Agent	
R Code Signing	Code Signing	
R Cross Certification Authority	<all></all>	
🚇 Enrollment Agent	Certificate Request Agent	
Richard Rent (Computer)	Certificate Request Agent	
Rechange Enrollment Agent (Offline request)	Certificate Request Agent	
Rechange Signature Only	Secure Email	
🚇 Exchange User	Secure Email	~
	ОК Са	ncel

Figure 115. Enable Certificate Template

Next, the administrator of the domain needs to update the templates using the CryptoPro CSP control

panel. To do this, open the Winlogon tab and click the Fix templates button (Figure 116).

Minlagon Traca	Algorithm
Security Winlogon TLS Se	ttings
Default key reader	
Choose CSP to configure:	
Crypto-Pro GOST R 34. 10-2001 Cryptographic Service Provid	der 🗸 🗸
Choose reader:	
Not set	\sim
Parameters Disable CryptoPro Winlogon Use CryptoPro CSP algorithms on KDC	
Disable CryptoPro Winlogon	
Disable CryptoPro Winlogon	
Disable CryptoPro Winlogon	
Disable CryptoPro Winlogon Use CryptoPro CSP algorithms on KDC Identifiers of domain controllers	ort
Disable CryptoPro Winlogon Use CryptoPro CSP algorithms on KDC Identifiers of domain controllers Domain controller:	ort

Figure 116. CSP Winlogon tab

After the message that all the templates have been successfully updated, you can start creating certificates requests.

This action must be performed every time when new templates for the DC and the enrollment agent are edited or added.

5.2.1 Configuring certificate templates

In order to use the certificates in Winlogon, you need them to satisfy certain requirements described in the .

If the existing template does not meet these requirements, you must change it. To do this, create a copy of the template, edit it and include it in the list of CA templates.

Open the Certification Authority snap-in, select **Certificate Templates**, then from the context menu choose **Manage** (Figure 117).

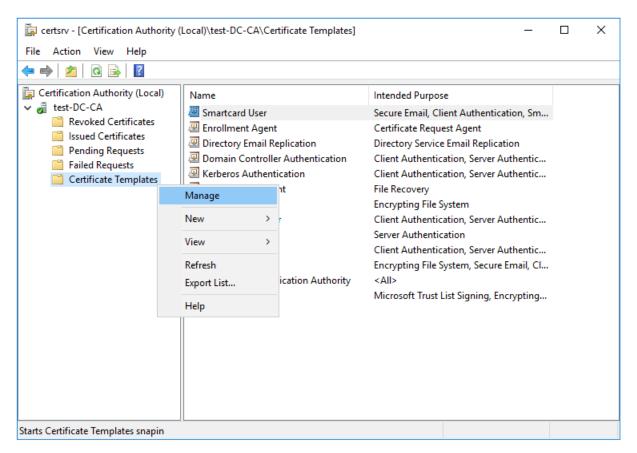


Figure 117. Certification Authority snap-in

The Certificate Templates Console opens. Select an editable template and click the **Duplicate Template** button in the context menu (Figure 118).

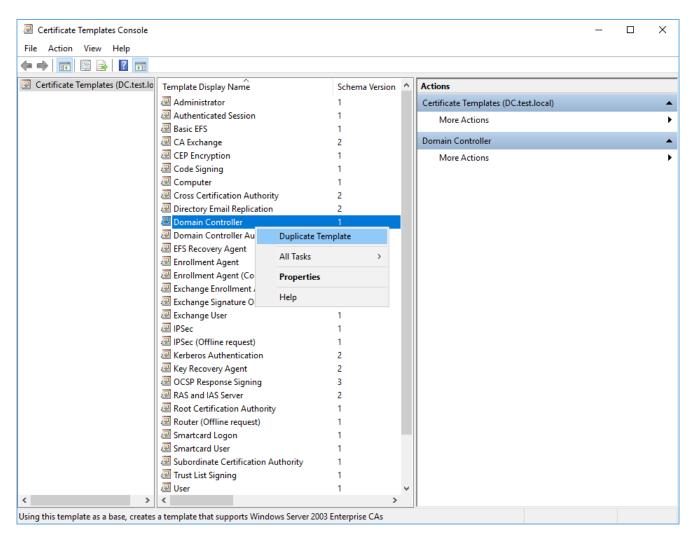


Figure 118. Certificate Templates Console

The «Properties of New Template» window opens, in which you can change the properties of the templates so that they meet the requirements for the certificate (Figure 119).

Figure 119. Copy of DC template

After saving the new template, you need to add it to the template list.

5.3 Issuing a DC certificate

A DC certificate must meet the requirements described in the Microsoft documentation.

The DC certificate must be issued on the server on which the AD services are deployed, by the user with domain administrator rights. To issue the DC certificate, open the **Certificates** snap-in, in the Personal Local Computer store select **All Tasks** — **Request New Certificate** (Figure 120).

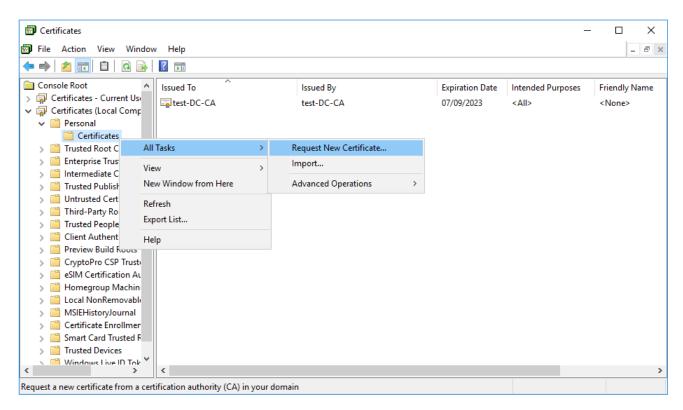


Figure 120. Certificates snap-in

The Certificate Enrollment wizard opens. In the «Select Certificate Enrollment Policy» window leave the default settings and click the **Next** button (Figure 121).

	_		×
🔄 Certificate Enrollment			
Select Certificate Enrollment Policy			
Certificate enrollment policy enables enrollment for certificates based on predefined Certificate enrollment policy may already be configured for you.	certificate	e templat	es.
Configured by your administrator			
Active Directory Enrollment Policy			*
Configured by you		Add N	lew
	Next	Can	icel

Figure 121. Select Certificate Enrollment Policy

In the «Request Certificates» window select **Domain Controller** from the list of certificate types (Figure 122). Verify the certificate details and, if necessary, select the cryptographic service provider in the **Certificate Properties** on the **Private Key** tab (Figure 123).

Request Certificates			
You can request the following types o click Enroll.	f certificates. Select the certificates you w	vant to request, and then	
Active Directory Enrollment Policy	y		
Directory Email Replication	③ STATUS: Available	Details 💙	
Domain Controller	(i) STATUS: Available	Details 🔺	
<u> </u>	he uses and validity period that apply to	this type of certificate:	
	l signature ncipherment		
Application policies: Client	Authentication		
Validity period (days): 365			
		Properties	
Show all templates			

Figure 122. Request Certificates

Certificat	e Propert	ies					×
General	Subject	Extensions	Private Key	Certification Au	thority		
Crypto	ographic	Service Prov	ider			^	^
		am that gen d processes		ic and private k	ey pair used in m	hany	
Select	cryptogra	phic service	provider (CS	P):			
Mic	crosoft St	rong Crypto	graphic Provi	ider (Encryptior	ı)	^	
					e Provider (Encry		
Cry	pto-Pro (GOST R 34.10	0-2012 Crypto	ographic Service	e Provider (Encry	ption)	
	pto-Pro (cryption))-2012 Strong) Cryptographic	Service Provider	r	
🗌 Mic	crosoft Ba	ise Cryptogr	aphic Provide	er v1.0 (Encrypti	ion)		
	rrocoft D-	nee pee and	Niffia Uallima	n Cointearabh	is Drovidor (Enco	(ntion) Y	
Sho	w all CSP:	s					
Key op	otions					*	
Key ty	pe					*	
Key pe	ermission	s				*	~
				ОК	Cancel	Appl	y

Figure 123. Certificate Properties

During the DC private key generation, the Biological RNG window is displayed and CSP requests a password for the container (no password is required in this case). In the «Certificate Installation Results» window (Figure 124) expand the **Details** and click **View Certificate** to view certificate details (Figure 125).

Active Directory Enrollmen	t Policy		
Key usage:	STATUS: Succeeded cribe the uses and validity period that apply to Digital signature Key encipherment Client Authentication Server Authentication 365	 Details tificate: Certificate	^

Figure 124. Certificate Installation Results

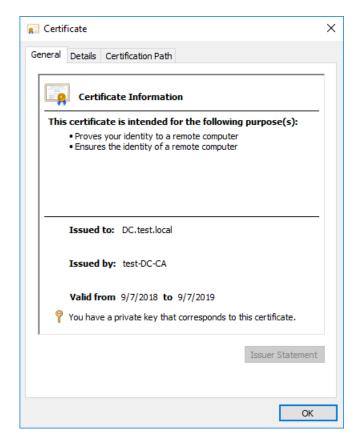


Figure 125. DC certificate

The certificate of the domain controller must be installed in the Personal Local Computer certificate store. After the certificate is issued, the domain controller must be restarted.

Note. For certificates with GOST keys, automatic issuance of certificates for a domain controller is not available, so you need to monitor the validity of the certificate and update it before expiration.

5.4 Issuing an Enrollment Agent certificate

By default, permission to request certificates on behalf of the user is granted only to domain administrators. However, a user who is not a domain administrator can be granted permission to become an enrollment agent.



Note. An enrollment agent certificate allows you to apply for certificates and create smart cards on behalf of any user in the organization. The resulting smart card can then be used to log on to the network under the user name without his knowledge.

Because the Enrollment Agent certificate provides wide opportunities, it is strongly recommended to maintain strict security policies for these certificates.

To become an enrollment agent, you must apply for the certificate using **Certificates** — **Current User** snap-in.

To do this, open the **Certificates** snap-in, in the Personal Current User store select **All Tasks** — **Request New Certificate**. In the «Request Certificates» wizard window select **Enrollment Agent** from the list of

certificate types (Figure 126).

		—		\times
🙀 Certificate Enrollment				
Request Certificates You can request the following t click Enroll.	ypes of certificates. Select the certificates you want to) request, a	and then	
				^
Key usage:	 STATUS: Available scribe the uses and validity period that apply to this ty Digital signature Certificate Request Agent 730 	-	etails 🔺 ficate:	
		Prop	erties	
Smartcard User	STATUS: Available	D	etails 💙	
User	(1) STATUS: Available	D	etails 💙	~
Show all templates				
		Enroll	Can	cel

Figure 126. Request Certificates

Click Properties button and select the cryptographic service provider in the **Certificate Properties** on the **Private Key** tab (Figure 127). On the **Certification Authority** tab specify the corresponding CA (Figure 128).

Certificate Properties	×
General Subject Extensions Private Key Certification Authority	
Cryptographic Service Provider	^
A CSP is a program that generates a public and private key pair used in many certificate-related processes.	
Select cryptographic service provider (CSP):	
Microsoft Strong Cryptographic Provider (Signature)	^
Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider (Signature)	
Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider (Signature)	
Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider (Signature)	
Microsoft Base Cryptographic Provider v1.0 (Signature)	
Microsoft Pass DSS and Diffis Hollman Countegraphic Drovider (Signature)	×
Show all CSPs	
Key options	~
Key type	~
OK Cancel	Apply

Figure 127. Certificate Properties

General	Subject	Extensions	Private Key	Certification Authority	
				l renew certificates. Th process certificate requ	connect to
				each enrollment server available enrollment s	ic
	cation Au -DC-CA	thority		Type: Enterprise root CA	
Shov	v all enrol	Iment server	s		

Figure 128. Certification Authority

After saving the changes, click **Enroll** button to start the container generation. During the private key generation, the Biological RNG window is displayed and CSP requests a password for the container.

The certificate of the enrollment agent must be installed in the Personal Current User certificate store.

5.5 Issuing a Smartcard User certificate

A user who is a member of the Users group and has the Enrollment Agent certificate can issue certificates to other domain users using a computer in the domain with pre-installed CryptoPro CSP.

The smart card certificate must meet the requirements described in the Microsoft documentation.

To issue a SmartCard User certificate, open the **Certificates** snap-in, in the Personal Current User store select **All Tasks** — **Advanced Options** — **Enroll On Behalf Of** (Figure 129).

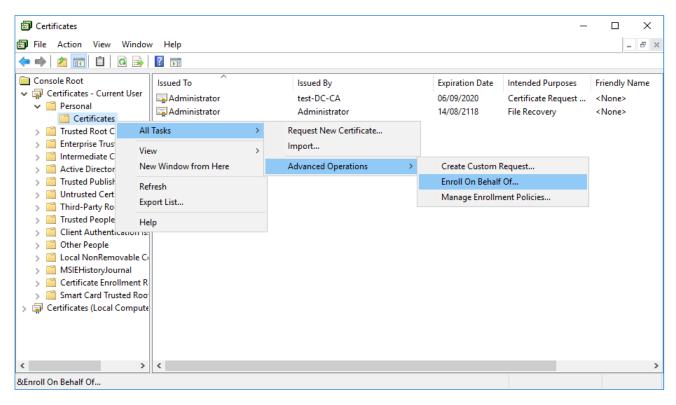


Figure 129. Certificates snap-in

In the «Select Enrollment Agent Certificate» window of the Certificate Enrollment wizard select the certificate of the Enrollment Agent that will be used to sign the processed certificate request (Figure 130).

	_		\times
🙀 Certificate Enrollment			
Select Enrollment Agent Certificate			
You need an enrollment agent certificate in order to sign a certificate request or Browse to locate a signing certificate, and then click Next.	behalf of ot	her users. (Click
Signing certificate Administrator		Browse .	
Administrator		Browse .	
	Next	Car	ncel

Figure 130. Select Enrollment Agent Certificate

In the «Request Certificates» wizard window select **Smartcard User** from the list of certificate types (Figure 131). Click the **Properties** button to edit the certificate settings.

		_		×
📮 Certificate Enrollment				
Request Certificates				
You can request the following click Next.	types of certificates. Select the certificates you want	to request,	and then	
Smartcard User	(i) STATUS: Available	-	etails 🔺	^
	scribe the uses and validity period that apply to this	type of cert	ificate:	
Key usage:	Digital signature			
Application policies:	Key encipherment Secure Email			
Application policies.	Client Authentication			
	Smart Card Logon			
Validity period (days):	: 365			
		Prop	erties	
() User	🗘 STATUS: Available	D	etails 👻	~
Show all templates				
_ ·				
]	Next	Can	cel

Figure 131. Request Certificates

Select the cryptographic service provider in the **Certificate Properties** on the **Private Key** tab (Figure 132). On the **Certification Authority** tab specify the corresponding CA (Figure 133).

Certificate Properties	\times
Private Key Certification Authority	
Cryptographic Service Provider	^
A CSP is a program that generates a public and private key pair used in many certificate-related processes.	
Select cryptographic service provider (CSP):	
Microsoft Strong Cryptographic Provider (Encryption)	^
Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider (Encryption)	
Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider (Encryption)	
Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider (Encryption)	
Microsoft Base Cryptographic Provider v1.0 (Encryption)	
Microsoft Pace DSS and Diffic Hollman Comtographic Drovider (Encountion)	~
Show all CSPs	
OK Cancel Ap	ply

Figure 132. Certificate Properties

Certificate Properties	×
	ue and renew certificates. The system will connect to
enrollment servers in the following l Not all certificate templates are avai purposes, it may be helpful to identi	lable each enrollment server. For diagnostic
Certification Authority ☑ test-DC-CA	Type: Enterprise root CA
Show all enrollment servers	
	OK Cancel Apply

Figure 133. Certification Authority

To save the selected settings, click the **Apply** button and close the form. In the Certificate Enrollment

wizard, click **Next** to continue. Select the domain user by clicking the **Browse** button and click the **Enroll** button to begin the container and private key generation (Figure 134).

		_		\times
🔄 Co	ertificate Enrollment			
	Select a user			
	To request a certificate on behalf of another user, enter the formal name or domain reample, Firstname Lastname, username, or domain\username.	name of	that user. F	or
	Before enrolling for a certificate, make sure the device on which the user certificate r attached.	eeds to	be installed	l is
	User name or alias:			
	TEST\Administrator		Browse	
		Enroll	Can	cel

Figure 134. Select a user

Next, the key carrier is selected to create the container. The carrier must be connected to the computer, and the smart card must be identified. During the private key generation, the Biological RNG window is displayed and CSP requests a password for the container.

In the password setting dialog you need to enter the password for the created container. For the correct operation of the smart card, the password for the created container and smart card must be the same.

After the container is written to the carrier, the user can login with a domain account using the smart card.

To authorize a domain user to the computer, connect the reader and insert a smart card into it, then select the «Smart Card» icon from the input parameters and enter the PIN code.

6 Using CryptoPro CSP with Microsoft Outlook 2016

CryptoPro CSP allows you to use the public key infrastructure and standard Microsoft products (including Microsoft Outlook, Microsoft Outlook Express, Windows Mail and Windows Live Mail) with strong russian cryptographic algorithms and 256 or 512-bit keys.

This section contains instructions for integrating CryptoPro CSP with the Microsoft Outlook 2016 mail client.

6.1 Configuring Microsoft Outlook 2016

Open Microsoft Outlook 2016 application, open File menu and click Options button (Figure 135).

¢	
Info	Account Information
Open & Export	test_user2019@mail.ru
Save As	Add Account
Print	Account Settings Account Settings *
Office Account Options Exit	Mailbox Cleanup Manage the size of your mailbox by emptying Deleted Items and archiving. Cleanup Tools •
	Rules and Alerts Use Rules and Alerts to help organize your incoming e-mail messages, and receive updates when items are added, changed, or removed.

Figure 135. Outlook File menu

In the «Outlook options» window open the **Trust Center** tab and click **Trust Center Settings** button (Figure 136).

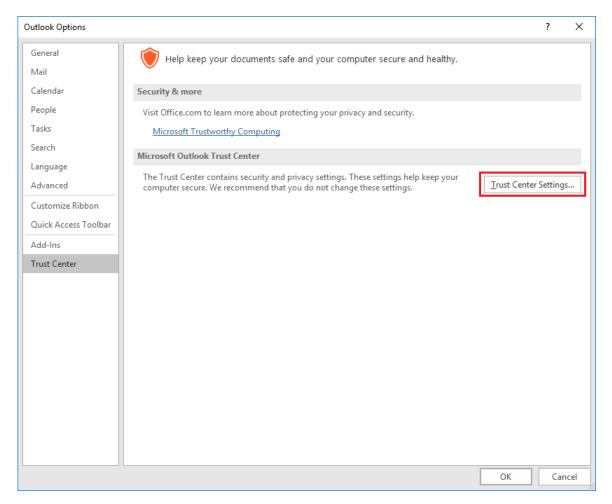


Figure 136. Trust Center tab

Next open the **E-mail Security** tab and click **Settings** button in the Encrypted e-mail section (Figure 137).

Trust Center		?	×
Trusted Publishers	Encrypted e-mail		
Privacy Options Email Security Attachment Handling Automatic Download Macro Settings Programmatic Access	 Encrypt contents and attachments for outgoing messages Add digital signature to outgoing messages Send clear text signed message when sending signed messages Bequest S/MIME receipt for all S/MIME signed messages Default Setting: Settings Digital IDs (Certificates) Digital IDs or Certificates are documents that allow you to prove your identity in electronic transaction Import/Export Get a Digital ID Read as Plain Text	15.	
	Read all standard mail in plain text Read all digitally signed mail in plain text		
	Script in Folders		
	Allow script in Shared folders Allow script in Public Folders		
	ОК	Can	cel

Figure 137. E-mail Security tab

In the opened «Change Security Settings» window (Figure 138) in the Certificates and Algorithms section select personal certificates that match the signature and encryption keys using the **Choose** button. Check the **Send these certificates with signed messages** box. Then specify the **Security Settings Name** and click **OK**.

Change Security Settings			×				
Security Setting Preference Security Settings Name:							
My S/MIME Settings (t	My S/MIME Settings (test_user2019@mail.ru)						
Cryptography Format:	S/MIME		\sim				
🗹 Default Security Sett	ting for this cryptog	graphic message f	ormat				
🗹 Default Security Sett	ting for all cryptogr	aphic messages					
Security Labels	. New	Delete					
Certificates and Algorit	hms						
Signing Certificate:	test_user2019		Choose				
Hash Algorithm:		\sim					
Encryption Certificate:	test_user2019		Choose				
Encryption Algorithm:		\sim					
Send these certificat	es with signed mes	ssages					
		ОК	Cancel				

Figure 138. Changing e-mail security settings

On the E-mail Security tab you can also turn on the **Encrypt contents and attachments for outgoing messages** and **Add digital signature to outgoing messages** options to automatically encrypt and add digital signature to each outgoing message. If these modes are not enabled, the encryption and signing options will need to be enabled for each message sent.

You can also select the **Send clear text signed message when sending signed messages** options. When the mode is enabled, the signature is formed as one separate attachment for the message. Otherwise, the message text and all attachments are combined and encoded according to the BASE64 encoding rules, after which the encoding result is signed.

6.2 Sending signed messages

To create and send a signed message, click **New E-mail** button. Select the message recipient (**To**) and enter the subject of the message (**Subject**). If the message contains some files, add them to the email using the **Attach File** button. To sign message, click the **Sign** button in the **Options** tab (Figure 139). Click **Send** button to send message.

	5	ð	Ŷ	.↓	Te	est - Message (H	ITML)		Ŧ	-	×
File	Me	ssage	Insert	Options	Format Text	t Review	♀ Tell me wh	at you wan	t to do		
Aa Themes	• · c		∎ Bcc E From	Permission *		Request a	Delivery Receipt Read Receipt	Save Sent Item To •	- onece nep	olies To	
	Themes		Show Fields	Perm	nission	Trac	cing 🗔	M	ore Options	- G	~
توالي Send	Cc Subje		user_test2019 Test	9@mail.ru							

Figure 139. Signing a message

If the certificate with which the message was signed has been has been revoked or the e-mail address specified in the certificate does not match the address of this account, a warning will appear (Figure 140) and the message will not be sent.

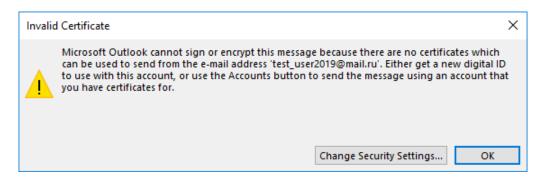


Figure 140. Message signing error

6.3 Obtaining a user public key certificate for message encryption

To encrypt messages to other users, you need certificates of recipients of letters.

If the sender and all recipients of the message are users of the same domain, you can use the global address book. In this case, the domain user e-mail security certificates must be installed in AD.

If you use the CryptoPro CA for issuing certificates, you can configure the certificates export to the AD

(see the documentation for CryptoPro CA). If the CA is not configured to publish certificates to AD, the domain user can publish his certificate himself so that it is available to other domain users to encrypt the mail.

To import the certificate into the global address book, follow these steps:

• open the E-mail Security tab of the Trust Center;

• in the Digital IDs (Certificates) section click **Publish to GAL** button (Figure 141). The current user certificate, selected by default, will be imported into the global address book.

Trust Center	?		×
Trusted Publishers	Encrypted e-mail		
Privacy Options Email Security Attachment Handling Automatic Download	 Encrypt contents and attachments for outgoing messages Add digital signature to outgoing messages Send clear text signed message when sending signed messages Request S/MIME receipt for all S/MIME signed messages 		
Macro Settings	Default Setting:		
Programmatic Access	Digital IDs (Certificates)		
	Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions Publish to GAL Import/Export Get a Digital ID Read as Plain Text Read all standard mail in plain text Read all digitally signed mail in plain text Script in Folders Allow script in shared folders	i.	
	Allow script in Public <u>F</u> olders		
	ОК	Cance	el

Figure 141. Publishing certificate to GAL

Instead of global address book a local copy of the address book can be used. To update the information about the recipient certificate in the local copy of the address book, perform the following actions:

1) in the Microsoft Outlook 2016 main view open the Send/Receive tab, select Send/Receive Groups — Download Address Book (Figure 142).

2) in the opened window select the address book and click **OK**. The information in the address book will be updated.

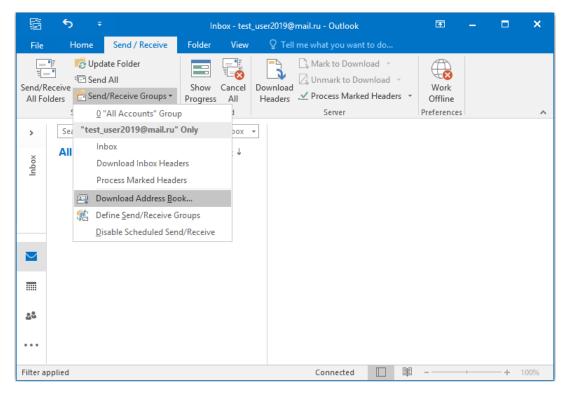


Figure 142. Downloading address book

If the sender and recipients of messages are not domain users or they are users of different domains or the domain does not use the publication of certificates to protect e-mail, you can use the contact list instead of the global address book to obtain information about recipient certificates.

To do this, user A should send a signed message to the user B. User B should add the sender of the signed message to the Outlook contacts by right-clicking the sender name and selecting Add to Outlook Contacts (Figure 143).

🔓 Reply	🛱 Reply All 🔤 Forward							
	User Test <user_test2019@mail.ru></user_test2019@mail.ru>							
\mathbf{m}	Test	8	Cu <u>t</u>					
		Ē	<u>C</u> opy					
Test		Ē	<u>P</u> aste					
Test me	essage	2	Cle <u>a</u> r					
		Eb	Select A <u>I</u> I					
 User Te	t		Add to <u>F</u> avorites					
OSCI IV	Lat	8	Add to Outlook Contacts					
			Open <u>O</u> utlook Properties					
			Open Co <u>n</u> tact Card					

Figure 143. Adding user to contacts

To verify that a certificate is added:

- 1) open the local address book by clicking the Address Book button of the Find tab;
- 2) in the opened window (Figure 144) open the required contact with a double click;

	More columns Address Book	
	Go Contacts - test_use	er2019@mail.ru V Advanced Fi
Name	Display Name	E-mail Address
🚨 User Test	User Test	user_test2019@mail.ru

Figure 144. Local address book

3) in the contact card click the **Certificates** button in the **Show** section (Figure 145);

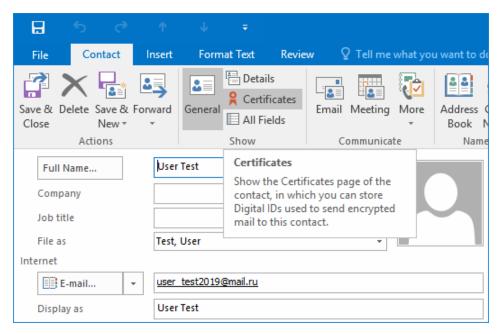


Figure 145. Address book contact

4) make sure that there is a user certificate (Figure 146);

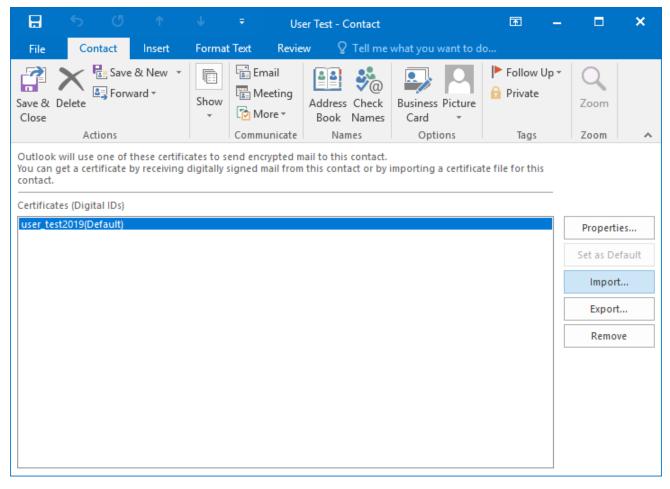


Figure 146. Contact certificate

6.4 Sending encrypted messages

To create and send an encrypted message, click **New E-mail** button. Select the message recipient (**To**) and enter the subject of the message (**Subject**). If the message contains some files, add them to the email using the **Attach File** button. To encrypt message, click the **Encrypt** button in the **Options** tab (Figure 147). Click **Send** button to send message.

	5	ð	Ŷ		Te	st - Message (H	ITML)		ħ	-	×
File	Mess	sage	Insert	Options	Format Text	Review	♀ Tell me wha	at you wan	t to do		
Aa Themes	A - Pi Co		Bcc	Permission	🔒 Encrypt 🎗 Sign		Delivery Receipt Read Receipt	Save Sent Item To •			~
ت ا ا	To Cc Subjec	. [. [t [user_test2019								

Figure 147. Encrypting a message

If there is no certificate of the recipient in the certificate store or the certificate is invalid (for example, expired or revoked), the following warning appears (Figure 148).

Encry	ption Problems X
	Microsoft Outlook had problems encrypting this message because the following recipients had missing or invalid certificates, or conflicting or unsupported encryption capabilities:
	user_test2019@mail.ru
	Continue will encrypt and send the message but the listed recipients may not be able to read it.
	Send Unencrypted Continue Cancel

Figure 148. Message encryption error

6.5 Viewing encrypted messages

Viewing encrypted messages is only available to users who have a certificate that was used by the sender when encrypting the message.

To view information about the user certificate, open the encrypted message and click $\widehat{\mathbf{b}}$ button — the

sign of the encrypted message.

The «Message Security Properties» window opens (Figure 149).

Message Security	Properties		:	×
Subject: Te	st			
Messages may cont digital signature la Security Layers	yer may contain mu	Iltiple signature		
Select a layer belov				
Description:				
OK: Protected by 2 test_user2019@ma		89 encryption.	Encrypted for	
Click any of the fol make changes to th		view more info	rmation about o	or
Edit Trust	View Details	Trust Certific	ate Authority	
🗹 Warn me about	errors in digitally s	igned e-mail.	Close	

Figure 149. Message Security Properties

If the recipient of the encrypted message does not have a certificate that was used to encrypt this message, the preview of the message content is not available, and the following message is displayed in the Microsoft Outlook 2016 window (Figure 150).

Search Current Mailbox (🔎 Current Mailbox	 This item cannot be displayed in the Reading Pane. Open the item to read its contents.
All Unread By Date ▼ Newest ↓	
▲ Today	
test_user2019@mail.ru 🔒 Test 10:51 AM	

Figure 150. Viewing an encrypted message without certificate

If the recipient tries to open such a message, a window with an error opens (Figure 151).

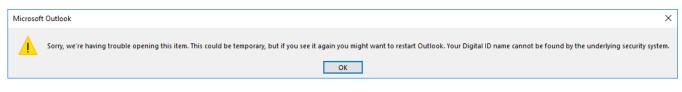


Figure 151. Error viewing the encrypted message

6.6 Verifying the signed message sender certificate

To verify the user certificate, open the signed message and click $\stackrel{\textbf{Q}}{\leftarrow}$ button — the sign of the signed message.

The digital signature verification window opens (Figure 152).

Digital Signature: Valid					
Subject: From: Signed	Test user_test2019@mail.ru user_test2019@mail.ru				
	The digital signature on this message is Valid and Trusted For more information about the certificate used to digita sign the message, click Details.				
🗌 Warn	Details me about errors in digitally signed e-mail before message Close	oper			

Figure 152. Verifying the message signature

To view information about the certificate, click the **Details** button. If you see the following window (Figure 153), the sender certificate is valid.

Message Security	Properties		×			
Subject: T	est					
	tain encryption and ayer may contain mu					
Select a layer belo	w to view its descrip	tion.				
	•	ail.ru				
Description:						
OK: Signed messa	ge.					
Click any of the following buttons to view more information about or make changes to the selected layer:						
Edit Trust	View Details	Trust Certifica	te Authority			
Warn me abou	t errors in digitally s	igned e-mail.	Close			

Figure 153. Digital signature details

If the sender certificate of the signed letter is issued by CA that is not trusted by the recipient computer, the following warning will be displayed when the signed letter is opened (Figure 154).

Digital Signature:	Invalid			Х		
Certificate Authority Information Your message was digitally signed with a certificate issued by a Certificate Authority.						
The signature is invalid because you have either distrusted or not yet chosen to trust the following Certificate Authority:						
Issued by:	CRYPTO-PRO Test C	enter 2				
Valid From:	8/5/2014 to 8/5/201	9				
For more informa message, click De	tion about the certifi tails.	cate used to digital	ly sign the			
			Details			
Trusting the Cert	ificate Authority					
	ate Authority means ates issued from that					
Do you want to t	rust this Certificate A	uthority?				
If you choose Trust, you must also click Yes on the Root Certificate Store dialog that follows to add the certificate to your system.						
View Certifi	cate Authority	Trust	Close			
Warn me abo	Warn me about errors in digitally signed e-mail before message opens.					

Figure 154. Warning about an untrusted CA

If the validity of the sender certificate could not be verified or if this certificate was revoked, the following window opens (Figure 155).

Message Security Properties	\times
Subject: Test	
Messages may contain encryption and digital signature layers. Eac digital signature layer may contain multiple signatures. Security Layers	h
Select a layer below to view its description.	
Q Subject: Test	
Digital Signature Layer	
Signer: user_test2019@mail.ru	
Description:	
Error:	^
The system cannot determine whether the certificate used to create this signature is trusted or not.	
Signad by user test2010@mail rulusing COST D 34 10 2012 256	Y
Click any of the following buttons to view more information about make changes to the selected layer:	t or
Edit Trust View Details Trust Certificate Authority.	
Warn me about errors in digitally signed e-mail.	

Figure 155. Message Security Properties

This error may occur if the CRL and/or the address of the OCSP services in the sender certificate is missing or inaccessible or contain out-of-date information, and at the same time the CRL of the CA that issued a certificate of the sender is not installed on the recipient computer or has expired. In this case, install the current CRL in the certificate store on the recipient computer to verify the sender certificate.

If the digital signature verification is not possible or the signature is invalid, the preview of the message content is not available, and the following message is displayed in the Microsoft Outlook 2016 window (Figure 156).

Search Current Mailbox (🔎 Current Mailbox 👻	This message has an invalid Digital Signature. Open the message for more information.
All Unread By Date ▼ Newest ↓	
▲ Today	
user_test2019@mail.ru 🔒	
Test 9:49 AM	
Test message < end>	

Figure 156. Viewing a signed message without certificate