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

Cryptographic
Service
Provider

CryptoPro CSP
version 4.0 2-Lic
User guide for Microsoft Windows

Pages 109

2018

Table of contents

1 CryptoPro CSP installation **4**

2 CryptoPro CSP interface **11**
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 . . . 23
2.5 Certificates and containers . . . 27
2.5.1 Checking a private key container . . . 28
2.5.2 Copying a private key container . . . 31
2.5.3 Deleting a private key container . . . 33
2.5.4 Viewing certificates in a private key container . . . 35
2.5.5 Installing a personal certificate stored in a private key container . . . 38
2.5.6 Installing a certificate stored in a file . . . 39
2.5.7 Changing the password for a private key container . . . 42
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 Key generation interface **51**
3.1 Crypto-Pro LLC Test Certificate Authority . . . 51
3.2 Creating a key container . . . 52
3.2.1 Selecting a key carrier . . . 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 CryptoPro 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 . . . 73
4.6 Testing two-way client-server authentication . . . 73

5 CryptoPro 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 Using CryptoPro CSP with Microsoft Outlook 2016 **96**
6.1 Configuring Microsoft Outlook 2016 . . . 96
6.2 Sending signed messages . . . 99
6.3 Obtaining a user public key certificate for message encryption . . . 100
6.4 Sending encrypted messages . . . 104
6.5 Viewing encrypted messages . . . 105
6.6 Verifying the signed message sender certificate . . . 107

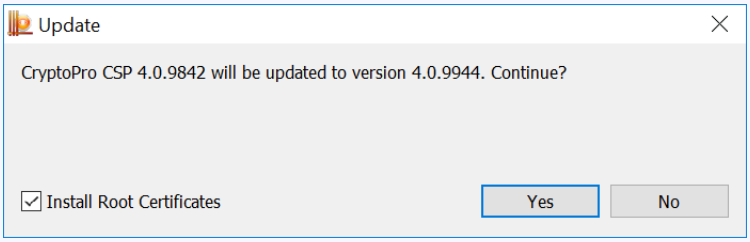
1 CryptoPro CSP installation

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).

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.

Note. If an earlier version of CryptoPro CSP is already installed on your computer, the «CSP update confirmation» window opens:



In case of the security level updating, the base program features and other settings will be saved. In order to change the security level you should previously remove an earlier version from the computer.

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.

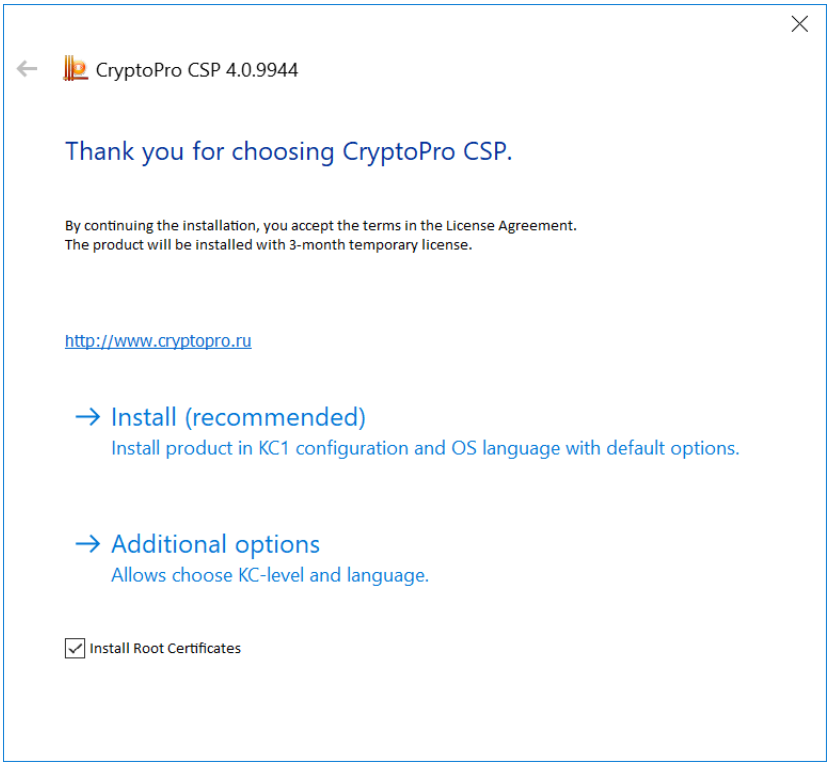


Figure 2. CSP welcome window

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).

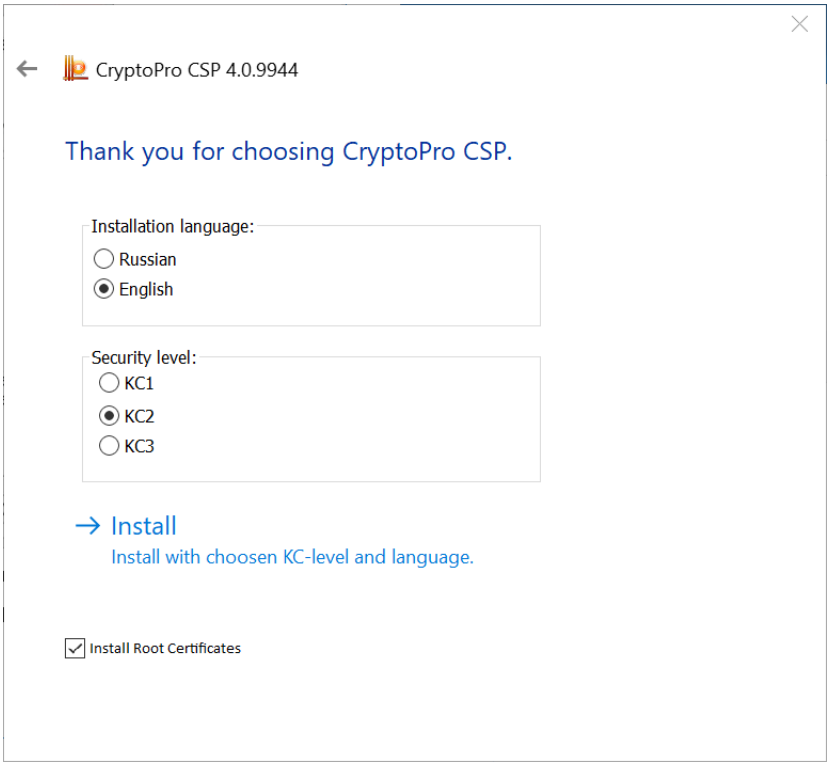


Figure 3. Installation options

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
- additional physical random number generator (RNG)

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).

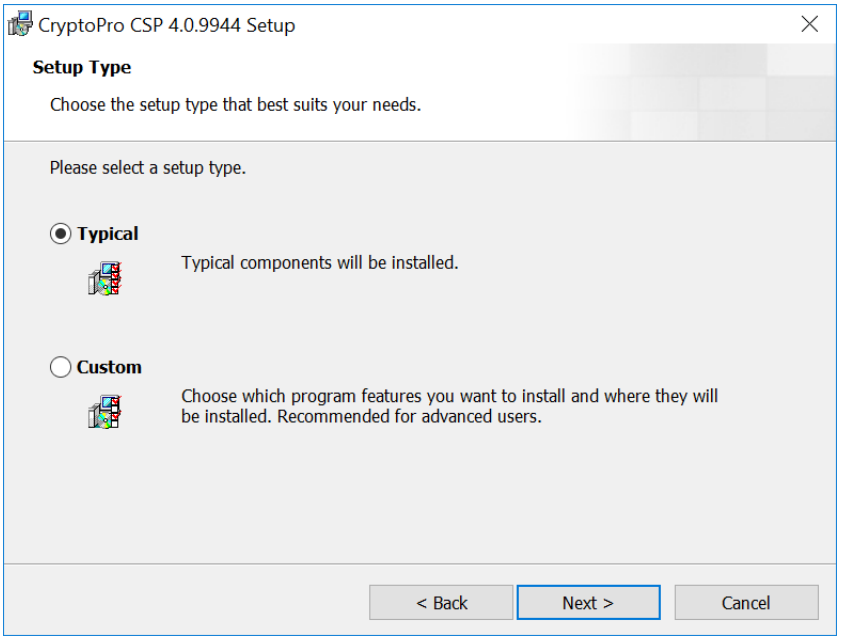


Figure 5. The installation type selection window

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.
- **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».

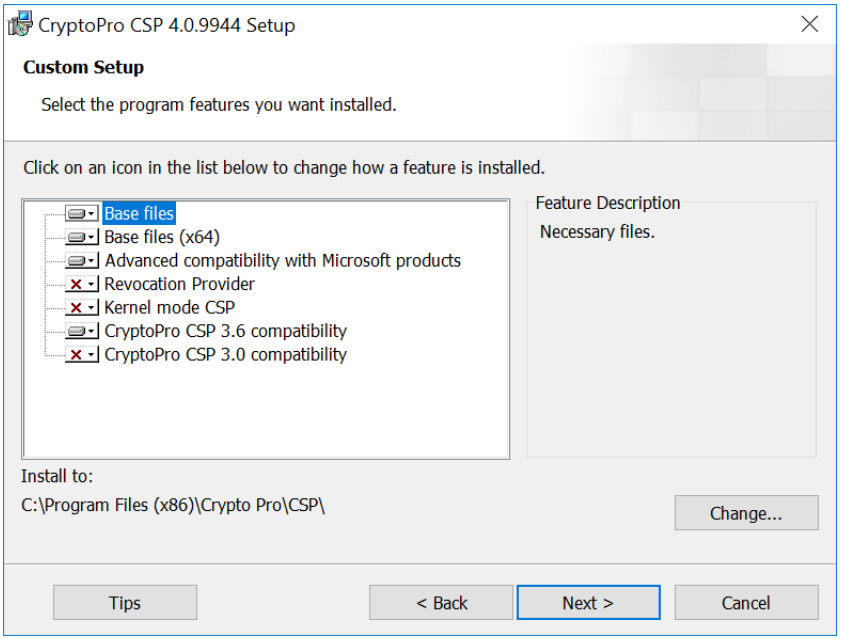


Figure 6. Custom Setup window

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.

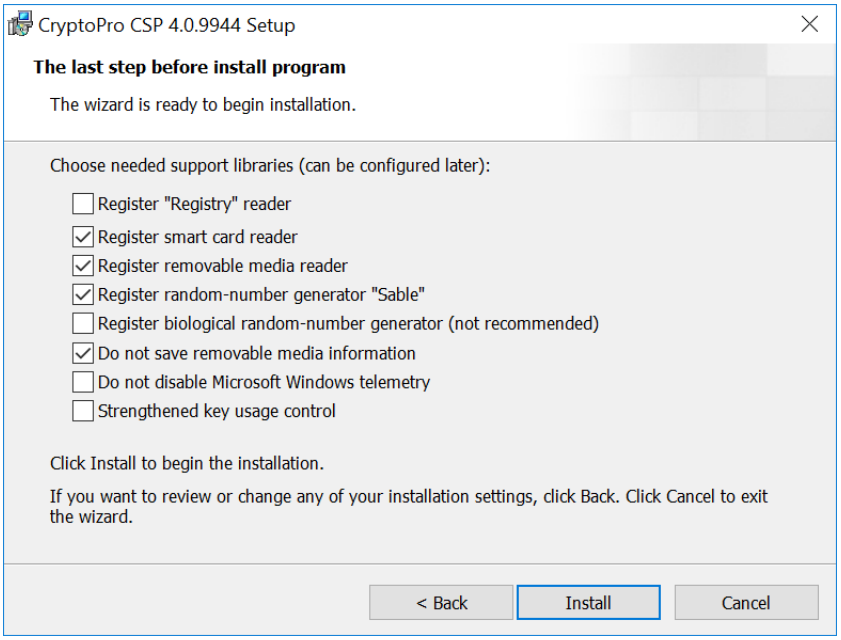


Figure 7. The supported libraries and security settings window

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.

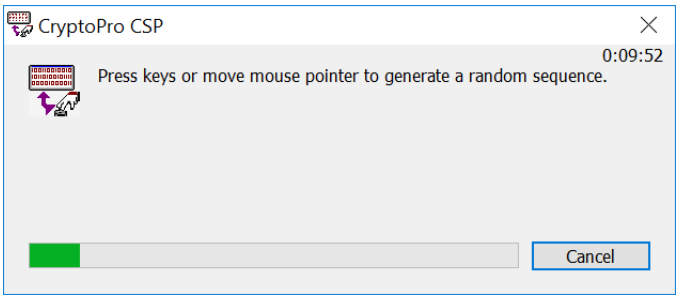


Figure 8. Biological RNG window

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

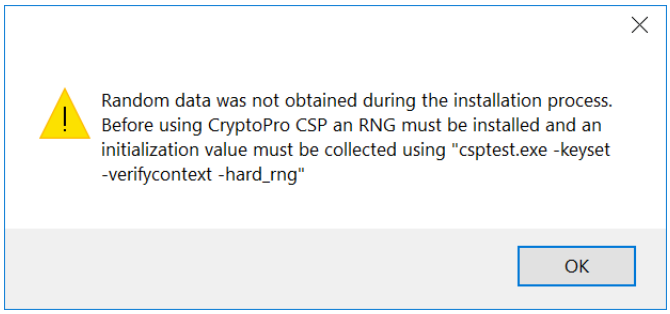


Figure 9. Random data acquisition error message

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.

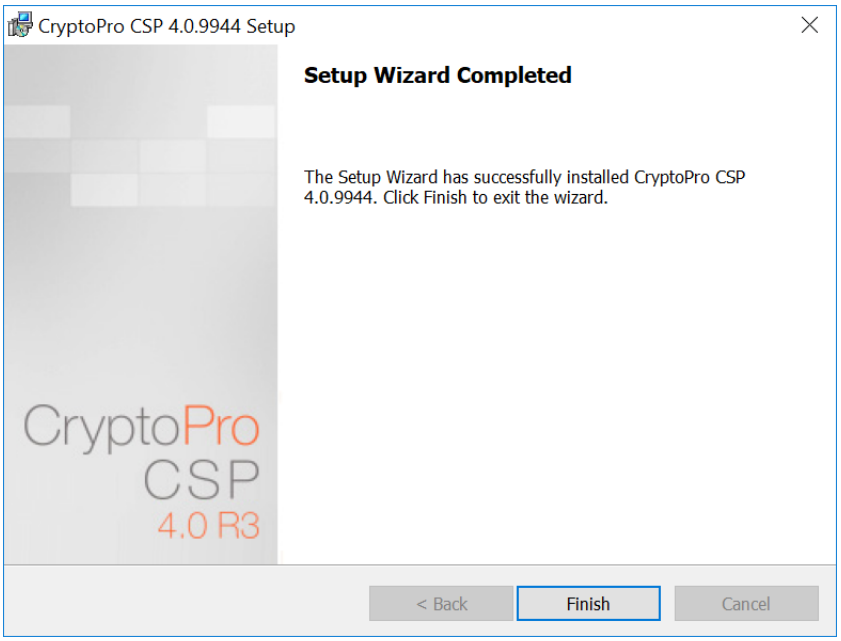


Figure 10. Final Wizard window

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 ⇒ **All Programs** ⇒ **Crypto-Pro** ⇒ **CryptoPro CSP**) (Figure 11).

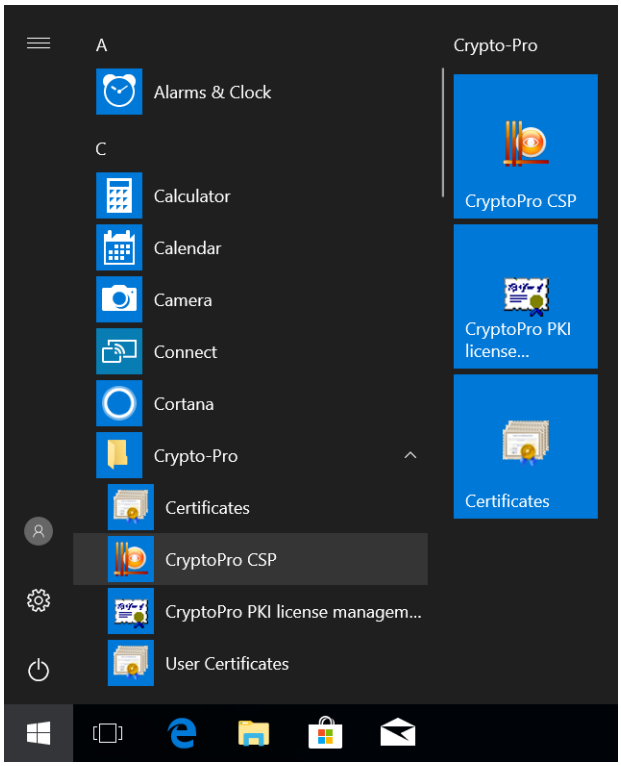


Figure 11. Access to the CSP control panel

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.

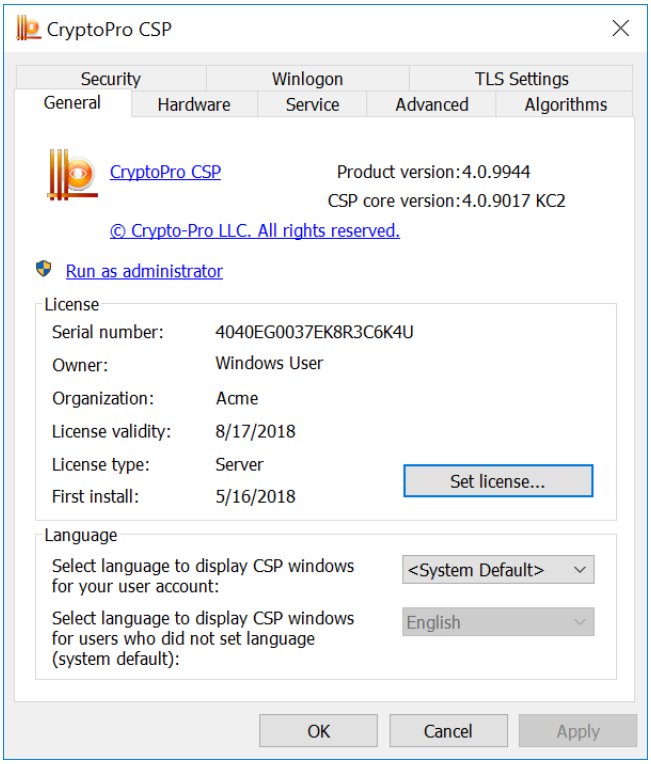


Figure 12. General tab

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.

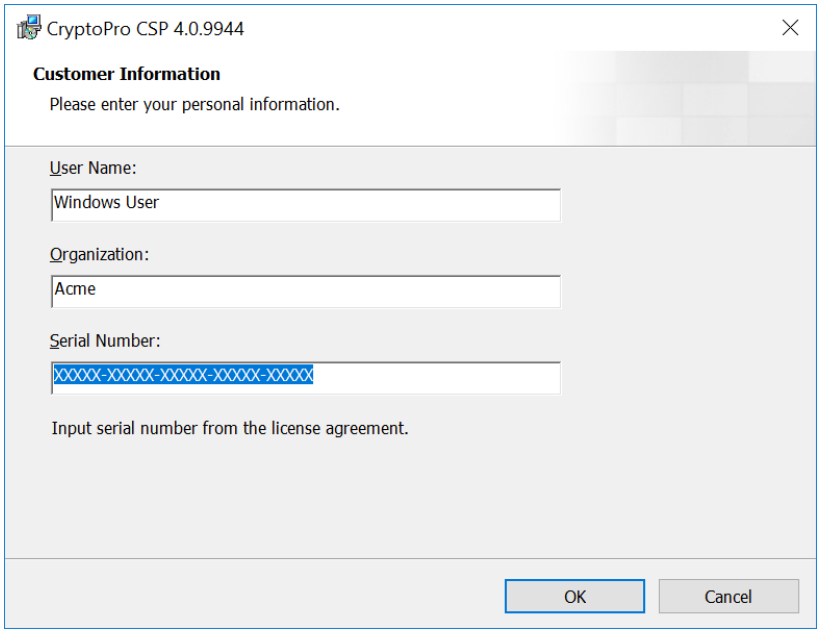


Figure 13. Customer information window

You can also enter the license number using the CryptoPro PKI license management snap-in (**Start** menu ⇒ **All Programs** ⇒ **Crypto-Pro** ⇒ **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.

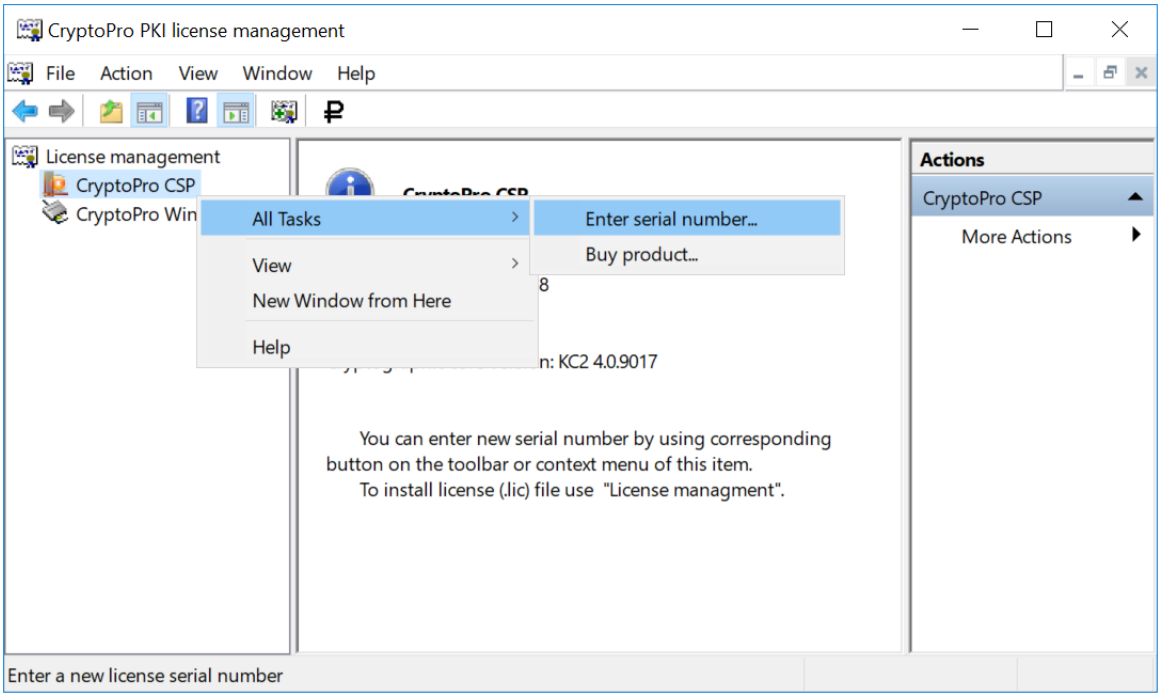


Figure 14. «CryptoPro PKI license management» snap-in

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 KC2 security level, you can add a a «Registry» reader, biological RNG or the «Sable» hardware RNG during the installation process.

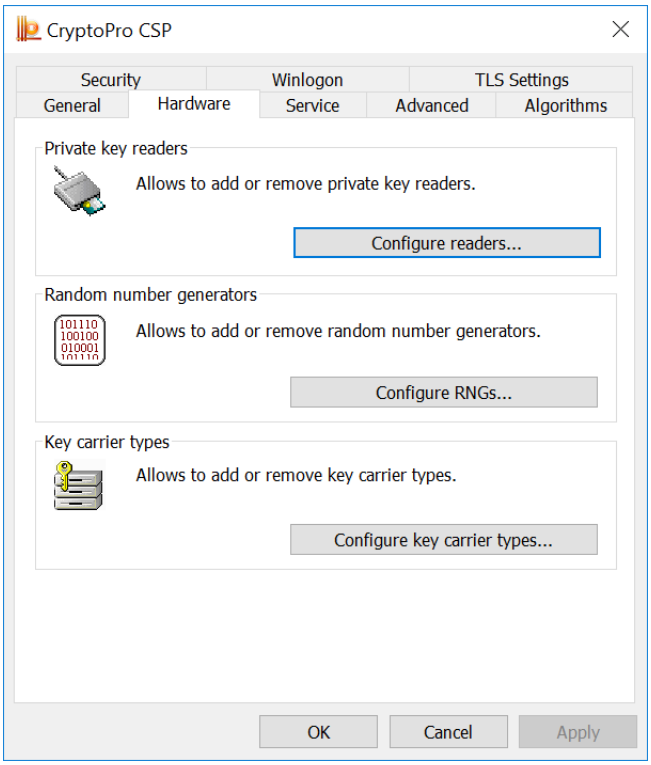


Figure 15. Hardware tab

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).

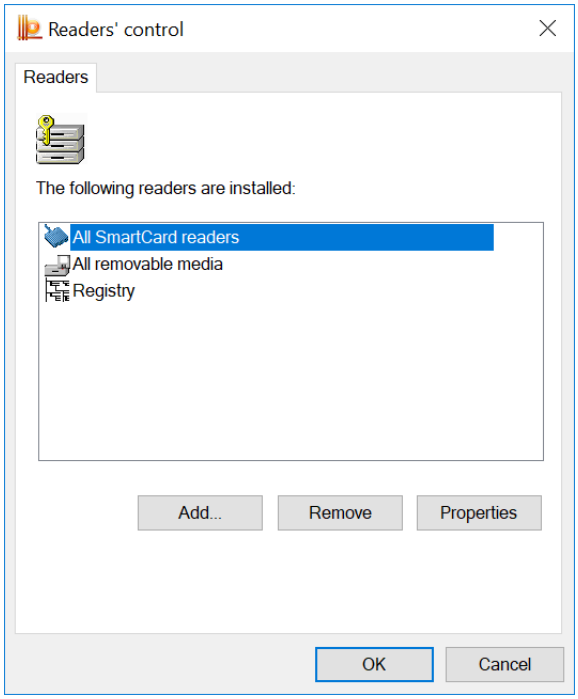


Figure 16. Readers' control window

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**.

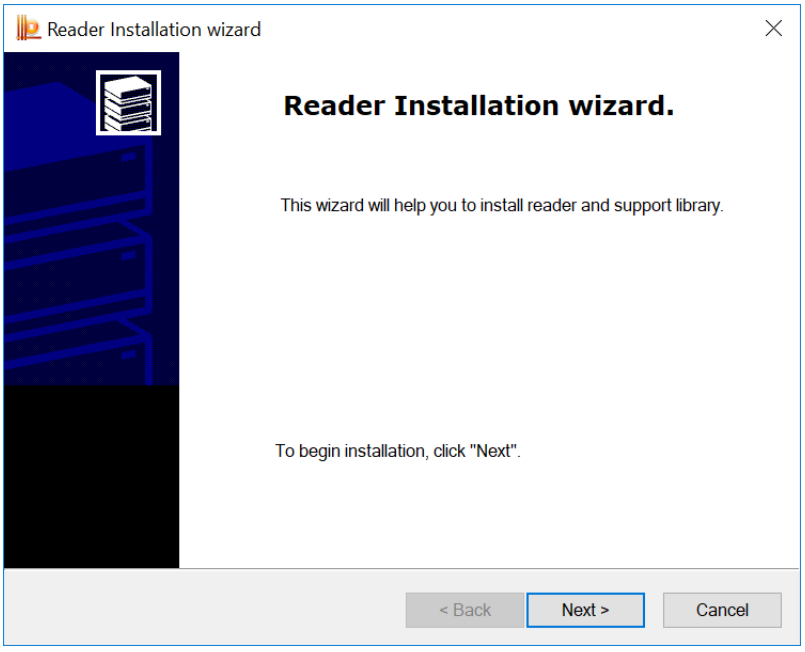


Figure 17. Reader Installation Wizard

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

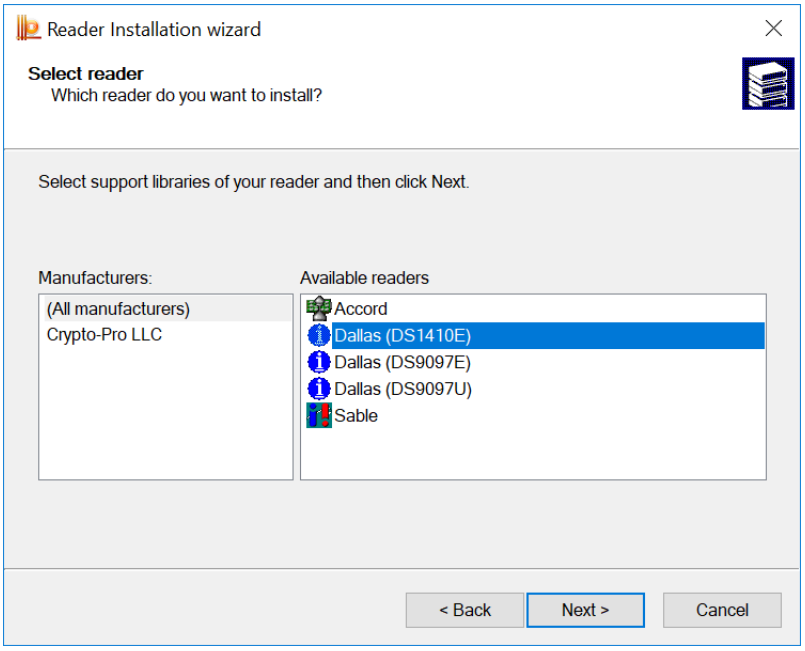


Figure 18. Choosing a reader

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).

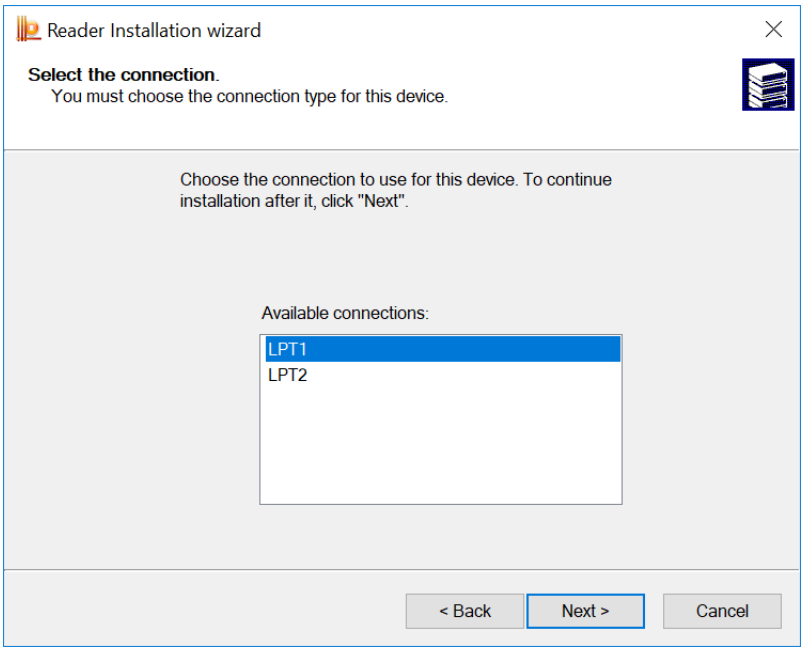


Figure 19. Choosing the reader connection

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

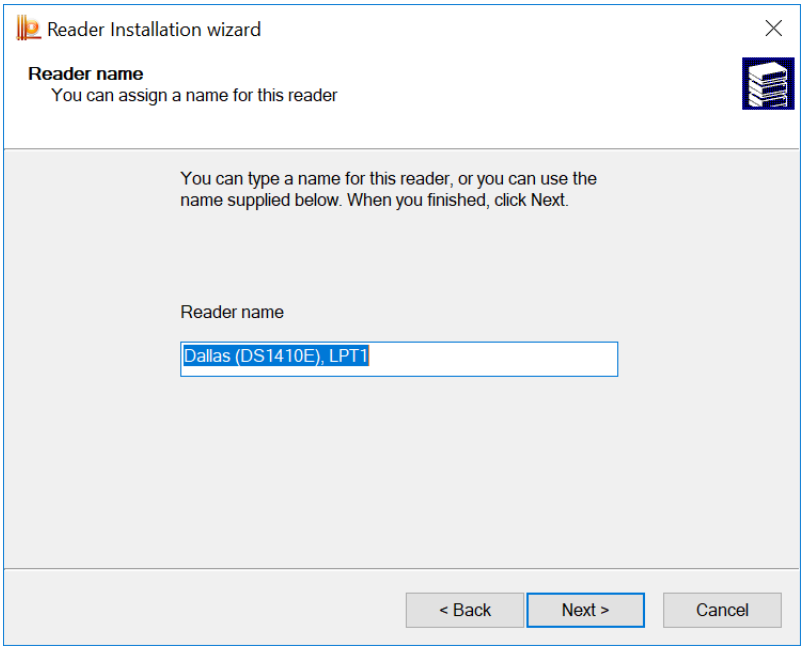


Figure 20. Setting the reader name

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.

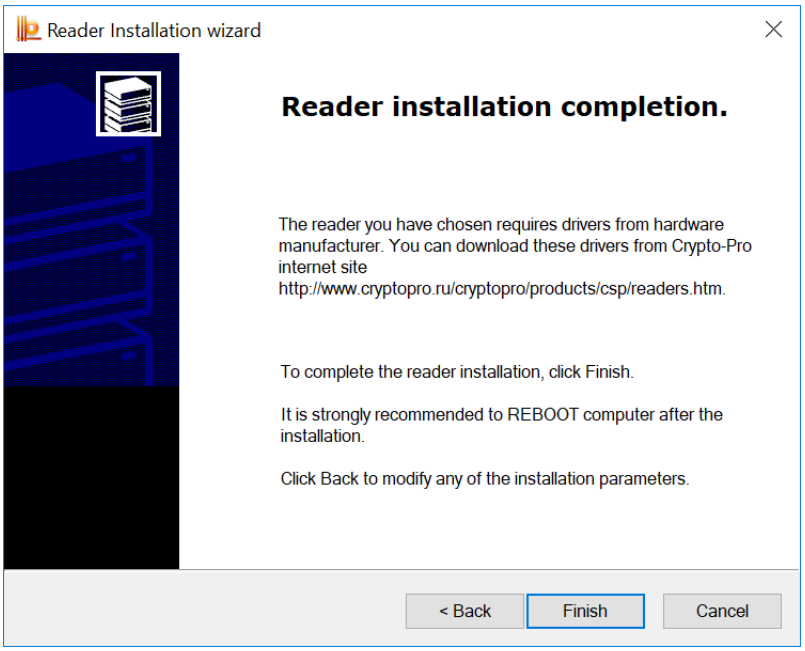


Figure 21. Reader installation completion

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).

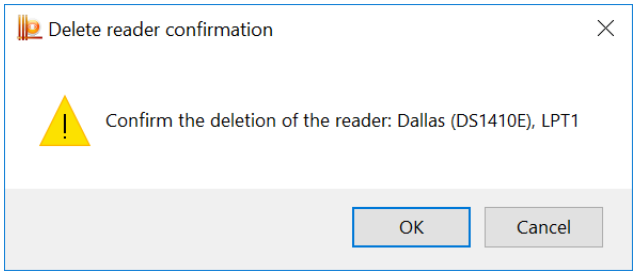


Figure 22. The reader deletion confirmation window

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).

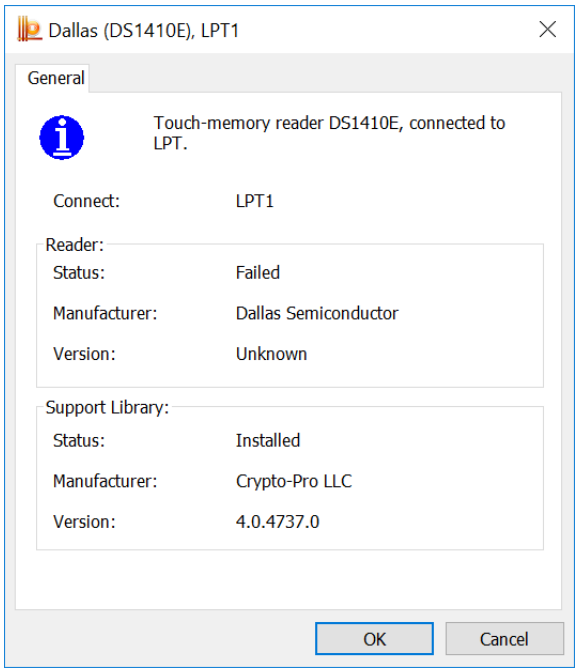


Figure 23. The reader properties window

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).

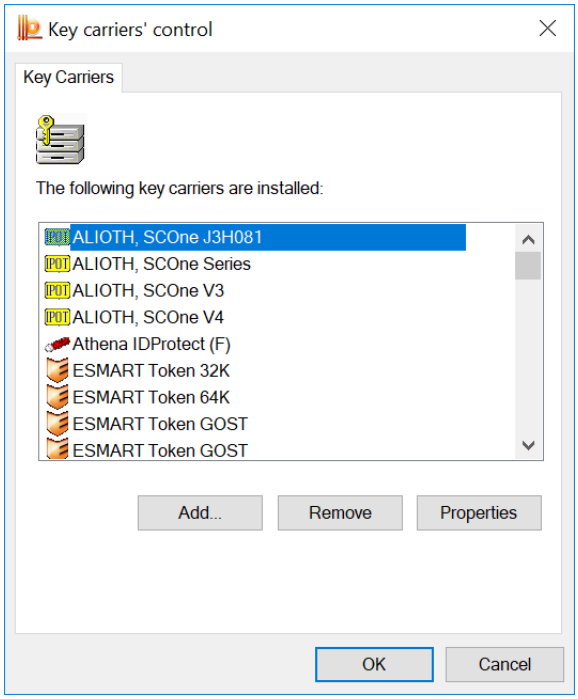


Figure 24. Key carriers' control window

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**.

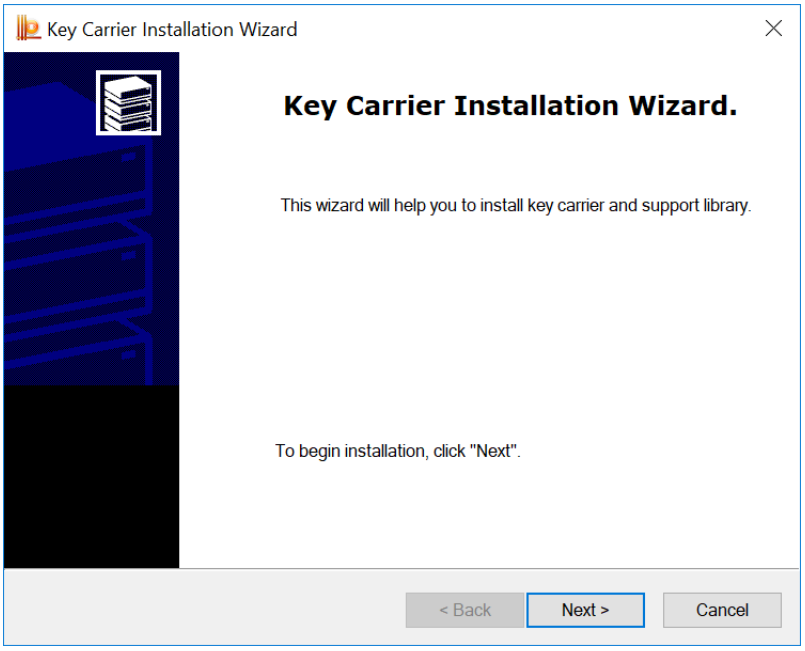


Figure 25. Key Carrier Installation Wizard

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

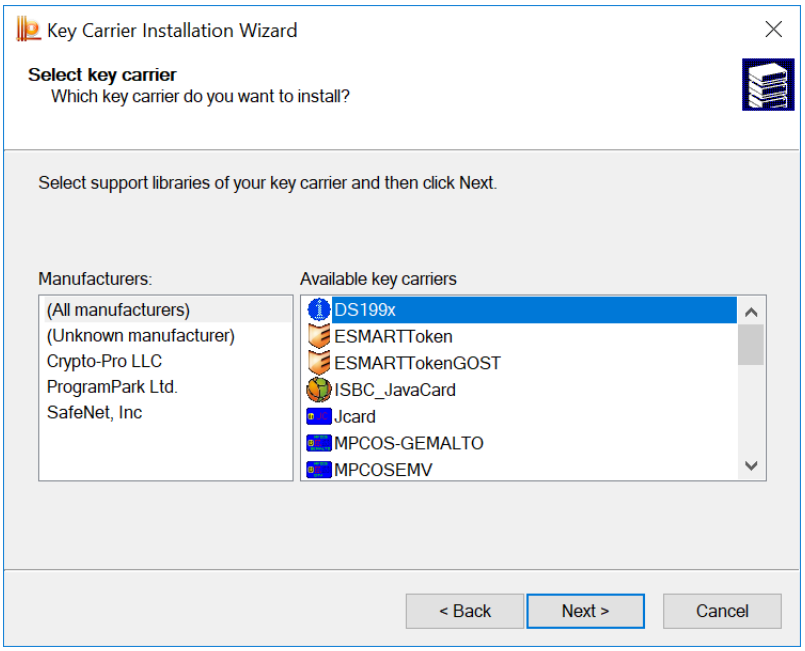


Figure 26. Choosing a carrier type

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

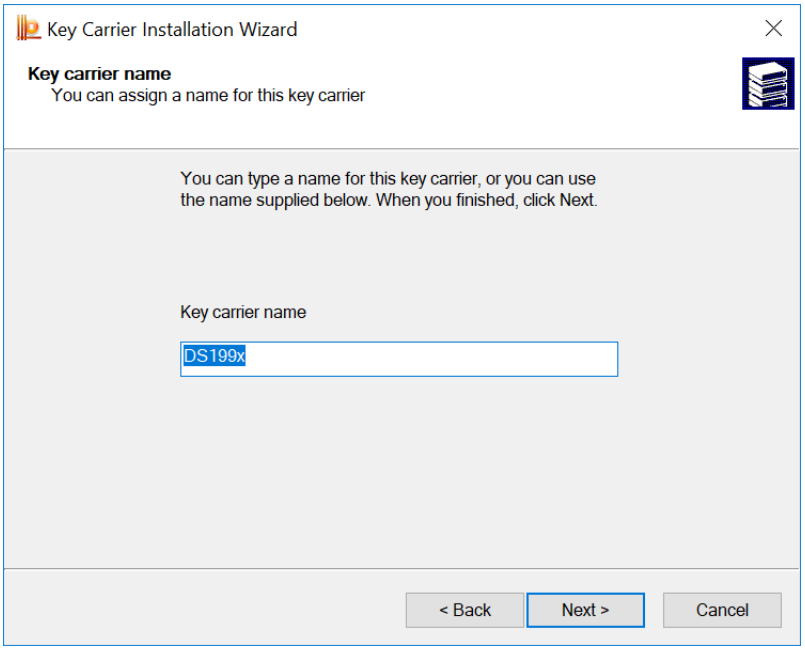


Figure 27. Setting the carrier name

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.

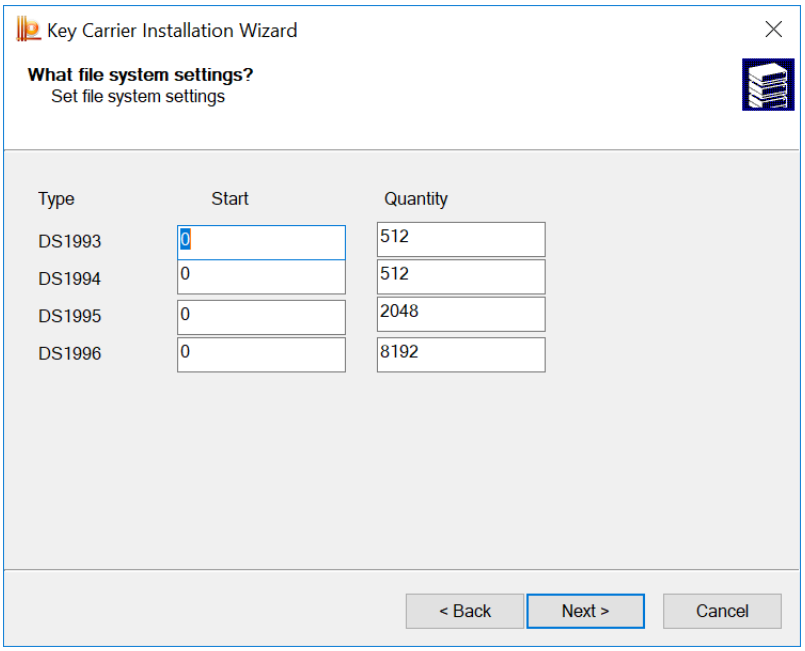


Figure 28. The carrier parameters setting

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

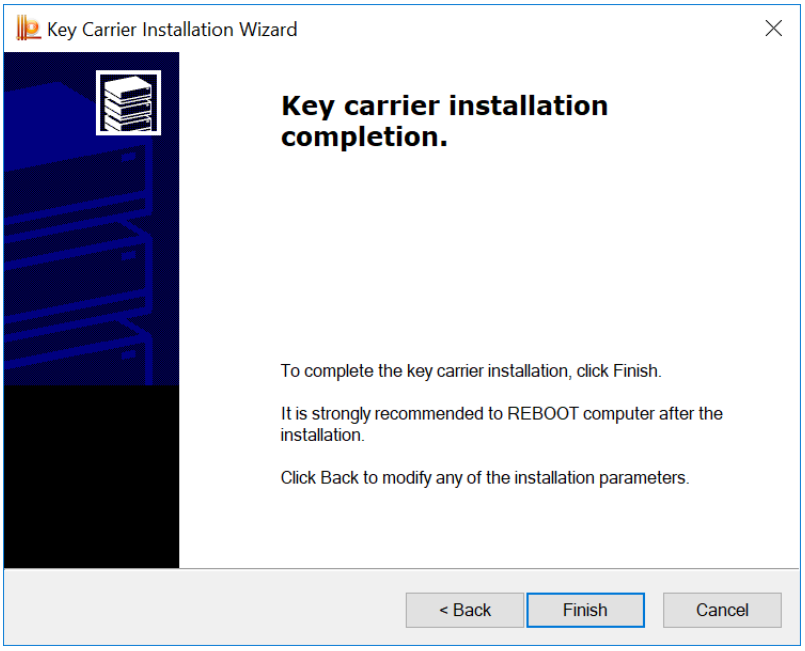


Figure 29. Key carrier installation completion

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).

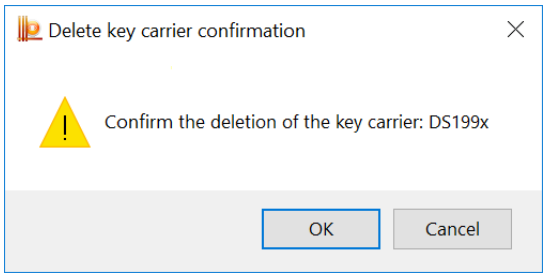


Figure 30. The carrier deletion confirmation window

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.

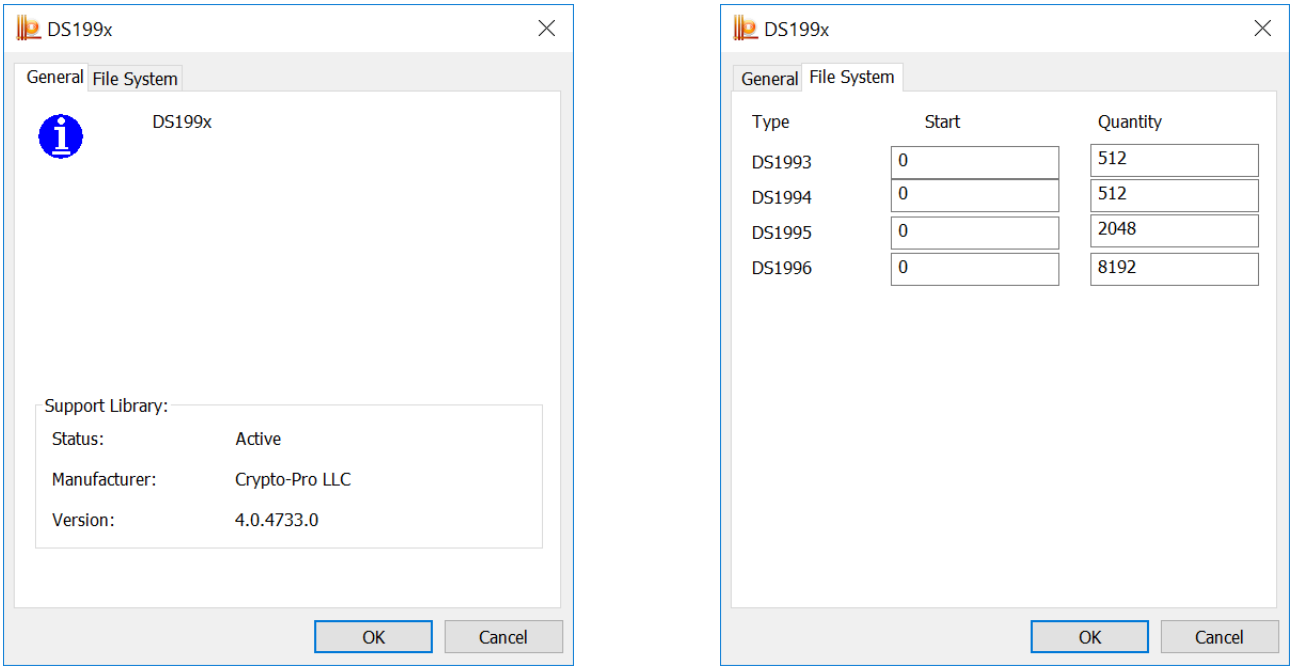


Figure 31. The carrier properties window

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 and .

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).

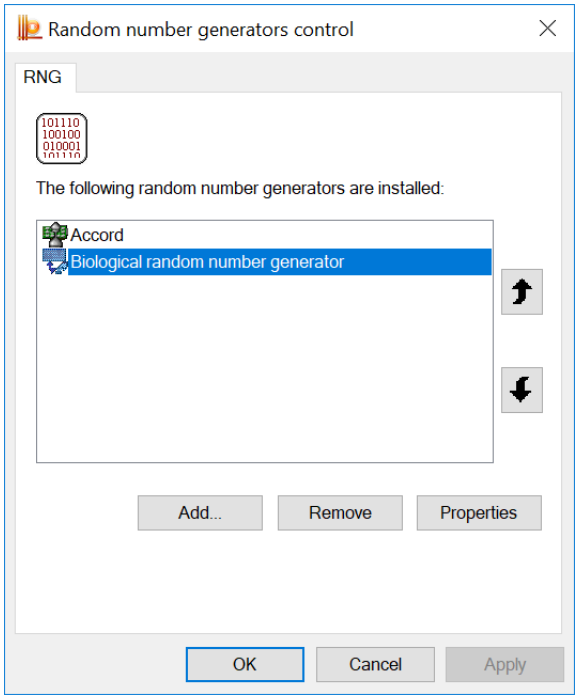


Figure 32. Random number generator control window

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**.

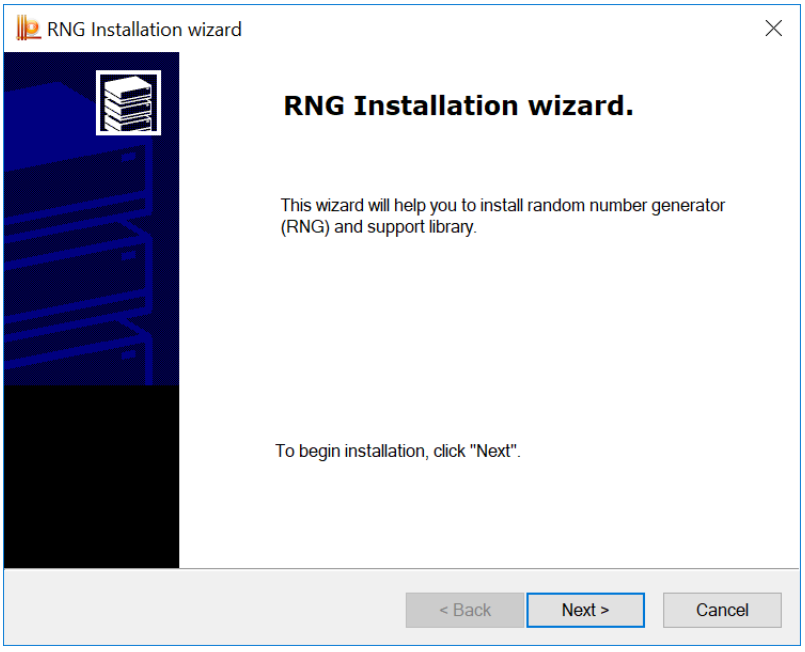


Figure 33. RNG Installation Wizard

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

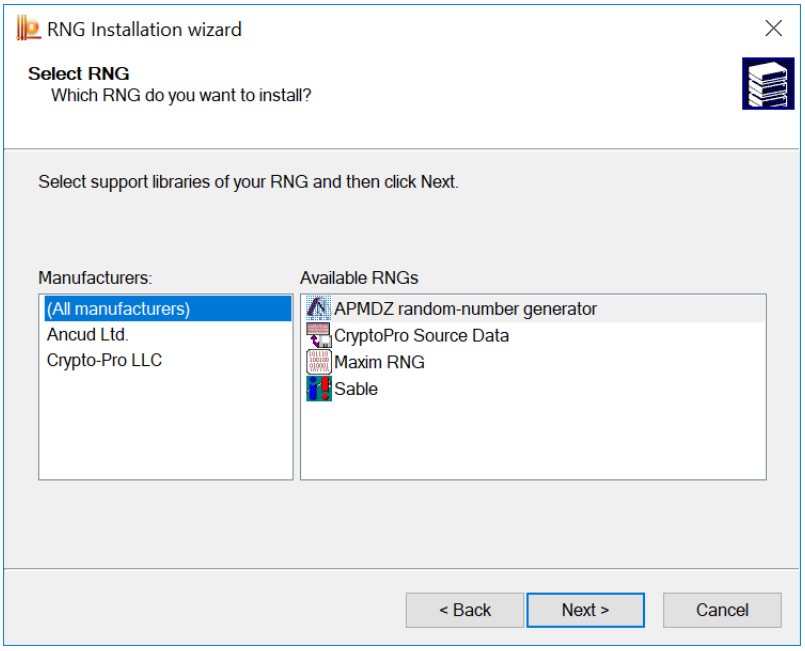


Figure 34. Choosing a RNG type

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

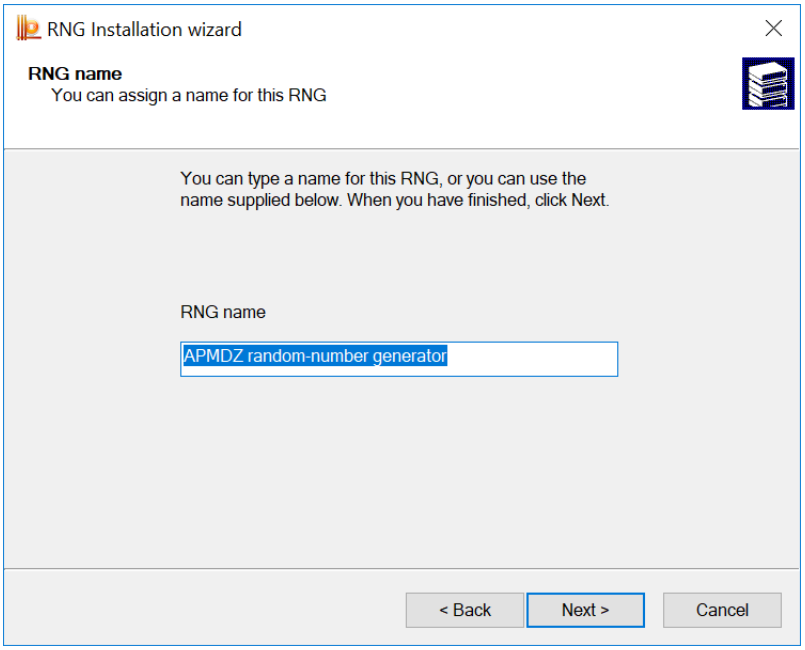


Figure 35. Setting the RNG name

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

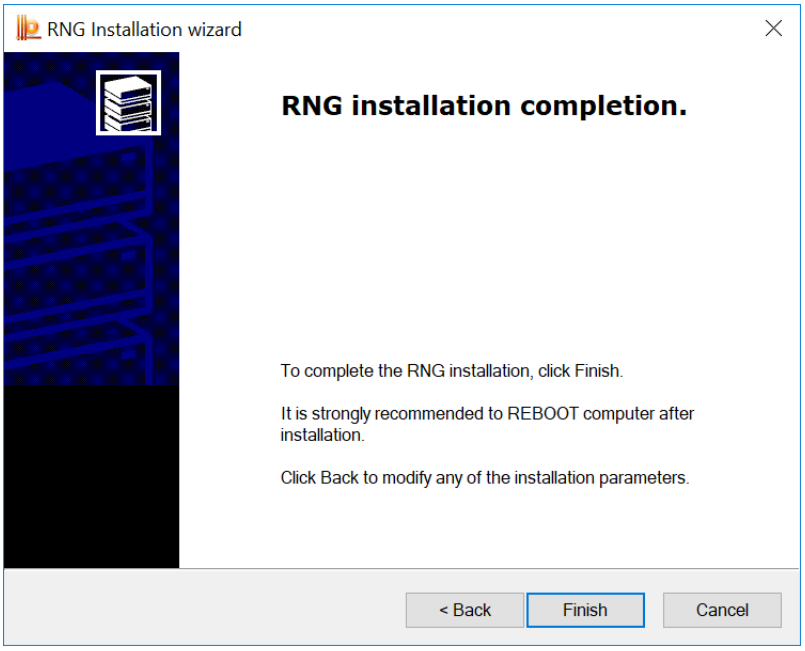


Figure 36. RNG installation completion

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).

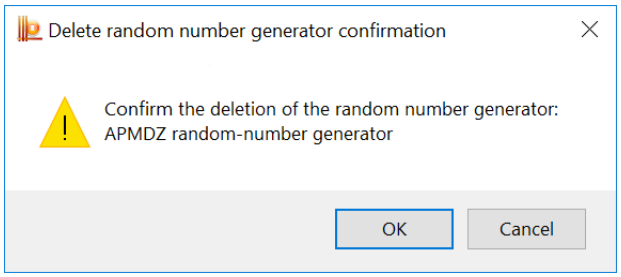


Figure 37. RNG deletion confirmation window

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).

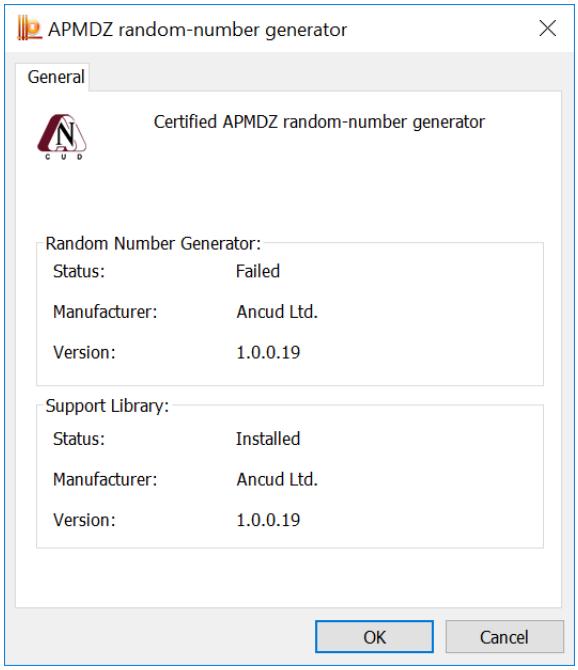


Figure 38. RNG properties window

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.

Note. To perform operations with certificates (and corresponding containers) stored in the Local Computer certificate storage the CSP control panel must be run with administrator privileges.

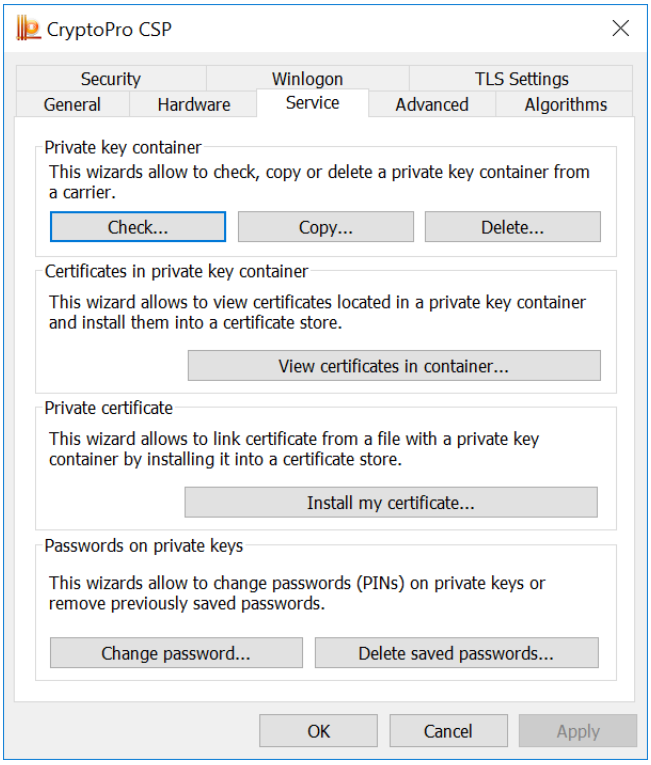


Figure 39. Service tab

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).

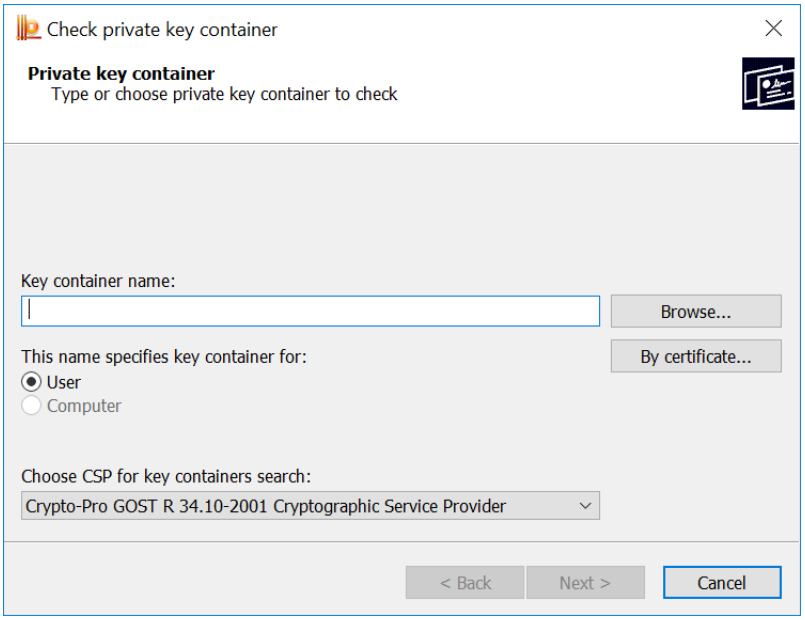


Figure 40. Check private key container window

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**.

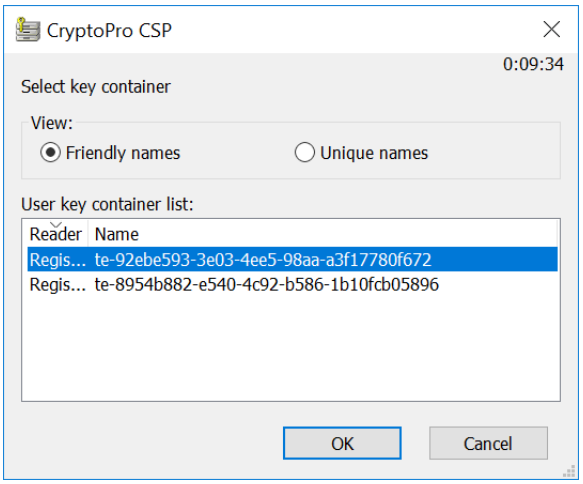


Figure 41. Selecting a key container

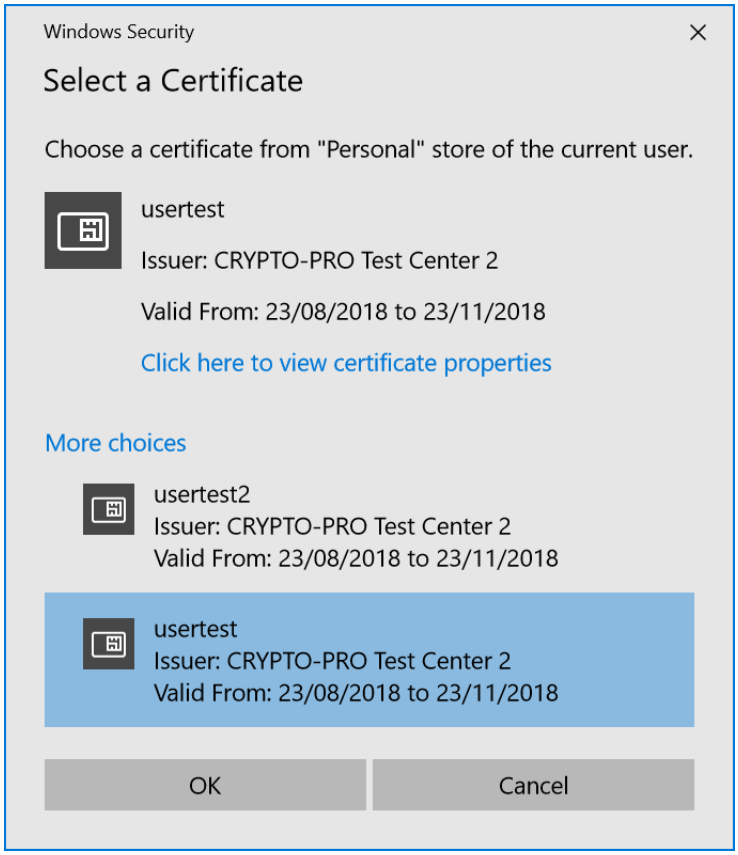


Figure 42. Selecting a certificate

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**.

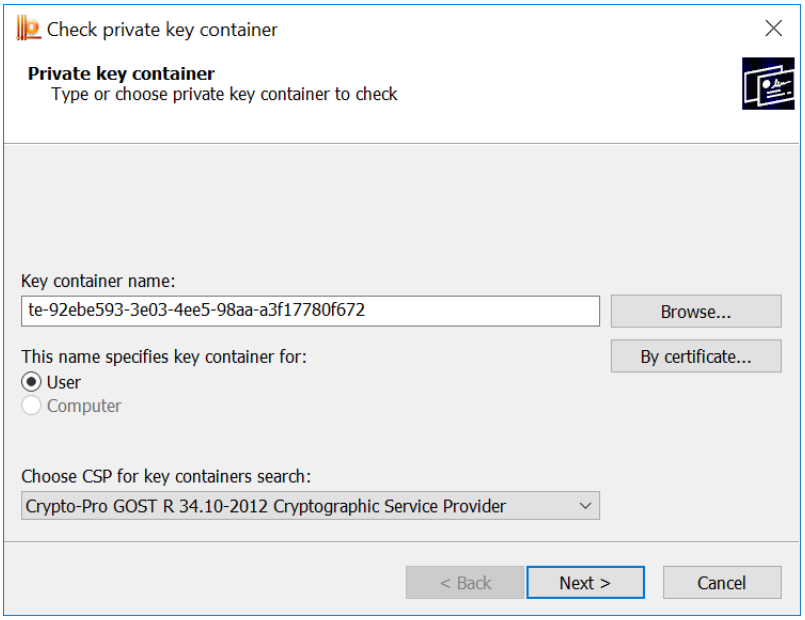


Figure 43. Filing in Check private key container form

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.

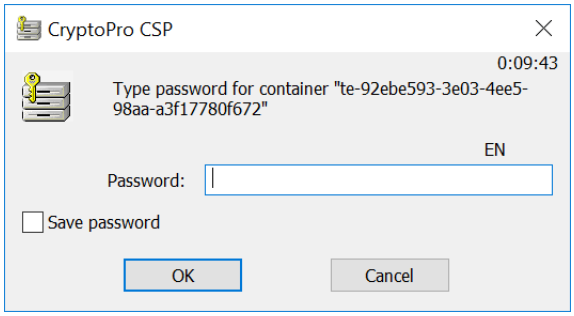


Figure 44. Entering a container password

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

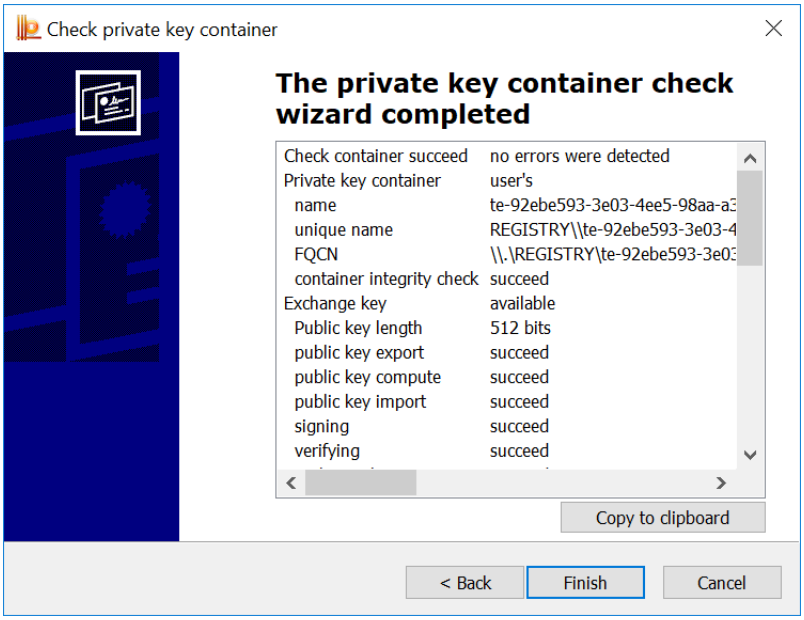


Figure 45. Key container check results

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**.

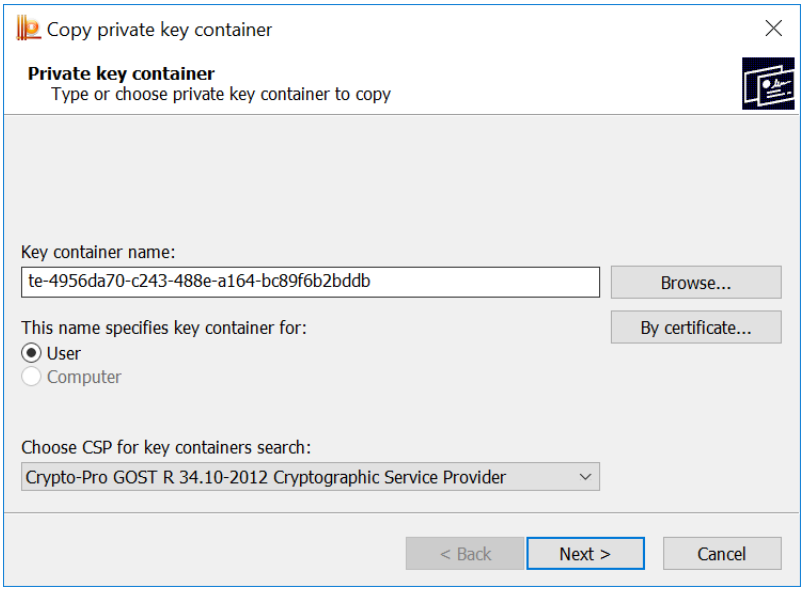


Figure 46. Copy private key container window

If a password is set for the selected container, it will be requested in the password input window. Enter the password and click **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.

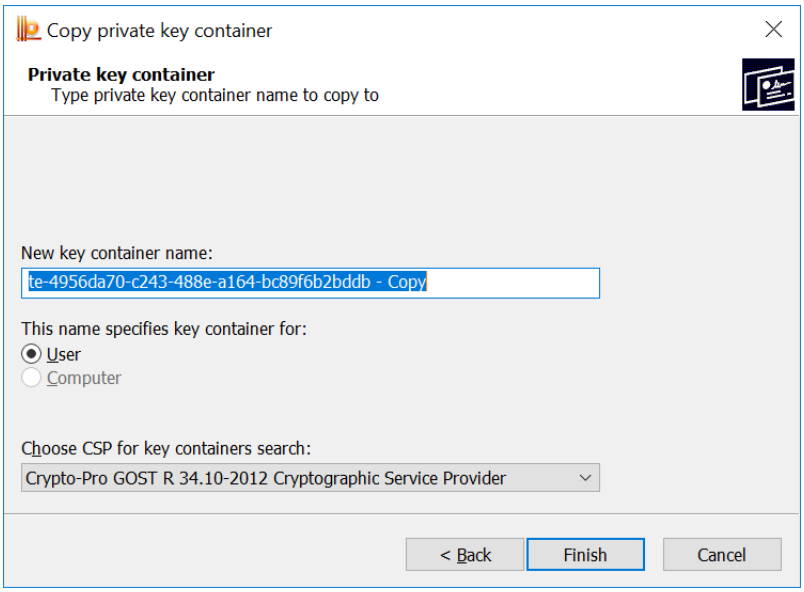


Figure 47. Setting a name for the new key container

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

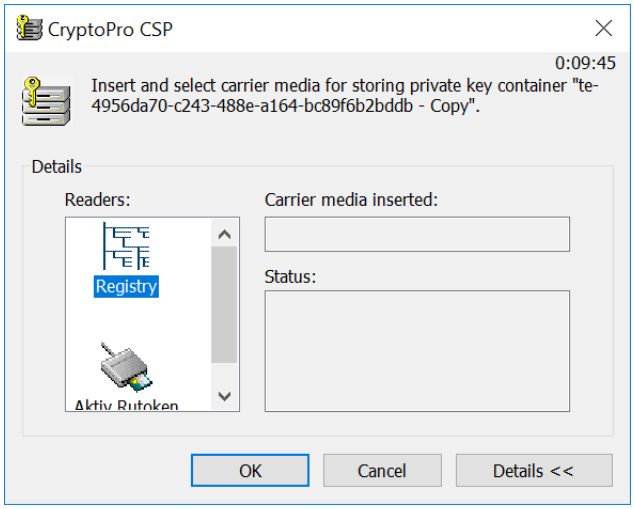


Figure 48. Choosing the carrier for the new key container

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).

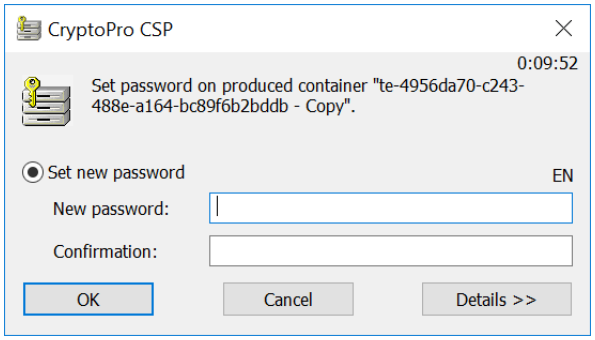


Figure 49. Setting a password for the produced container

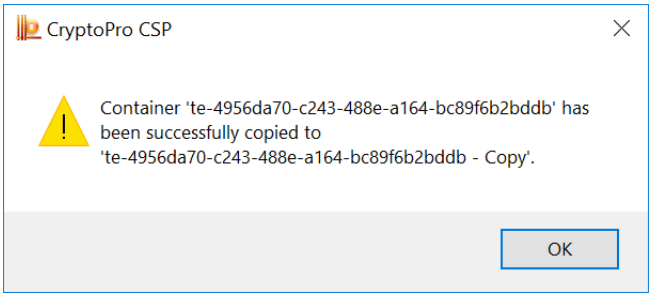


Figure 50. Successful container copy completion

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).

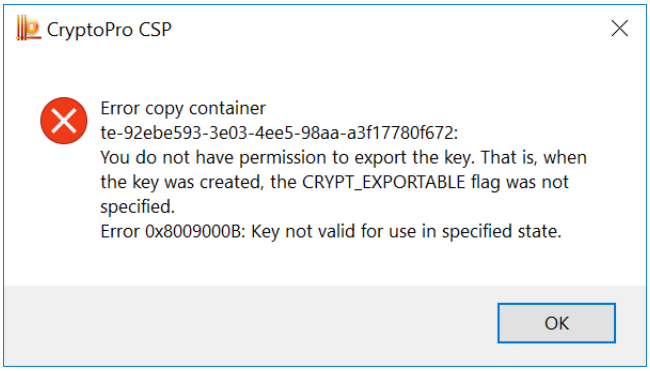


Figure 51. Container copy error message

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**.

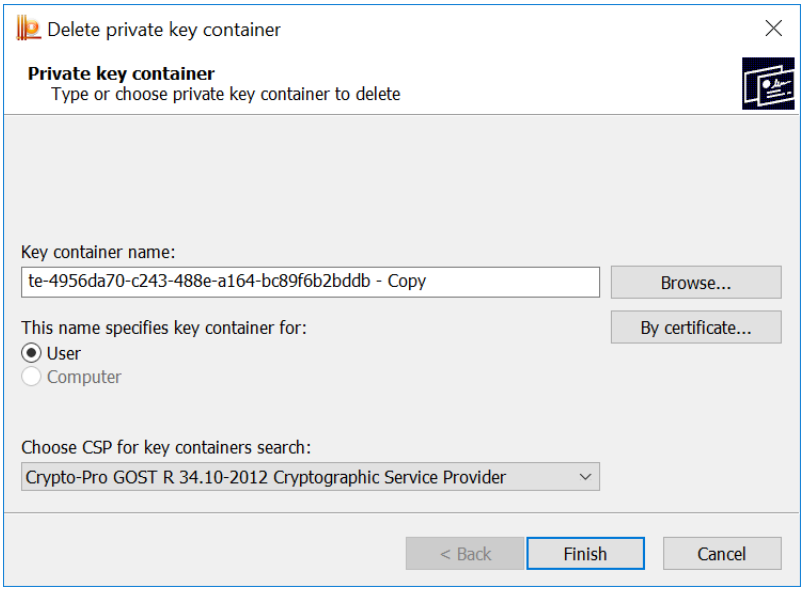


Figure 52. Delete private key container window

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

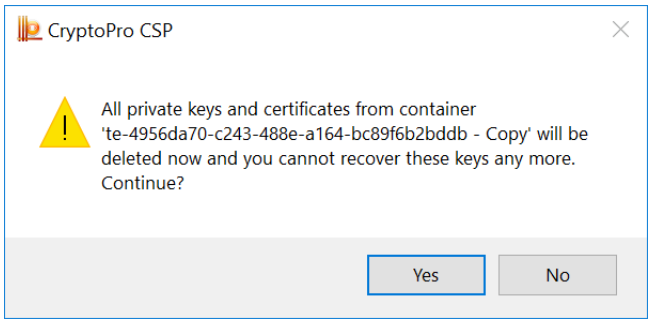


Figure 53. The key container deletion confirmation window

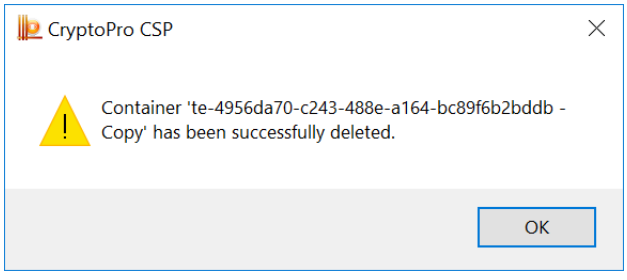


Figure 54. Successful container delete completion

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).

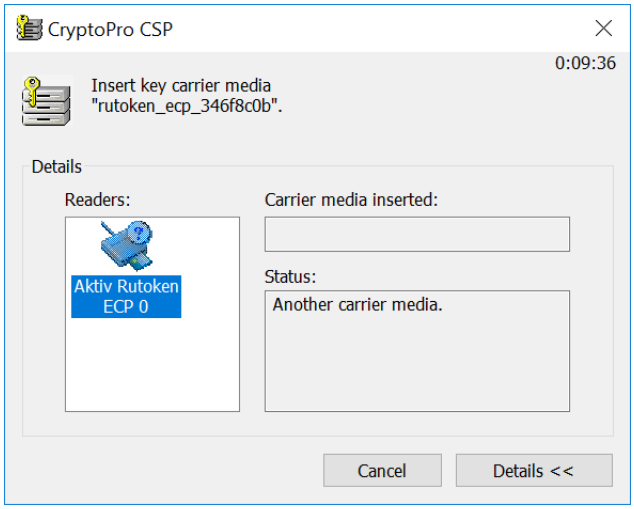


Figure 55. Key carrier media request

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.

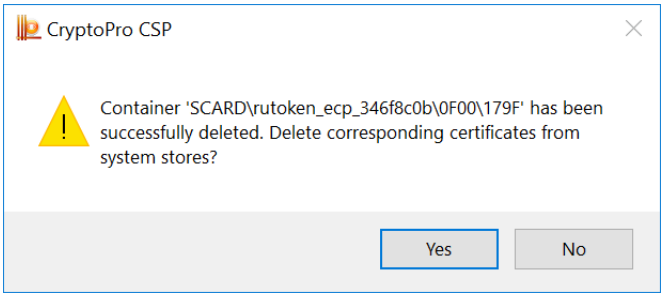


Figure 56. Successful container delete completion

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**.

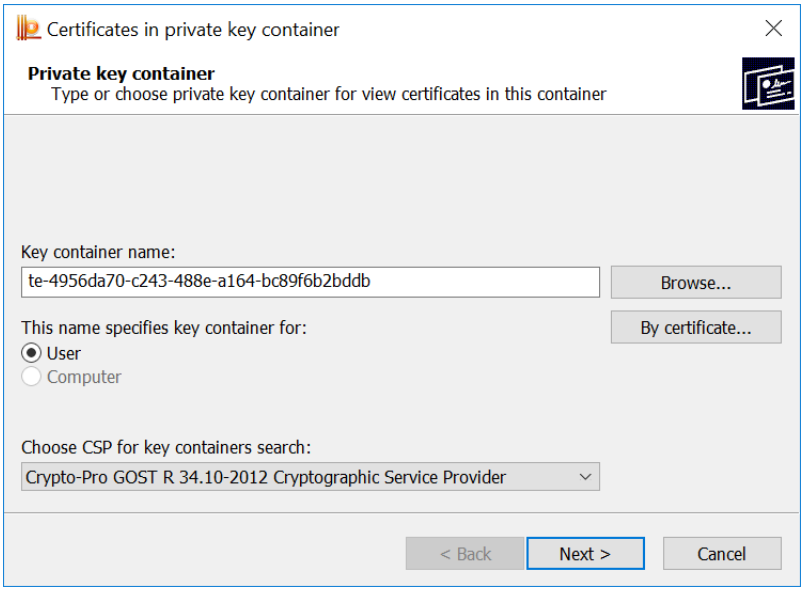


Figure 57. Certificates in private key container window

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

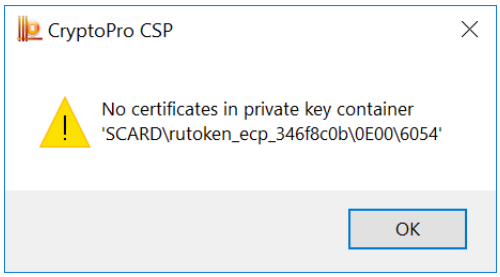


Figure 58. No certificates in private key container

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

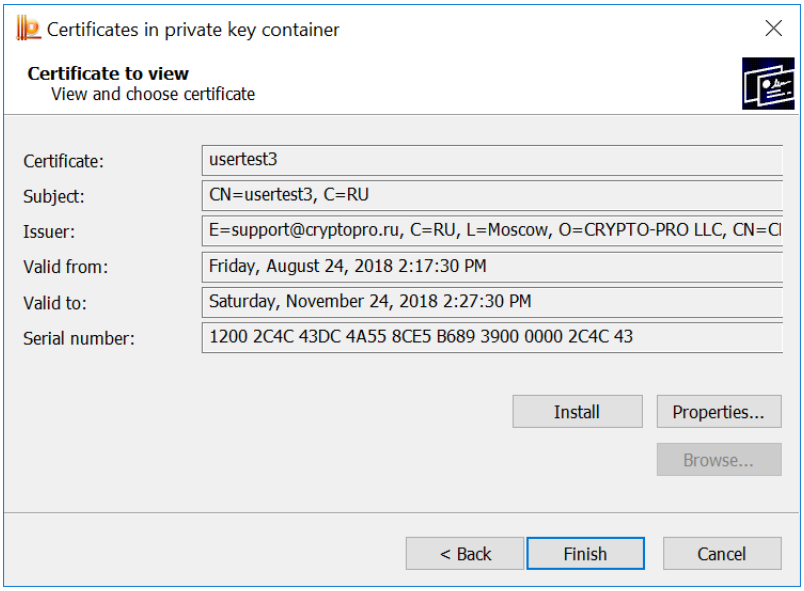


Figure 59. Certificates in the private key container

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.

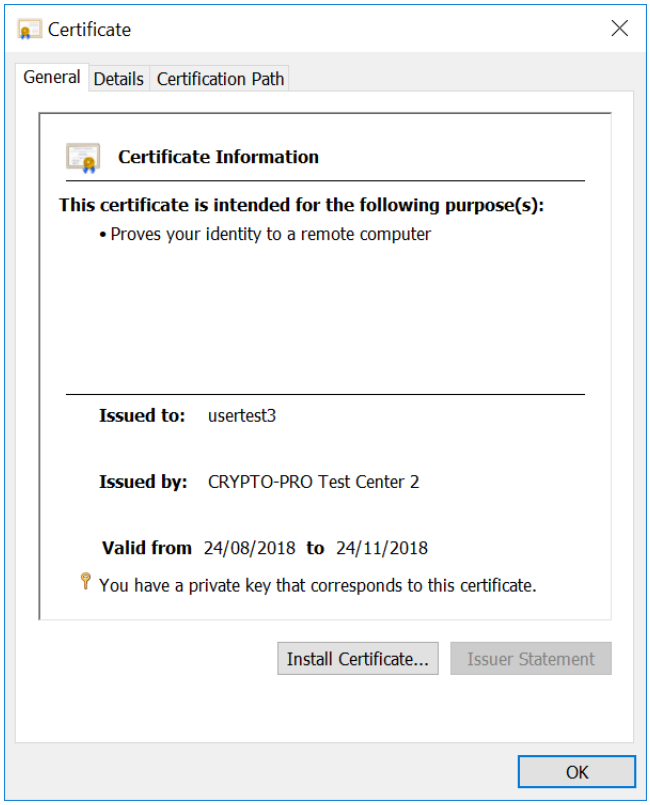


Figure 60. Certificate properties

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).

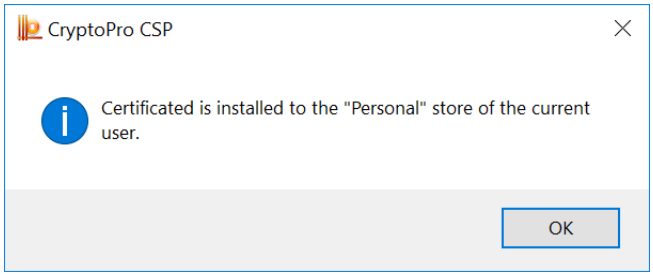


Figure 61. Successful certificate installation completion

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).

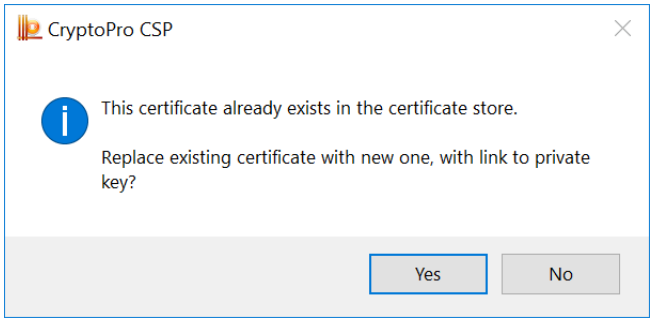


Figure 62. Replace the certificate in the store

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.

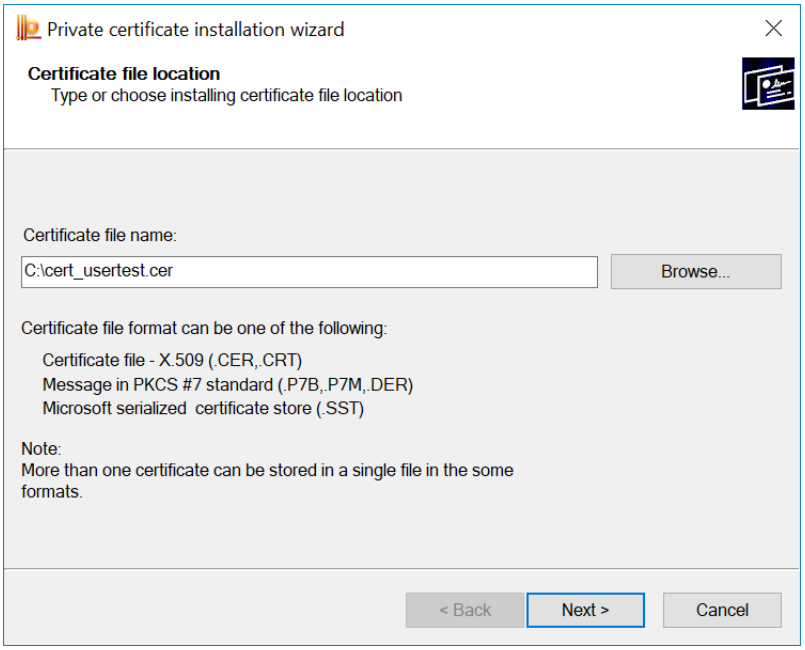


Figure 63. Private certificate installation wizard

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

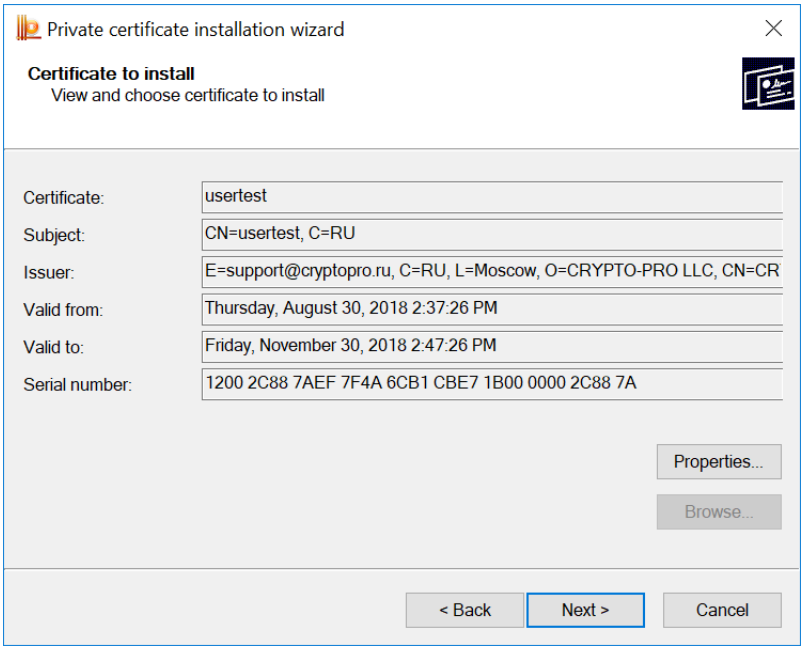


Figure 64. Choosing a certificate for installation

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).

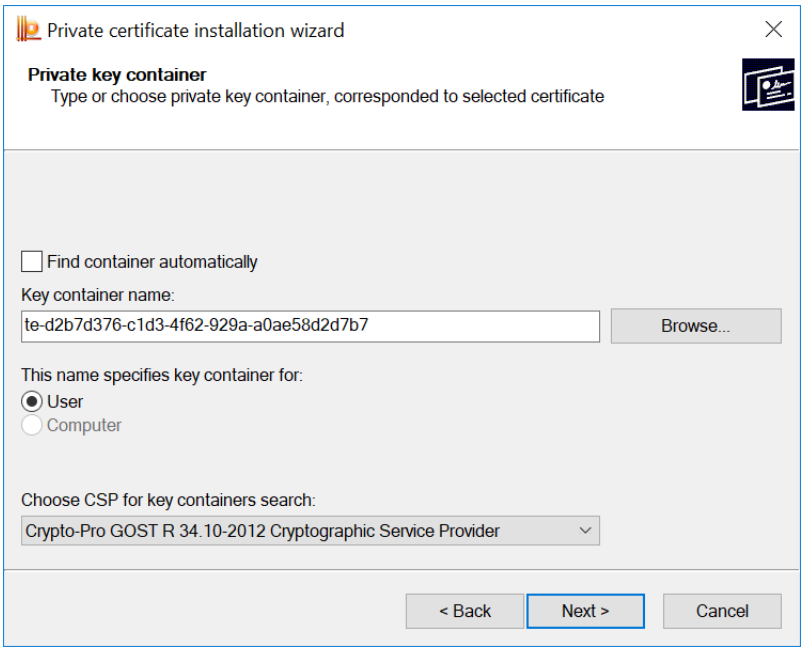


Figure 65. Choosing a private key container

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.

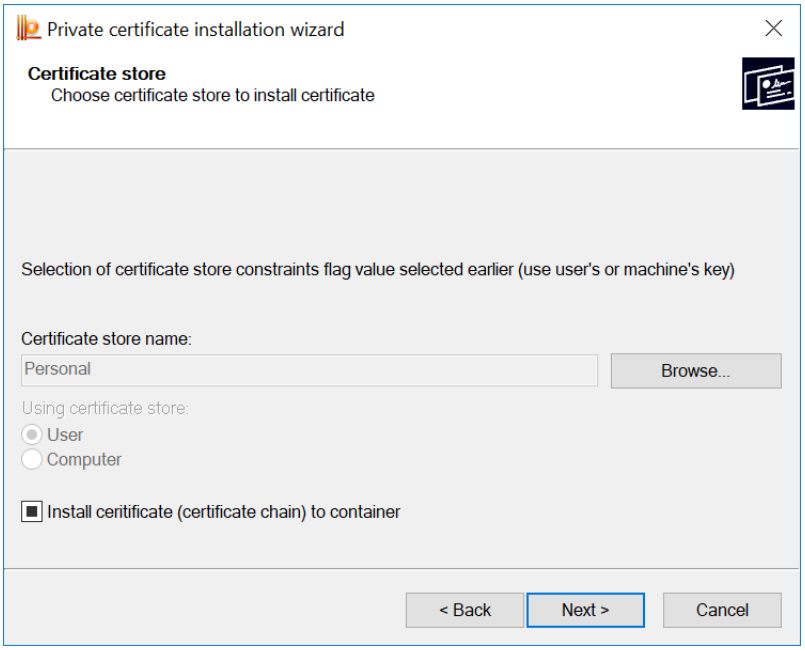


Figure 66. Choosing a certificate store

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

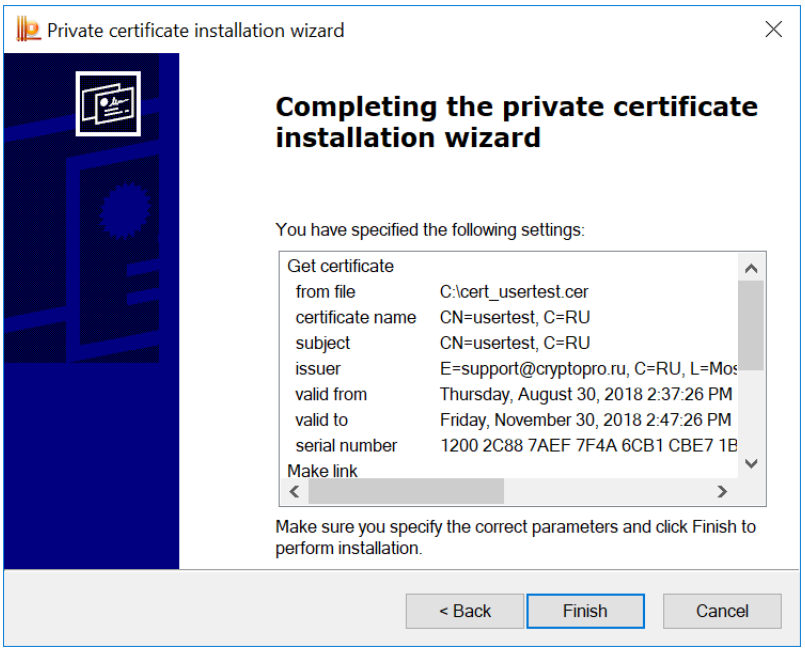


Figure 67. Private certificate installation wizard completion

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**.

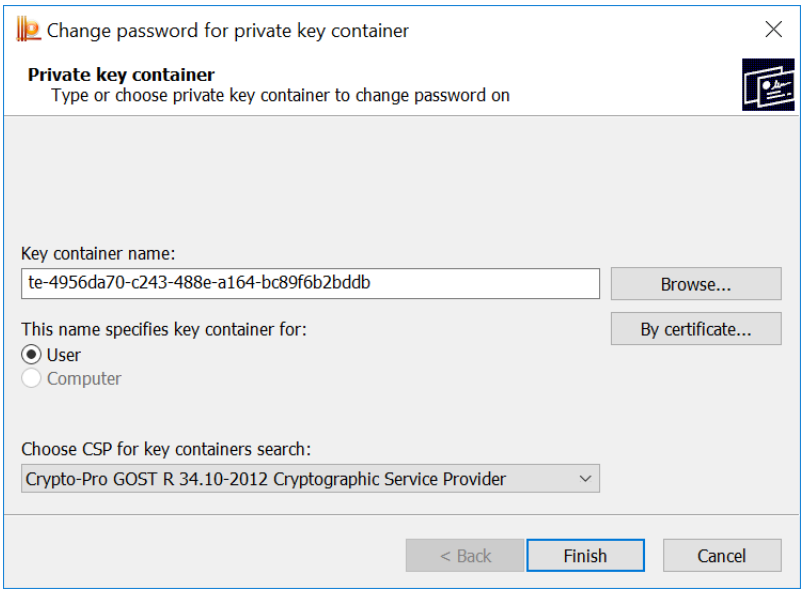


Figure 68. Change password for private key container

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.

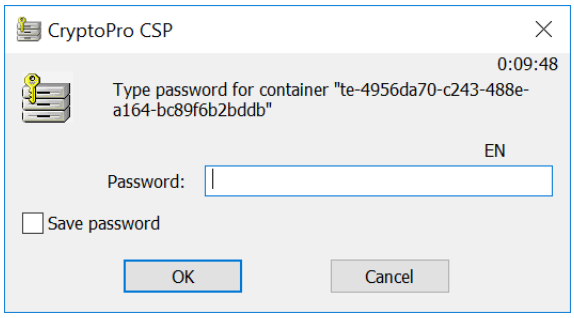


Figure 69. Entering the password

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.

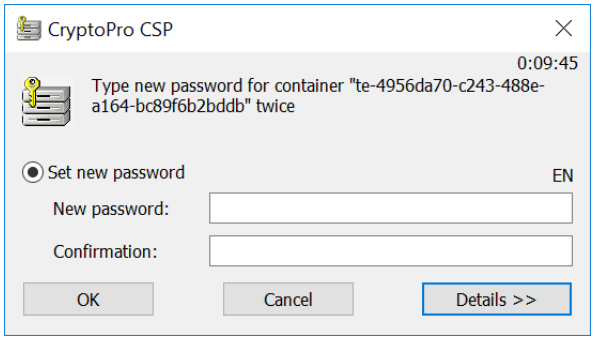


Figure 70. Setting the new password

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).

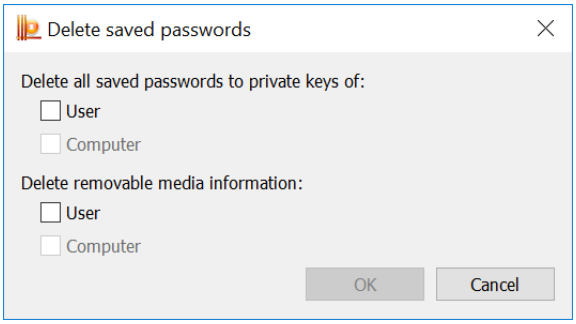


Figure 71. Delete saved passwords

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).

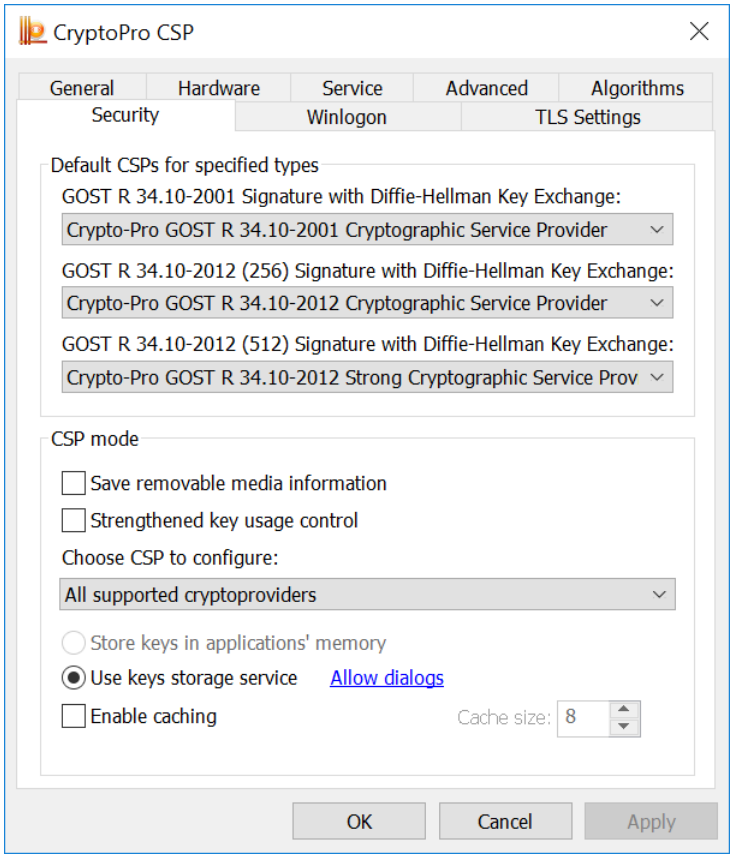


Figure 72. Security tab

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 KC2 security levels only the keys storage service operating mode is available.

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).

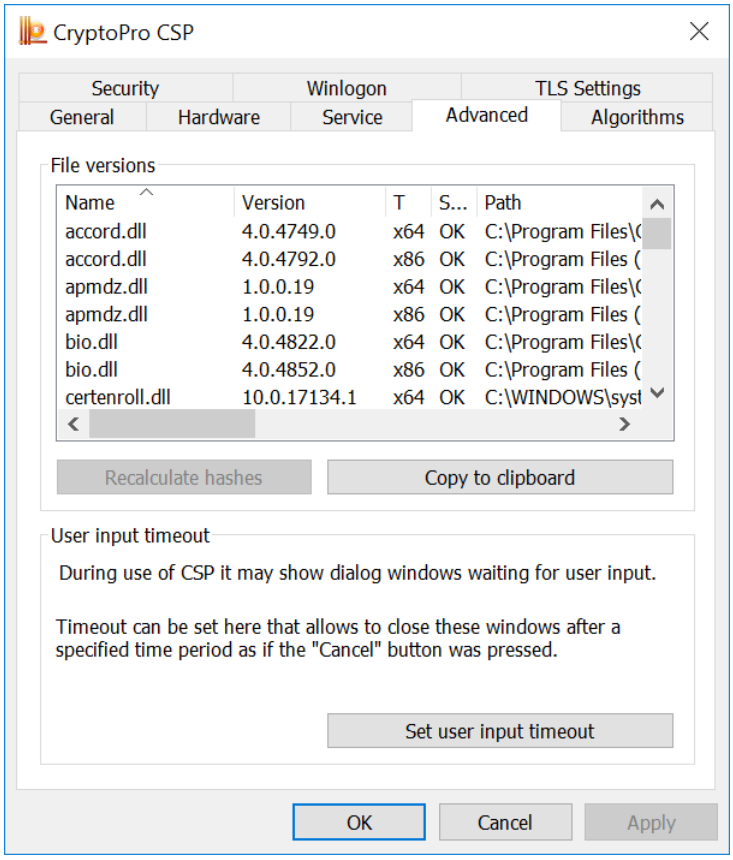


Figure 73. Advanced tab

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).

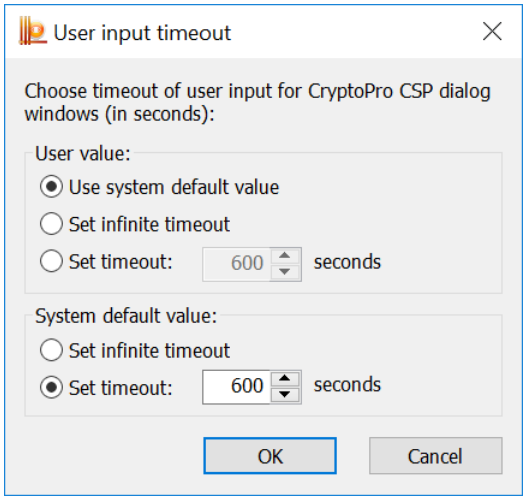


Figure 74. User input timeout

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).

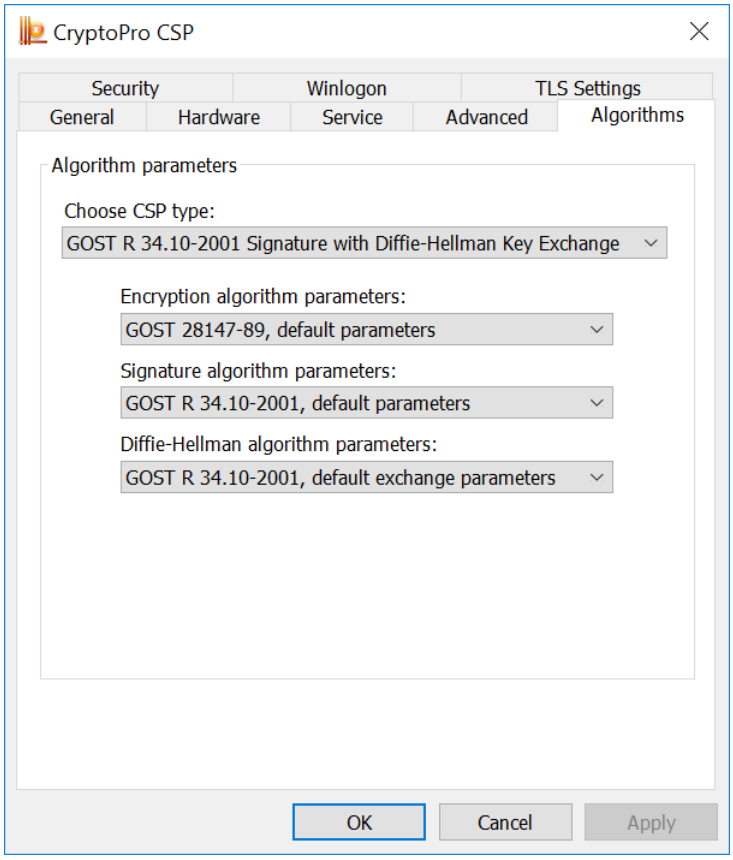


Figure 75. Algorithms tab

Note. For most uses of CryptoPro CSP, changing the parameters of the cryptographic algorithms used is not required. If the parameters are changed by users, the correct working of the CSP is not guaranteed.

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).

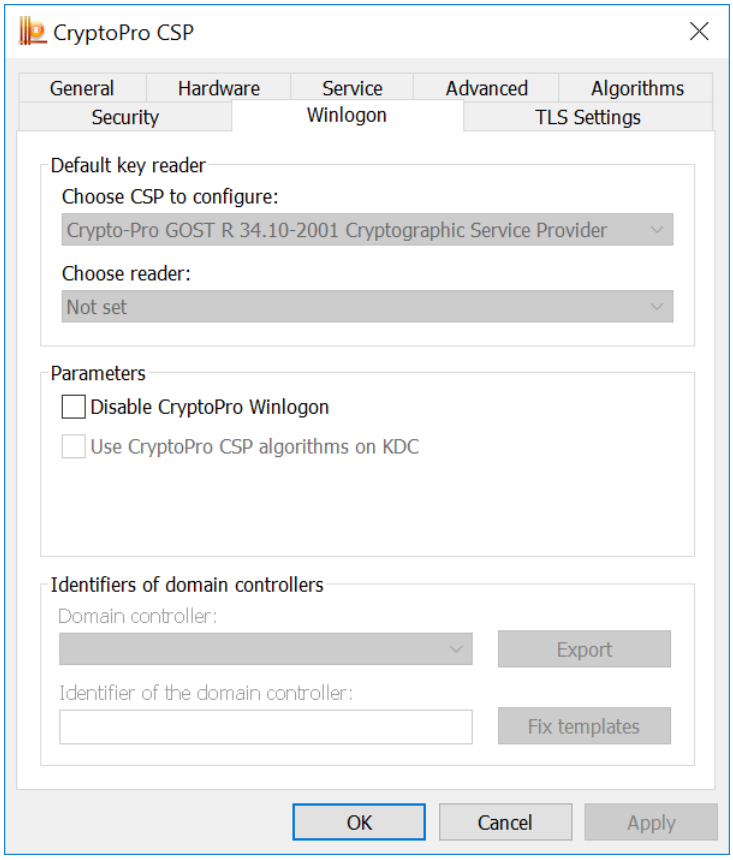


Figure 76. Winlogon tab

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).

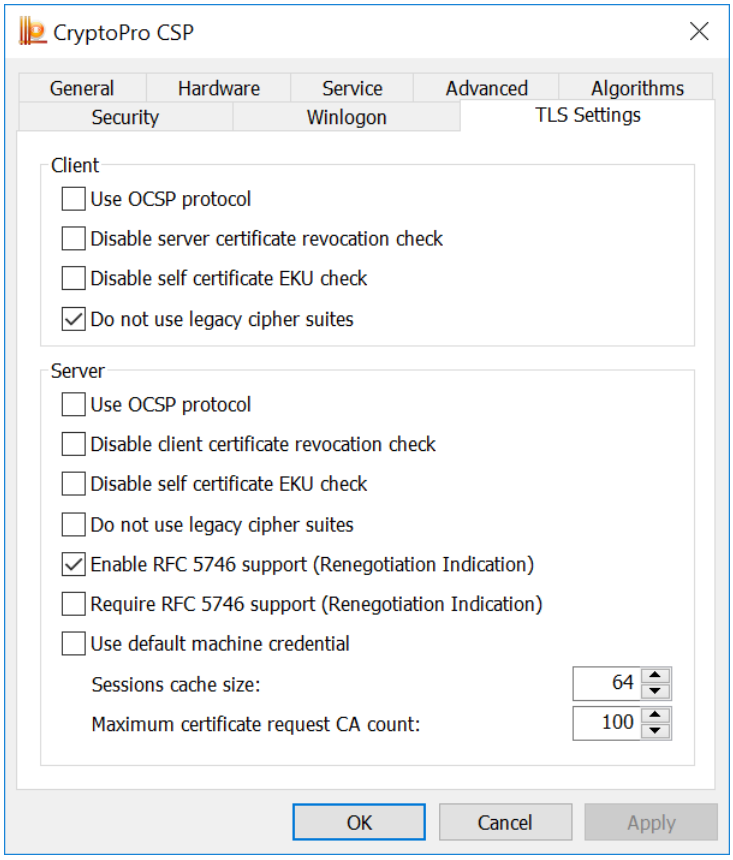


Figure 77. TLS settings tab

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;
- 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);
- 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).

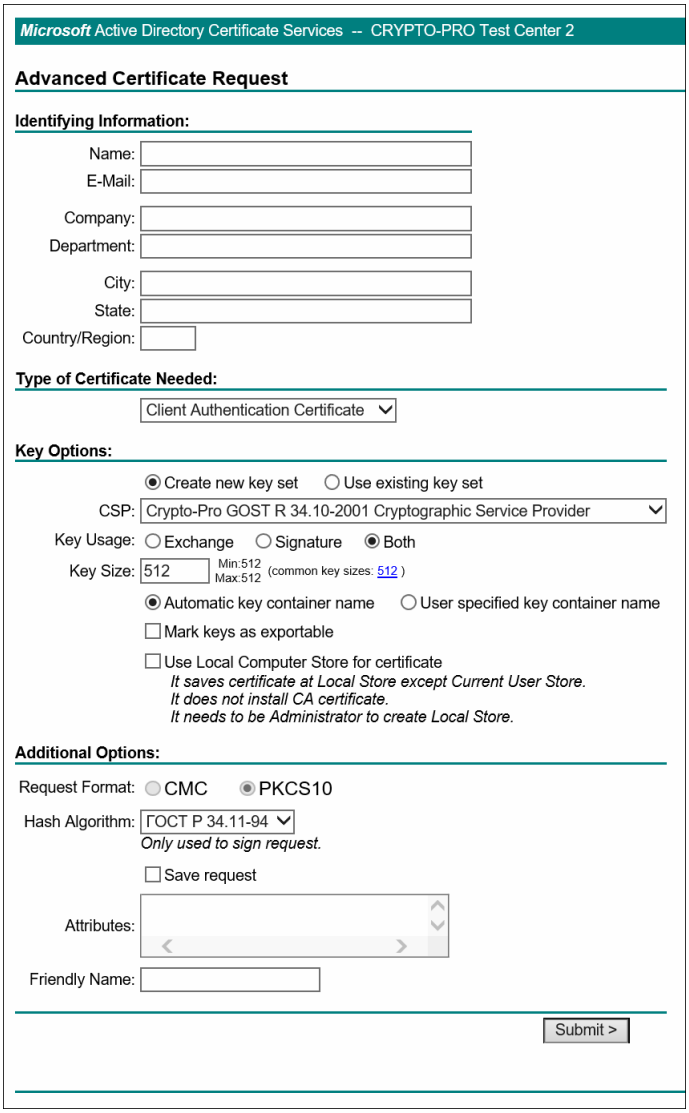


Figure 78. Advanced Certificate Request form

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 **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 **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).

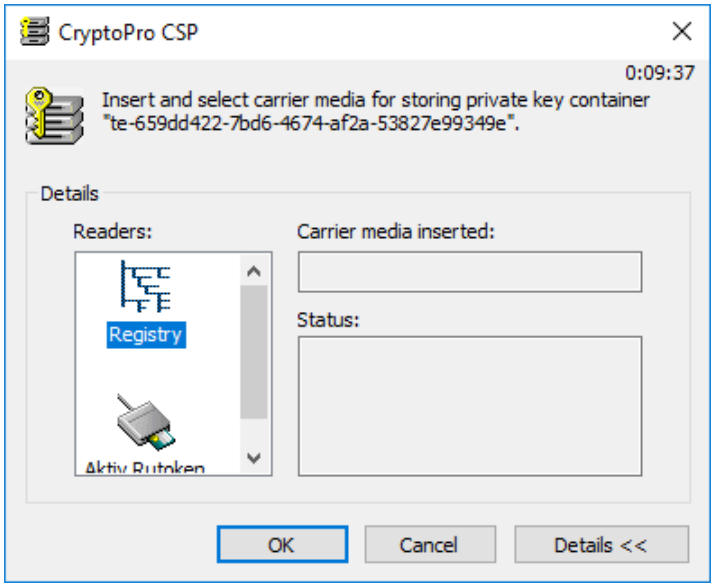


Figure 79. Choosing a key carrier

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).

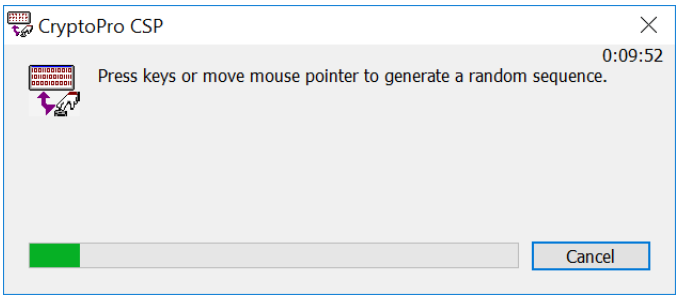


Figure 80. Biological RNG window

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).

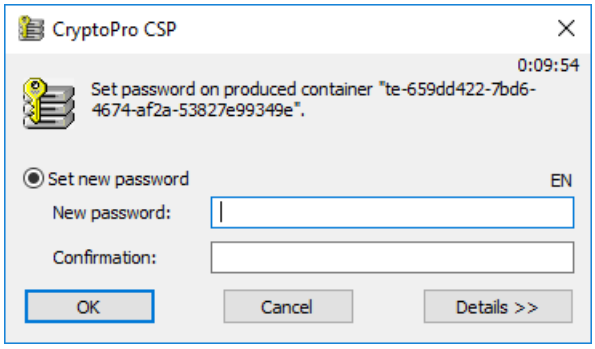


Figure 81. Setting the key container password

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).

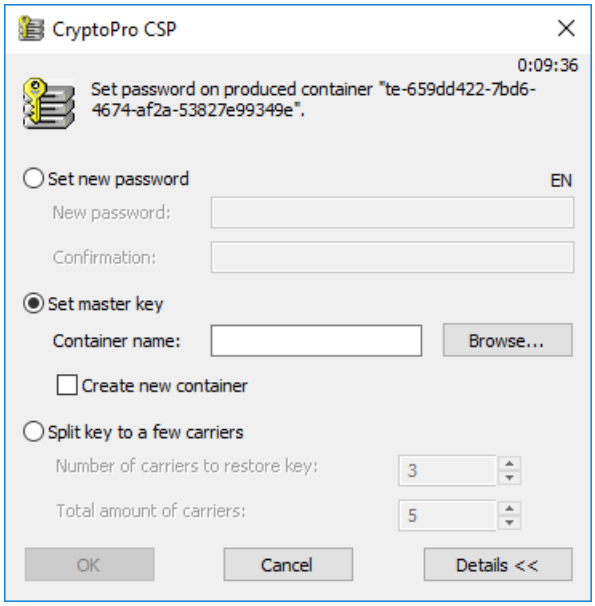


Figure 82. Selecting a key container authentication method

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.

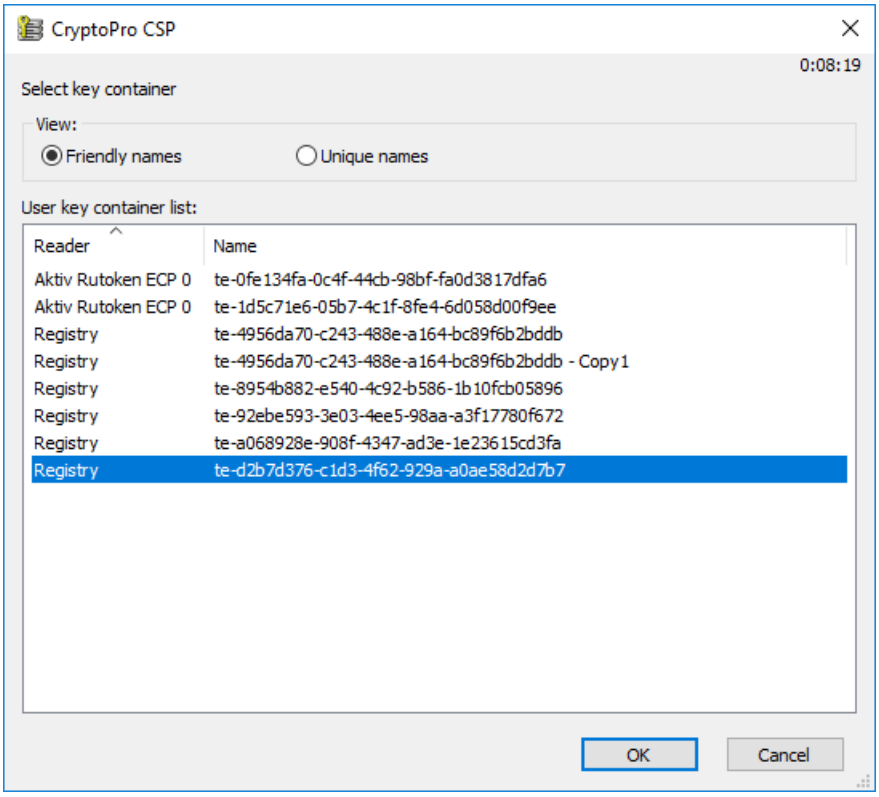


Figure 83. Selecting a key container for the master key

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.

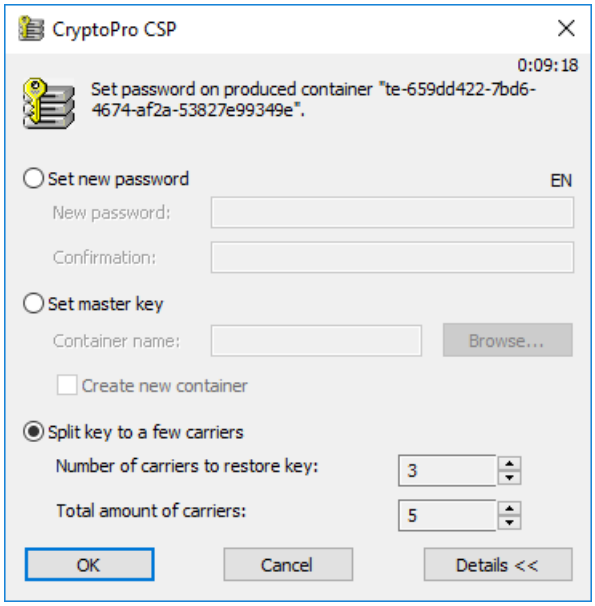


Figure 84. Splitting a key into a few carriers

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.

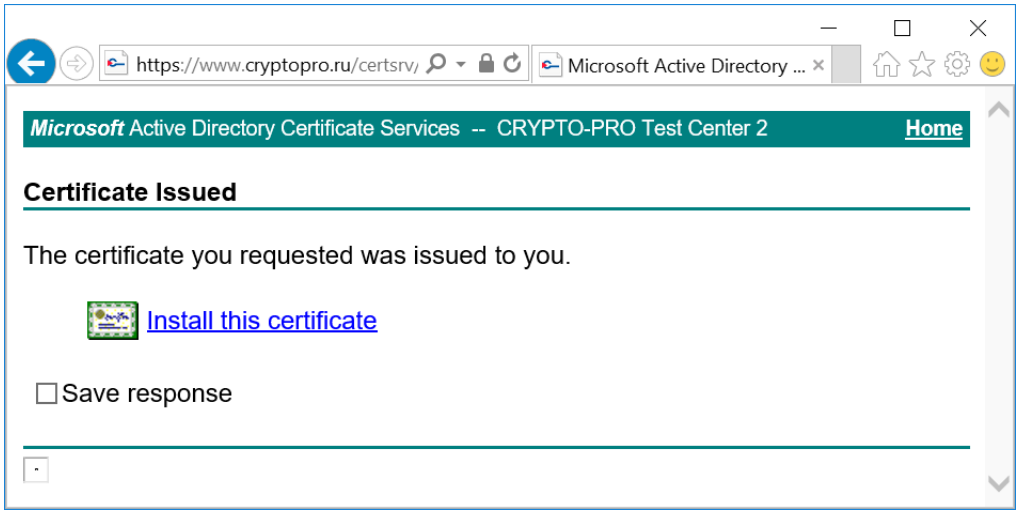


Figure 85. Installing a certificate

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).

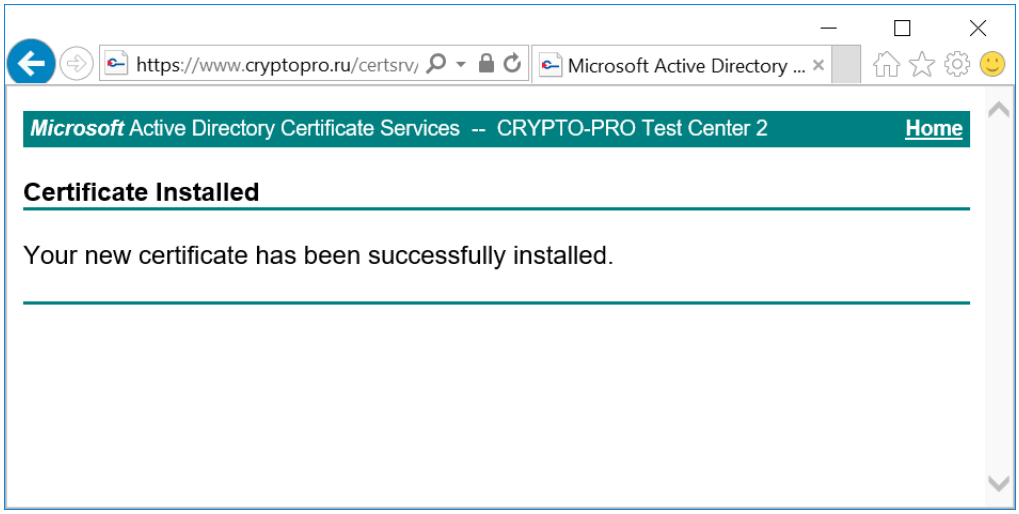


Figure 86. Successful certificate installation completion

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

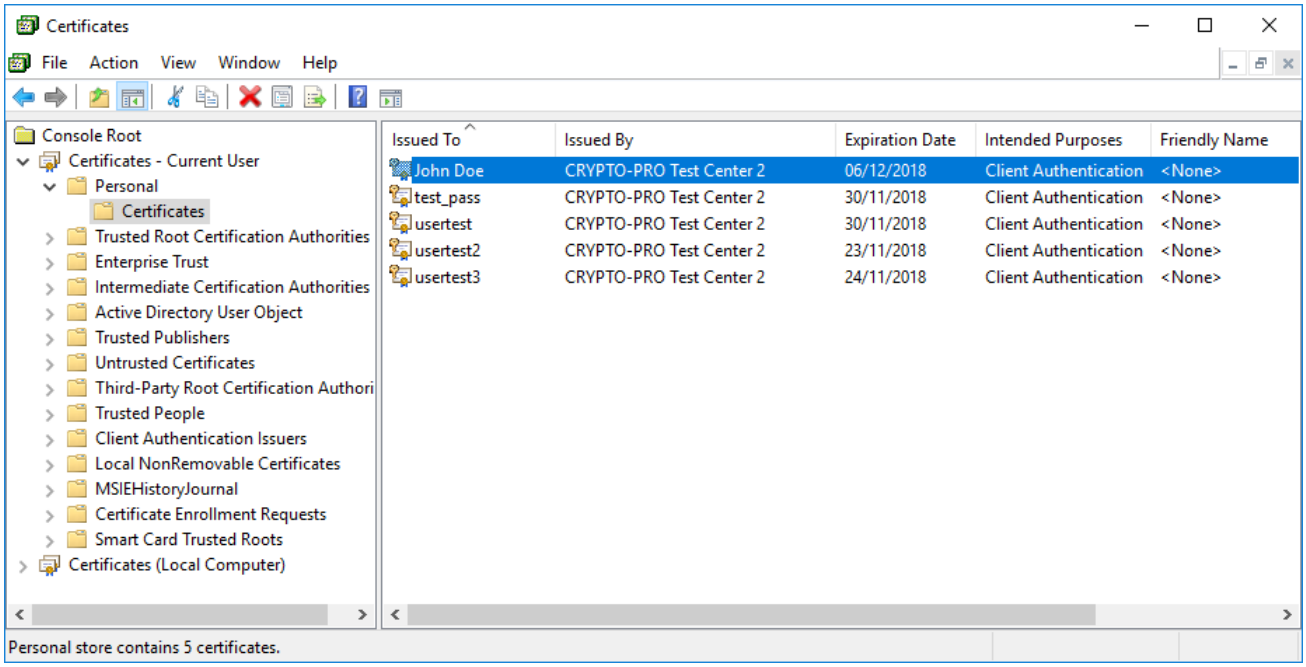


Figure 87. Certificates snap-in

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** ⇒ **Programs** ⇒ **Programs and Features** ⇒ **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**.

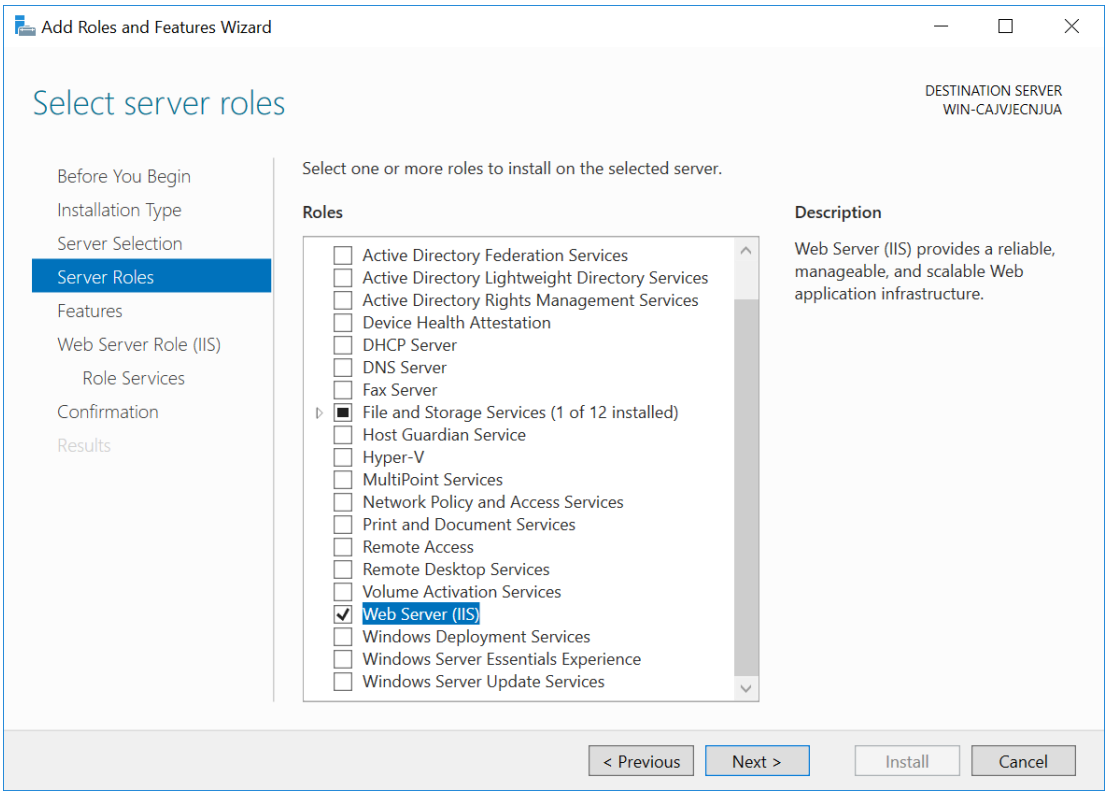


Figure 88. Selecting server roles

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

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

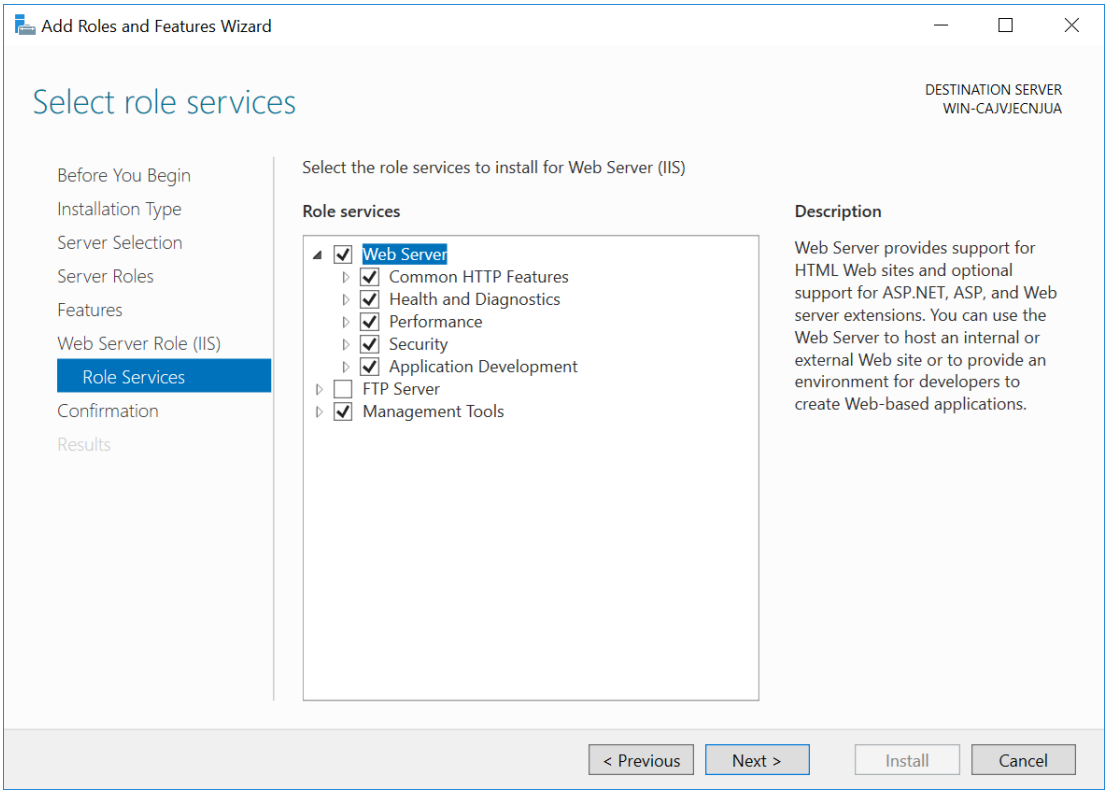


Figure 89. Selecting the role services

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).

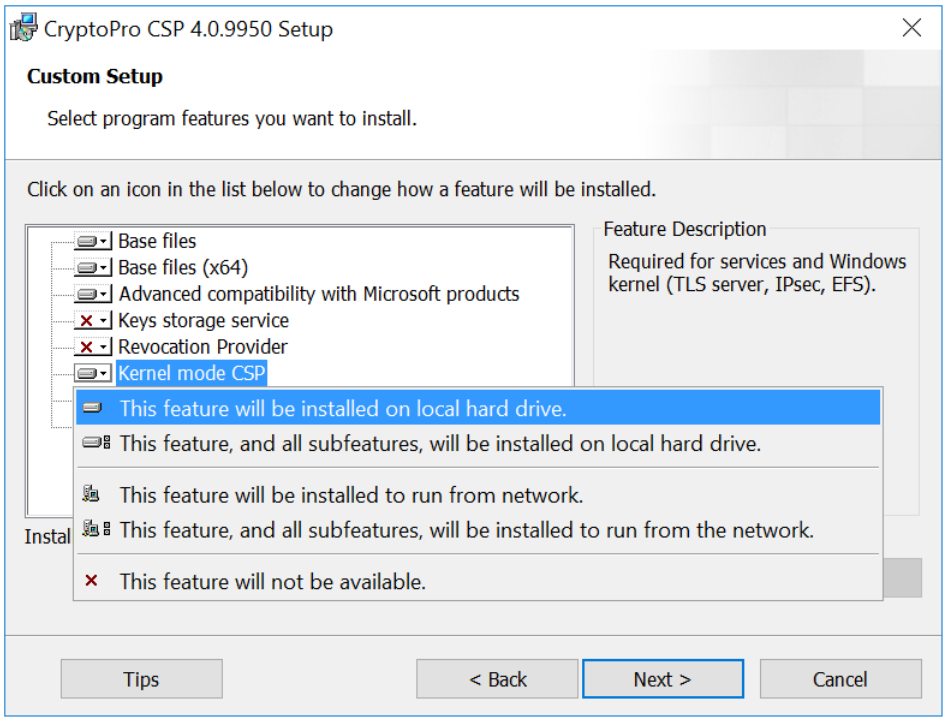


Figure 90. Selecting server roles

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 ⇒ **All Programs** ⇒ **Crypto-Pro** ⇒ **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).

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).

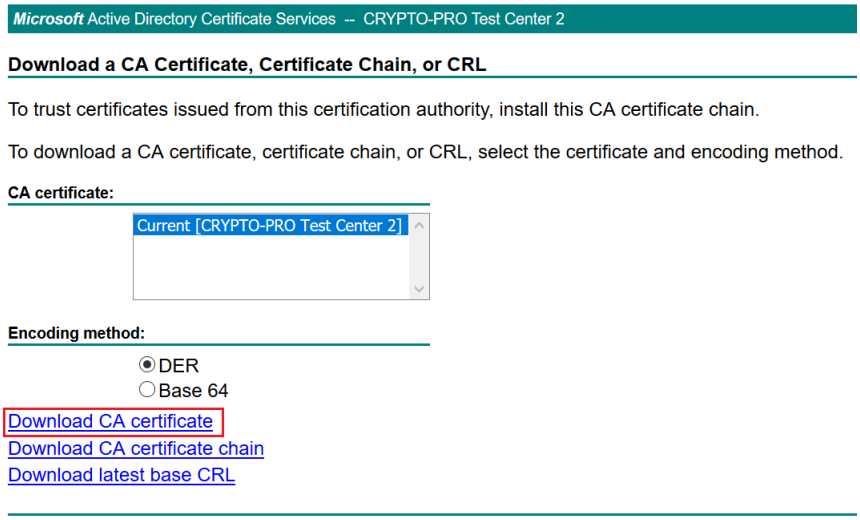


Figure 92. Downloading the CryptoPro LLC Test CA certificate

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).

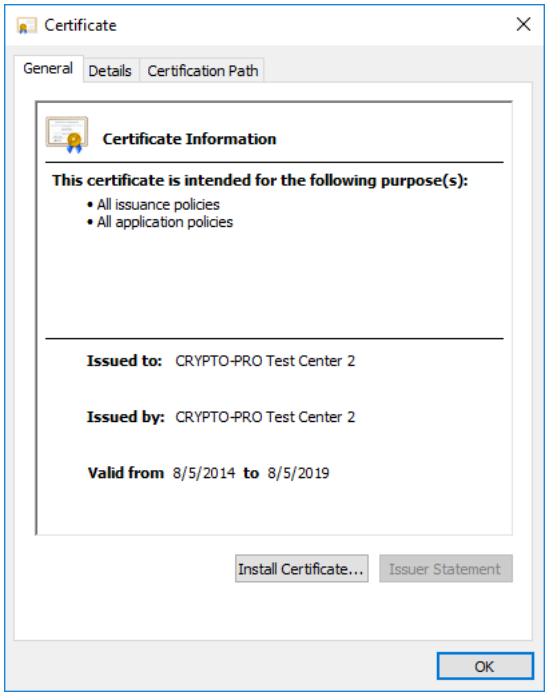


Figure 93. Installing the CryptoPro LLC Test CA certificate

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

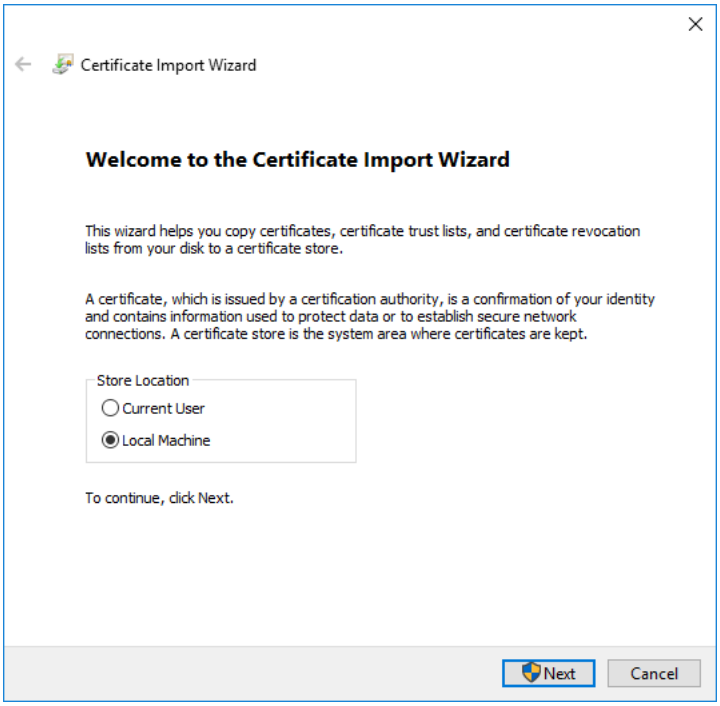


Figure 94. Certificate Import Wizard

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

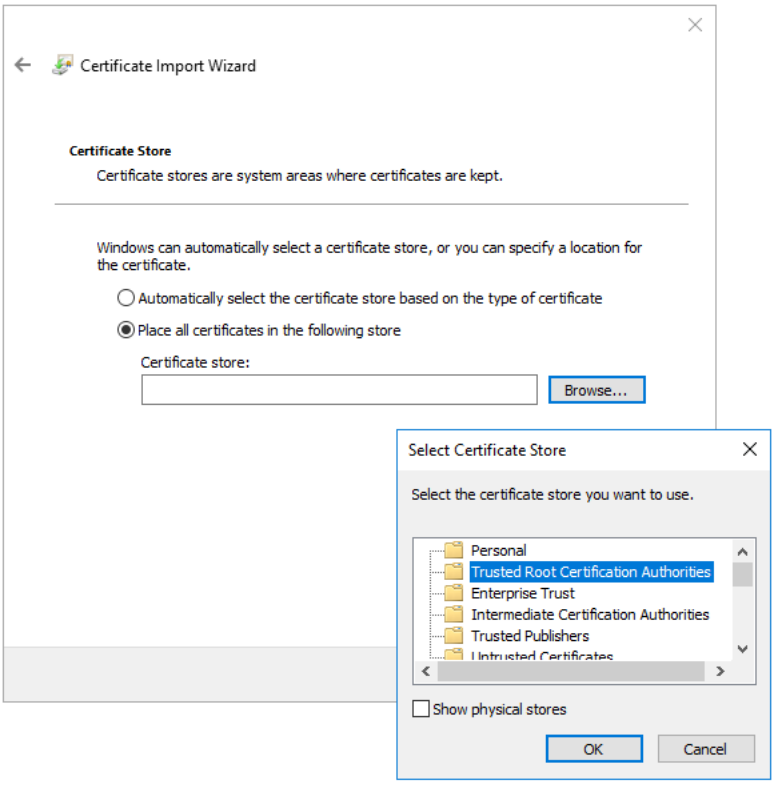


Figure 95. Specifying the CA certificate location

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 ⇒ **All Programs** ⇒ **Crypto-Pro** ⇒ **Certificates**). If the certificate is properly installed, you will find it in the Local Computer Trusted Root Certificate Authorities store (Figure 96).

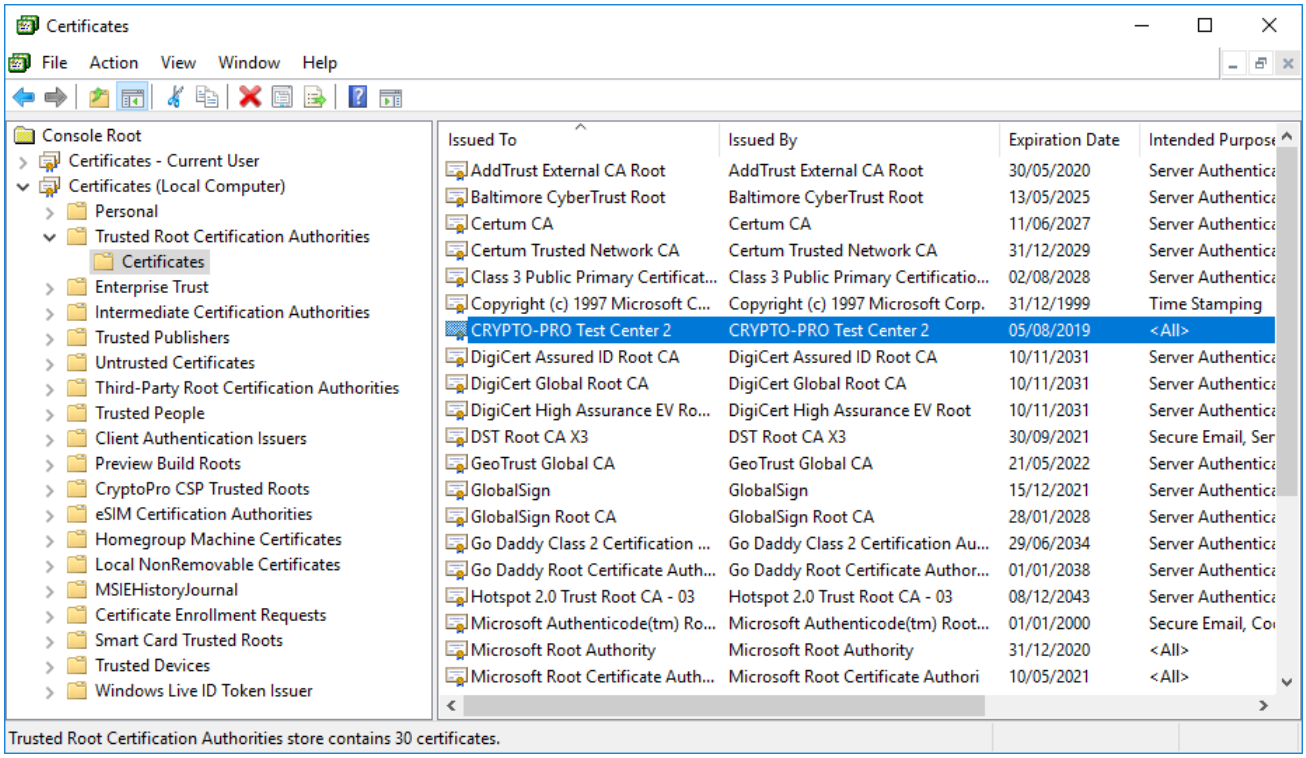


Figure 96. Certificates snap-in

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**.

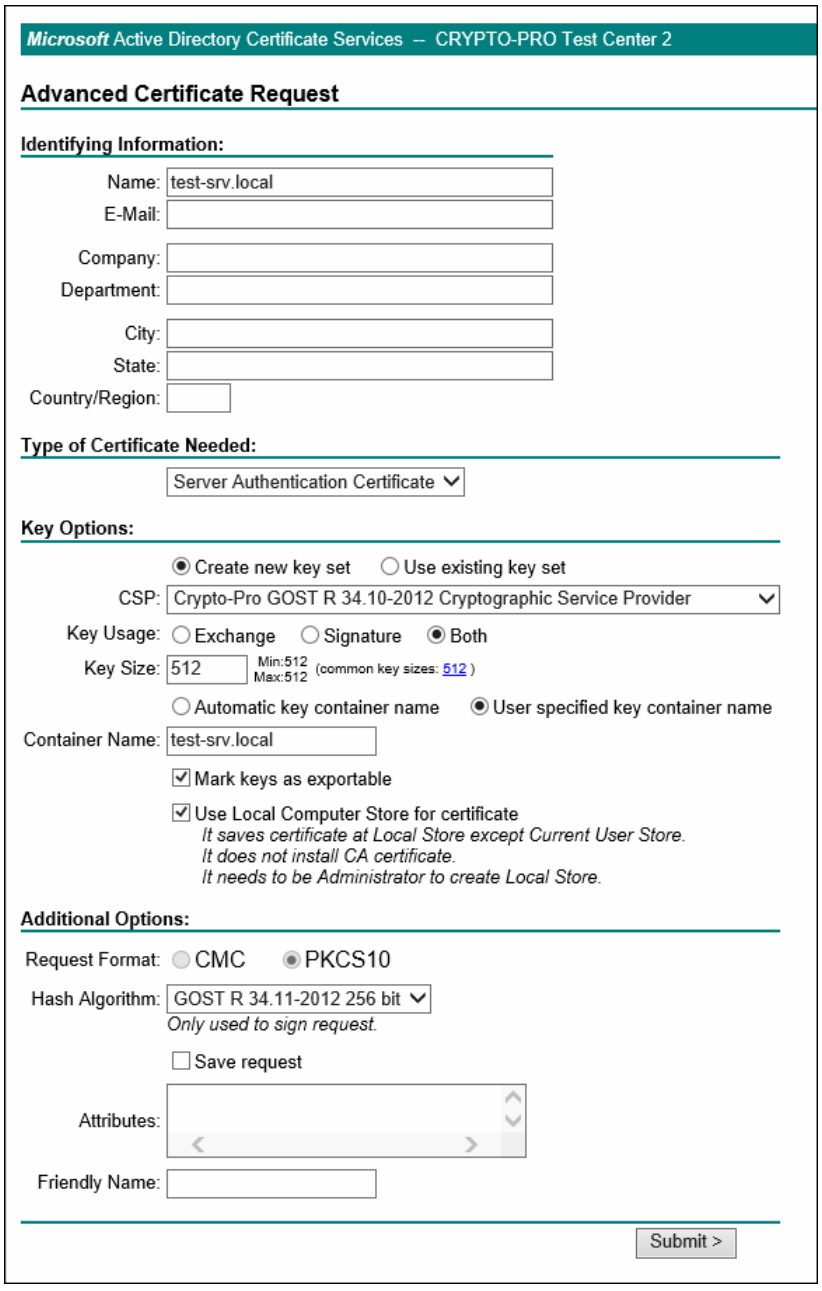


Figure 97. IIS certificate request

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

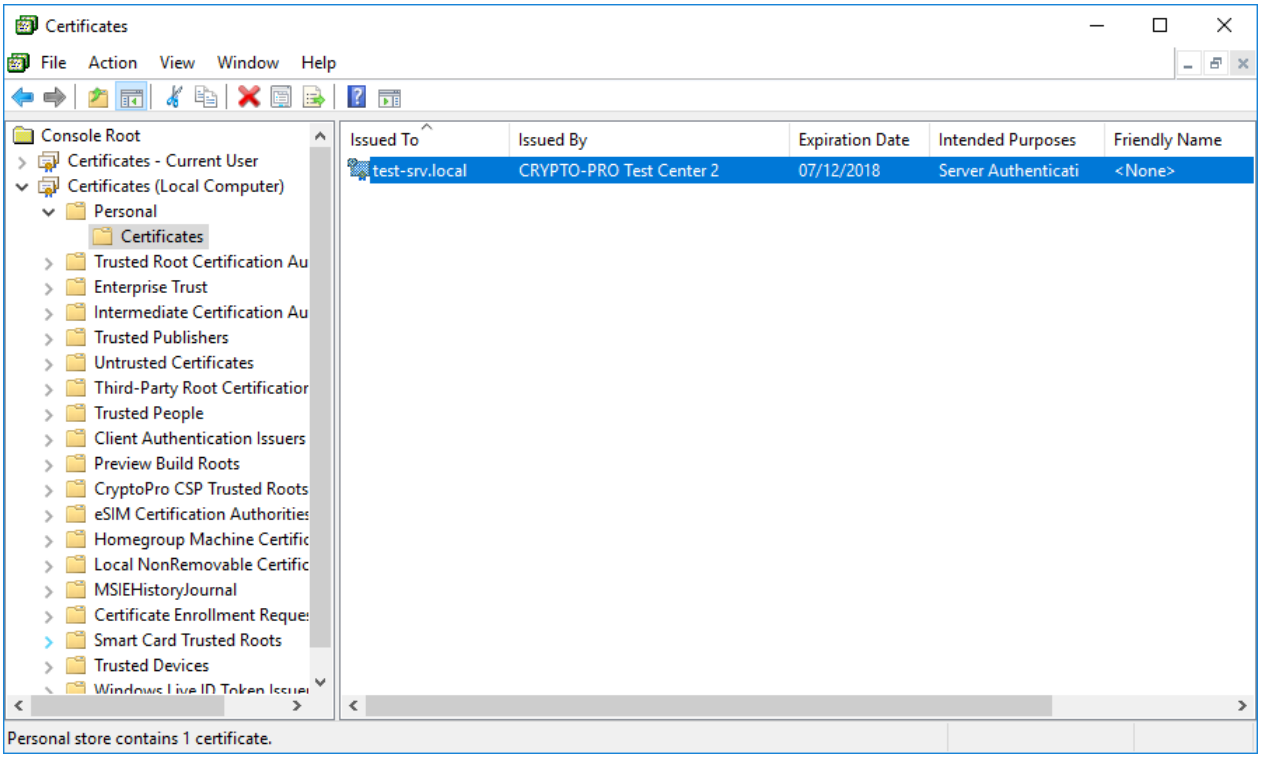


Figure 98. Certificates snap-in

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** ⇒ **Tools** ⇒ **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).

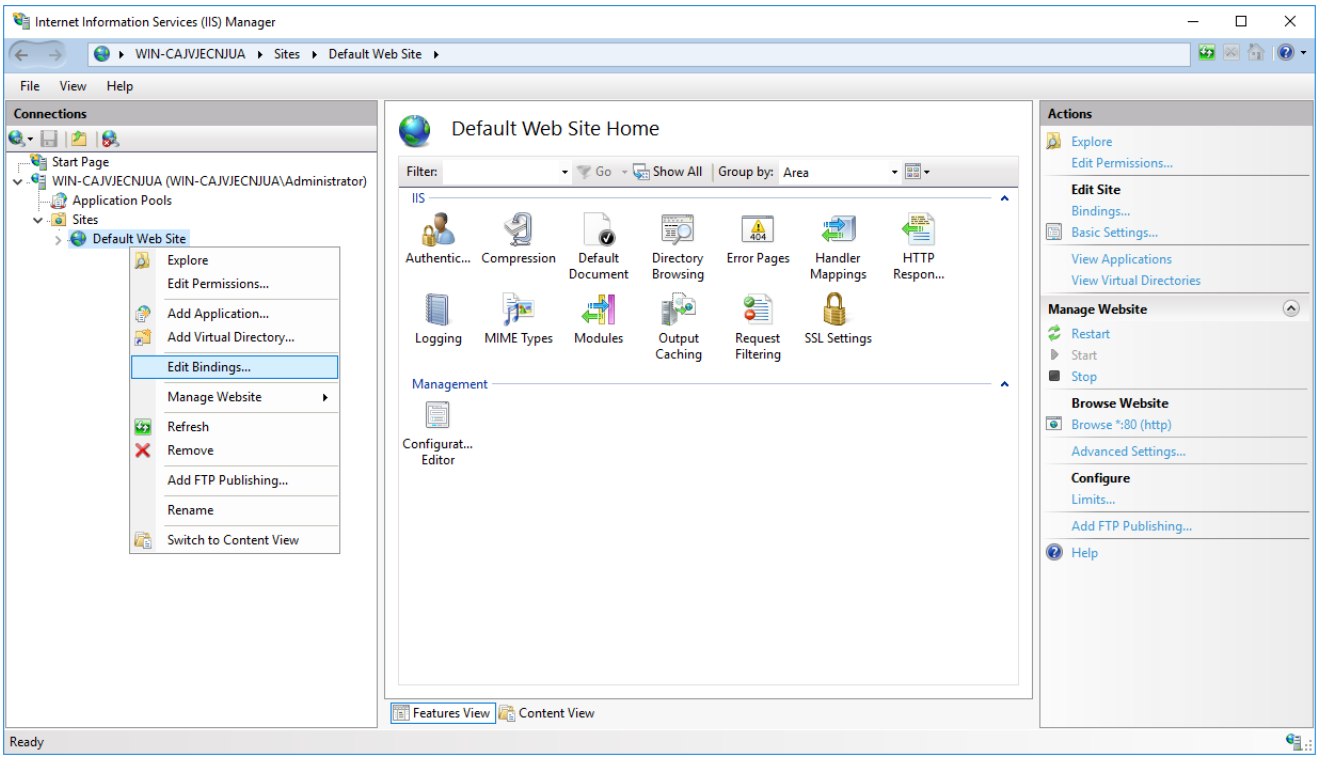


Figure 99. IIS Manager

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.

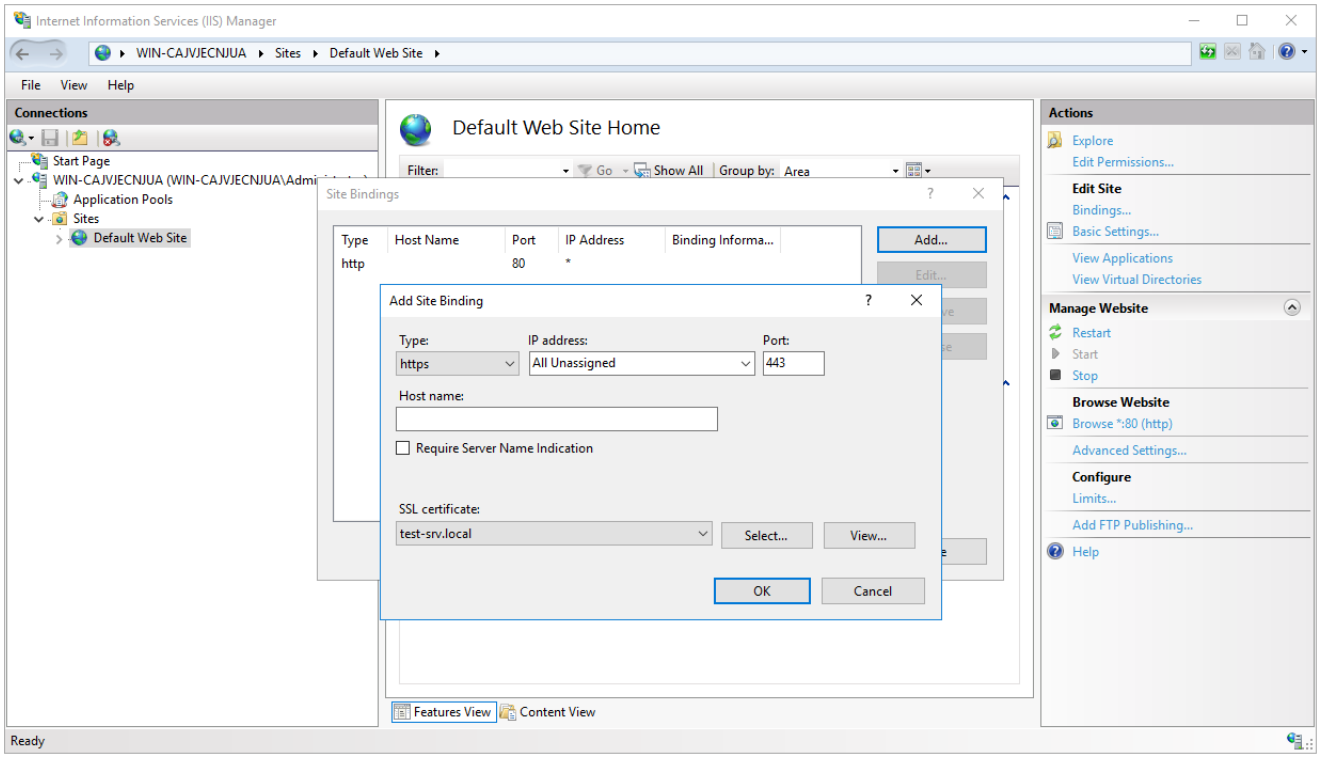


Figure 100. Adding a site binding

Close the «Site Bindings» window and restart IIS by clicking the **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).

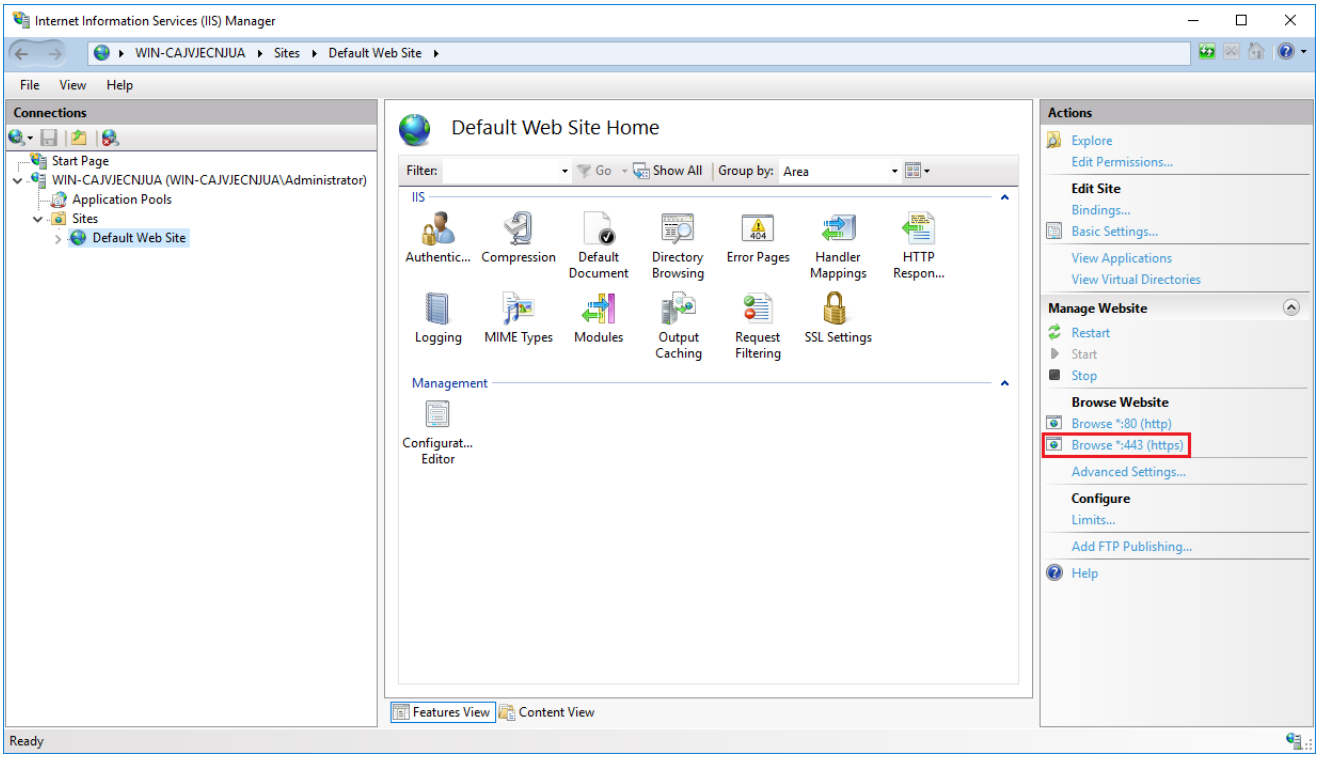


Figure 101. Testing HTTPS connection

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).

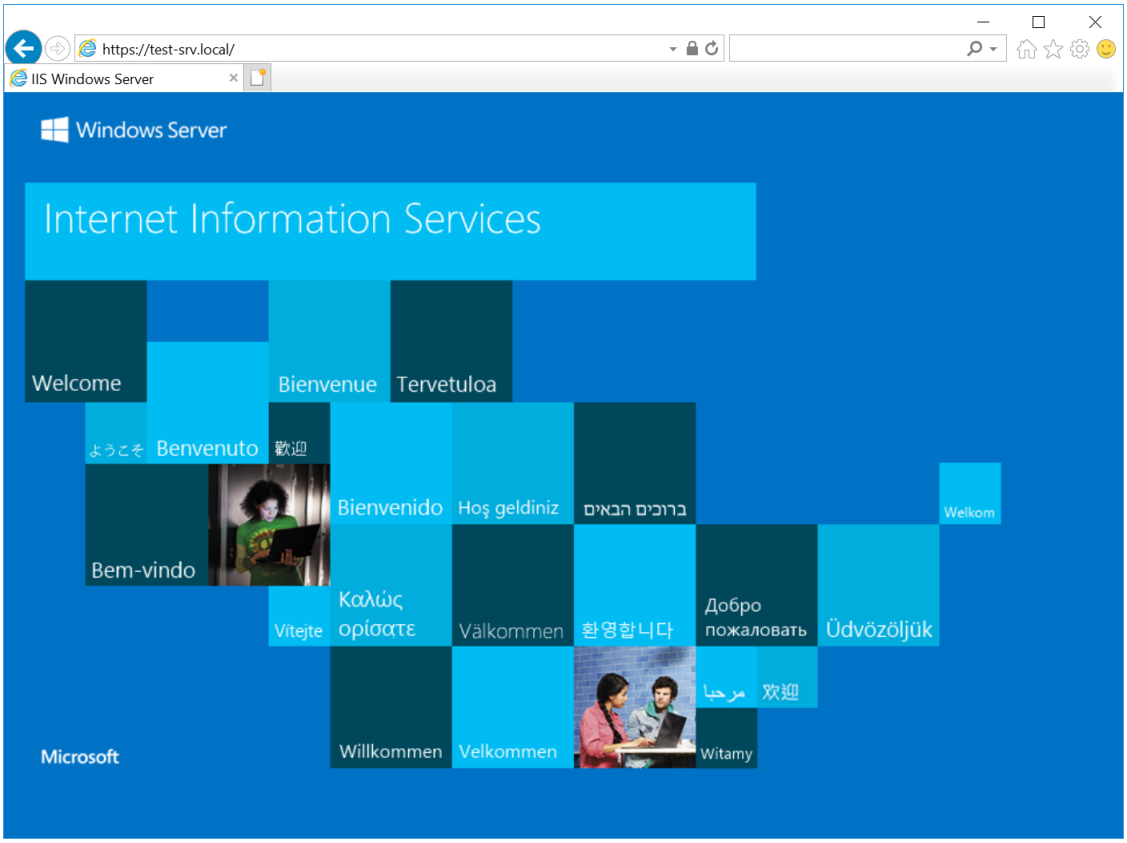


Figure 102. IIS welcome page

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).

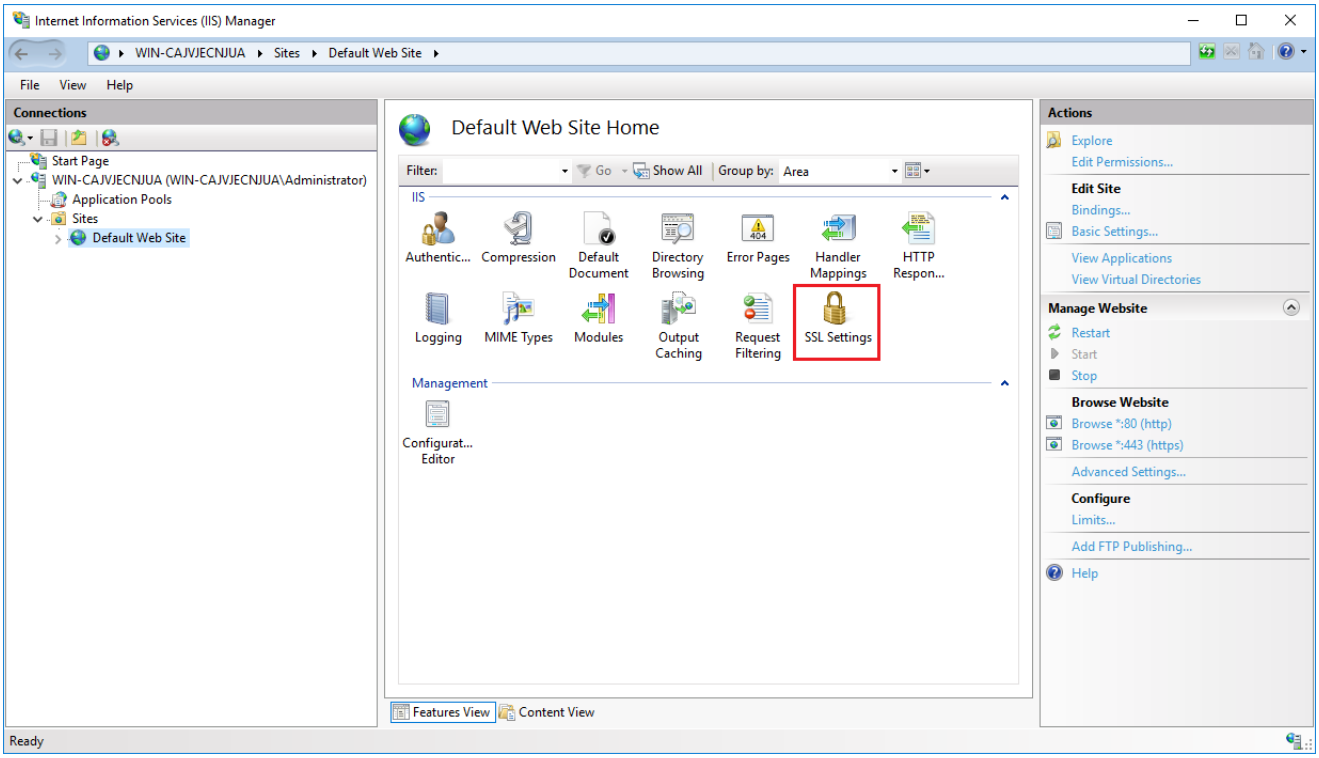


Figure 103. IIS manager Features view

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.

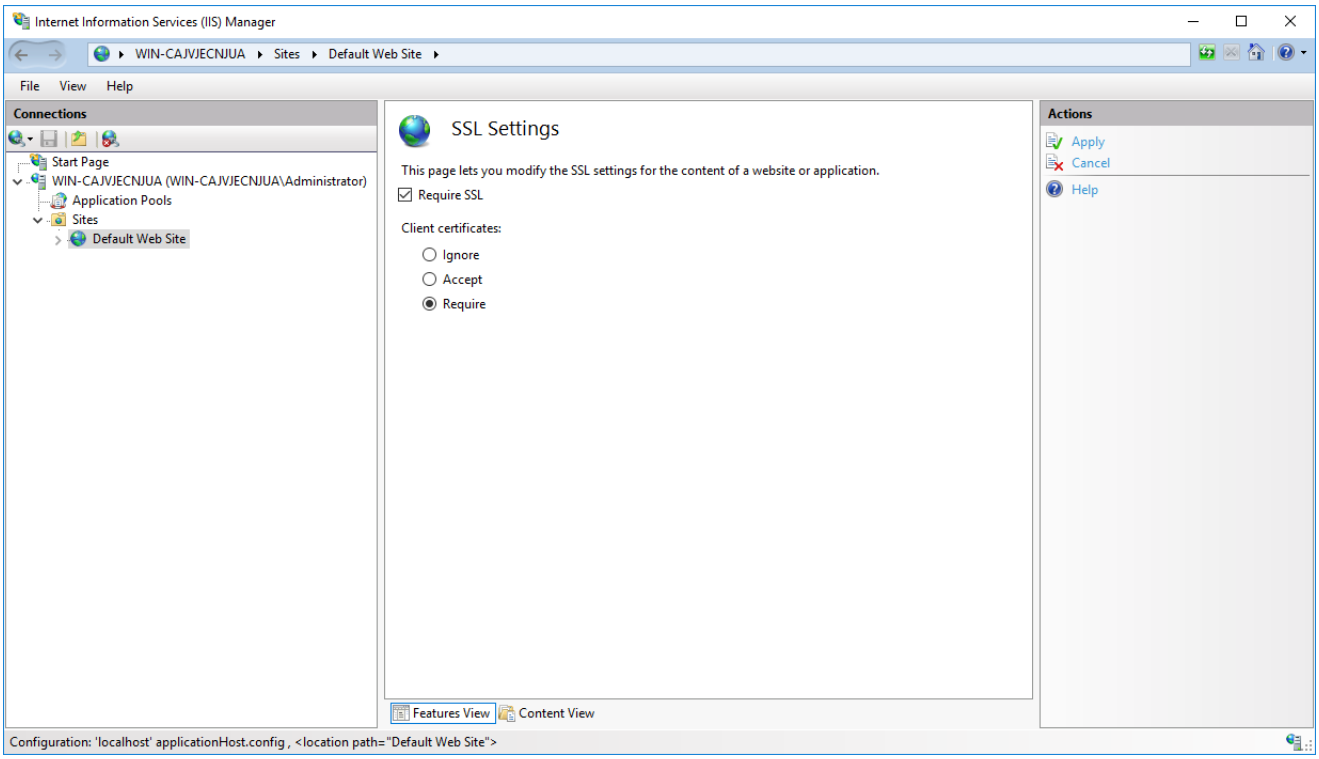


Figure 104. SSL settings

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 ⇒ **All Programs** ⇒ **Crypto-Pro** ⇒ **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).

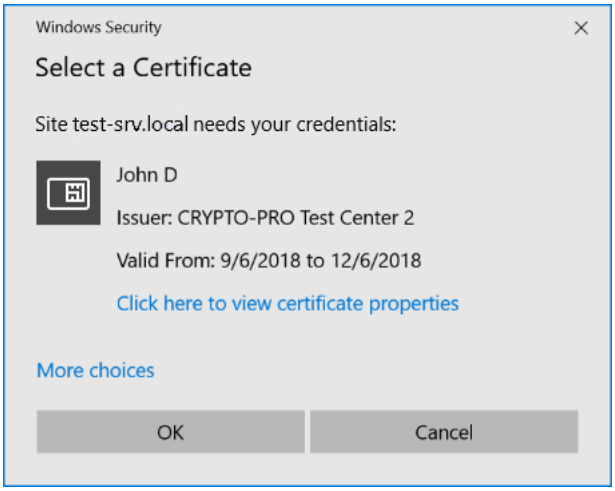


Figure 105. Selecting a user certificate

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** ⇒ **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**.

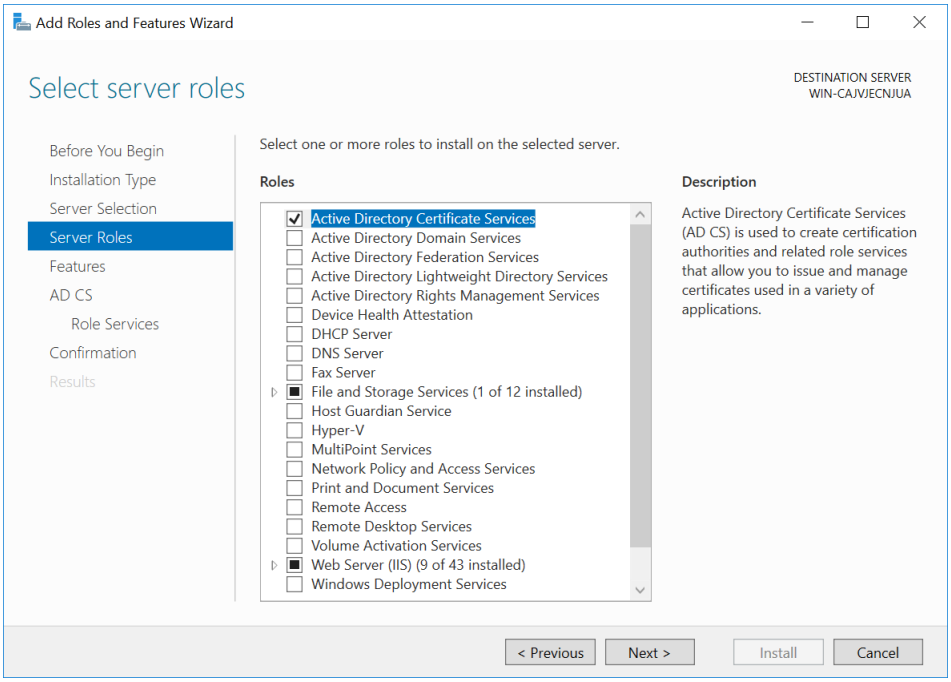


Figure 106. Selecting server roles

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

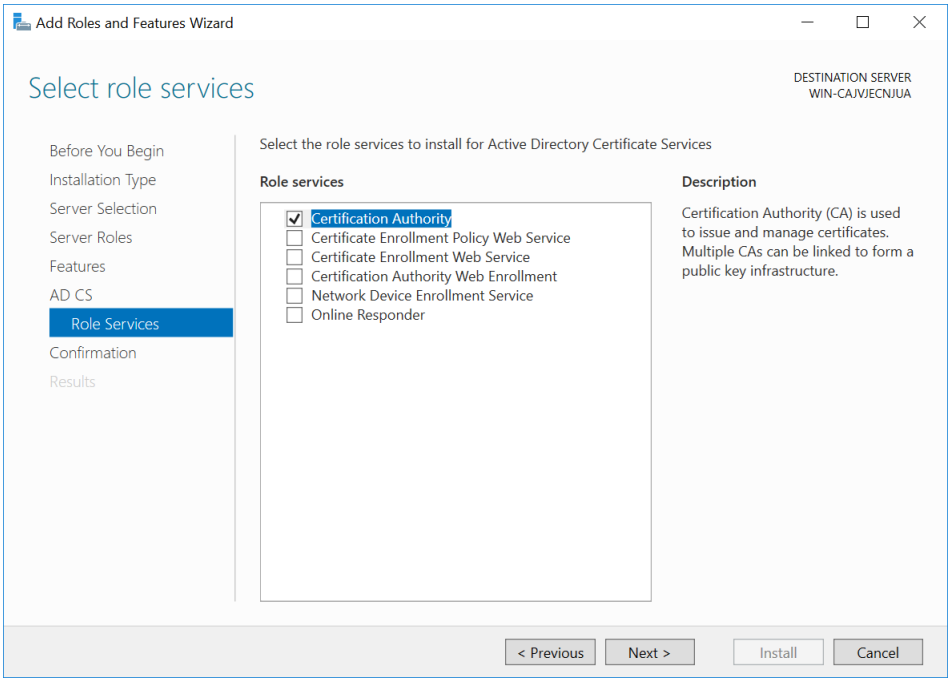


Figure 107. Selecting AD CS roles

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).

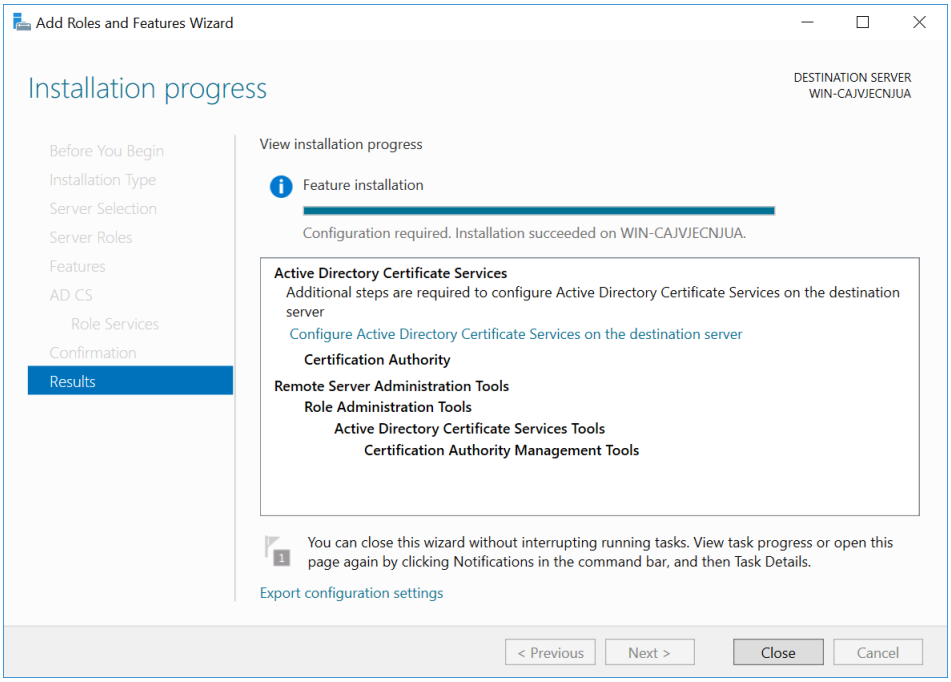


Figure 108. AD CS installation progress

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**.

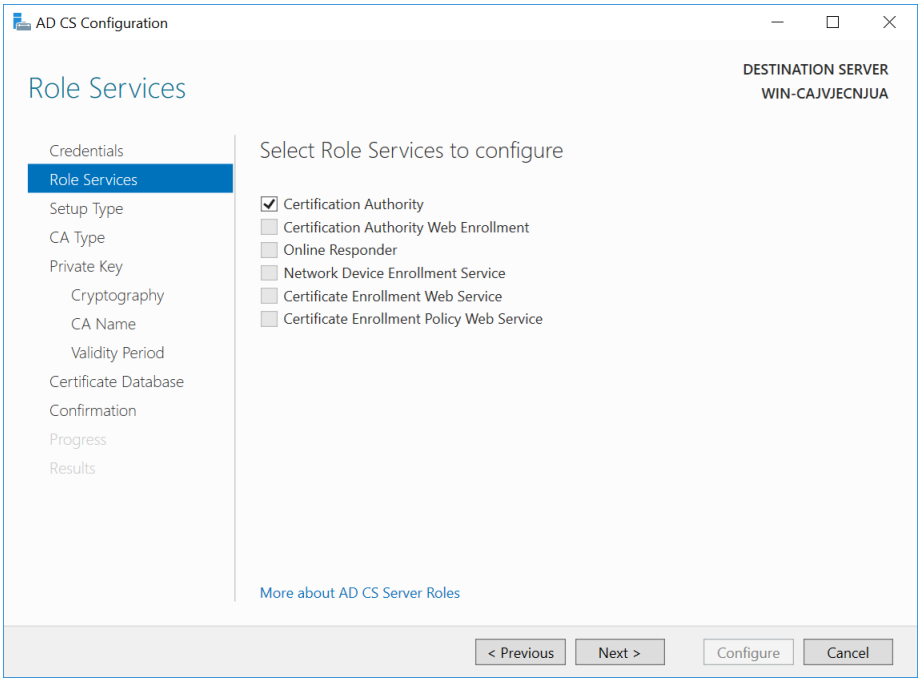


Figure 109. Selecting role services

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**.

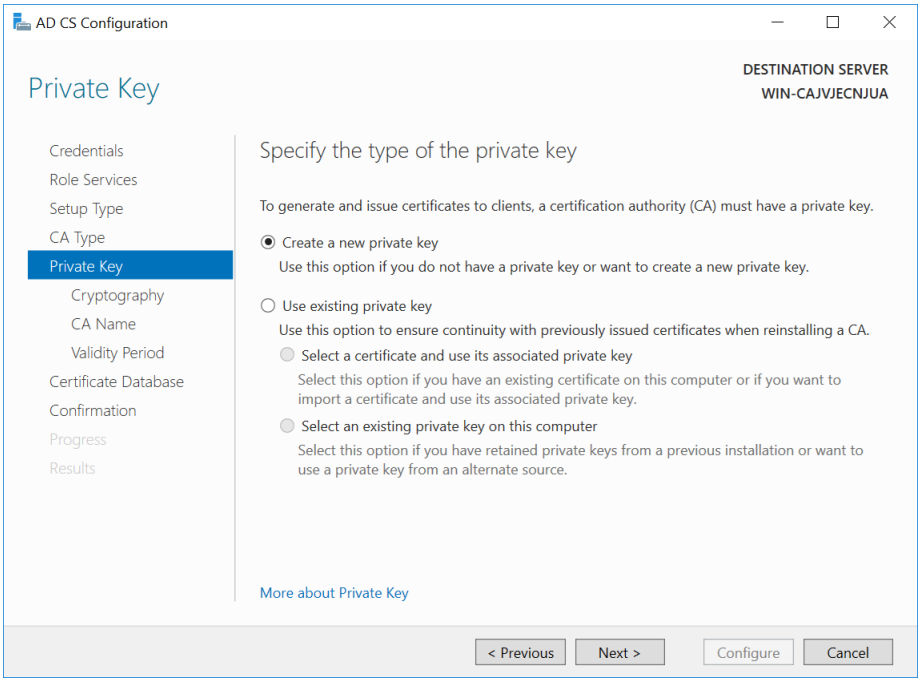


Figure 110. Creating a new private key

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.

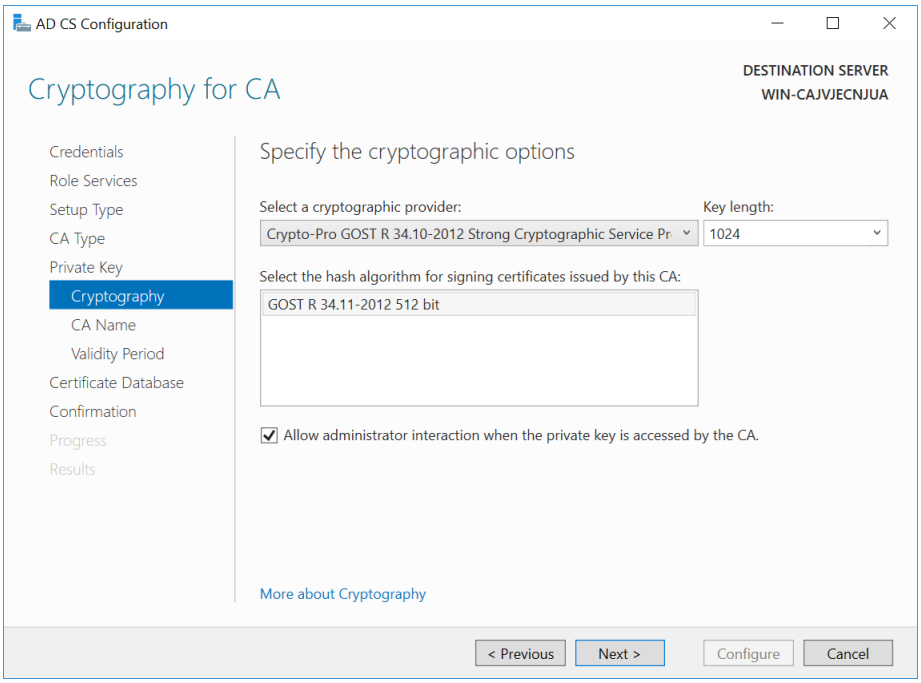


Figure 111. Specifying the cryptographic options

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

Next.

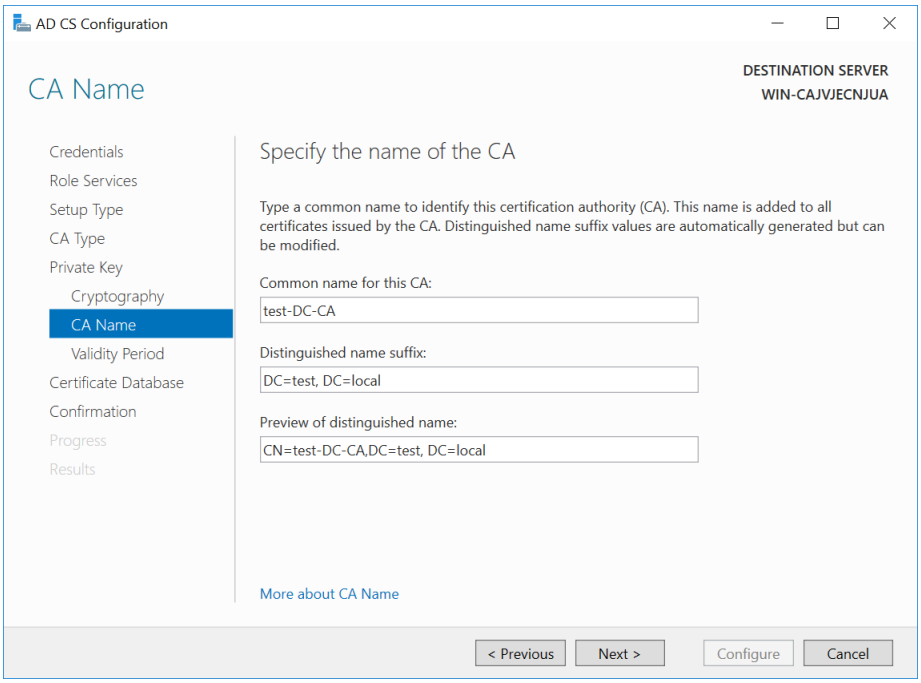


Figure 112. Specifying the CA name

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 ⇒ **All Programs** ⇒ **CryptoPro** ⇒ **Certificates**) to check for a certificate in the Trusted Root Certification Authorities store of the Local Computer (Figure 113).

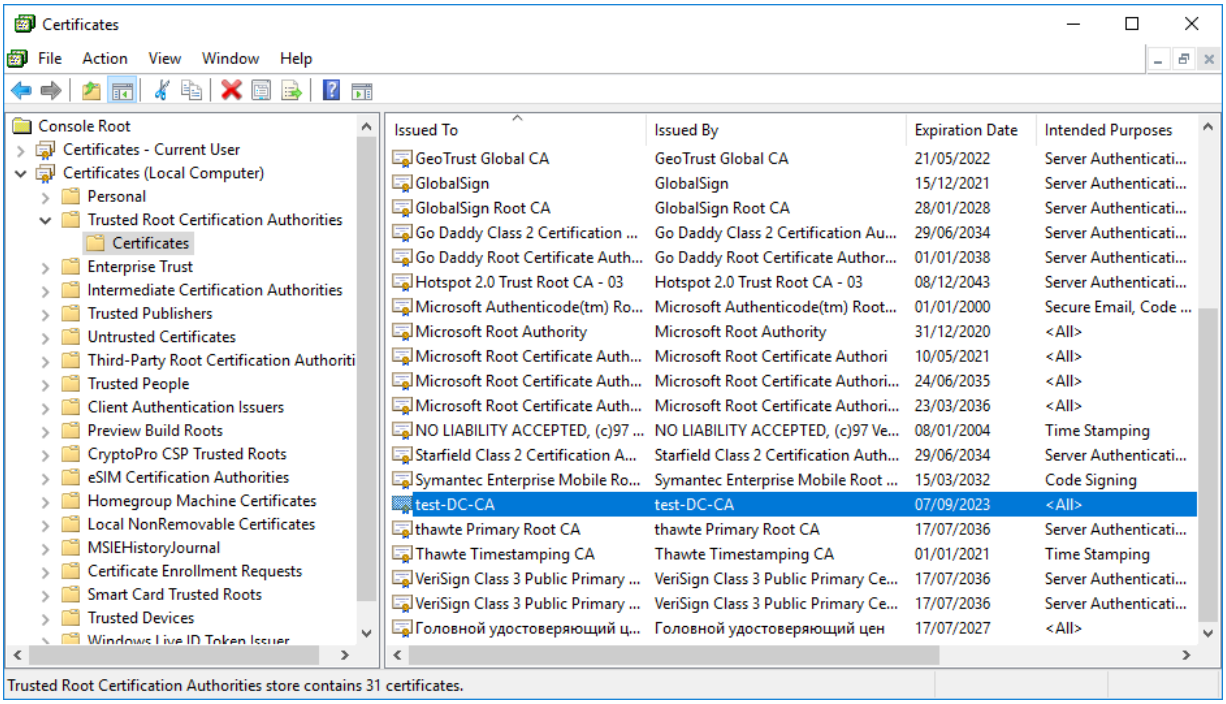


Figure 113. Certificates snap-in

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** ⇒ **System and Security** ⇒ **Administrative Tools** ⇒ **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** — **Certificate Template to Issue** (Figure 114).

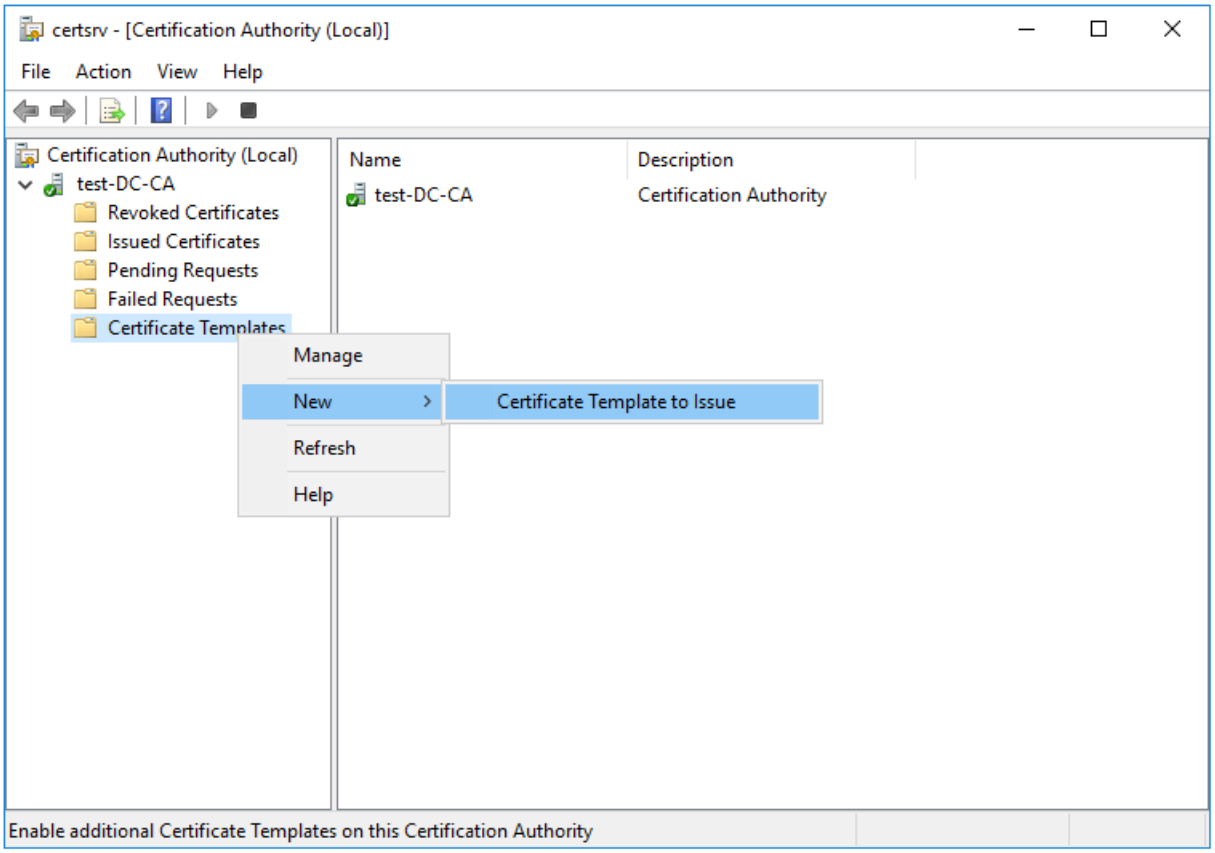


Figure 114. Adding certificate templates

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

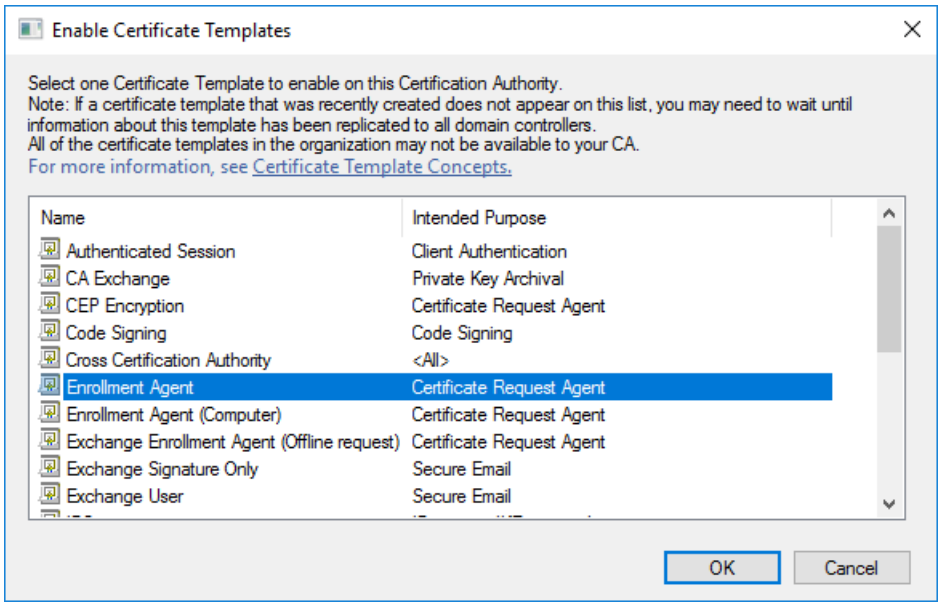


Figure 115. Enable Certificate Template

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).

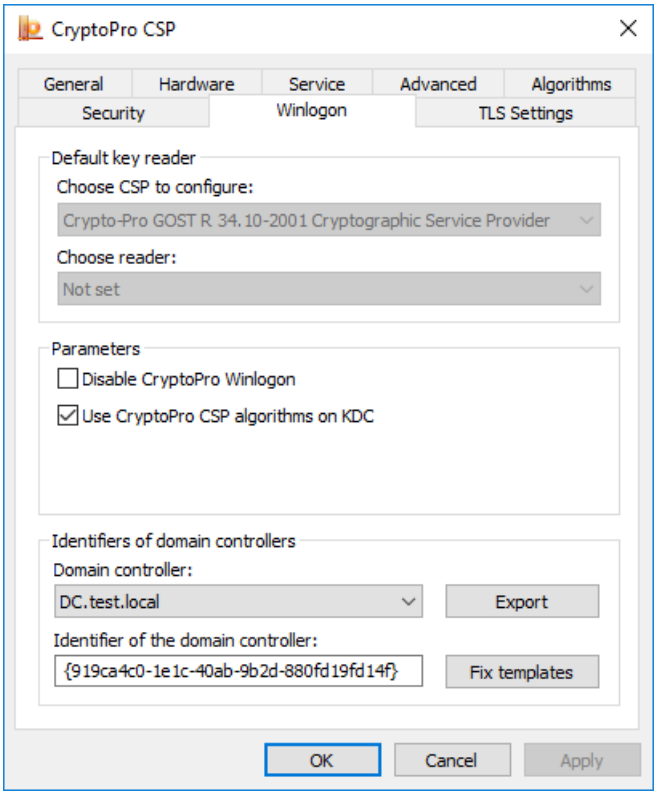


Figure 116. CSP Winlogon tab

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).

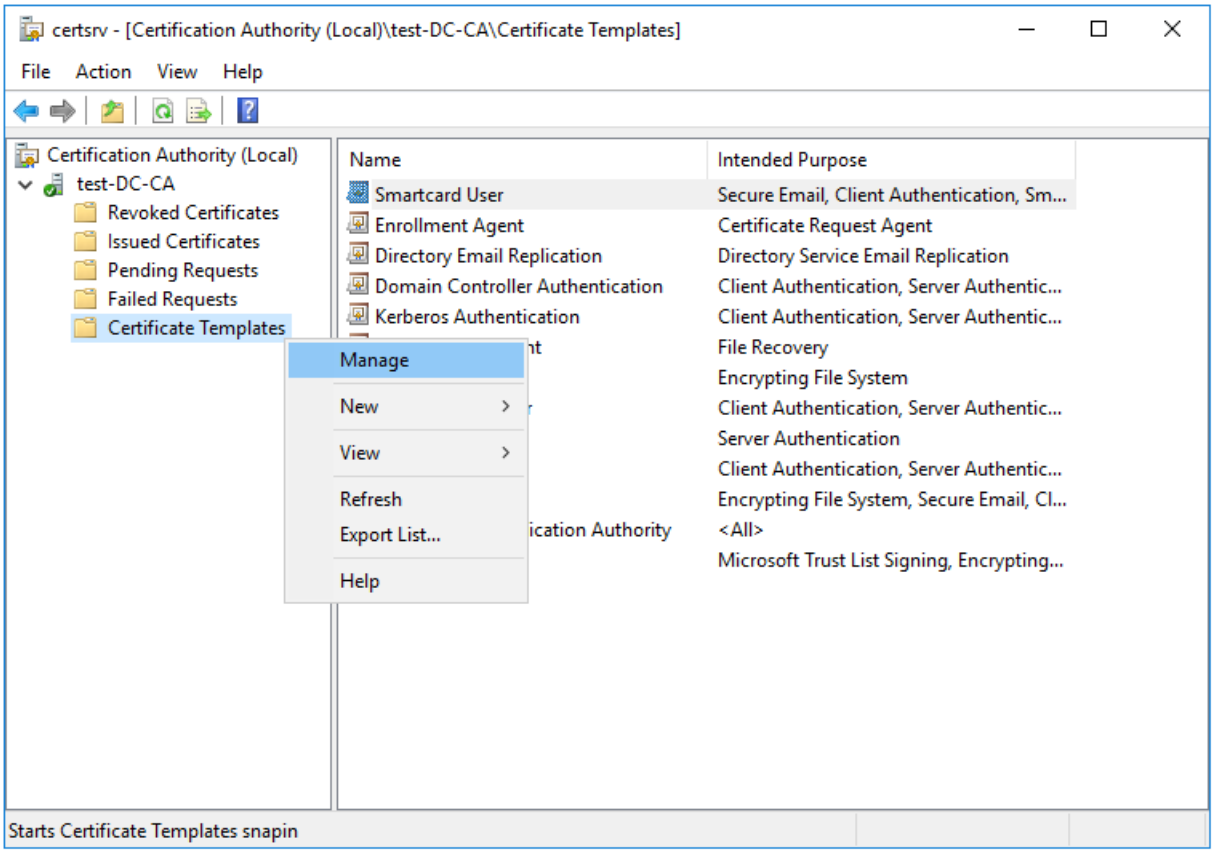


Figure 117. Certification Authority snap-in

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

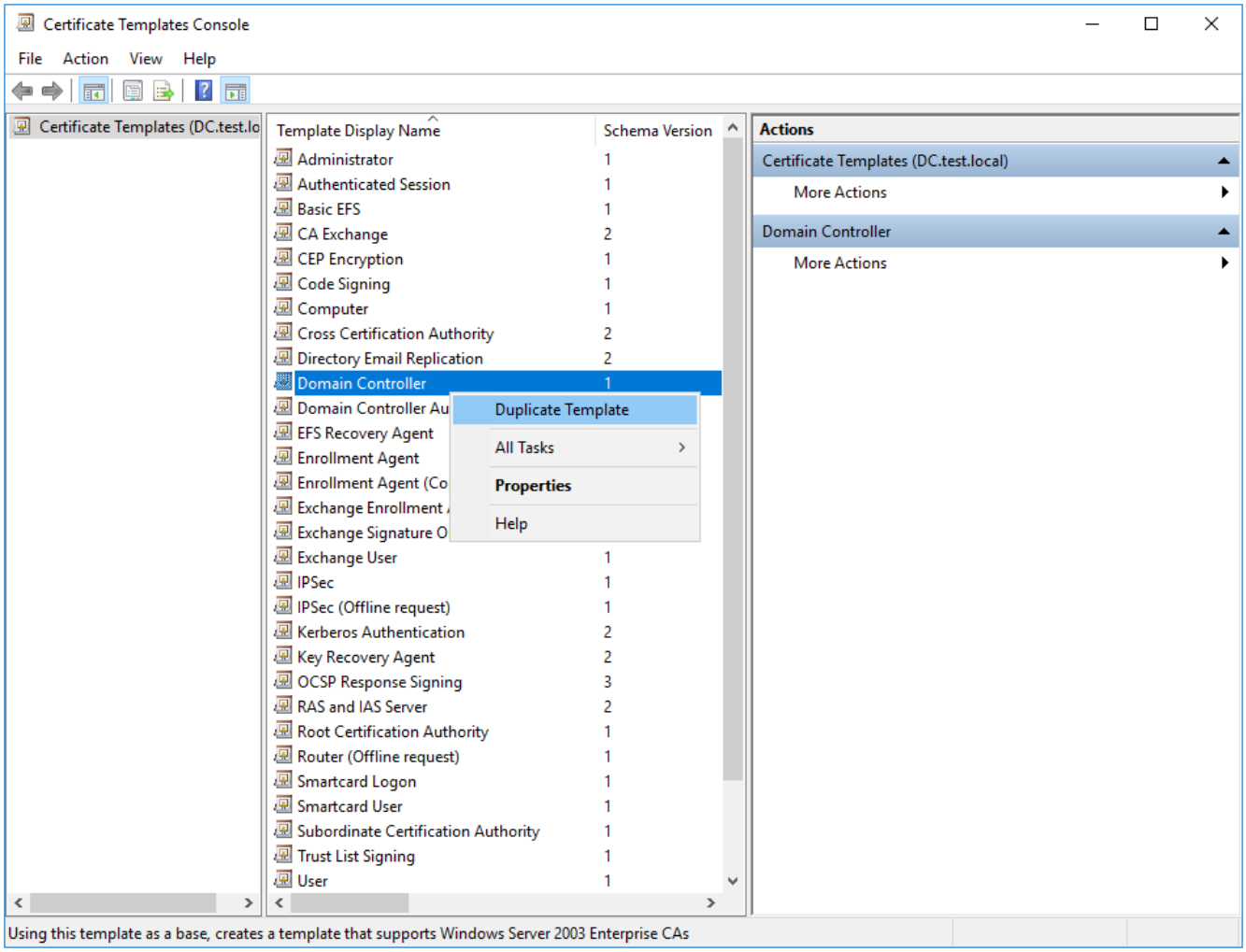


Figure 118. Certificate Templates Console

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).

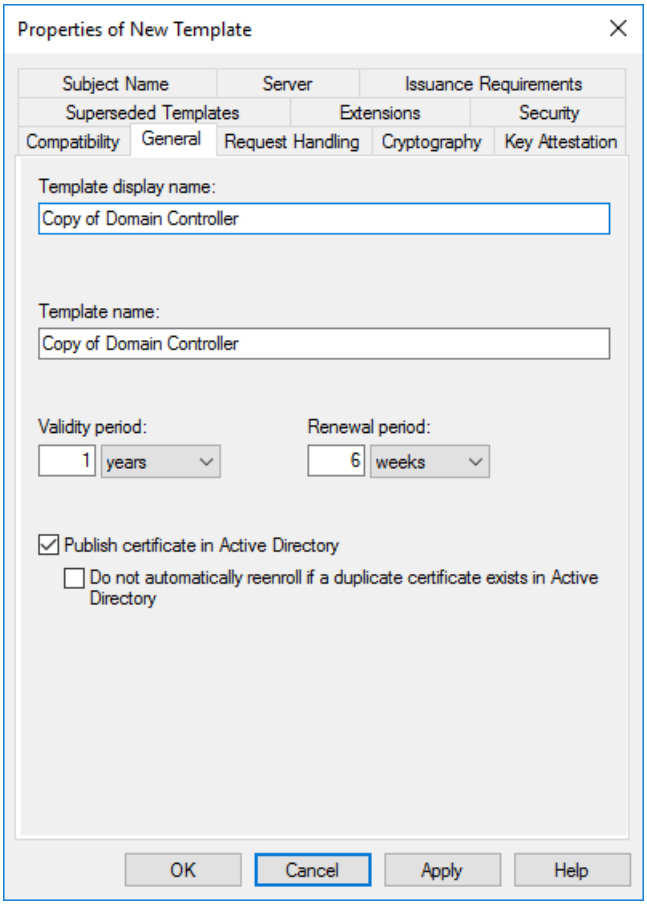


Figure 119. Copy of DC template

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).

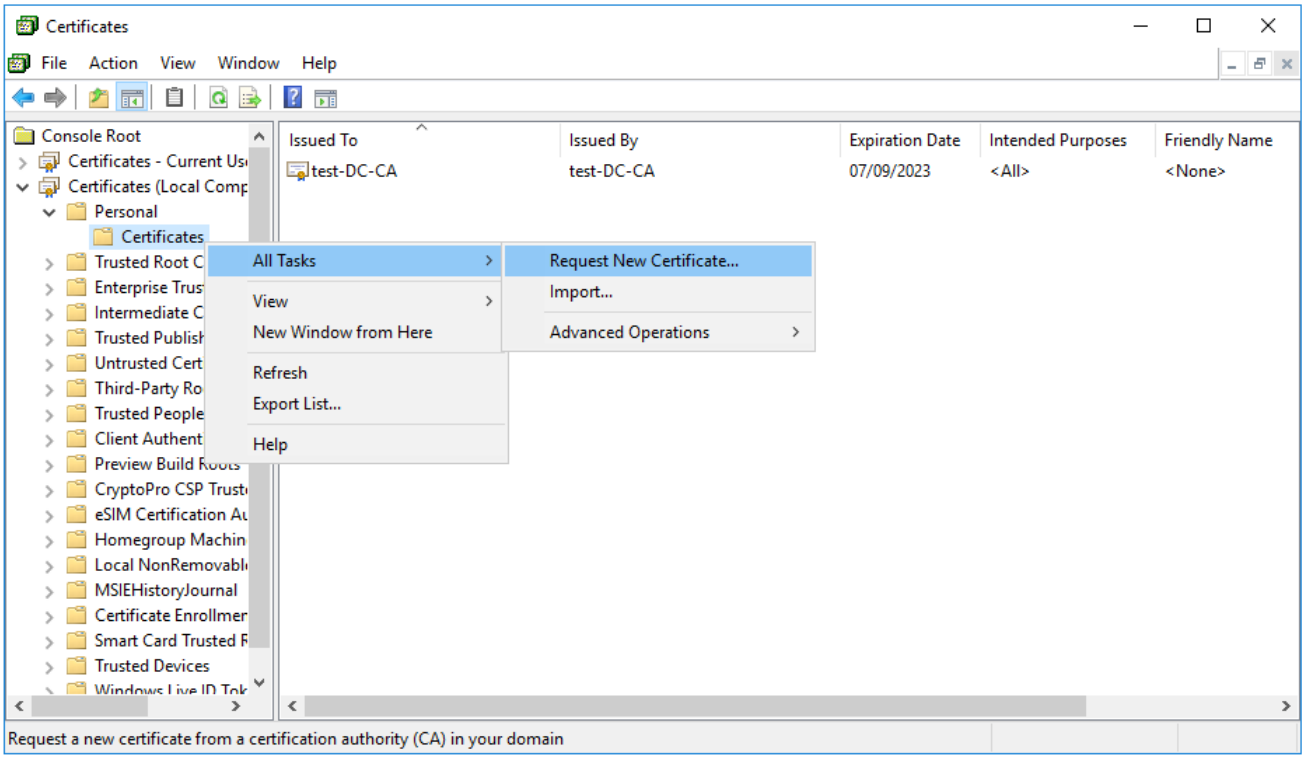


Figure 120. Certificates snap-in

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

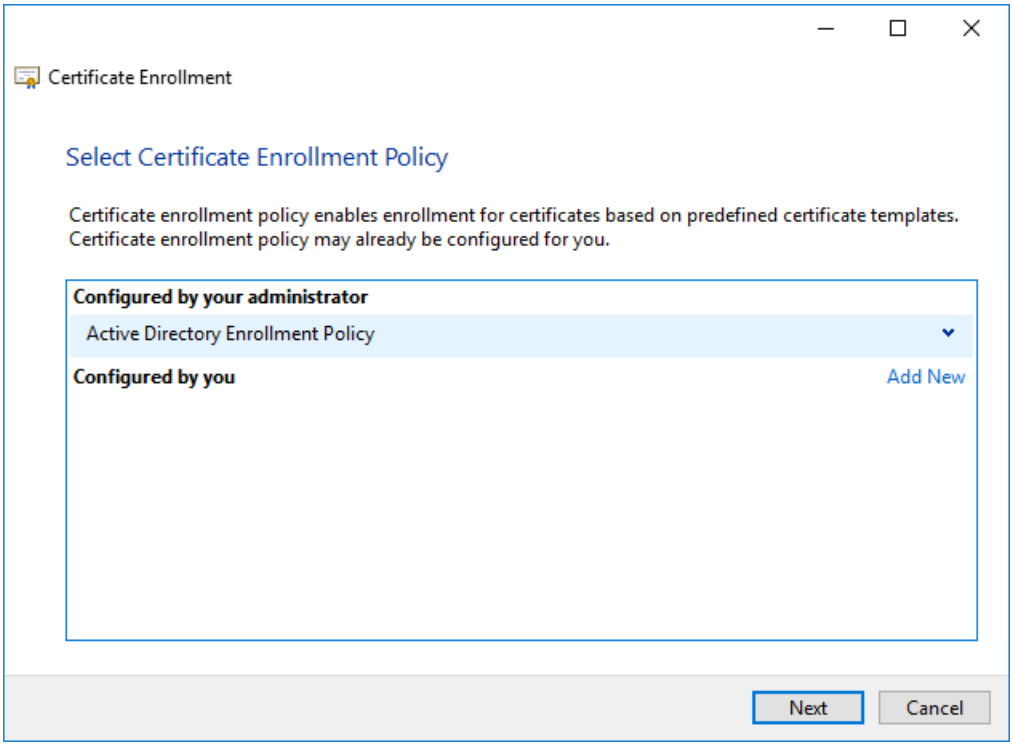


Figure 121. Select Certificate Enrollment Policy

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).

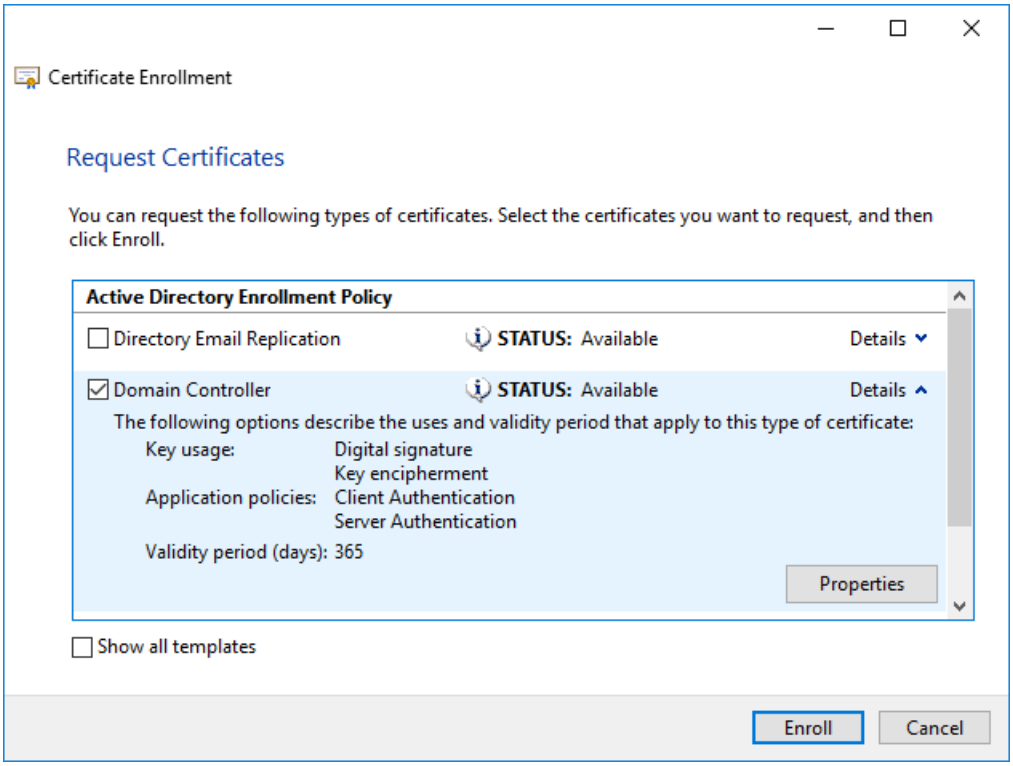


Figure 122. Request Certificates

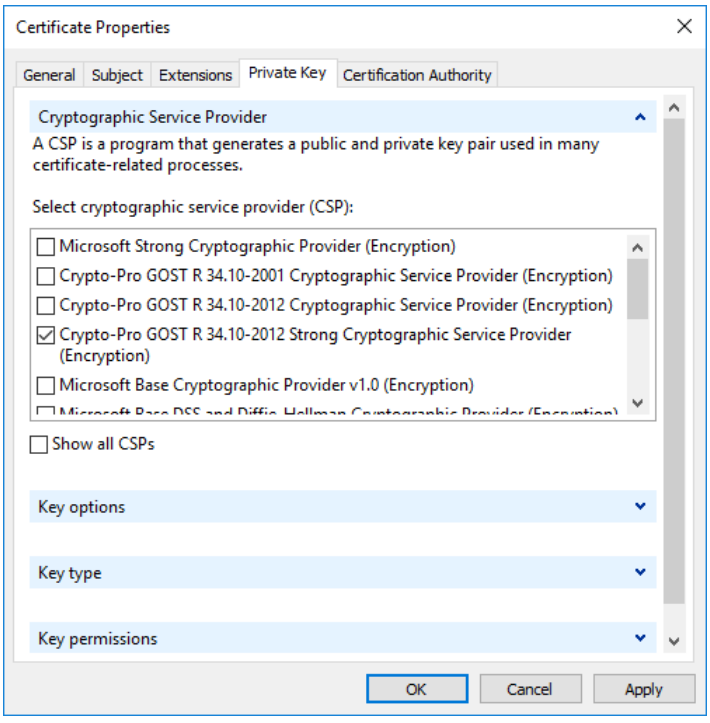


Figure 123. Certificate Properties

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).

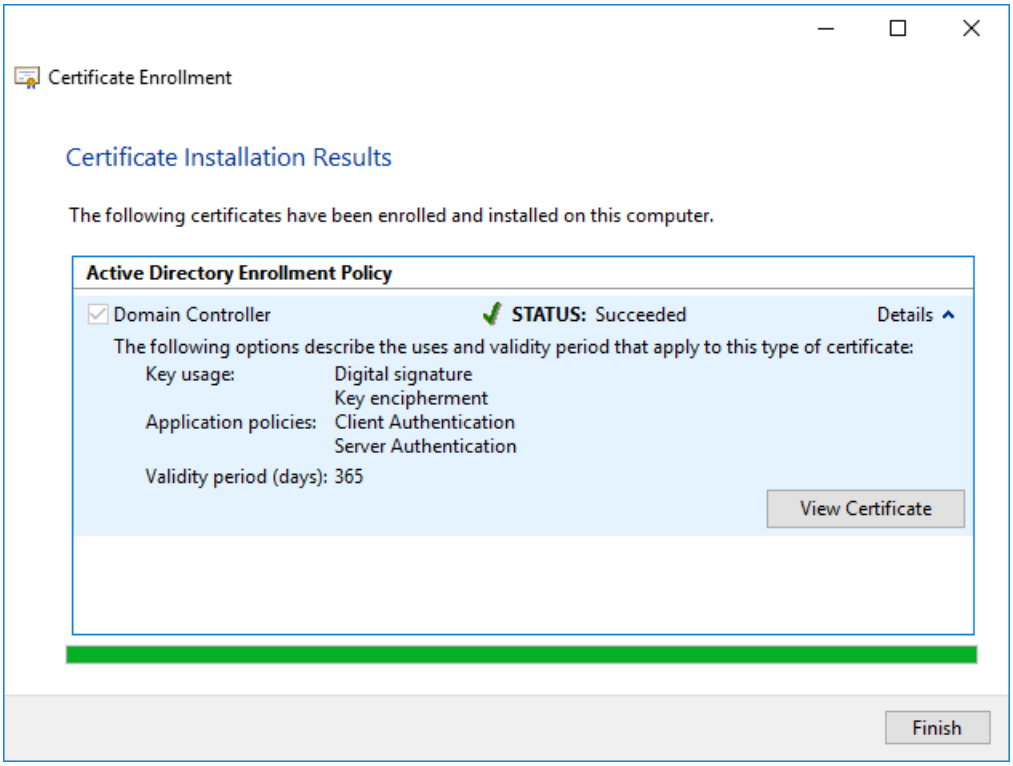


Figure 124. Certificate Installation Results

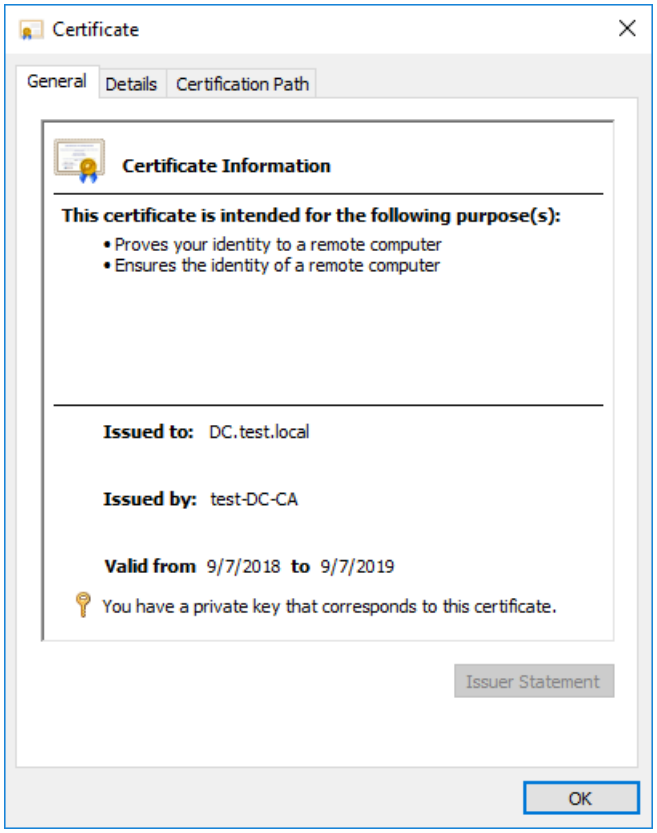


Figure 125. DC certificate

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).

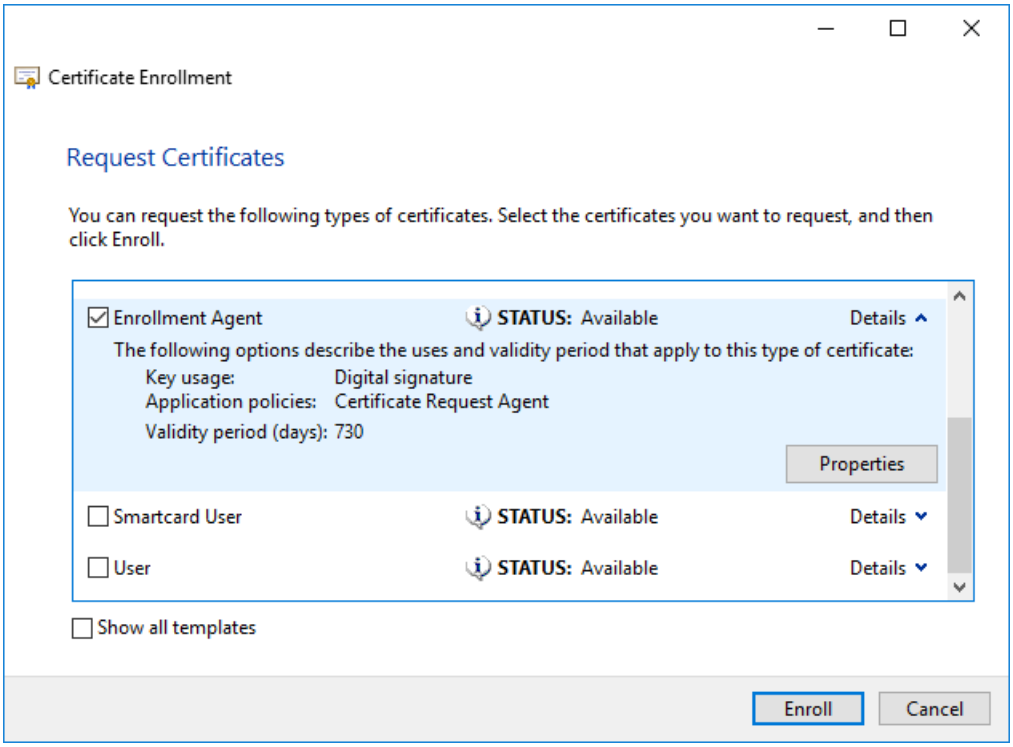


Figure 126. Request Certificates

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).

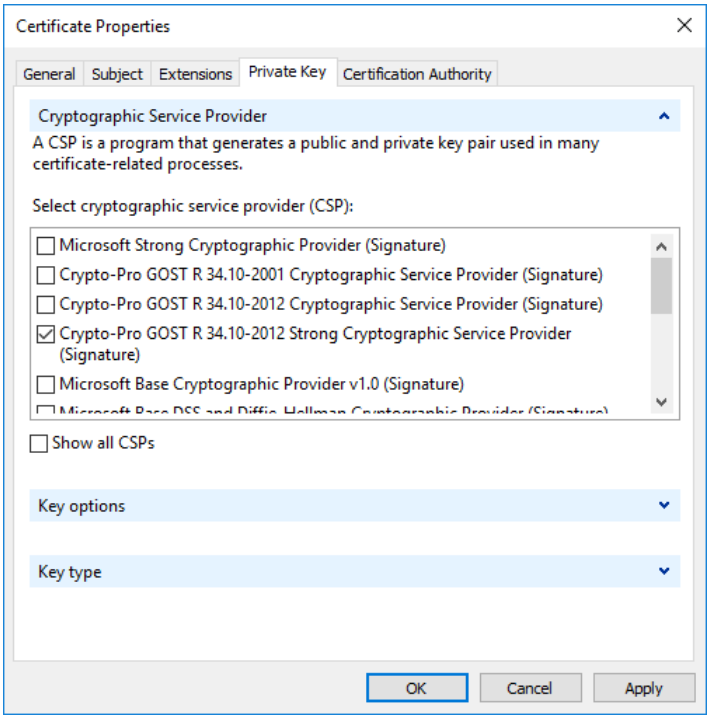


Figure 127. Certificate Properties

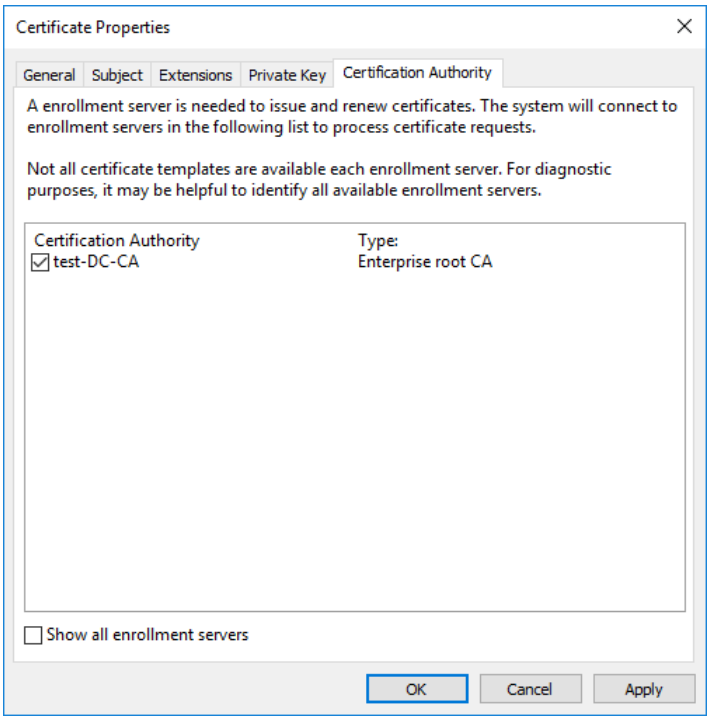


Figure 128. Certification Authority

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).

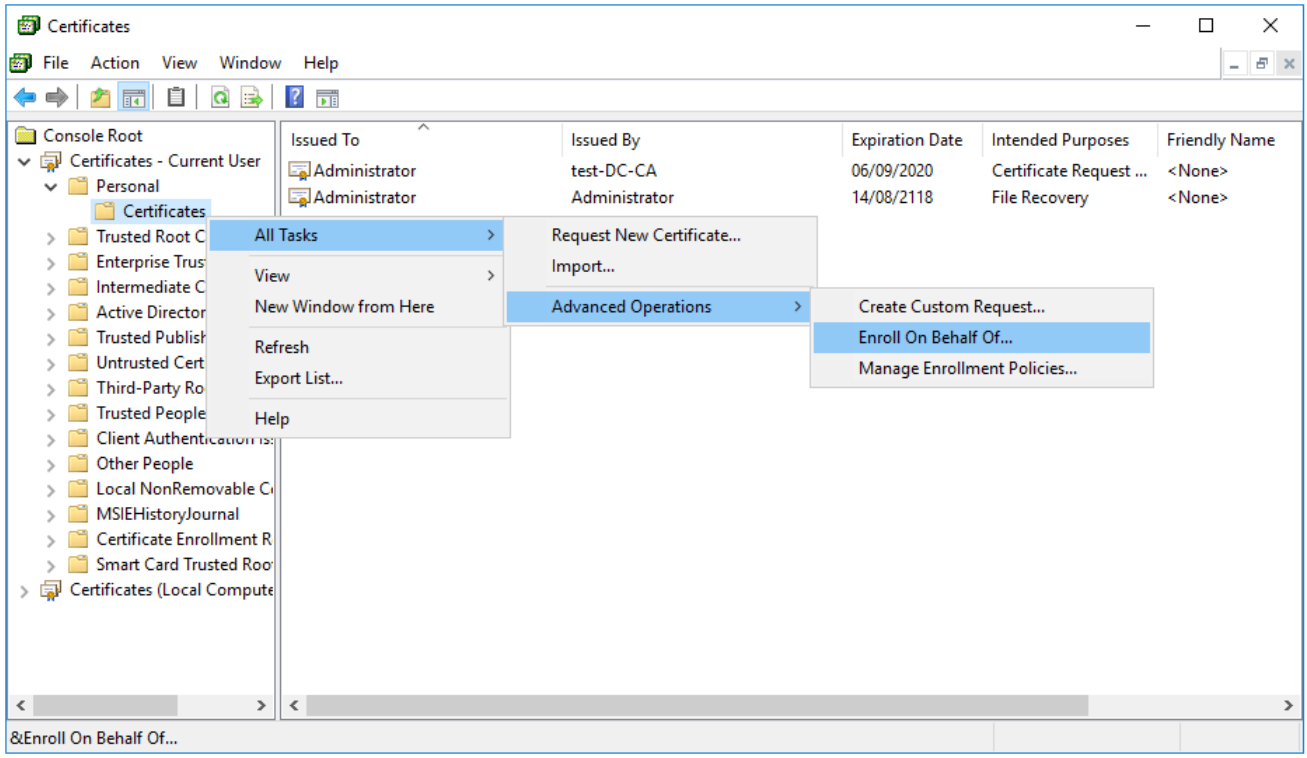


Figure 129. Certificates snap-in

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).

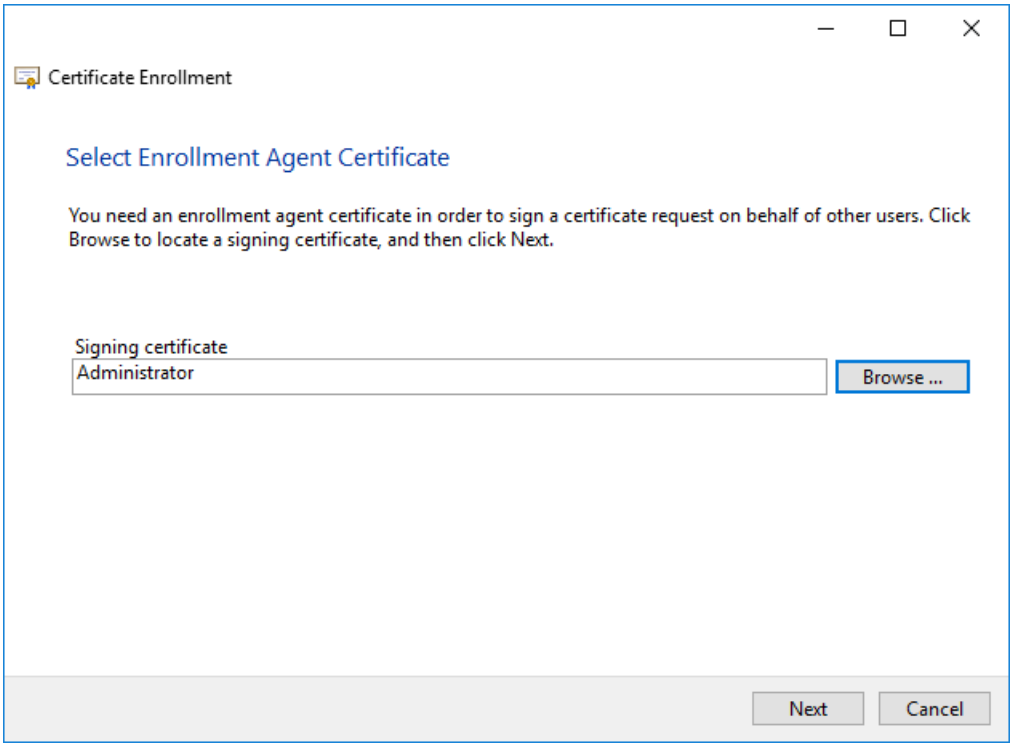


Figure 130. Select Enrollment Agent Certificate

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.

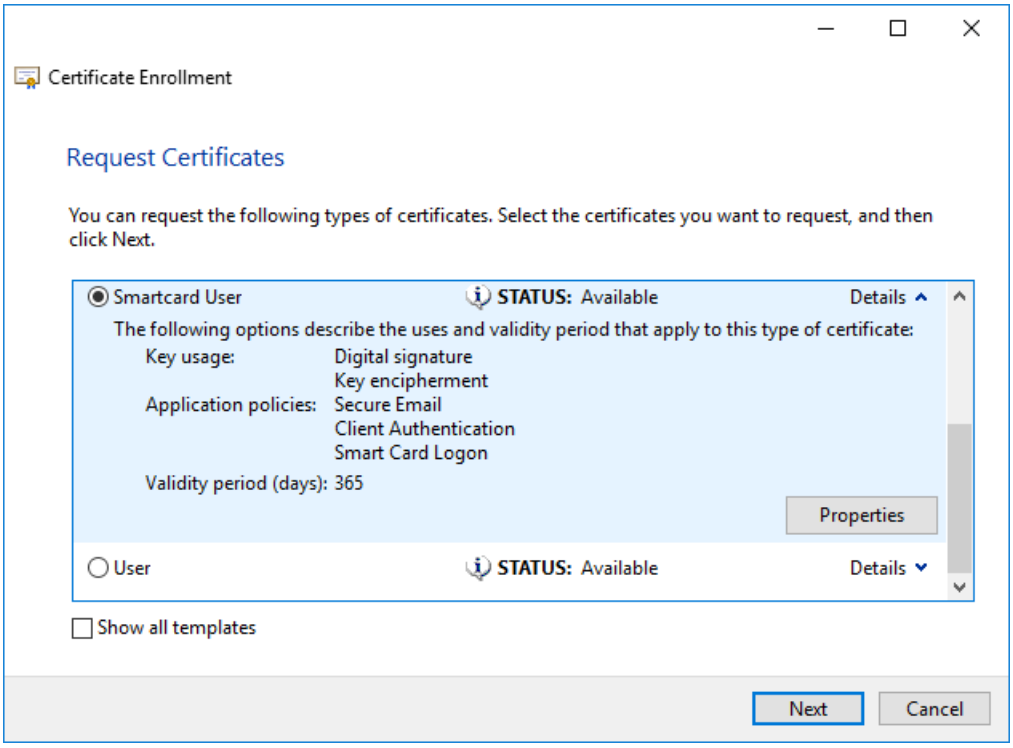


Figure 131. Request Certificates

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).

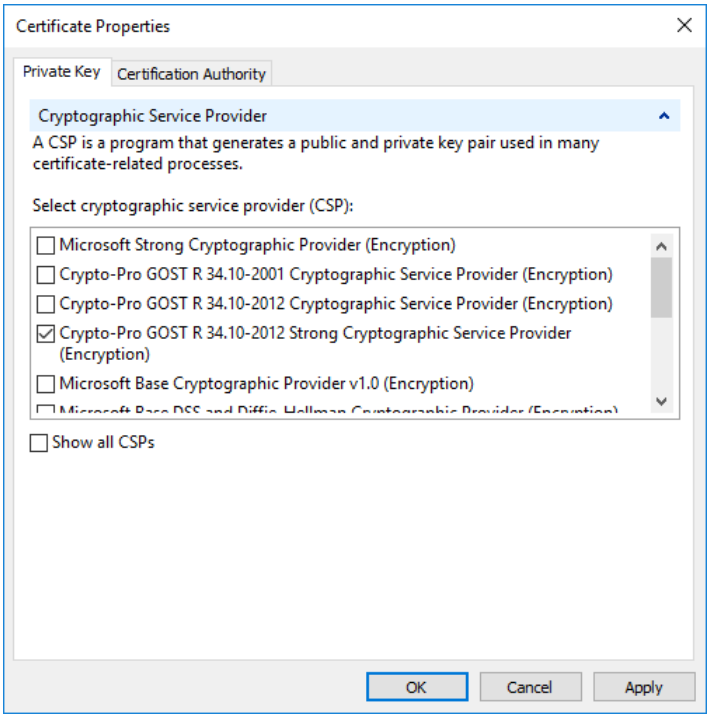


Figure 132. Certificate Properties

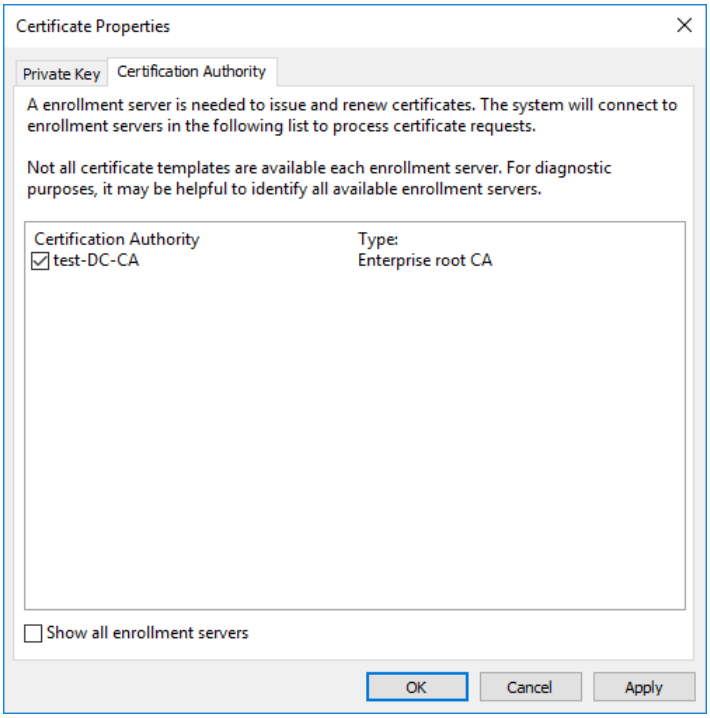


Figure 133. Certification Authority

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).

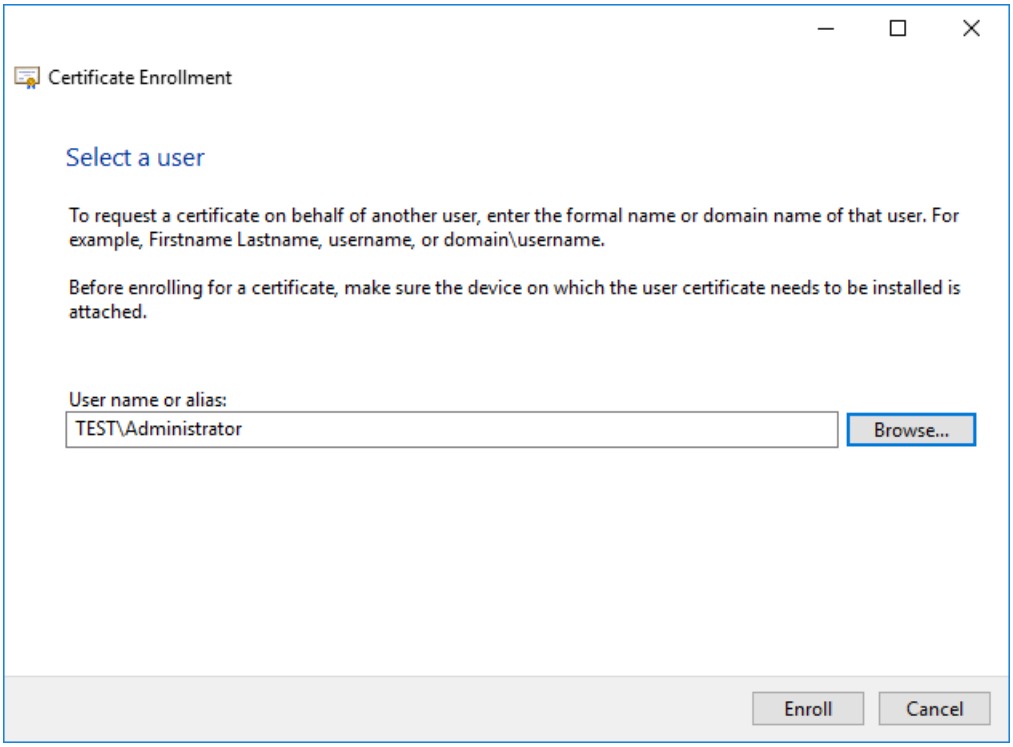


Figure 134. Select a user

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).

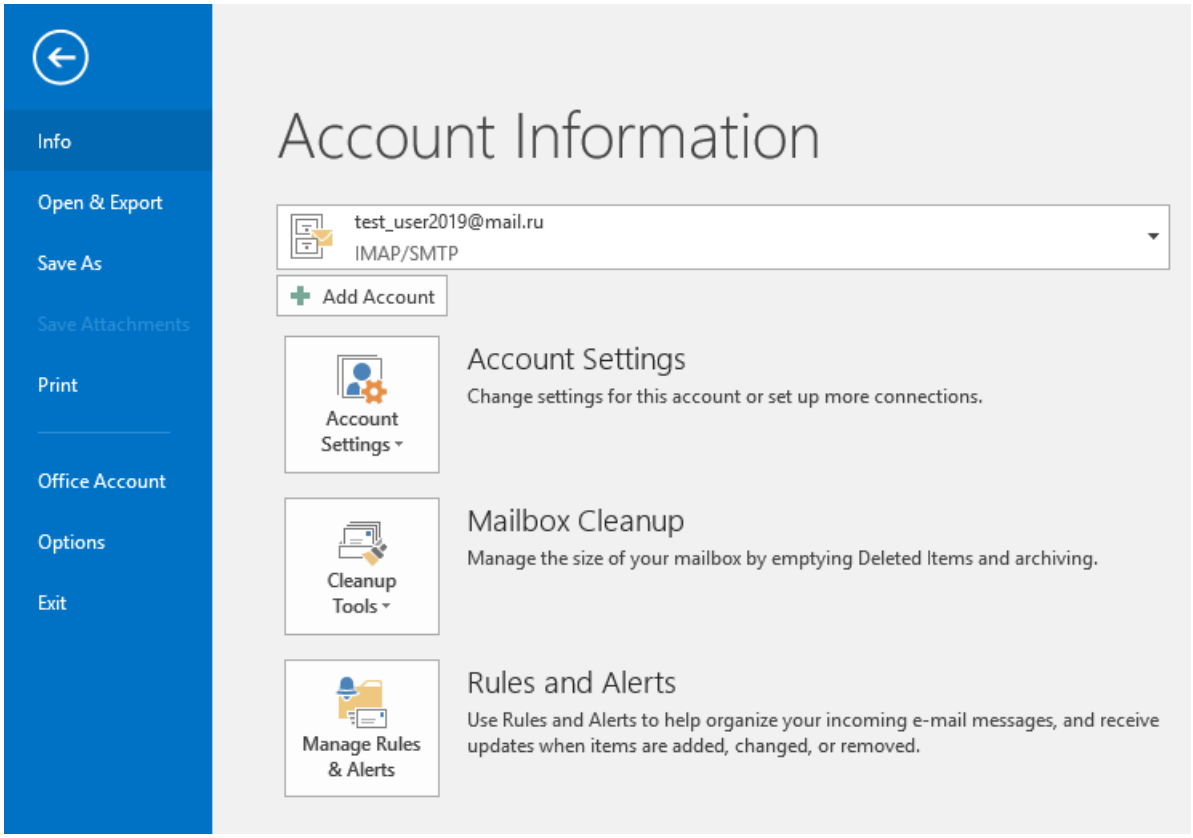


Figure 135. Outlook File menu

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

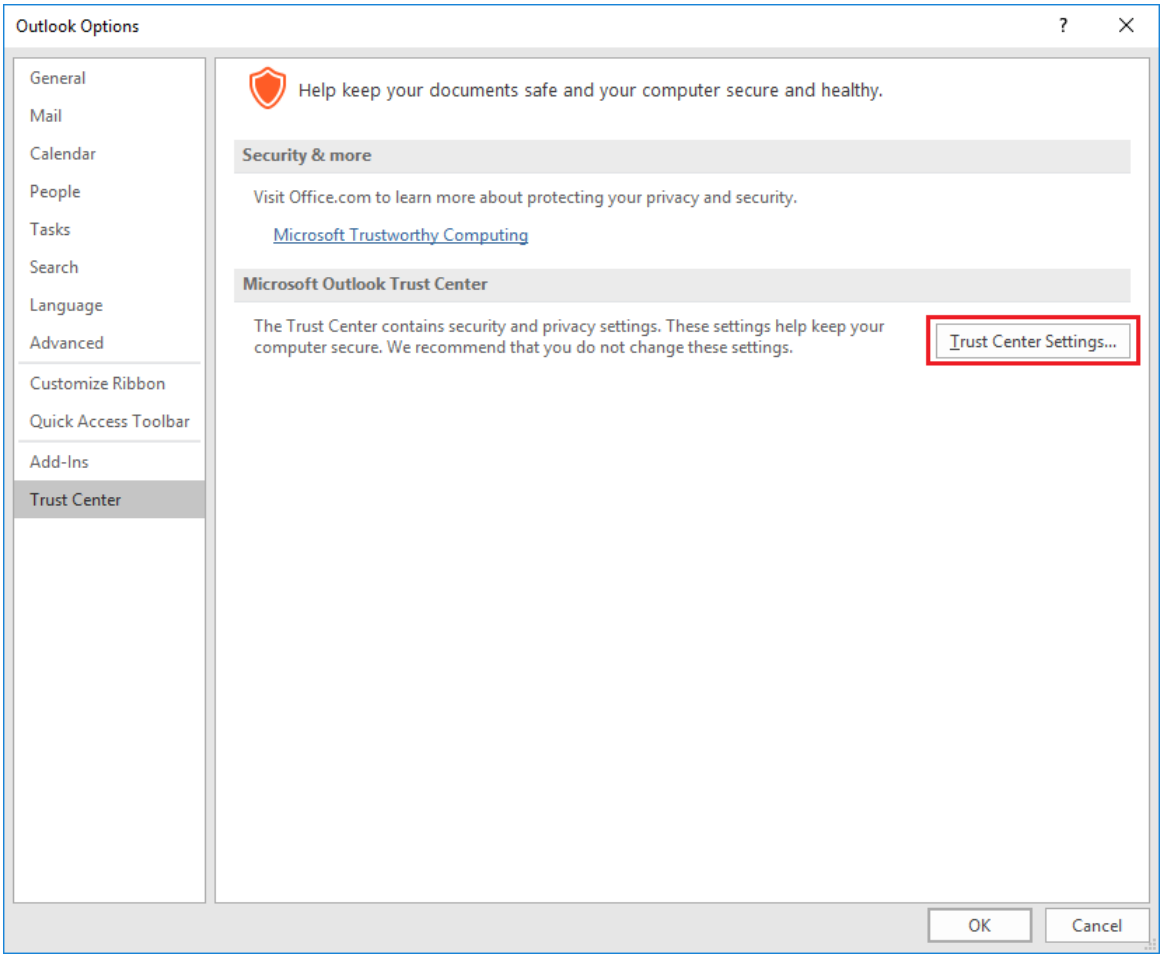


Figure 136. Trust Center tab

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

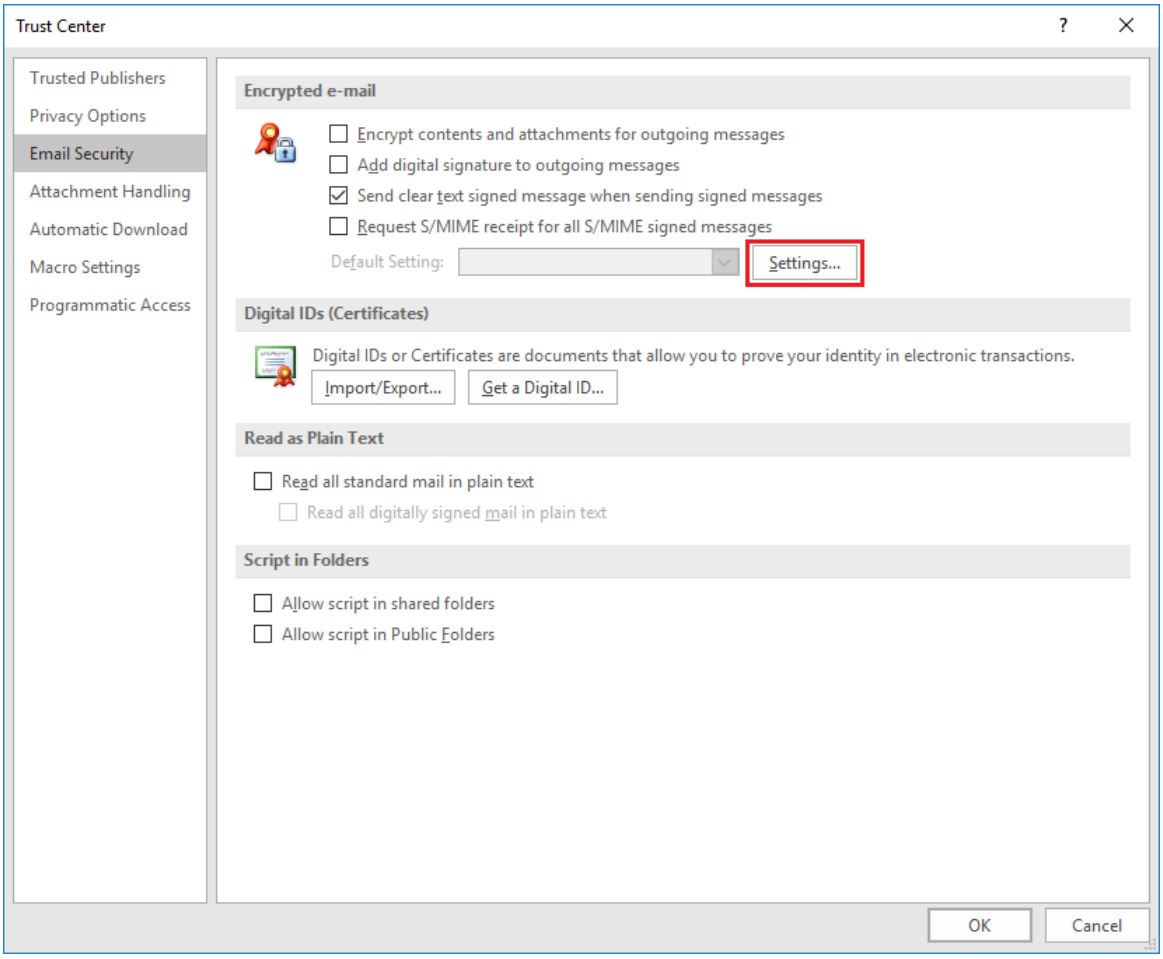


Figure 137. E-mail Security tab

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**.

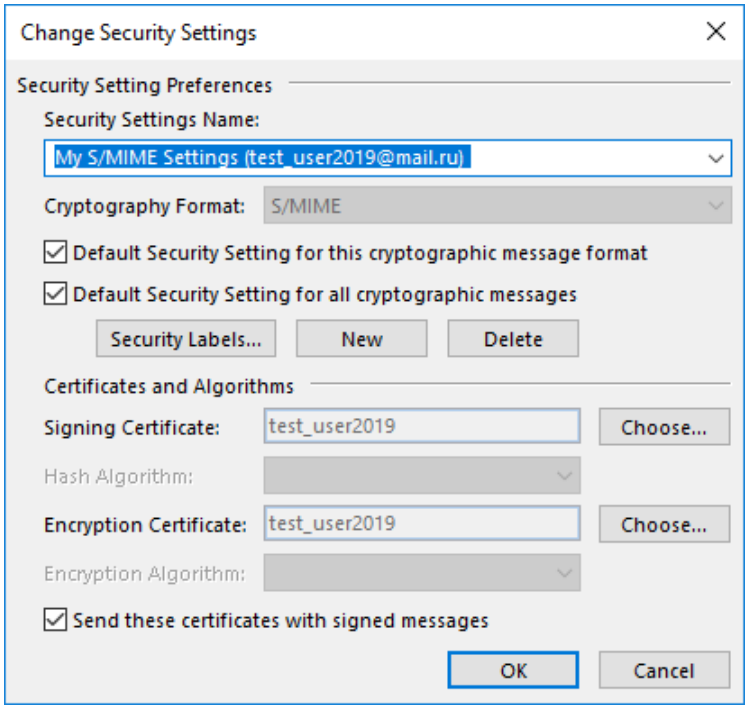


Figure 138. Changing e-mail security settings

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.

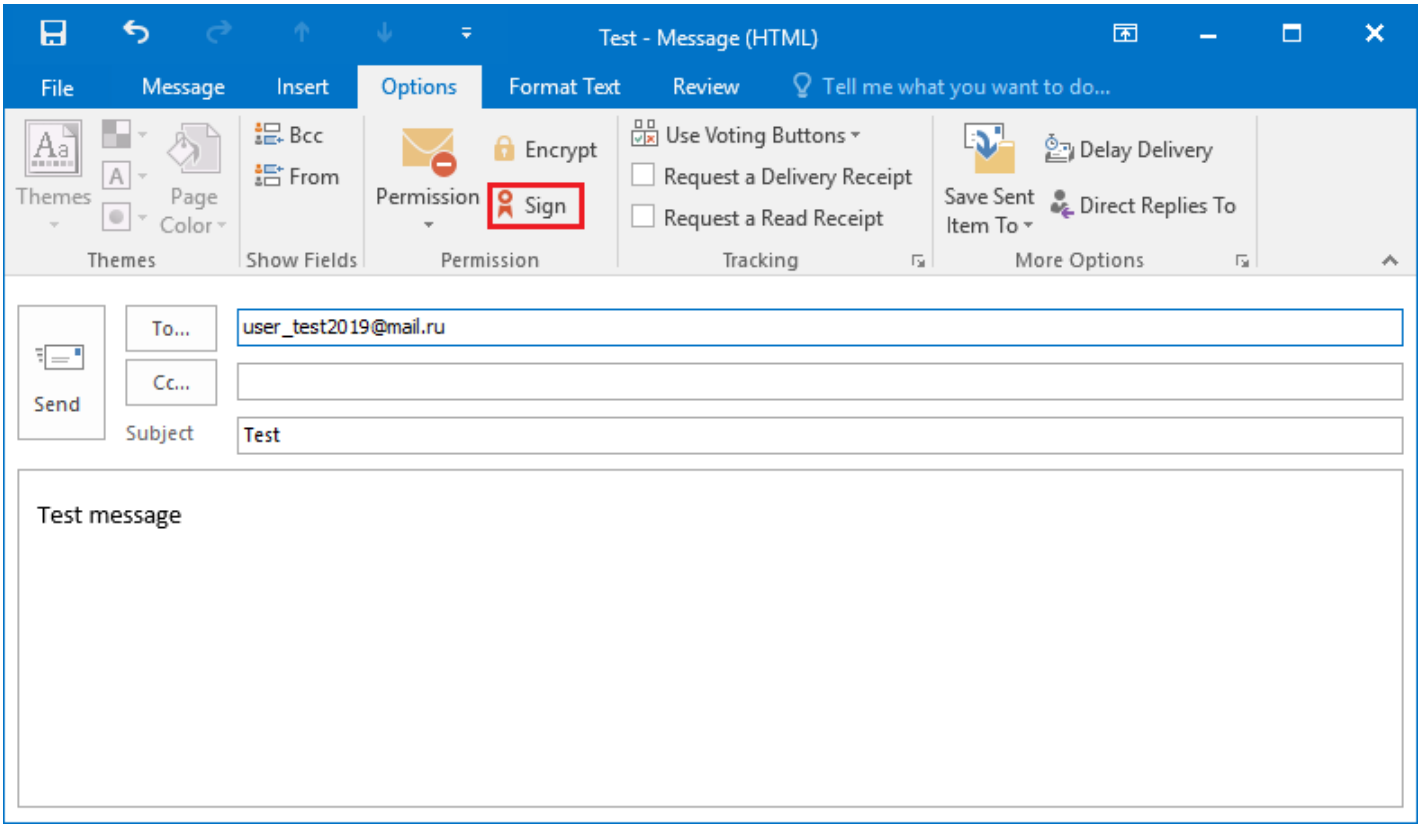


Figure 139. Signing a message

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.

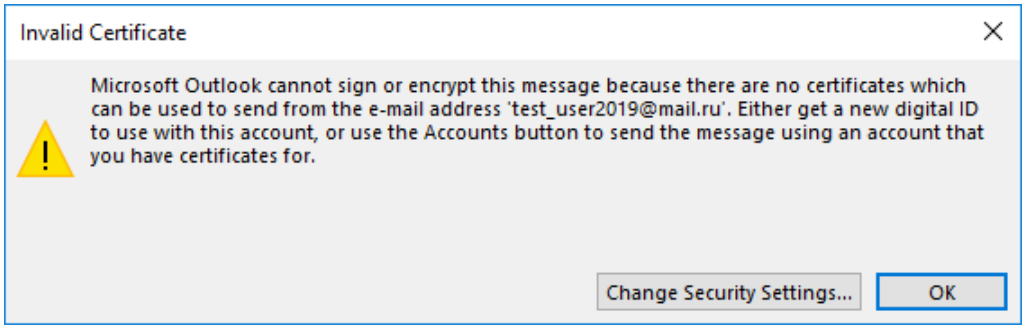


Figure 140. Message signing error

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.

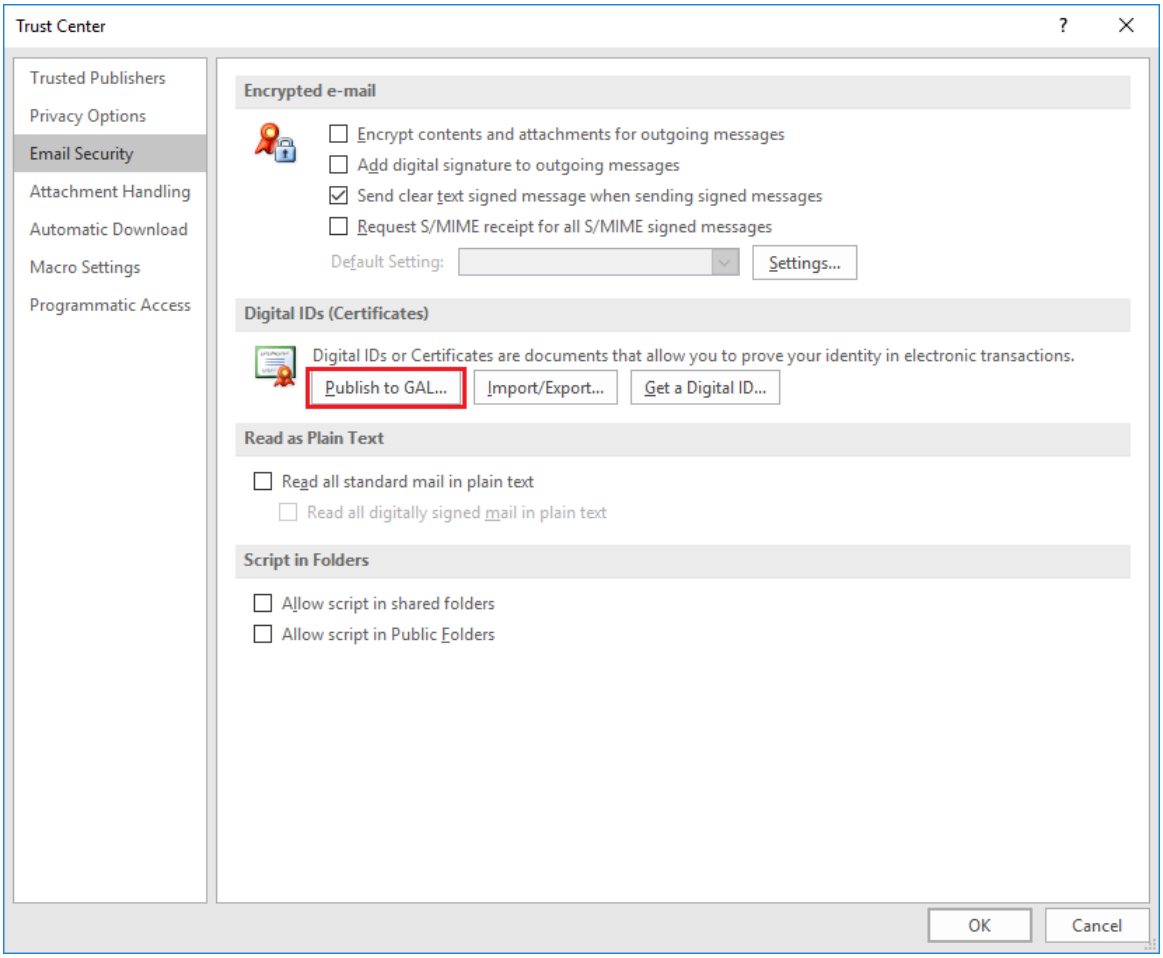


Figure 141. Publishing certificate to GAL

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.

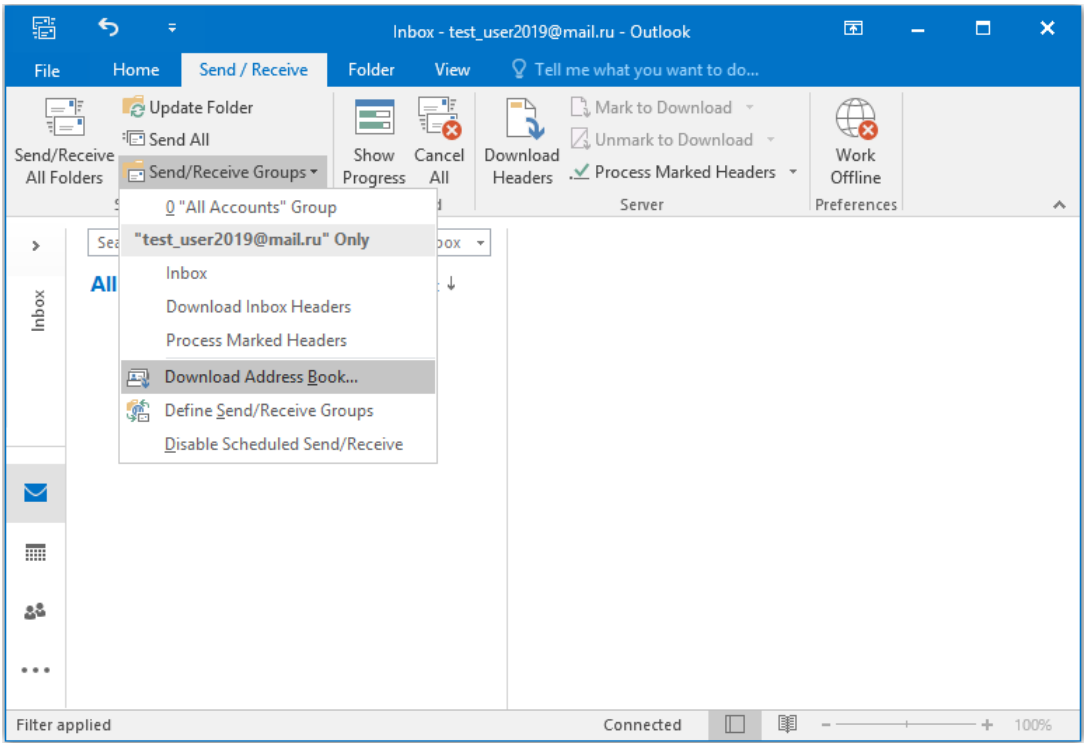


Figure 142. Downloading address book

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).

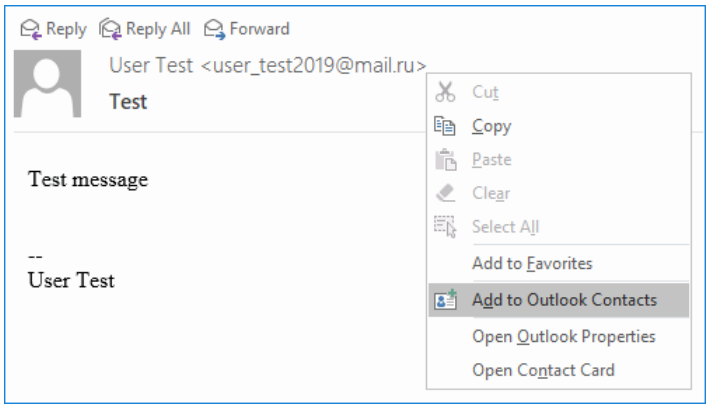


Figure 143. Adding user to contacts

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;

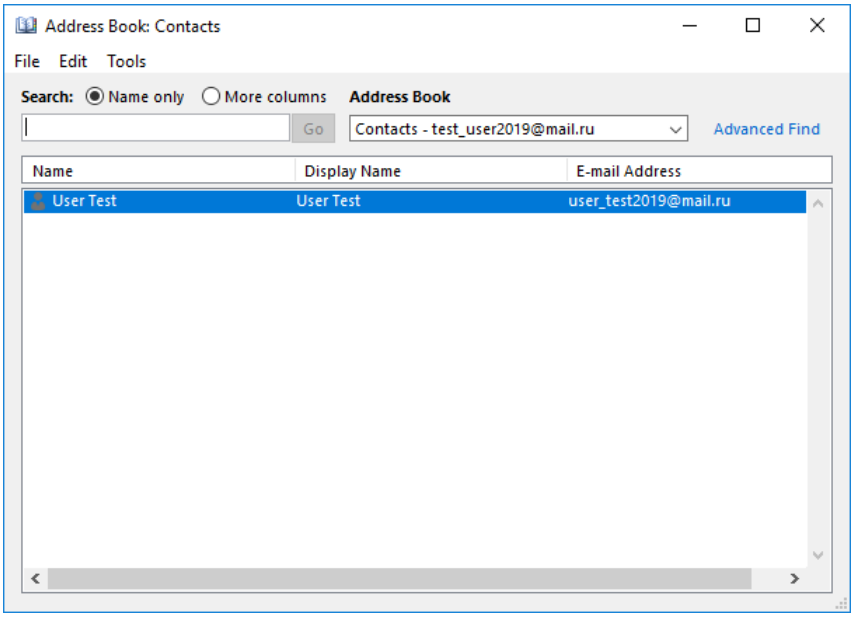


Figure 144. Local address book

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

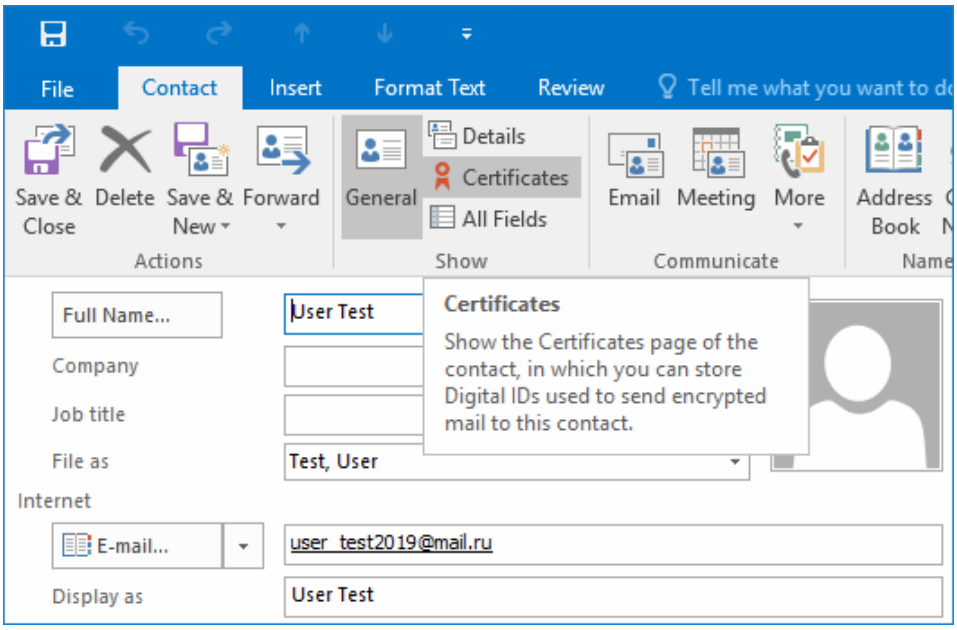


Figure 145. Address book contact

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

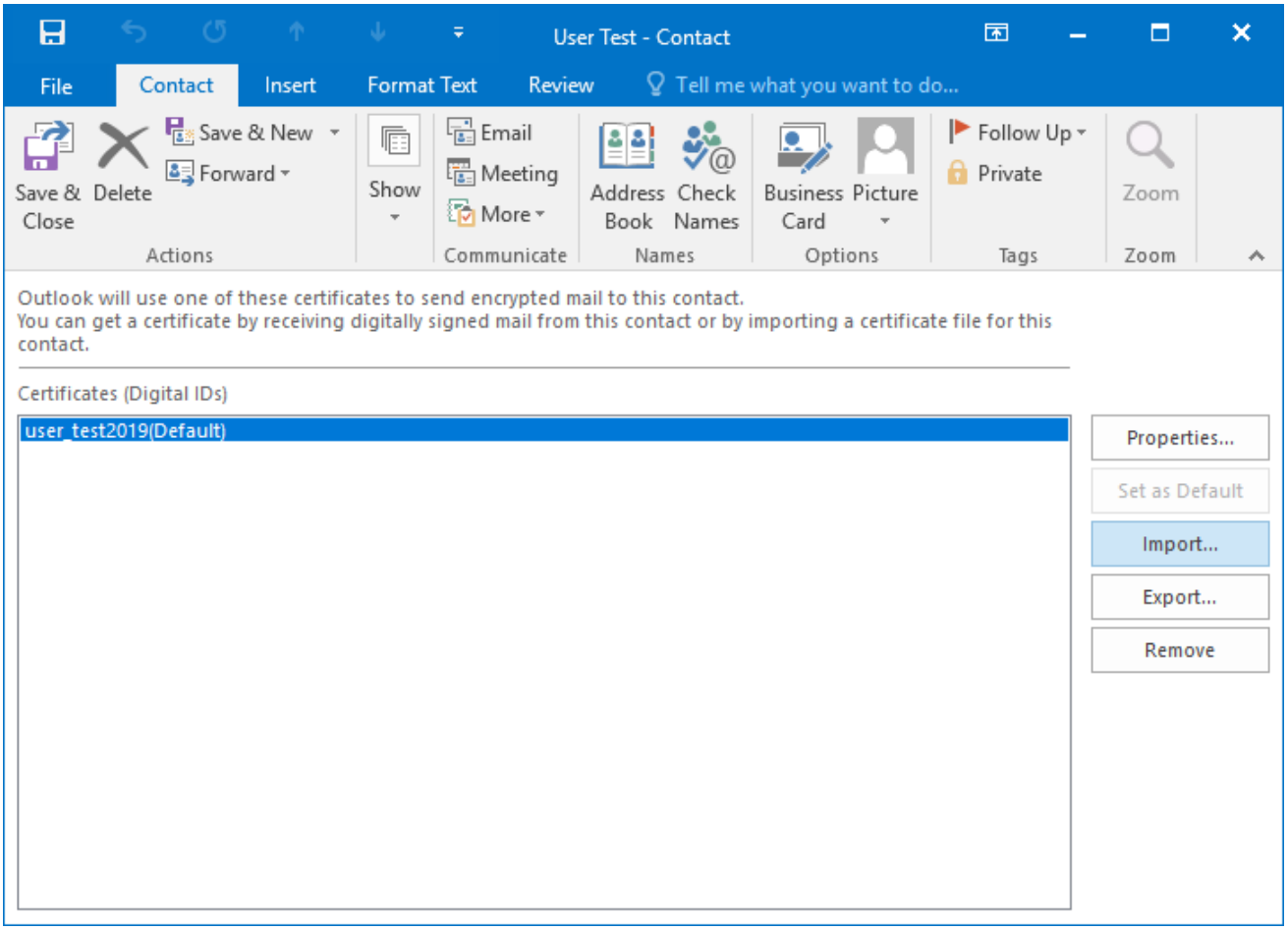


Figure 146. Contact certificate

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.

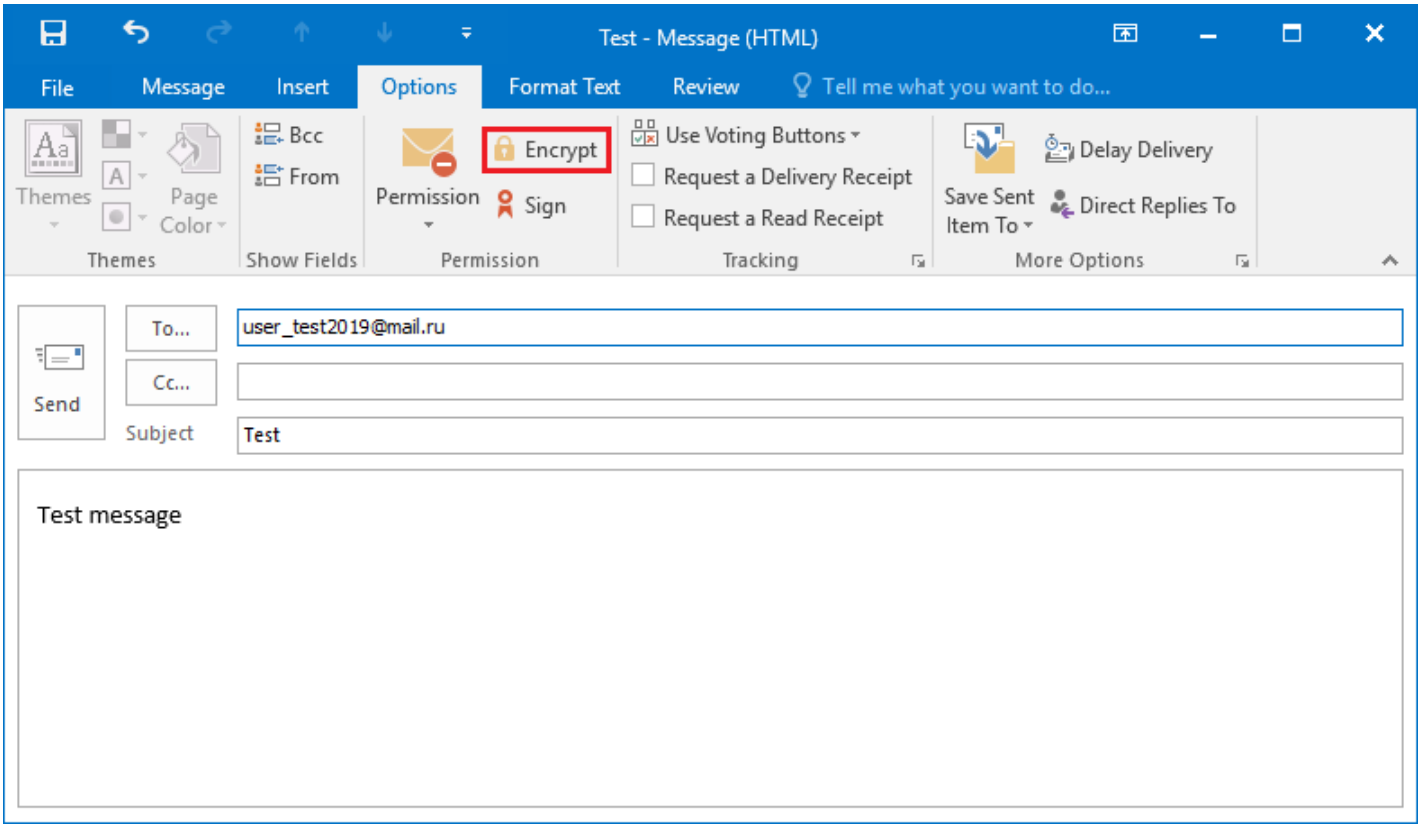


Figure 147. Encrypting a message

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).

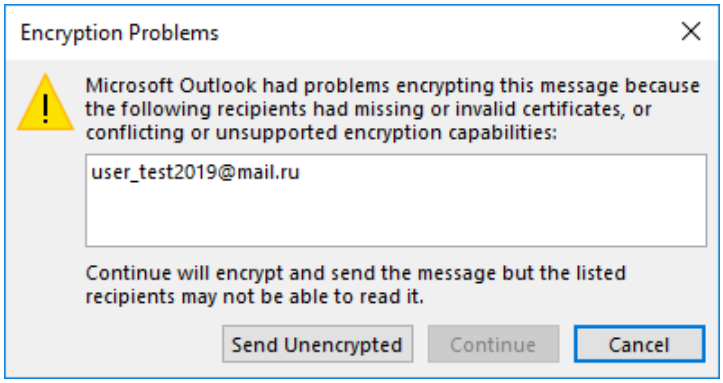


Figure 148. Message encryption error

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 button — the

sign of the encrypted message.

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

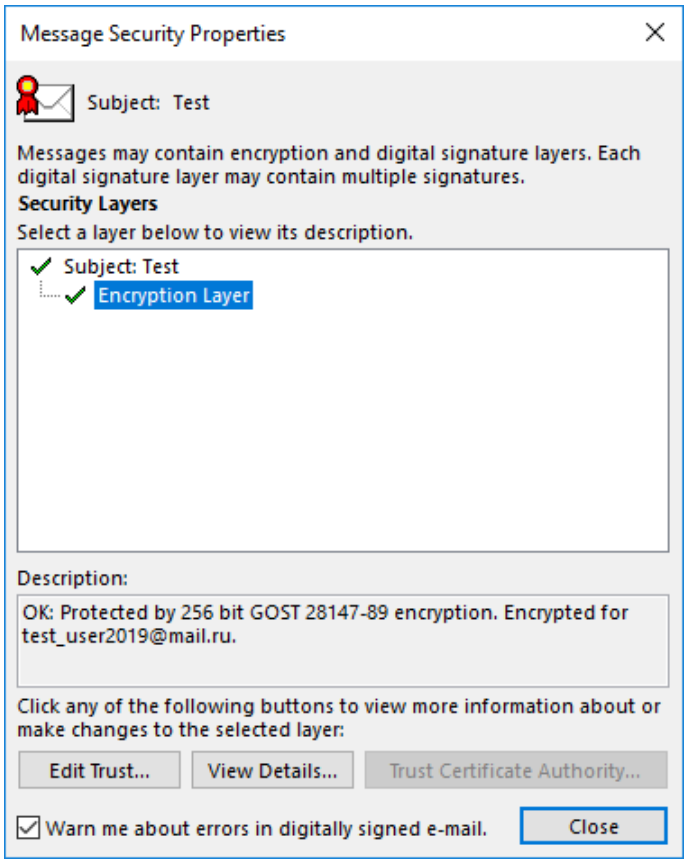


Figure 149. Message Security Properties

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).

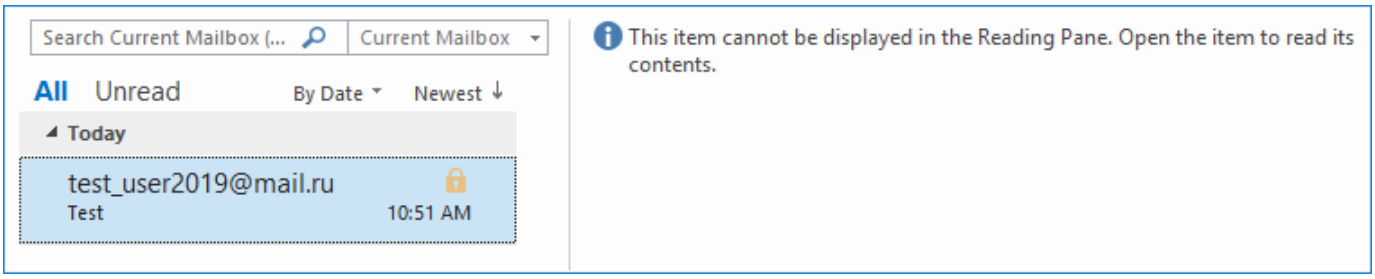


Figure 150. Viewing an encrypted message without certificate

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

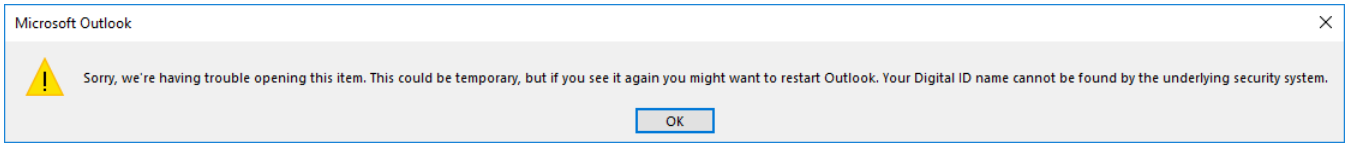


Figure 151. Error viewing the encrypted message

6.6 Verifying the signed message sender certificate

To verify the user certificate, open the signed message and click button — the sign of the signed message.

The digital signature verification window opens (Figure 152).

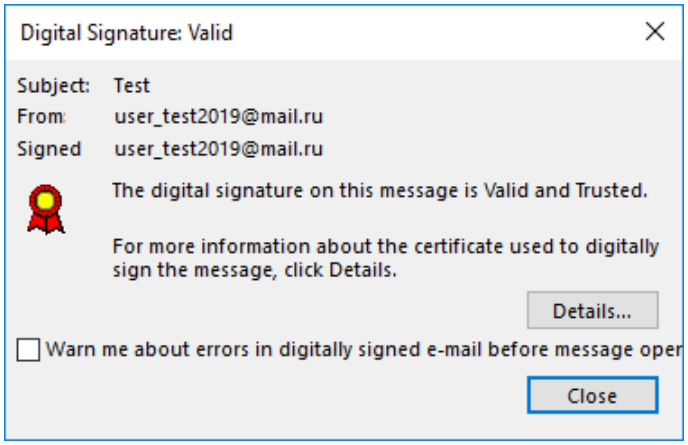


Figure 152. Verifying the message signature

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

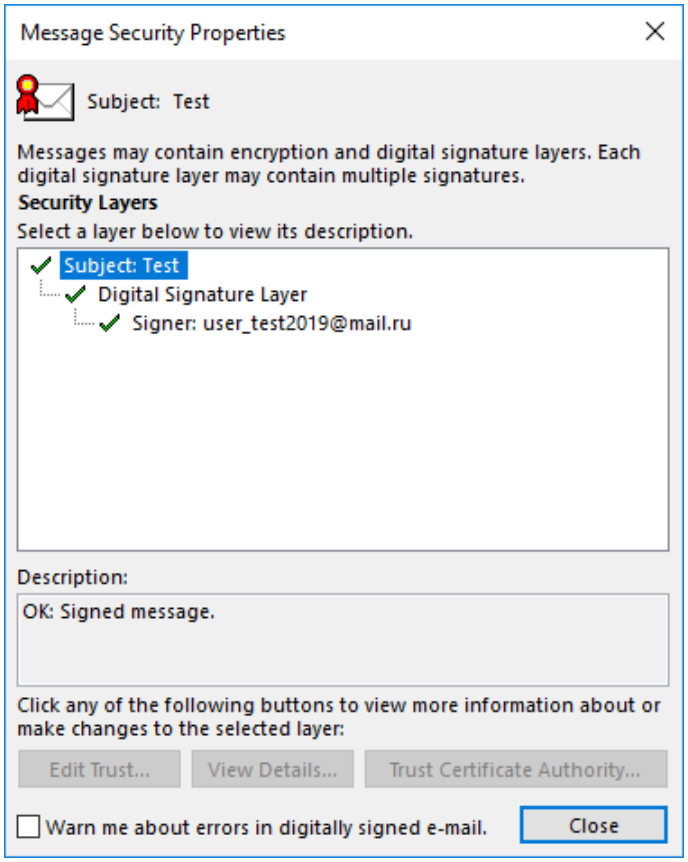


Figure 153. Digital signature details

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).

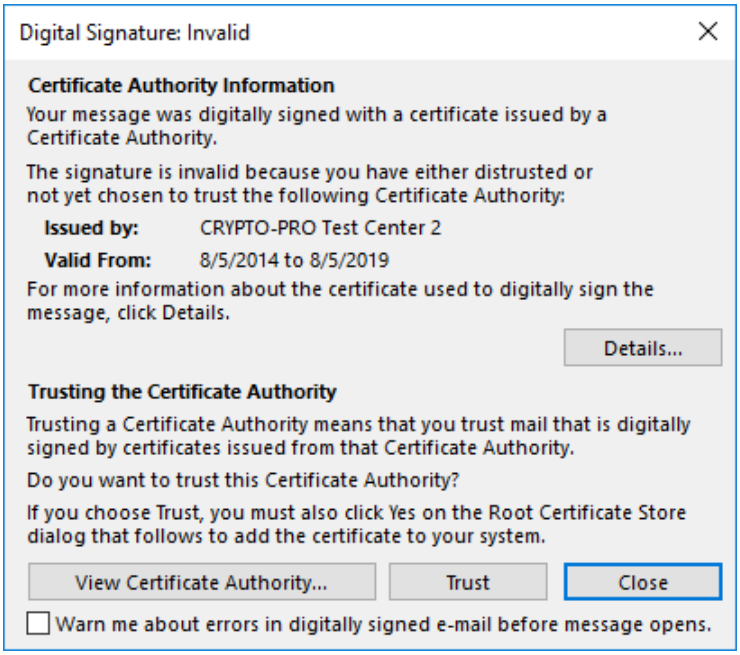


Figure 154. Warning about an untrusted CA

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

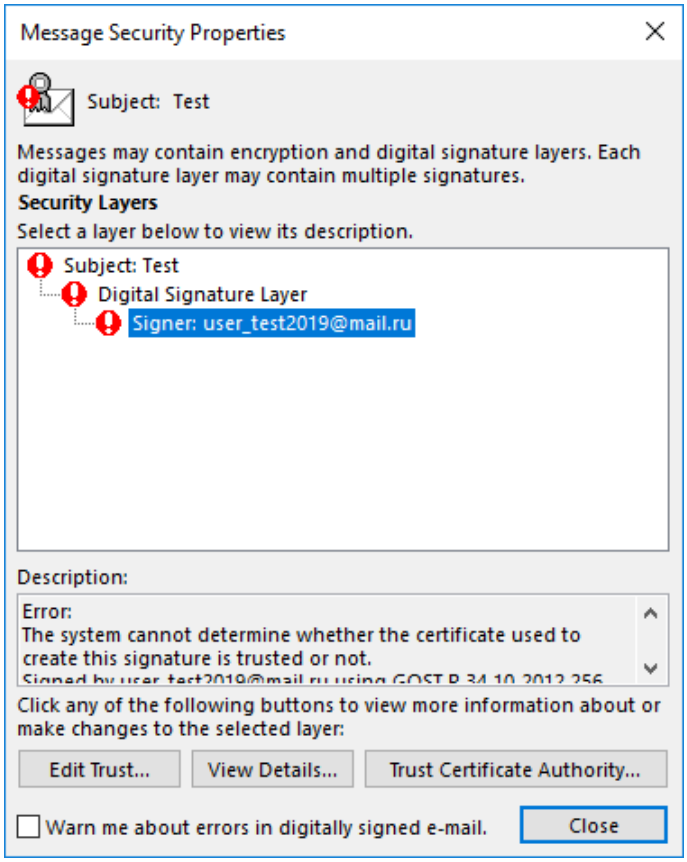


Figure 155. Message Security Properties

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).

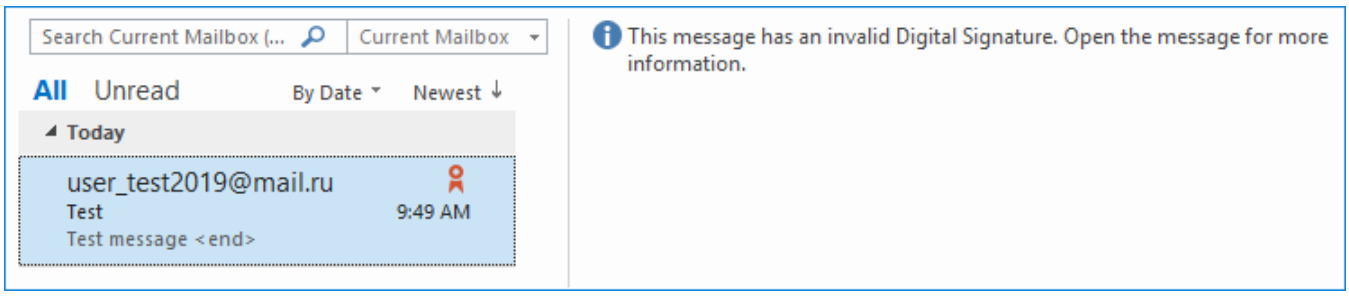


Figure 156. Viewing a signed message without certificate