



**Guide –**

# **Certum Commercial SSL**

**Certum Commercial SSL [Certificate Activation Guide](#)**

version 1.2



## Table of Contents

1. Product description.....	3
2. Product activation.....	3
2.1. Adding the activation code.....	3
2.2. Start of certificate activation.....	4
2.2.1. Activation method – key pair generation.....	5
2.2.2. Activation method - CSR request.....	7
3. Filling in the form during activation.....	10
4. Verification of access to the domain.....	11
4.1. Verification of the administrator's email address.....	12
4.2. Verification of the access to the domain by placing a file on the server.....	13
4.3. Verification of the access to the domain by creating an appropriate TXT record in the DNS...	13
5. Certificate downloading.....	14
5.1. Downloading the pfx/p12 file after activation via key pair generation.....	14
5.2. Downloading the certificate and private key files (CSR method).....	16

## 1. Product description

An SSL certificate (TLS) is a security protocol certifying the authenticity of a domain and its owner. It encrypts and secures traffic on websites, including the transmission of confidential data that customers enter on your site. Thanks to an SSL certificate all personal data, logins and passwords, credit card numbers and other data of your customers will be secured.

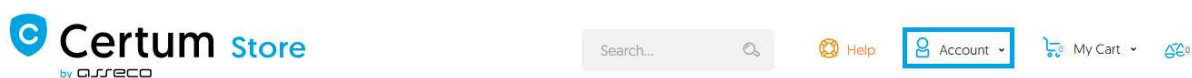
## 2. Product activation

The guide is prepared using the example of Google Chrome browser and concerns the process of activating the [Certum Commercial SSL](#) certificate.

After placing an order in the Certum shop, activation will be available in the [Certificate Activation](#) tab (see section 2.2).

### 2.1. Adding the activation code

If you want to activate the product from an electronic code received e.g. on your e-mail address - before you begin the activation, add the code in the [Electronic Codes](#) tab. To do so, log in to your account on <https://sklep.certum.pl>



In case you do not have an account, click on the [Create an Account](#) button to create one. If you already have an account, select [Log in](#).

## Customer Login

### Registered Customers

[Log In](#)[Forgot Your Password?](#)

### New Customers

Creating an account has many benefits: check out faster, keep more than one address, track orders and more.

[Create an Account](#)

After logging in, click on the customer panel - [Your Account](#).

To add a code select the [Electronic Codes](#) tab. Enter the code in the [Electronic code](#) field and click [Add](#) button.

**Note!** Remember that the activation code consists of 16 characters. After entering or copying the code make sure that the number of characters is correct.

## My Account

My Account  
 My Orders  
 My Downloadable Products  
 Address Book  
 Account Information  
[Electronic codes](#)  
 Newsletter Subscriptions  
 Account balance  
 Cards saved in Dotpay  
 My Archive Orders  
 Activate Certificates  
 Manage Certificates  
 Tools ▾  
 Domain verification

### Electronic codes

New activation code from activation card


### Your codes

[Purchased in the store](#)

[Entered manually](#)

Search code

All codes ▾

No eligible codes found.

If you enter the code correctly, the product will appear on the list in the [Your codes/Entered manually](#) section. After processing the code, go to the [Activate Certificates](#) tab [see next point 2.2].

## 2.2. Start of certificate activation

After placing an order or adding a code to your account, start activation in the [Activate Certificates](#) tab.

- Electronic codes
- Activate Certificates
- Certificates' management
- Orders history
- Address details
- Tools
- Newsletter
- Domain verification
- Technical support
- Knowledge

### Activate Certificates

Service name:

Activation state:

Order Number:

Payment state:

In accordance with Article 13 sec. 1 and 2 of the General Data Protection Regulation (GDPR) of 27 April 2016 (hereinafter referred to as the "Regulation") I hereby inform that:

1. The Administrator of your personal data is Asseco Data Systems S.A. seated in Gdynia, ul. Podolska 21, 81-321 Gdynia;
2. The Data Protection Officer of Asseco Data Systems S.A. can be reached at the email address: [IOD@asseccods.pl](mailto:IOD@asseccods.pl), or phone number +48 42 675 63 60.
3. Your personal data will be processed for the purpose necessary for the performance of the non-qualified certificate agreement pursuant to Article 6 sec. 1 letter b of the Regulation.
4. Your personal data will be stored for a period of: 7 years from the date of revocation or expiration of the last certificate issued

Find the correct certificate in the list and click [Activate](#).

Service name	Order date	Order Number	Payment state
Commercial SSL, 1 year Issue	September 1, 2020		Payment booked Inactive certificate <span style="border: 2px solid orange; padding: 2px;">Activate</span>

**Important!** You can select between two methods of certificate activation. We recommend using the CSR method, which will provide you with a certificate file (public part) and a private key. For this method, a CSR request must first be generated:

- either by the server administrator or
- via [the CSR generator](#), available in the Certum shop user account.

If you need the pfx/p12 file, you can choose the method of key pair generation.

### 2.2.1. Activation method – key pair generation

If you want to perform the activation using the key pair generation method, click on the [Next](#) button.

**Activation** ⓘ

1.Orders 2.Method Choice ⓘ 3.Keys 4.Data 5.Confirmation

---

Service name **Commercial SSL, 1 year Issue**

---

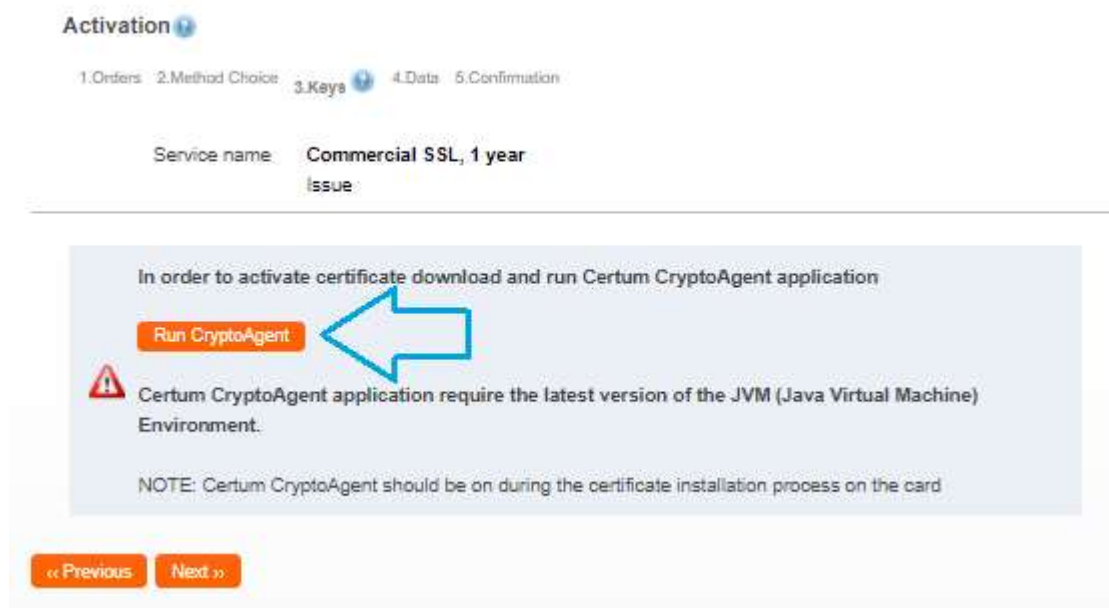
Select delivery method of key pair for certificate

Key pair generation ⓘ  
 CSR ⓘ

Additional info about CSR can be found in Help section or can be obtained from infoline consultants.

Next >>

In order to generate the keys, download and run the [Certum CryptoAgent](#) app (to run the app you need a Java environment installed on your computer <https://www.java.com/pl/>).



A warning communicate will appear in the bottom bar of your browser, where you can click [Save](#) to download the [Certum](#) app.

When the [Certum CryptoAgent](#) window appears, run the app by clicking [Run](#).



After a short while, the app will run in the background and during the activation process there will be a possibility to save the keys in the [Certum](#) app. The default settings, i.e. RSA key algorithm [change to EC possible] and 2048 key length are correct for SSL certificate operation.



**Activation**

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name: **Commercial SSL, 1 year Issue**

---

Keys safety level \*  Save your keys on the Certum Crypto Agent.  Certum Smart Card

Key algorithm: RSA  
Key size: 2048

**Generate keys**

« Previous Next »

After clicking on the [Generate Keys](#) button, a message will appear that the certificate keys have been generated. Clicking the [Next](#) button will take you to the next activation step [see chapter 3 - Filling in the form during activation].

**Activation**

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name: **Commercial SSL, 1 year Issue**

---

Keys safety level \* Certificate keys have been generated

« Previous **Next »**

### 2.2.2. Activation method - CSR request

The CSR (Certificate Signing Request) should be at least 2048 bits long, after it has been generated it will be sent to a certifying institution for signing, i.e. creating an appropriate public key. The file can be generated on the server or in the Certum shop user account. In addition to the CSR file, a private key file [privateKey.pem] will be generated.

In order to generate a CSR file in your user account, wait with the activation and select the [Tools](#) section on the left.

In the list that will expand, select the option [CSR Generator](#).

To obtain a CSR, fill in the fields in the form as indicated on the page. After checking the details and selecting the checkbox next to the required consent, click on the [Generate](#) button.

**\* required fields**

- I agree to the Certification Authority server generating a private key and CSR. I also acknowledge that the private key generated with the CRS is not stored by the Certification Authority in any form. It is displayed and available exclusively in the browser window upon its generation.

The next step is to save two files: the CSR and the private key using the [Download](#) buttons (the files will be saved on your computer, you can open them in a text editor e.g. Notepad). The CSR request file will be needed to activate the certificate, while the private key will be required to implement the certificate on the server.

**Important!** Remember not to lose these files and not to disclose your private key to anyone else. If the private key is lost after the SSL certificate has been issued, it will be possible to reissue the certificate.



Generated CSR

```

-----BEGIN CERTIFICATE REQUEST-----
MIICZDCCAUwCAQAwITESMBAGA1UEAwY2VydHViLnBsMQswCQYDVQQGEwJQTDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnMStY/MjXgL9oRjuatKBUy5
2knboIE9j0IMqLE4oZnY778NBXXaFTZCvJoUWYPKW6MNg/vPbH4qk0uzYrMn8eXw
jnMFTxliCiussYkTK6/4zBIU43y8Bgb+dNeK3EpnVi/0QEX3z4y9Ia+hW/DKWqX9
LkPm/8gK1XNA0NMZ8aKT9sWkHpZ7LbvUqg8hxxJv0kC71ttNBBN+BL3iv1dI+fG
xF14GH77q7V/RayIZNppqHiwvBvEFZi5/POdiRsrM4Y7YO3baveJXBei/qmZn39o
UaxQqZgxWs5ATut55/VybNtK1L/SadOvYvJ5gHAHlrZDzIqAm2td2vy0WSkYr88C
AwEAATANBgkqhkiG9w0BAQsFAAOCAQEAIvBmSbZ74E2TGfeCKIKF4+HDXii/ALn2
UR4jocwCrywU+7kC1zODET84JEb9tiayCC3EJLmBqpp+Jv498/5fctiCpiOILs+

```

[Download](#)

---

Generated private key:

```

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAcqK1gyNaAv2hGO5q0oFTLnaSduiUT2PQgyosTihmdjvww0F
ddoV/NkK8mhRZg8pbow2D+89sfqTS7Nisyfp5fCOcwW1eWIKK8yxiRMmjMGVTj
fLwGBv5014rcSmdWL/RARfPJL0hr6Fb8Mpapf0uQ+blyArVc0DQ0xxnopP2xaQe
Instu+5CDSHHAml/SQLvW22c0EE34EveK/VQj58bEXXgYfvurtX9Frikh2mmoeLC8
G8QVkjn8852JGyszhtg7dtq94lcF6L+qZmHf2hrRfCpmDFazkBO63nn9XJs20rU
v9Up0698nmAcAcitkPMioCba13a/LRZKRivzwlDAQABaolBABEXjGzxhlgSBDWd
aElyyEfJ6YxHvJYa8UGizndQcQvwh2me4O7VDg+RNJT4Ww5nv0Oxh5igb5ZfqMYU
/5izKhtlVL6FU5gtY0K0NobK1Dn5fGoMXn3e22h20sljqzseHdHj71hbspvDKhHo
1z1s0SUmUDLmNHLW1VI++4C9fGJR3BXcMAq7RdPE5bGoQ8Wd4J1dCoEomQfWmx

```

[Download](#)

Once you have saved the files, you can return to the certificate activation. The first step is to paste the contents of the CSR file.

**Important!** Make sure to paste the whole character string.

**Activation**

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name **Commercial SSL, 1 year**  
Issue

CSR \*

```

-----BEGIN CERTIFICATE REQUEST-----
MIICZDCCAUwCAQAwITESMBAGA1UEAwY2VydHViLnBsMQswCQYDVQQGEwJQTDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKnMStY/MjXgL9oRjuatKBUy5
2knboIE9j0IMqLE4oZnY778NBXXaFTZCvJoUWYPKW6MNg/vPbH4qk0uzYrMn8eXw
jnMFTxliCiussYkTK6/4zBIU43y8Bgb+dNeK3EpnVi/0QEX3z4y9Ia+hW/DKWqX9
LkPm/8gK1XNA0NMZ8aKT9sWkHpZ7LbvUqg8hxxJv0kC71ttNBBN+BL3iv1dI+fG
xF14GH77q7V/RayIZNppqHiwvBvEFZi5/POdiRsrM4Y7YO3baveJXBei/qmZn39o
UaxQqZgxWs5ATut55/VybNtK1L/SadOvYvJ5gHAHlrZDzIqAm2td2vy0WSkYr88C
AwEAATANBgkqhkiG9w0BAQsFAAOCAQEAIvBmSbZ74E2TGfeCKIKF4+HDXii/ALn2
UR4jocwCrywU+7kC1zODET84JEb9tiayCC3EJLmBqpp+Jv498/5fctiCpiOILs+
ZgZn25PSj/56M7SDeoukZtbeSAVFjro/pcAHVDFzhYHta03jbl4g+hW9y/gS
WJ8W1ffzygq19Sar0x1mf3RS18dMh96D1ALgPrri4ef3H4plwBD3uDAZj2vLVgYMP
jUf0DCYZl+coCs9U1PaqsDUxL4c1CipEoV1Cud+B+QwX+M4whSY0nUm0WTQ/DzD
ngtcLDxRRpDpvTpwjhbWkV0/GrfAq2n50q/h/8yt0ppHGma4+8tQ==
-----END CERTIFICATE REQUEST-----

```

[Previous](#) [Next](#)

Next is the stage concerning the SSL certificate data.

### 3. Filling in the form during activation

In this stage, fill in the form with the applicant's details and the certificate data. In case of using the CSR method, the data entered in the request will automatically be entered as certificate data. Fields with an asterisk [\*] are mandatory.

**Note!** If you want the certificate to secure two variants of the domain [yourdomain.eu and www.yourdomain.eu] enter the name of the website alone in the **Domain 1** field and tick the checkbox **add variant with www** on the right.

**Activation**

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name: **Commercial SSL, 1 year Issue**

---

**Applicant data:**

Name:

Surname:

Phone:

Email:

**Certificate Data:**

Hash function: RSA-SHA256

Start of validity:

End of validity:

DNS Domain 1 \*   add variant with www

selecting the variant with www

« Previous **Next »**

\*Required

In the case of the wildcard SSL certificate issued for a group of subdomains within the main domain, e.g. \*.certum.pl, it will secure both the certum.pl and www.certum.pl domains (without selecting the checkbox) and subdomains within the certum.pl domain. Remember to start your domain name with \*.yourdomain.eu. After filling in the data, click the **Next** button.

In the last step (Confirmation), verify that the entered data is correct and select the required approvals and declarations, and then click **Activate**.

**Certificate Structure:**

Subject: CN=certum.pl

Subject Alt. Name: dNSName=certum.pl, dNSName=www.certum.pl

---

Terms of Use

BEFORE SENDING TO CERTUM A REQUEST TO ISSUE CERTIFICATE, OR ACCEPTING CERTIFICATE OR THE FIRST USE OF IT, PLEASE READ THE TEXT OF THESE „TERMS OF USE FOR NON-QUALIFIED CERTIFICATES“ REFERRED TO AS „TERMS OF USE“. IF YOU DO NOT ACCEPT THESE TERMS OF USE, DO NOT SEND THE REQUEST TO ISSUE CERTIFICATE, DO NOT ACCEPT IT AND DO NOT USE IT.

THESE TERMS OF USE BECOMES EFFECTIVE FROM THE MOMENT OF SUBMITTING THE CERTIFICATE REQUEST TO „CERTUM - Certification Authority“ (HEREINAFTER „CERTUM“) AND ARE VALID UNTIL THE END OF CERTIFICATE VALIDITY PERIOD OR UNTIL THE CERTIFICATE REVOCATION. SENDING THE CERTIFICATE REQUEST MEANS THAT YOU WANT CERTUM TO REVIEW THE APPLICATION AND ISSUE THE CERTIFICATE, AND MEANS THAT YOU

I agree to Terms of Use \*

I declare and confirm that I am aware of the fact that the certificate may expose my personal data to the extent it has been indicated for inclusion in the certificate. I also confirm that all activities carried out using this certificate may, at my discretion, be available without restriction, in particular with regard to location. The use of the certificate is not affected by Asseco Data Systems S.A., provider of security services. \*

I confirm that I am of age \*

I hereby confirm the accuracy of my personal data included in the application for the certificate. \*

[<< Previous](#) [Activate](#)

\*Required

## 4. Verification of access to the domain

In order for Certum to issue the SSL certificate, the user should prove that they have access to the domain to be secured. The verification of the access to the domain should be performed in ONE of THREE ways:

- verification of the e-mail address by confirming the verification link, which will be sent by [Certum](#) to the administrator's address (e.g.: [admin@yourdomain.eu](#), [administrator@yourdomain.eu](#), [webmaster@yourdomain.eu](#), [postmaster@yourdomain.eu](#), [hostmaster@yourdomain.eu](#)),
- verification of the access to the domain by placing on the server a file with a name that the user receives from [Certum](#),
- verification of the access to the domain by creating an appropriate TXT record in the DNS with a name that the user receives from [Certum](#)

You can select the method of verification of access to the domain in the [Activate Certificates](#) tab. Select the certificate you are interested in from the list and click on the [Verify Domain](#) button.

**Note!** The option to verify the access to the domain will be possible only after the activation of the product. The verification code is valid for 72 hours from the moment of sending, in case the link is no longer valid you can send the code again in the same way as the first code.

Electronic codes

**Activate Certificates**

Certificates' management

Orders history

Address details

Tools

Newsletter

Domain verification

Technical support

Knowledge

About Certum

### Activate Certificates

Service name:

Activation state:

Order Number:

Payment state:

[Search](#)

In accordance with Article 13 sec. 1 and 2 of the General Data Protection Regulation (GDPR) of 27 April 2016 (hereinafter referred to as the "Regulation") I hereby inform that:

1. The Administrator of your personal data is Asseco Data Systems S.A. seated in Gdynia, ul. Podolska 21, 81-321 Gdynia;
2. The Data Protection Officer of Asseco Data Systems S.A. can be reached at the email address: [IOD@assecods.pl](mailto:IOD@assecods.pl), or phone number +48 42 876 83 60.
3. Your personal data will be processed for the purpose necessary for the performance of the non-qualified certificate agreement pursuant to Article 6 sec. 1 letter b of the Regulation.
4. Your personal data will be stored for a period of: 7 years from the date of revocation or expiration of the last certificate issued

Service name	Order date	Order Number	Payment state
Commercial SSL, 1 year Issue	September 1, 2020		<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Payment booked</span> <span>Awaiting submission</span> </div> <div style="text-align: right; margin-top: 5px;"> <a href="#">Verify domain</a> </div>

In the next step you will see a list of domains to verify. Click on the domain name you want to verify.

Domain	Verified	End of Validity
 certum.pl	<span style="color: red;">✘</span> Not verified	

Note: Archived verifications are NOT available on this page.

When you click on the domain, the verification methods to choose from will appear.

#### 4.1. Verification of the administrator's email address

Using this method, select one from the list of available addresses and send a verification link there. After selecting the address to which we have access, click the [Send](#) button. In the email you receive there will be a verification link which you can click on to verify the access to the domain.

Domain	Verified	End of Validity
certum.pl	✗ Not verified	

Email address	admin@certum.pl	<input type="button" value="Send"/>
DNS Domain	<input type="text" value="Email address *"/> <input type="button" value="Send"/>	

Note: Archived verifications are NOT available on this page.

#### 4.2. Verification of the access to the domain by placing a file on the server

The method consists in placing a special web page on a server supporting the certified domain, and then confirming the change by clicking the link in the message sent to the given email address.

In the **DNS Domain** section, select verification by placing a file on the server (FILE), enter any email address to which instructions will be sent along with the file.

Email address	admin@certum.pl	<input type="button" value="Send"/>	<b>send the manual with the file</b>
DNS Domain	<input type="text" value="File upload verification"/> <input type="button" value="Send"/>	<input type="text" value="dominik.lowczynowski@assecods.pl"/> <input type="button" value="Send"/>	

Note: Archived verifications are NOT available on this page.

Place the file [received by email] on your website in the area `/.well-known/pki-validation/`

After performing the above action, in order to verify the correct placement of the file, click on the verification link from the e-mail - [Verify the domain](#).

#### 4.3. Verification of the access to the domain by creating an appropriate TXT record in the DNS

The method consists in placing an appropriate entry in the TXT record in the DNS for the certified domain, and then confirming the change by clicking the link in the email sent.





Note: Archived verifications are NOT available on this page.

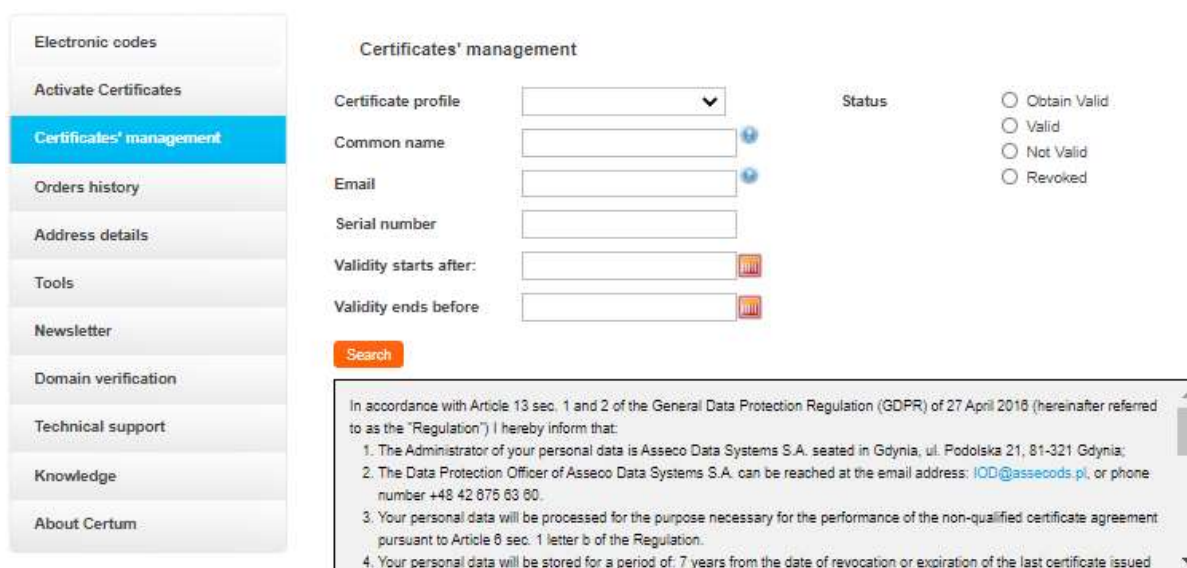
The received email will contain an instruction for placing the relevant entry in the TXT record in the DNS for the certified domain and confirming the change by clicking the link given in the email. Please note that it can take up to 24 hours to refresh/update the DNS entries.

## 5. Certificate downloading

After correct verification, wait for the certificate to be issued.

**Important!** In the case of an order placed by a traditional transfer, it is also necessary to register the payment in order to issue the certificate.

To download the certificate file, log in to <https://certum.store/>. Issued certificates can be found in the [Certificates Management](#) tab.



In accordance with Article 13 sec. 1 and 2 of the General Data Protection Regulation (GDPR) of 27 April 2016 (hereinafter referred to as the "Regulation") I hereby inform that:

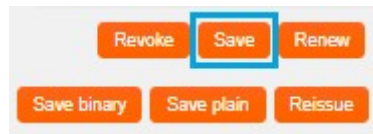
1. The Administrator of your personal data is Asseco Data Systems S.A. seated in Gdynia, ul. Podolska 21, 81-321 Gdynia;
2. The Data Protection Officer of Asseco Data Systems S.A. can be reached at the email address: [IOD@assecods.pl](mailto:IOD@assecods.pl), or phone number +48 42 876 63 60.
3. Your personal data will be processed for the purpose necessary for the performance of the non-qualified certificate agreement pursuant to Article 6 sec. 1 letter b of the Regulation.
4. Your personal data will be stored for a period of: 7 years from the date of revocation or expiration of the last certificate issued

At the bottom of the page there is a list of issued certificates. After clicking on the selected certificate, the available options for the certificate will expand.

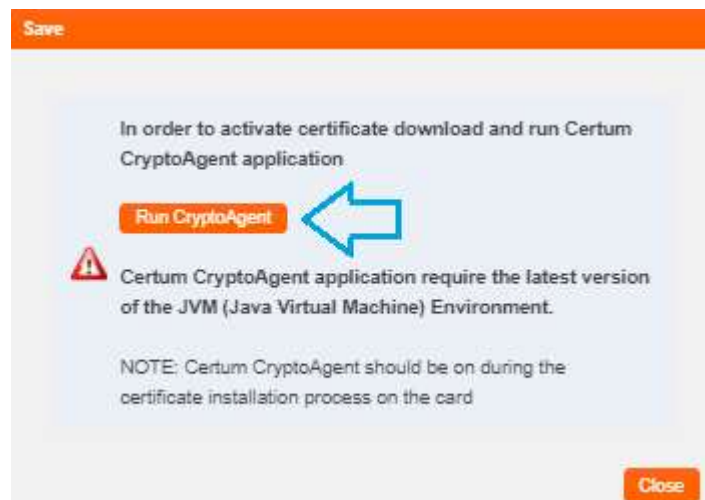
### 5.1. Downloading the pfx/p12 file after activation via key pair generation



If you have activated the certificate by generating a key pair, after selecting the certificate in [Certificate Management](#) click on the [Download PFX file](#) button.



In the next step, run the [CryptoAgent](#) app.

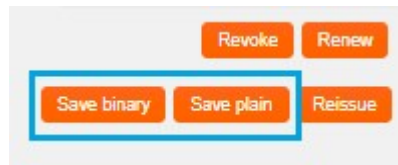


The application will run in the background, and on the website it will be possible to download the certificate. A password will also be generated to the file, which must be saved for it to be possible to access the file. The certificate will be downloaded after clicking on the [Get binary](#) button.



## 5.2. Downloading the certificate and private key files (CSR method)

If you have activated the certificate using the CSR method, the certificate file [the public part] is downloaded directly from the [Certificate Management](#) tab in a binary [.cer - [Save binary](#) button] or text form [.pem - [Save plain](#) button].



To implement the certificate on the server you also need a private key file [privateKey.pem], which was generated earlier together with the CSR. In case the key is lost, use the [Reissue](#) option. This is a reissue of the certificate.