

# Certum SSL certificate – Reissue



## Certum SSL certificates Reissue

version 2.0

## 1. Introduction

This instruction describes the way to use the reissue mechanism.

### What is "reissue"?

It is a repeated issue of a certificate with the end of validity date of the certificate maintained. A certificate reissued using this mechanism is completely free. This mechanism is used in the following situations:

- The private key was lost;
- The SSL certificate was lost;
- The SSL certificate and the private key do not match;
- The certificate or the key were removed from the server;
- The owner of the SSL wants to replace it with a new one for any other reason.

Before you use the mechanism, please read the following information:

### Note - important information for users!

#### The reissue mechanism:

causes the original SSL certificate to be automatically Revoked by the Certum Certification Authority at least 14 days of the reissue of the certificate. Therefore, [we suggest that you install the newly issued SSL certificate](#) on your server instead of the original certificate. At the same time, the newly issued certificate will become the base certificate.

## 2. Reissue of SSL certificate

In order to reissue a certificate, go to the [Manage Certificates](#) tab in the [Certum shop](#) and find the original certificate to be reissued.

Electronic codes

Activate Certificates

Certificates' management

Orders history

Address details

Tools

Newsletter

Domain verification

Technical support

Knowledge

About Certum

### Certificates' management

Certificate profile

Common name

Email

Serial number

Validity starts after:

Validity ends before

Search

Status

Obtain Valid

Valid


Not Valid

Revoked

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:

- The Administrator of your personal data is Asseco Data Systems S.A. seated in Gdynia, ul. Podolska 21, 81-321 Gdynia;
- 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.
- 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.
- Your personal data will be stored for a period of: 7 years from the date of revocation or expiration of the last certificate issued

Serial Number	Certificate profile	Email	Common name	Valid from	Expire date	Status
3c2c0e0308 f88da5a630 9499bae83d 66	Trusted WildCard SSL	dominik.lowczynowski@asseccods.pl ki@asseccods.pl	*.certum.pl	August 6, 2019 2:22:55 PM	August 5, 2021 2:22:55 PM	Valid



Original certificate

Then click the certificate you found. Options for the selected certificate will be displayed

Hash function RSA-SHA256


Common name \*.certum.pl

Organization Asseco Data Systems S.A.

Email dominik.lowczynowski@asseccods.pl

DNS Domain 1 \*.certum.pl

DNS Domain 2 certum.pl




Revoke

Renew

Save binary

Save plan

Reissue



Press Reissue button

In the next step, select the way the keys for the certificate are to be delivered:

- **Key pair generation** - the keys will be save in the Certum CryptoAgent application,
- **CSR** - the keys will be delivered in the form of a CSR demand

Also, it is possible to select the function of the shortcut with which the certificate is to be selected. The options are: [RSA](#) or [ECC](#).

**Reissue**

Service name **Trusted WildCard SSL, 2 years Issue**

Select delivery method of key pair for certificate

Key pair generation

CSR

**CSR \***

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

**Hash function \***

RSA-SHA256

RSA-SHA256

ECC-SHA256

**Next >>**

The Reissue is a technology which enables to reissue your certificate with the same expiration date as the original certificate. The Reissue is available as long as the original certificate remains valid.

**When to use the Reissue:**

- Lost / deleted the private key or the SSL certificate
- Cannot configure the SSL certificate private key
- Intend to replace the received certificate with a new one for various other reasons.

In this document, it is assumed that the keys that the keys will be delivered using the CSR method. For this method, remember to generate a Certificate Signing Request (CSR).

After the method of key delivery is selected, press [Next](#). A summary will then be displayed..

**Reissue**

Service name **Trusted WildCard SSL, 2 years**  
Issue

---

Select delivery method of key pair for certificate

Key pair generation

CSR

**CSR \***

```

-----BEGIN CERTIFICATE REQUEST-----
MITCZDCCAlwCAQAwITEsBAGAIUEAwY2Y2dHVlLnBzMQswCQYDVQGEwJ0TDCC
ASITwDQY7KoZIHvcNAQEBBQADggEPADCCAQoCggEBBAKCGISQ5ZxYnJGsMxP
dusQ1wPBUH4+Hp7wNr+kFd95J0h3p9cKPTCzvXXXIJaK1BBB0YTJvZ9k3dr7eE
0k1uUkMzTrv6ntnIf6+fV6oeU1pY2t9c0LGNBgc3dXLXUs1YfmWzb70Cu301P
1C1H/IgFSfgHS/dDxzPHIHORDBaPSUdedMSxm/WLz2D/M6G4Q3B0q+NXx8WchC
AdNLVBkz3ybtwamD80aAkTzK+JAD3o5fVcVR8157bz0gpdzd1jFhFDXVKc+
+DFNQQ0d3d9FMEDChb2/F4X703EfvnyWBo5MYfWg1FnPh5gXJulMwJGqhgvsXKBEkeyS
xoemLfqVff4+kCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAnT3P1Ab/E7sZAFF
8pdD8BLGCTa2GJS0b09c8THAGgQkuNbwH00wfwIsIkgu4X71ayEhb/fBZEIwqeY
ueXZ9BoKw37wR54x7FzBGdxKQcdofFcBHE2tbcXazLSj6rs3rv+3HbALHKE2c
tv6Gbl.kL5QGp2Upq52JRLWNAF/MYc8C01B1YwHck/JETQ6nEDP131DbLffIqIGrIO7z
09sz/Tq8wew6ZCKuehs7G1THINXqHqjSoJc92WAE+YhJED52AZe9tzVCNhb/d
Ex2HRAL6Z2nDa7b4AEanvqVsIb2+5vA/8ag+cLXe/OgTkjWPKuHg3Tw/octdva
e5Ettfp26QFw=
-----END CERTIFICATE REQUEST-----

```

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

Hash function \*

After selecting the required approvals, click the [Save button](#). The certification application will then be submitted.

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. \*

After the new certificate is issued, the original certificate is automatically Revoked by the Certum Certification Authority.

The certificate will be available for download in the [Manage Certificates](#) tab.

Serial Number	Certificate profile	Email	Common name	Valid from	Expire date	Status
3c9410a6ff6eb035a6ce9d34000d8378	Trusted WildCard SSL	dominik.lowczynowski@assecods.pl	*.certum.pl	August 6, 2019 2:22:55 PM	August 5, 2021 2:22:55 PM	Valid
3c2c0e0208f88da5a6309499bae83d66	Trusted WildCard SSL	dominik.lowczynowski@assecods.pl	*.certum.pl	August 6, 2019 2:22:55 PM	August 5, 2021 2:22:55 PM	Revoked

New base certificate obtained using the Reissue mechanism.

Original base certificate is automatically Revoked by Certum.

## Remember!

### The reissue mechanism:

causes the original SSL certificate to be automatically Revoked by the Certum Certification Authority at least 14 days of the reissue of the certificate. Therefore, [we suggest that you install the newly issued SSL certificate](#) on your server instead of the original certificate. At the same time, the newly issued certificate will become the base certificate.