



Waisenhausgasse 36-38a
D-50676 Cologne
Tel.: +49 228 99307-0
Fax +49 221 4724-444
www.dimdi.de

Contact:
Technical Helpdesk
Tel: +49 228 99307-4949
helpdesk-technik@bfarm.de

Manual Certificates

Version 1.9

Content

1. What is a digital certificate and why do I need one?	2
2. Details of what I need.....	2
3. How do I obtain a certificate?	2
4. How do I import my personal certificate?	2
5. Exporting the public component of the certificate.....	6
6. Upload certificate	7
7. Renewal of a Certificate	8
8. Attachment: List of certificate authorities.....	10

Department



Bundesministerium
für Gesundheit

1. What is a digital certificate and why do I need one?

A certificate is a type of electronic ID. Encryption systems use this certificate as a proof of identity. The certificate contains two parts: your private key and the associated public key. For applications with a high need for protection, the certificate is used for 2-factor identification (user code / password and certificate) to authenticate an individual as an entitled user of single sign-on for PharmNet and BfArM. Users who do not have a certificate, that is, who are unable to "identify" themselves, do not obtain full access to applications with a high need for protection.

You can acquire a certificate for accessing PharmNet.Bund and BfArM from a Certificate Authority (CA) or from a distributor. The certificate can also be used for other purposes.

The certificate is the user's personal identification that has the function of an identity card. From the information in the certificate should indicate which person it identifies.

We accept only certificates from CAs that by default are supported by the Java programming language. A list of possible issuers can be found in the appendix.

2. Details of what I need

To obtain a certificate and to use this to access PharmNet.Bund and BfArM, the following three steps are required:

- Apply to a certificate authority or a distributor for a certificate. The certificate must be issued for a TLS WWW client authentication and must be SHA2 signed (Extended key usage for client authentication, see <http://www.ietf.org/rfc/rfc3280.txt>, section 4.2.1.13).
- Collect the personal certificate issued to you and import it into your browser. (Every user needs own certificate. Please, pay attention to the fact that your name or your e-mail address are noted in the certificate.)
- Back up your certificate.

3. How do I obtain a certificate?

To apply for a certificate, you should contact a certificate authority or a distributor. Normally, you need to enter your name, address, email address, country and possibly a company name or province. The issuer in question will inform you as to the exact application procedure. You should take care to store your private key securely. You also need to identify yourself (e.g. Postident). The issuer makes available forms for applying for a certificate and descriptions for importing the certificate in a browser.

The process of applying for and collecting a certificate can vary considerably. The standard procedure is that you visit an issuer's website and enter your data in a form on the website. The browser on your computer then creates the private key and the public key.

The public key is then sent to the issuer and signed there, while the private key remains on your browser. In most cases, you then receive an email in which you are requested to visit the website, again using the same browser. The signed public key is then added to the private key and the certificate is finally issued. In this manner, the certificate is also installed in your browser at the same time. In this case, it is essential that you then secure your certificate.

Another variant is described in chapter 4. In this process, you receive the complete certificate either from the issuer or possibly from a colleague in your IT department who has applied for the certificate on your behalf.

4. How do I import my personal certificate?

When you have received your certificate, you need to import it into your browser before you can use it. The certificate is stored in the correct certificate location by means of the import process.

Importing is carried out exemplarily first for the browser Mozilla Firefox and then also for the Internet Explorer.

Mozilla Firefox

First select the *Options* item in the Options menu. Now select the *Advanced* item followed by the *Certificates* tab.

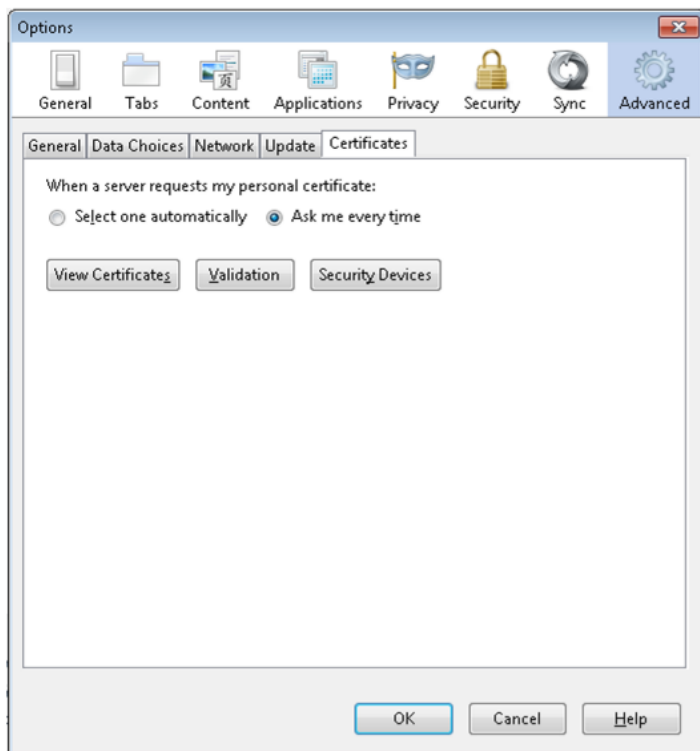


Figure 1: Options Advanced

Select "View Certificates". Select the "Your Certificates" tab in the window that subsequently opens.

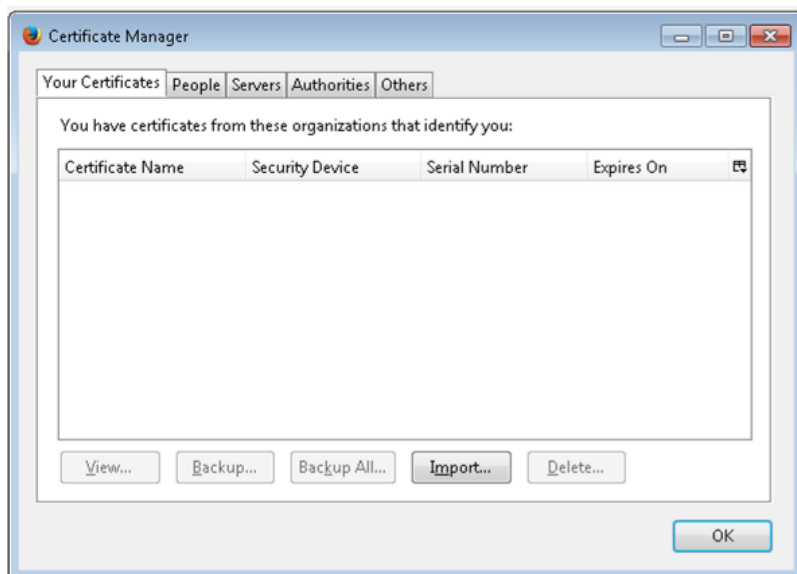


Figure 2: Overview certificates

You can now see an overview of all certificates already installed. In this case, no certificates have been installed. Click on "Import" to open a file selection box.

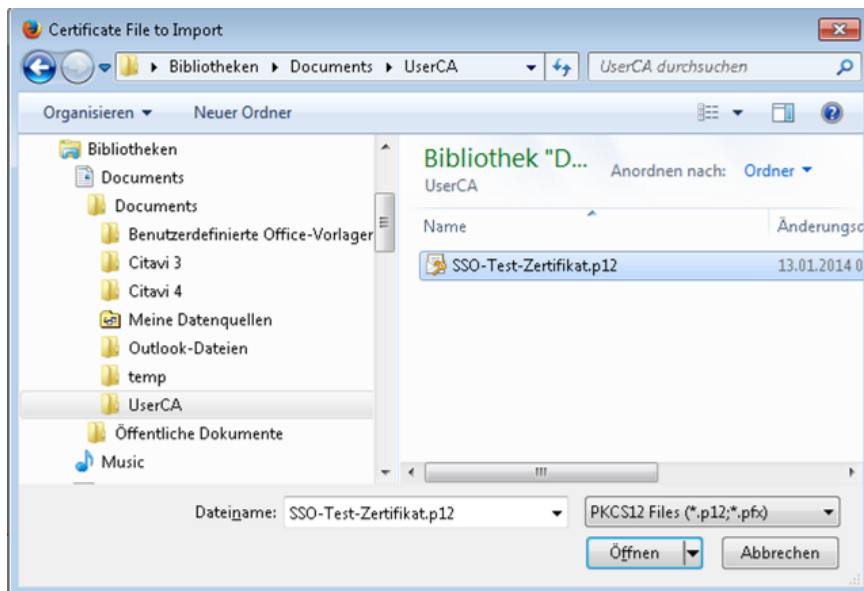


Figure 3: Import of certificate

Select your certificate and click on "Open". You are now requested to enter the password for the key file.



Figure 4: Passwort of the certificate

After a successful import, the certificate is entered under "Your Certificates".

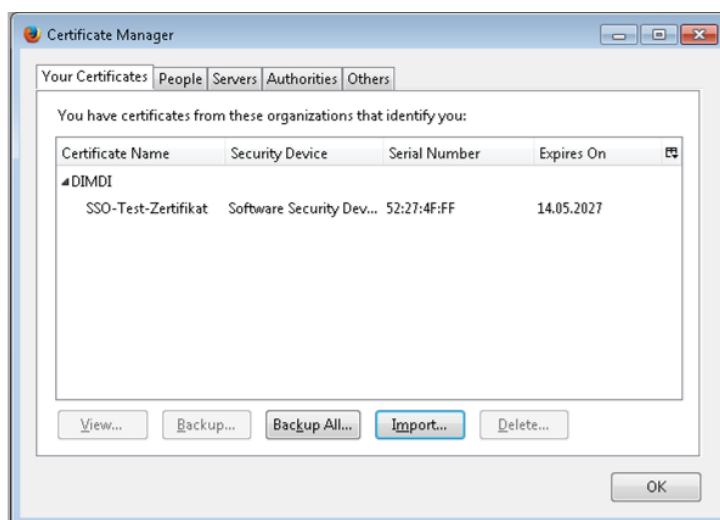


Figure 5: Overview with new certificate

Internet Explorer

Please choose in menu *Extras options* the point *options*, then the tab *contents* and in the middle of the page click on „certificates“.

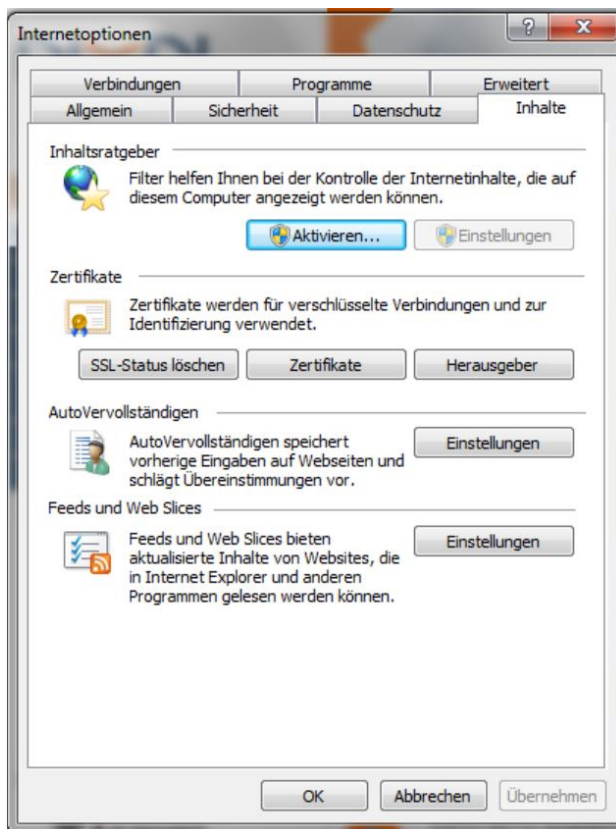


Figure 6: Call certificates

The following screens and steps correspond to at the one described above for Mozilla Firefox

You see an overview of the certificates already installed now. After a click on „Import“, the assistant for importing certificates appears. You click at the first screen “next. On the following screen you select the certificate.

5. Exporting the public component of the certificate

To export the public key of the certificate for registration at BfArM, extract the public part of your certificate. To do so, highlight the certificate under "Your Certificates" and then click on "View". Now select the *Details* tab.

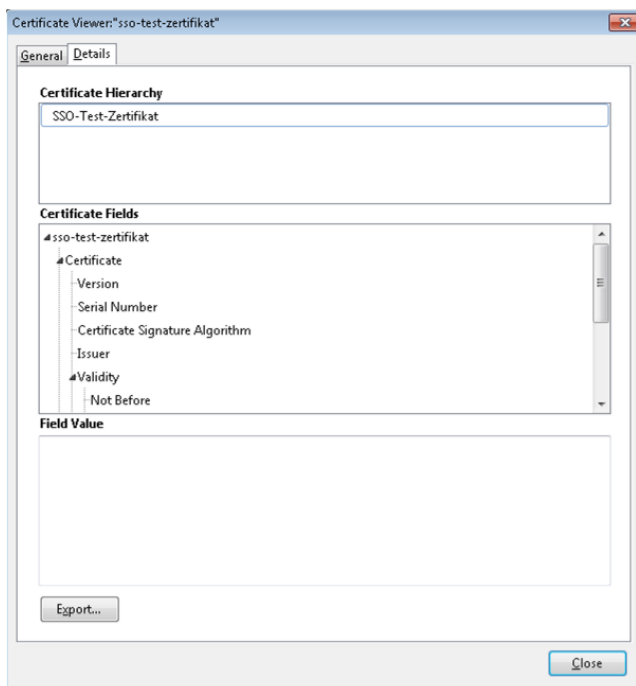


Figure 7: Certificate view

Click on *Export* to create a file containing the public component of your certificate (with a suffix of .cer, .crt or .der). Save this file locally on your computer.

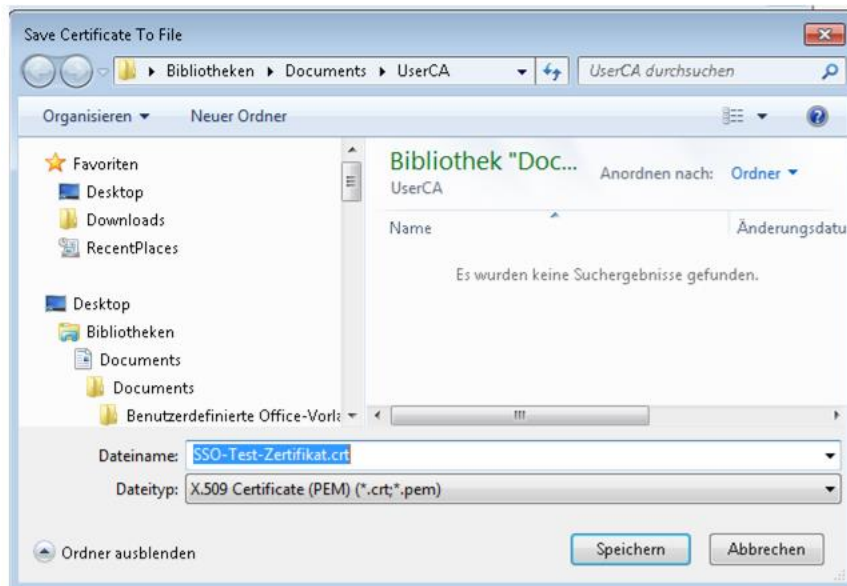


Figure 8: Saving of the certificate

6. Upload certificate

In the initial registration you can upload and store a personal certificate in the "Certificate" section. On the form there is a general indication, or a notice that a certificate is required for your chosen application.

The Certificate can also be uploaded after the registration, because the "My Data" area is accessible without a valid certificate. To do so you can sign in using the "My Data" area and choose the option "Certificate" from the navigation menu.

On the form, please click on the button "Browse", select the previously saved certificate file and upload it afterwards.

- Certificate

To use the selected applications no certificate is required. But you need a certificate if you want to use the DIMDI user administration as organization administrator to register further users of your company for the applications you apply for.

Here you can upload the public component (.cer, .crt or .der) of your personalised digital certificate.

More information: [Digital certificate for authentication](#)

No certificate available

Upload certificate:

1st step: Select certificate Durchsuchen... Keine Datei ausgewählt.

2nd step: Upload certificate Upload

Figure 9: Upload certificate -1

Certificate

To use the application **Batch release applications** a certificate is required.

Here you can upload the public component (.cer, .crt or .der) of your personalised digital certificate.

More information: [Digital certificate for authentication](#)

No certificate available

Upload certificate: *

1st step: Select certificate Durchsuchen... Keine Datei ausgewählt.

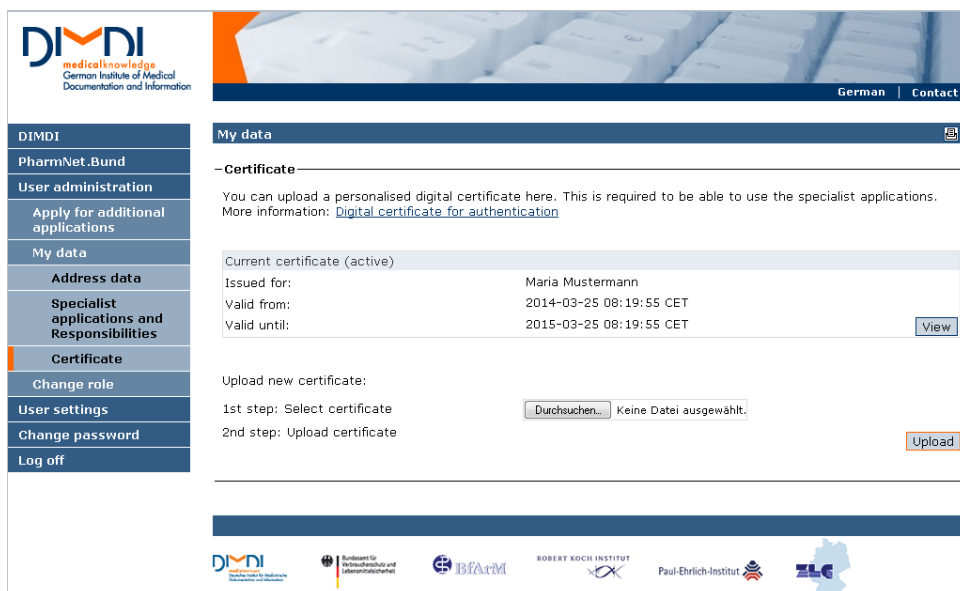
2nd step: Upload certificate Upload

Figure 10: Upload certificate -2

7. Renewal of a Certificate

You will receive from us a notification by mail before your certificate expires. Ask your exhibitor on time for a renewal of your certificate and load the new certificate in your browser as described before. Afterwards you sign in in our user management („My data“) and choose the option "Certificate" from the navigation menu. Now you are able to upload and store the public key of your certificate.

You can upload a new certificate still after the previous certificate expired because of the "My data" area still is accessible without a certificate.



DIMDI medicalknowledge
German Institute of Medical Documentation and Information

German | Contact

My data

– Certificate –

You can upload a personalised digital certificate here. This is required to be able to use the specialist applications.
More information: [Digital certificate for authentication](#)

Current certificate (active)

Issued for:	Maria Mustermann
Valid from:	2014-03-25 08:19:55 CET
Valid until:	2015-03-25 08:19:55 CET

[View](#)

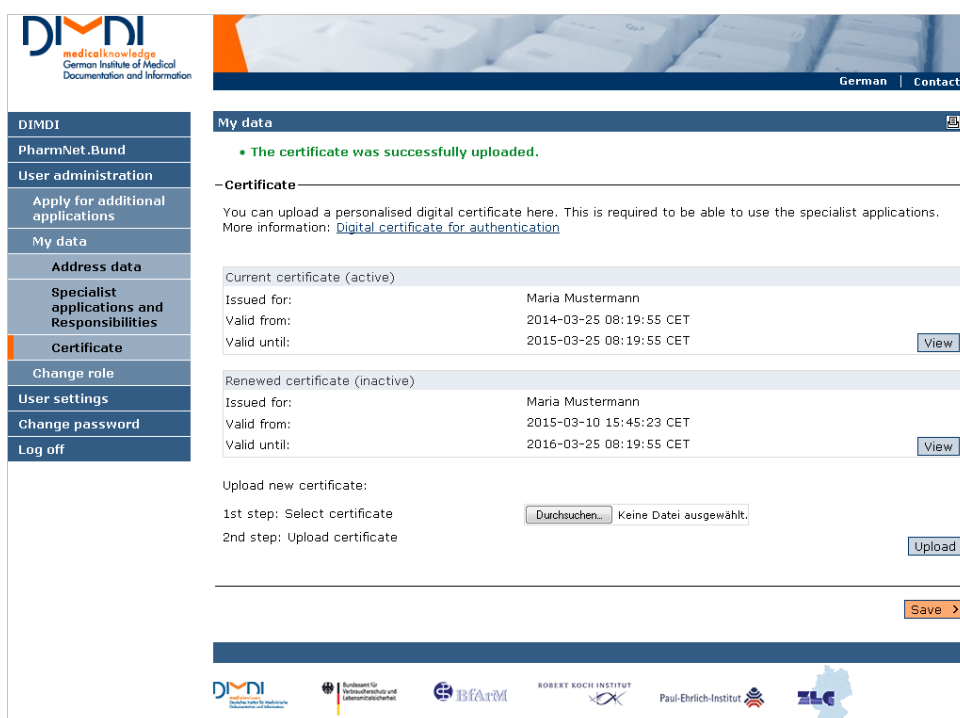
Upload new certificate:

1st step: Select certificate [Durchsuchen...](#) Keine Datei ausgewählt.

2nd step: Upload certificate [Upload](#)

DIMDI Bundesamt für Verbraucherschutz und Lebensmittelsicherheit BfArM ROBERT KOCH INSTITUT Paul-Ehrlich-Institut ZfE

Figure 10: Renewal of the certificate - step 1 upload



DIMDI medicalknowledge
German Institute of Medical Documentation and Information

German | Contact

My data

• The certificate was successfully uploaded.

– Certificate –

You can upload a personalised digital certificate here. This is required to be able to use the specialist applications.
More information: [Digital certificate for authentication](#)

Current certificate (active)

Issued for:	Maria Mustermann
Valid from:	2014-03-25 08:19:55 CET
Valid until:	2015-03-25 08:19:55 CET

[View](#)

Renewed certificate (inactive)

Issued for:	Maria Mustermann
Valid from:	2015-03-10 15:45:23 CET
Valid until:	2016-03-25 08:19:55 CET

[View](#)

Upload new certificate:

1st step: Select certificate [Durchsuchen...](#) Keine Datei ausgewählt.

2nd step: Upload certificate [Upload](#)

[Save](#)

DIMDI Bundesamt für Verbraucherschutz und Lebensmittelsicherheit BfArM ROBERT KOCH INSTITUT Paul-Ehrlich-Institut ZfE

Figure 11: Renewal of the certificate – step 2 save

After activating the button "Save" a confirmation is necessary to overwrite the existing certificate.

DIMDI
medical knowledge
German Institute of Medical
Documentation and Information

German | Contact

Certificate

Please confirm

There is already available a valid certificate. Do you want to overwrite the old certificate?

< Back Next >

Figure 11: Renewal of the certificate - step 3 question to overwrite

After clicking "Next" is checked if the uploaded certificate can be identified as the successor of the certificate previously active certificate. For this purpose the information on name, email address or address information must be identical.

If the uploaded certificate is recognized as the successor of the existing certificate, so the existing certificate will be overwritten with the newly uploaded certificate. Otherwise, the identity of the holder of the certificate, which is valid from a technical perspective and meets all requirements, must be confirmed by the administrator. He receives a mail stating that a succession certificate has to be checked.

DIMDI
medical knowledge
German Institute of Medical
Documentation and Information

German | Contact

My data

- The uploaded certificate could not be recognized as a succession certificate from the previously stored certificate and must be reviewed by the administrator in charge again. Your old certificate remains valid as long as further provided that the valid-to date has not been exceeded.

– Certificate

More information: [Digital certificate for authentication](#)

Current certificate (active)	
Issued for:	Maria Mustermann
Valid from:	2014-03-25 08:19:55 CEST
Valid until:	2015-03-25 08:19:55 CEST View

Renewed certificate (inactive)	
Issued for:	Maria Mustermann
Valid from:	2015-03-25 08:19:55 CEST
Valid until:	2016-03-25 08:19:55 CEST View

Upload new certificate:

1st step: Select certificate Durchsuchen... Keine Datei ausgewählt.

2nd step: Upload certificate Upload

Figure 11: Renewal of the certificate - step 3 verification

8. Attachment: List of certificate authorities

Provided below is a list of certificate authorities that to our knowledge issue digital X.509 user certificates. We accept only certificates from CAs that by default are supported by the Java programming language. The list should in no way be understood to be a reference or recommendation for purchase of the products from the listed companies (Stand August 2014).

GlobalSign nv-sa, BE
SwissSign AG, CH
DigiCert Inc, US
COMODO CA Limited, GB
AC Camerfirma SA CIF A82743287, EU
Buypass AS-983163327, NO
QuoVadis Limited, BM
Starfield Technologies, Inc., US
Thawte, ZA
thawte, Inc., US
T-Systems Enterprise Services GmbH, DE
VeriSign, Inc., US
The USERTRUST Network, US
GeoTrust Inc., US
AffirmTrust, US
AddTrust AB, SE
Actalis S.p.A./03358520967, IT
CyberTrust Root, Baltimore, IE
Entrust, Inc., US
SECOM Trust.net, JP
SECOM Trust Systems CO.,LTD., JP
Internet Security Research Group, US
IdenTrust, US
GoDaddy.com, Inc., US
The Go Daddy Group, Inc., US
Sonera, FI
Thawte Consulting cc, ZA
XRamp Security Services Inc, US
SecureTrust Corporation, US"
LuxTrust s.a., LU
KEYNECTIS, FR
AC Camerfirma S.A., EU
Unizeto Sp. z o.o., PL
Unizeto Technologies S.A., PL
Chunghwa Telecom Co., Ltd., TW

Hint: Not all certificate authorities provide X.509-Zertifikate with „Extended Key Usage: Client Authentication“ .