

TeleTrust EBCA

European Bridge Certificate Authority

Guideline "Enable Trust"

for users of the
TeleTrust European Bridge CA

Information

Version 1.4

11.06.2019

IT Security Association Germany (TeleTrustT)
Chausseestrasse 17
D-10115 Berlin

Phone: +49 30 / 400 54 310
Fax: +49 30 / 400 54 311

info@ebca.de
<https://www.ebca.de>

Table of contents

What is the EBCA?	3
Why enable trust with certificate lists?.....	3
How can certificate lists be verified and installed?	3
Instruction on installation of certificate lists (CTL)	7
Before you start.....	7
Step-by-step instruction on installation of certificate lists	7
Step-by-step instruction on installation of single certificates from lists	9

History

Version	Date	Modification	Author
1.0	2013-1-17	Writing documentation	Marieke Petersohn
1.1	2013-8-6	Amending the instruction on verification of CTL	Vi Linh Tran-Graef
1.2	2014-07-24	New EBCA logo inserted	Martin Fuhrmann
1.3	2014-10-30	Amending the instruction on installation for Thunderbird	Marieke Petersohn
1.4	11.06.2019	Association name revised	Morad Abou Nasser

What is the EBCA?

TeleTrustT European Bridge CA (EBCA) is a consolidation of individual, equal Public-Key-Infrastructures (PKI) in a PKI network of trust. It enables secure and authentic communication between businesses, institutions and public authorities.

Why enable trust with certificate lists?

An operating system regularly supports only certain Root CAs, mostly those of public trust centers. In comparison, Root CAs of corporate PKIs are not in the operating system and therefore must be manually installed.

A Certificate Trust List (CTL) is available free of charge to facilitate the installation of Root CAs for communication partner of EBCA participants. While installing certificate lists the user will be asked to verify the integrity for each certificate via a so-called fingerprint. The EBCA has already applied this procedure: only the signed list should be downloaded and verified.

The list will then be transferred to a so-called PKCS#7 container, adapted for immediate own certificate directory. Download current lists and the signature certificate at <https://www.ebca.de/en/utilisation-of-the-ebca/certificate-trust-list/>

How can certificate lists be verified and installed?

The electronic signature of CTL can be verified online with your browser without installing reader software with SecSigner Online Tool. Download of installable CTL is also possible then. A Java Applet will be started by loading the website. All you need is a Java Plugin version 1.4.2_08 or higher.

SecSigner® Online starten:

<https://www.seccommerce.de/en/products-en/secsigner/secsigner-online/verify-signature.html>

Learn more about the function of the signature verification and the installation of CTL in the following sections.

Instruction on verification with SecSigner® Online

The following images show how the integrity of certificate lists can be verified. The result of this verification should be known before the installation of CTL, and it should indicate that the signature is valid. (See 4. step).

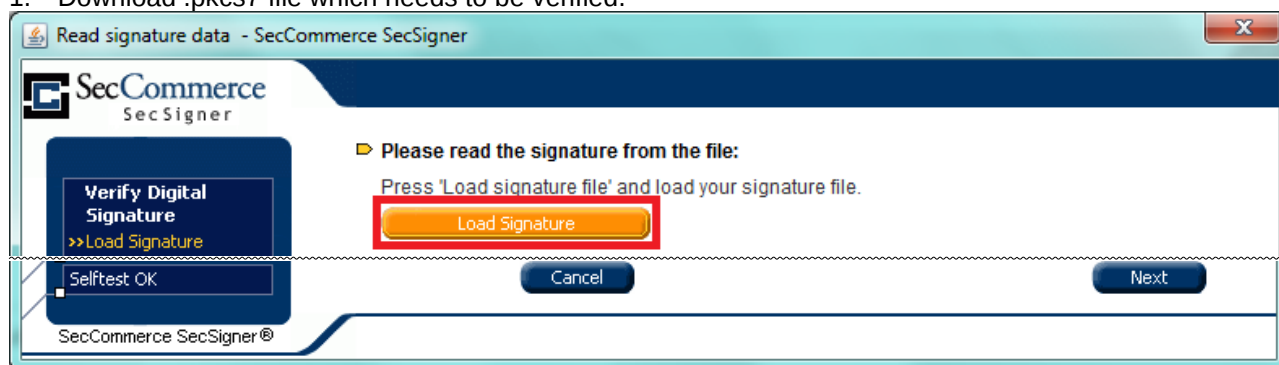
After a successful verification the signed file can be extracted from the tool and it can be saved then. Another instruction on the installation of certificate lists is available.

Before you start

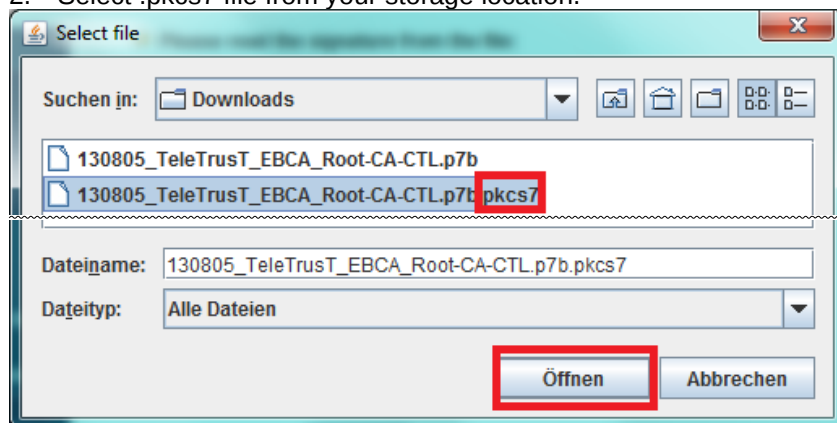
- Call up the verification tool:
<https://www.seccommerce.de/en/products-en/secsigner/secsigner-online/verify-signature.html>
- Download the file needed to be verified
<https://www.ebca.de/en/utilisation-of-the-ebca/certificate-trust-list/>

Step-by-step instruction on verification of certificate lists

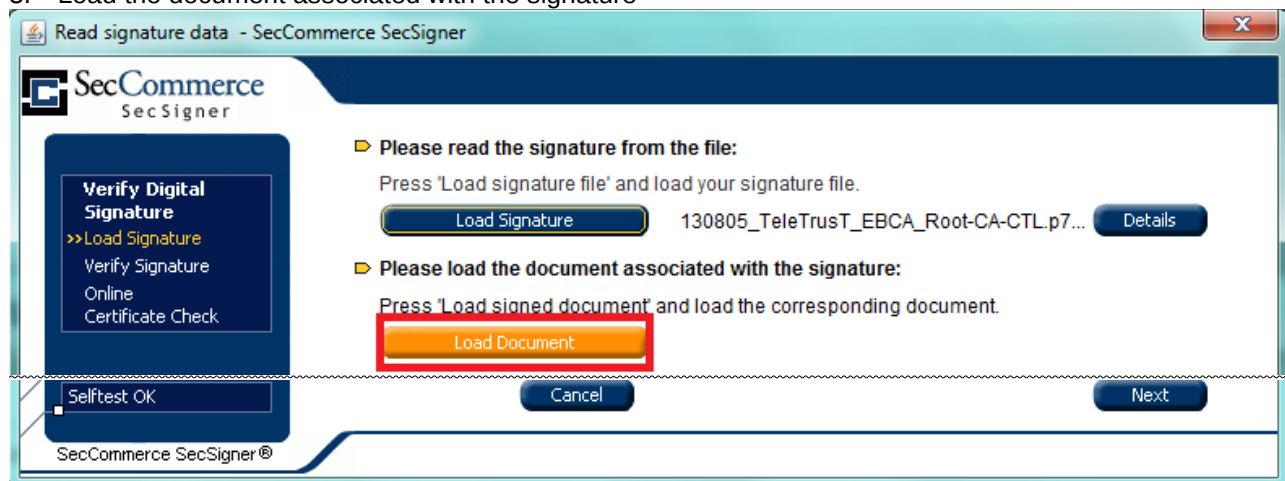
1. Download .pkcs7 file which needs to be verified.



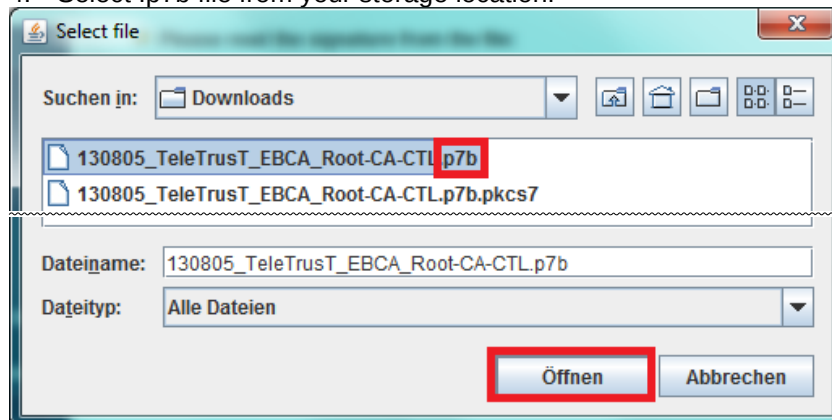
2. Select .pkcs7 file from your storage location.



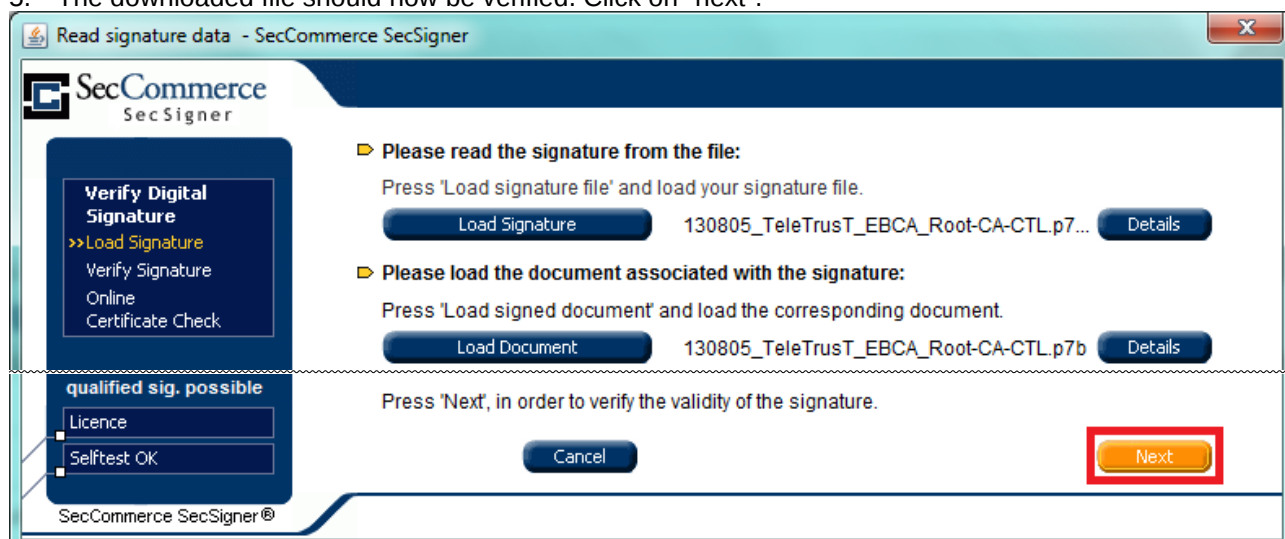
3. Load the document associated with the signature



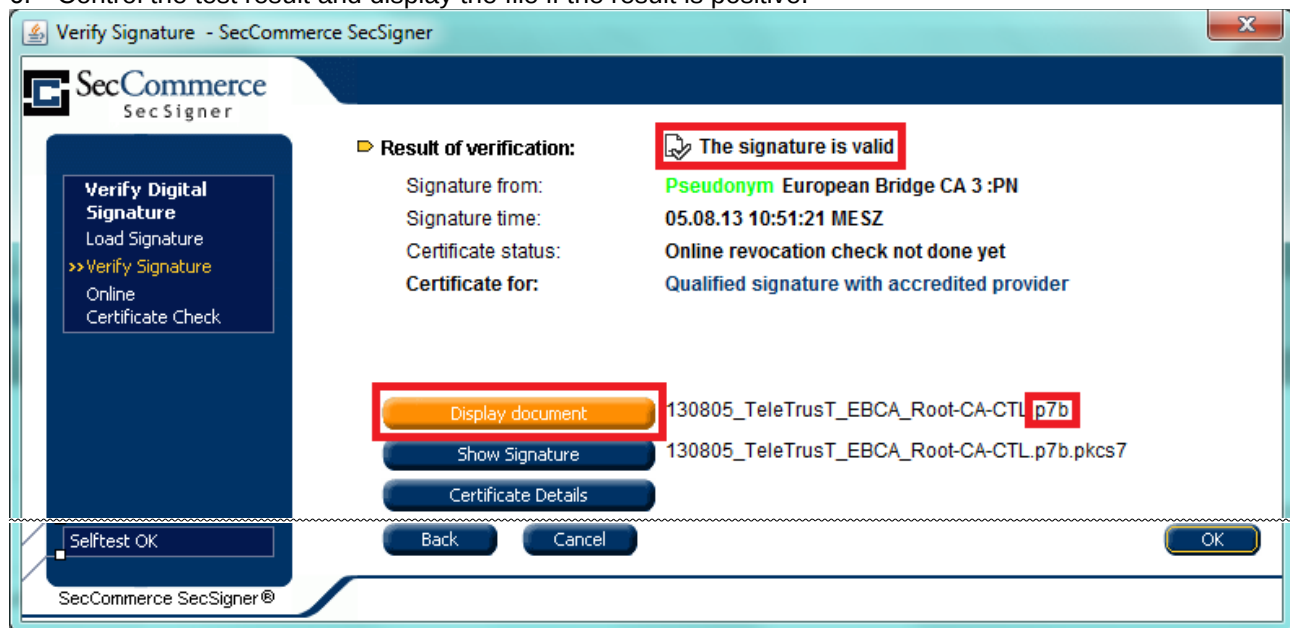
4. Select .p7b file from your storage location.



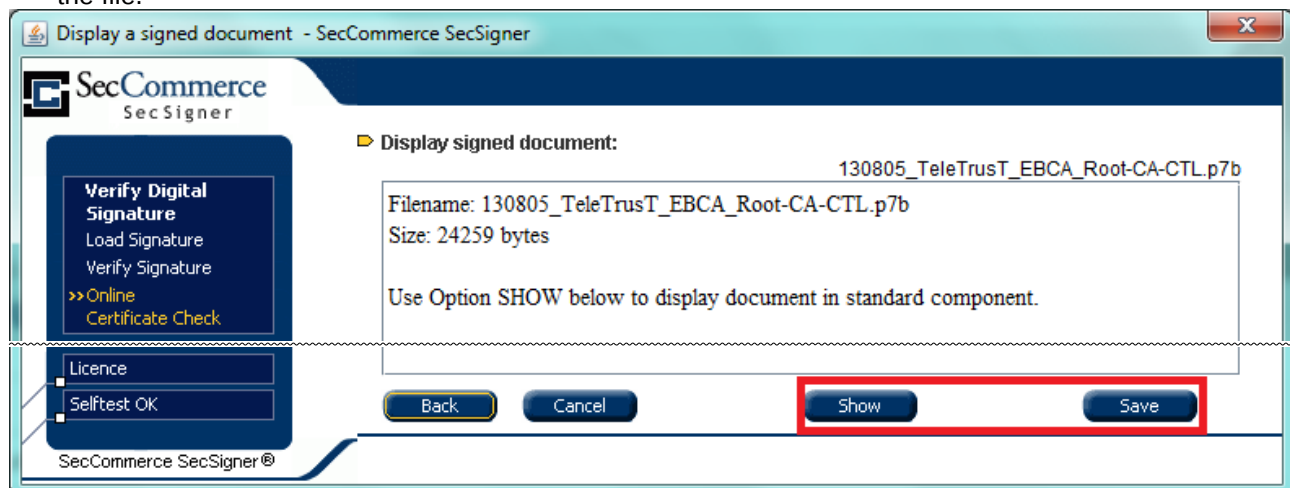
5. The downloaded file should now be verified. Click on "next".



6. Control the test result and display the file if the result is positive.



7. Select one of the options whether the certificate list should be saved or showed. It is advisable to save the file.



Instruction on installation of CTL

The following images show how certificate lists or certificates can be installed in your own storage.

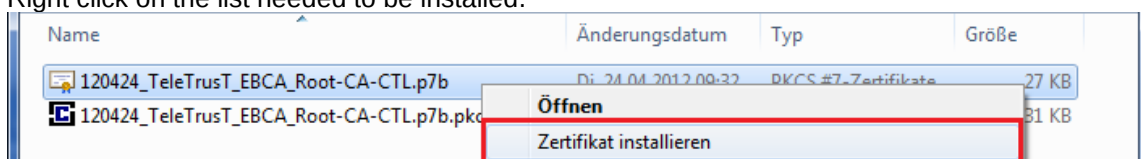
Before you start

- Verify signed files:
<https://www.seccommerce.de/en/products-en/secsigner/secsigner-online/verify-signature.html>
- Download unsigned file (if it was not prior extracted):
<https://www.ebca.de/en/utilisation-of-the-ebca/certificate-trust-list/>

Step-by-step instruction on installation of certificate lists

You are using Thunderbird? Please read further at page 10.

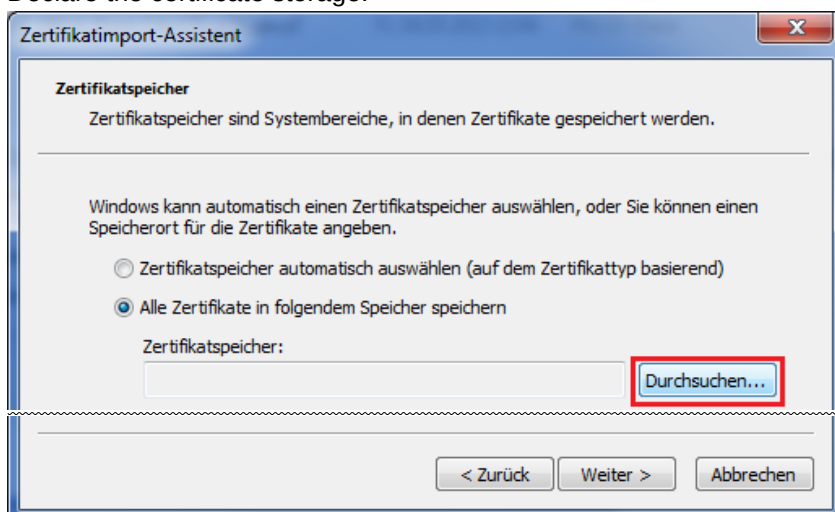
1. Right click on the list needed to be installed.



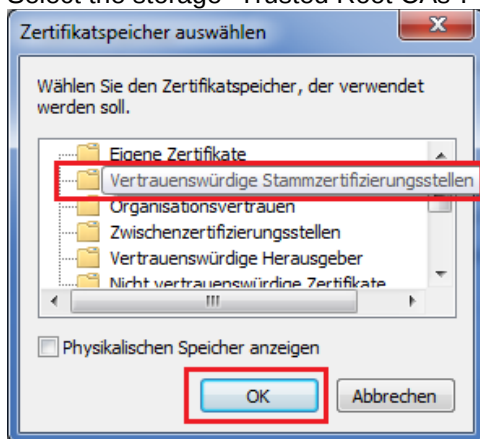
2. Start the assistant.



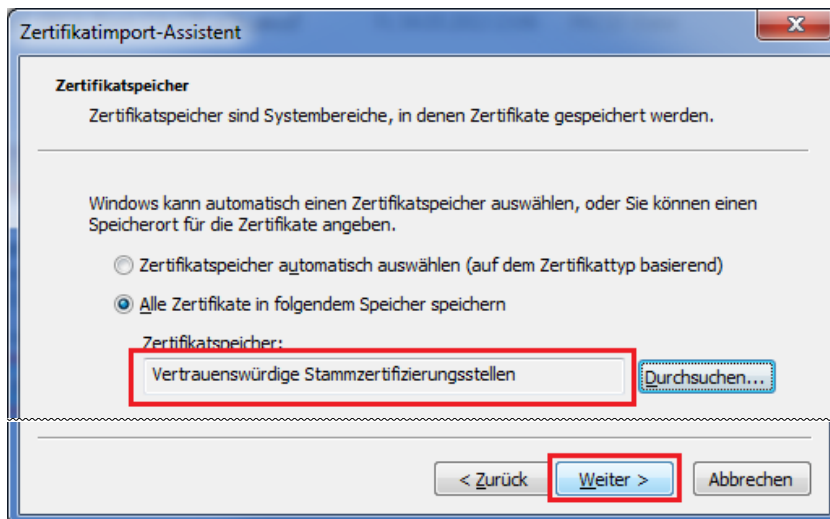
- 3a. Declare the certificate storage.



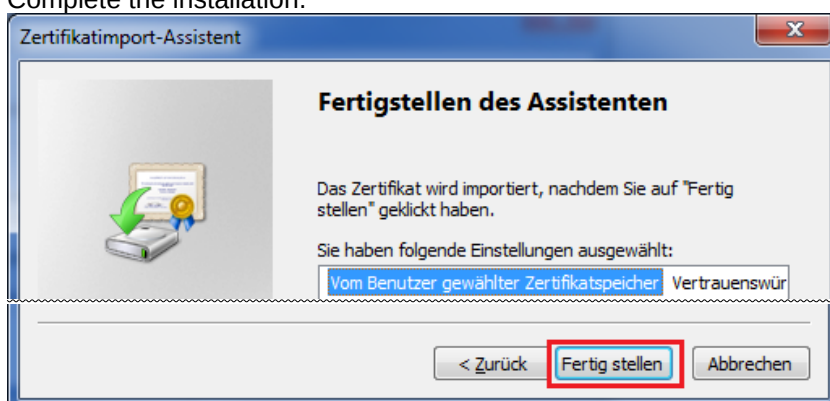
3b. Select the storage "Trusted Root CAs".



3c. End the selection of storage.



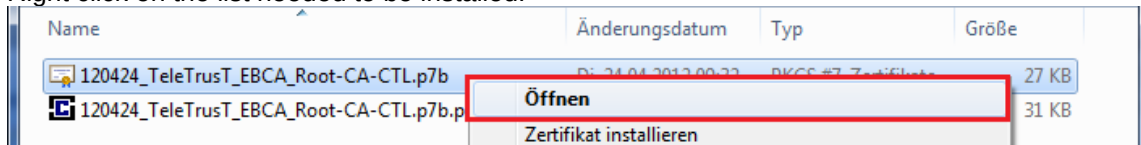
4. Complete the installation.



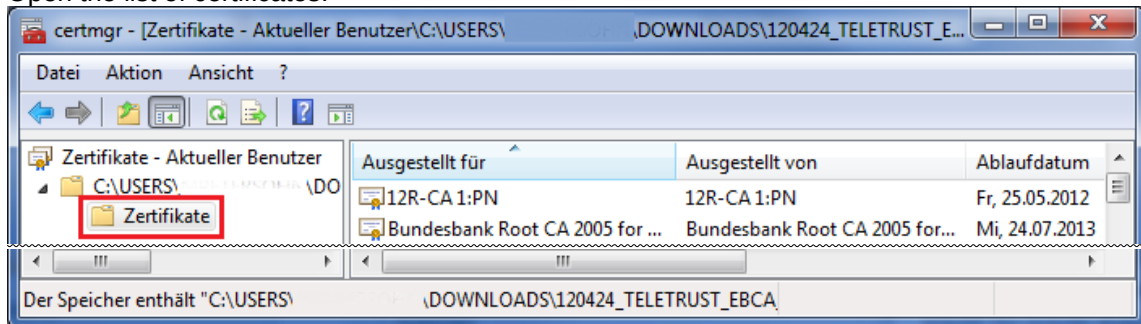
If only selected certificates from a certificate list should be installed, please follow this instruction.

Step-by-step instruction installation of single certificates from lists

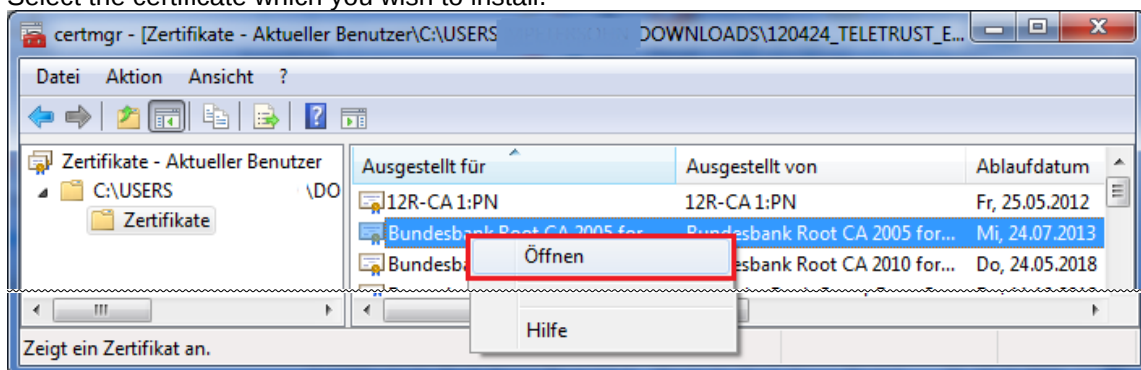
1. Right click on the list needed to be installed.



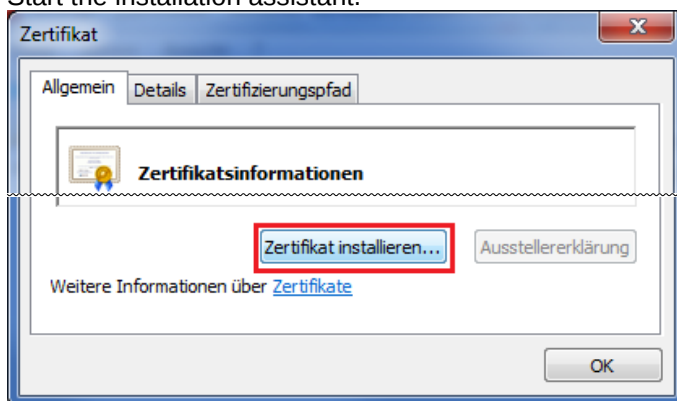
2. Open the list of certificates.



3. Select the certificate which you wish to install.



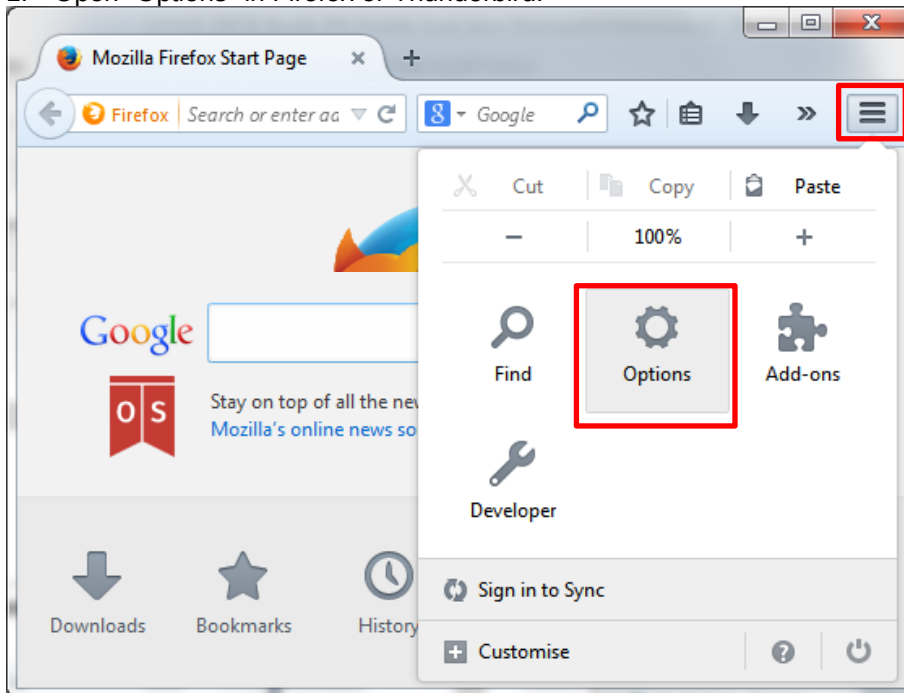
4. Start the installation assistant.



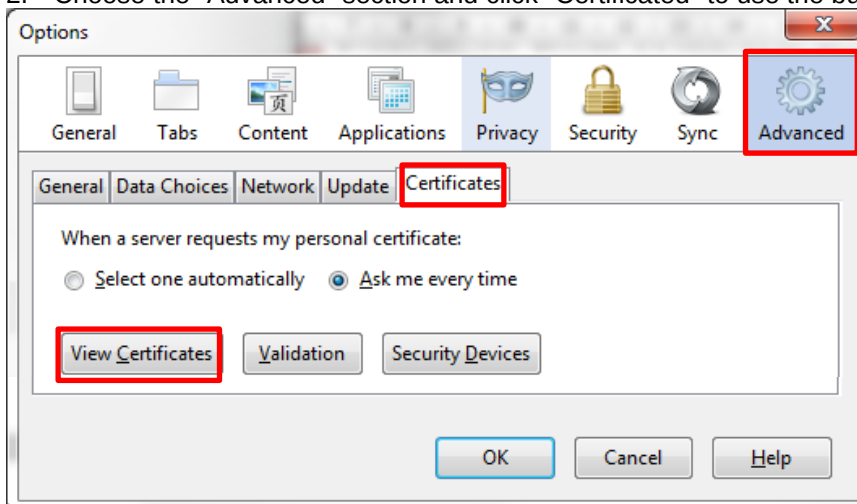
For further action please read the "Instruction on installation of certificate lists" from step 2 on.

Step-by-step instruction on installation of certificate lists in Thunderbird

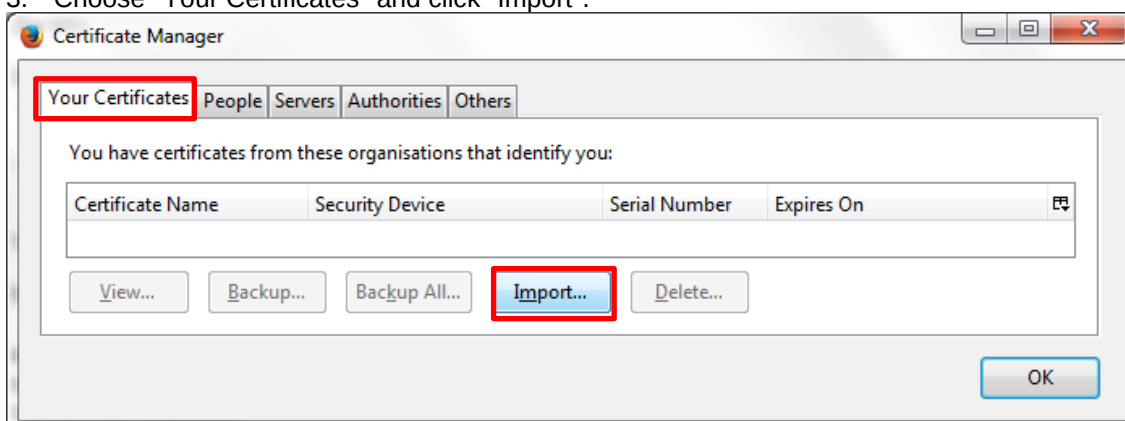
1. Open "Options" in Firefox or Thunderbird.



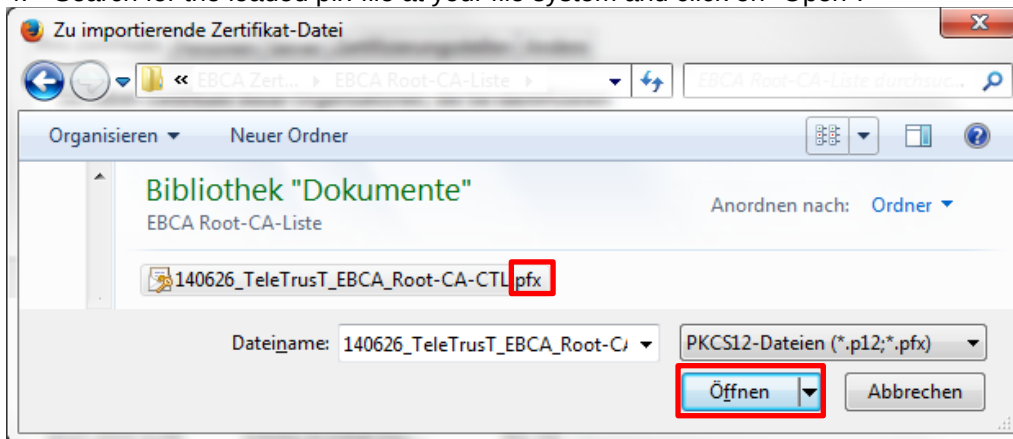
2. Choose the "Advanced" section and click "Certificated" to use the button "View Certificates".



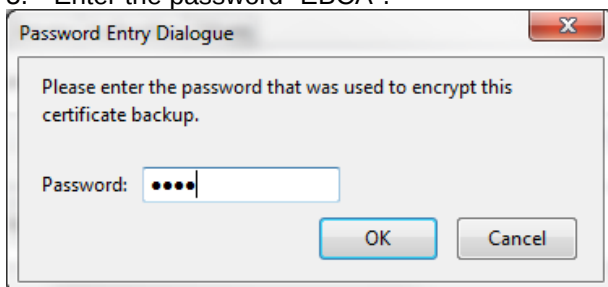
3. Choose "Your Certificates" and click "Import".



4. Search for the loaded pfx-file at your file system and click on "Open".



5. Enter the password "EBCA".



6. Now all EBCA-Root-CAs were installed. You can find them in the section "Authorities".

