



Content

1. Introduction	2
2. Requesting and setting up a certificate	2
2.1 Requesting a certificate	3
2.2. Creating a certificate	7
2.2.1. Obtaining license information	7
2.2.2. Create a certificate with your license code	8
2.3. Installing a certificate	12
2.4. Setting up the certificate in Outlook	18
2.5. Encryption with Outlook	21
3. Exporting and importing certificates	23
3.1 Exporting a certificate	23
3.2 Importing a certificate	29
4. Installing the ALDI Nord root certificate	32
5. Alternative procedures for receiving and providing certificates	38
5.1. Downloading a certificate of a communication partner	38
5.2. Matching a downloaded certificate to an Outlook contact	40
5.3. Uploading own certificates	42



1. Introduction

This document provides instructions on how to set up encrypted communication with ALDI Nord from the point of view of an external communication partner. If you have questions or queries, please contact your IT administrator. This guide was verified on 03/30/2016. Any changes from the side of the manufacturers can lead to a different behavior as described here.

This guideline was developed on the following system:

- Windows 7
- Internet Explorer 11
- MS Outlook 2013

The views on other systems may be different.

2. Requesting and setting up a certificate

This section explains how to request and set up a certificate for encrypted email communication with ALDI Nord. ALDI Nord currently recommends the Certification Authority (trustcenter) SwissSign.

This ensures the highest possible compatibility with the encryption mechanisms used by ALDI Nord.

As an example, in the following section the product "Personal ID Silver" from SwissSign is requested.

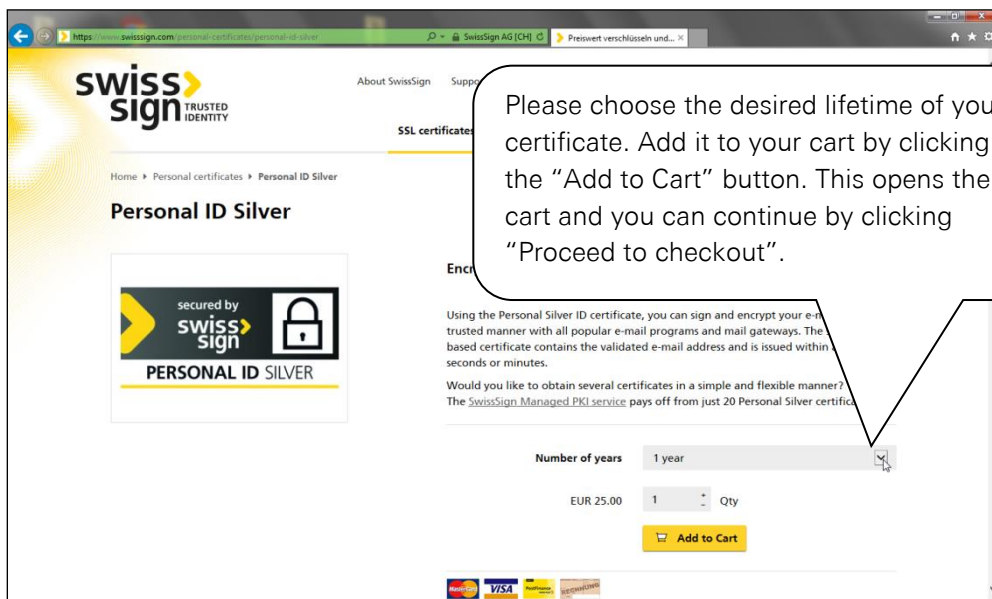
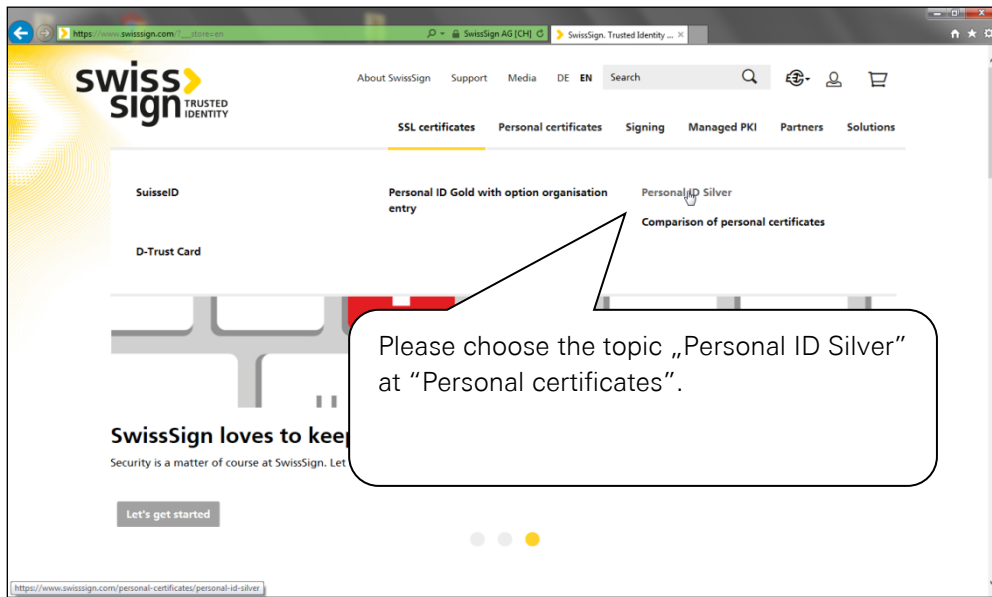
Please note that the described certificate in this section is issued for a single e-mail address and can only be used with this. Access to the email address has to be via Outlook and the protocol POP3.

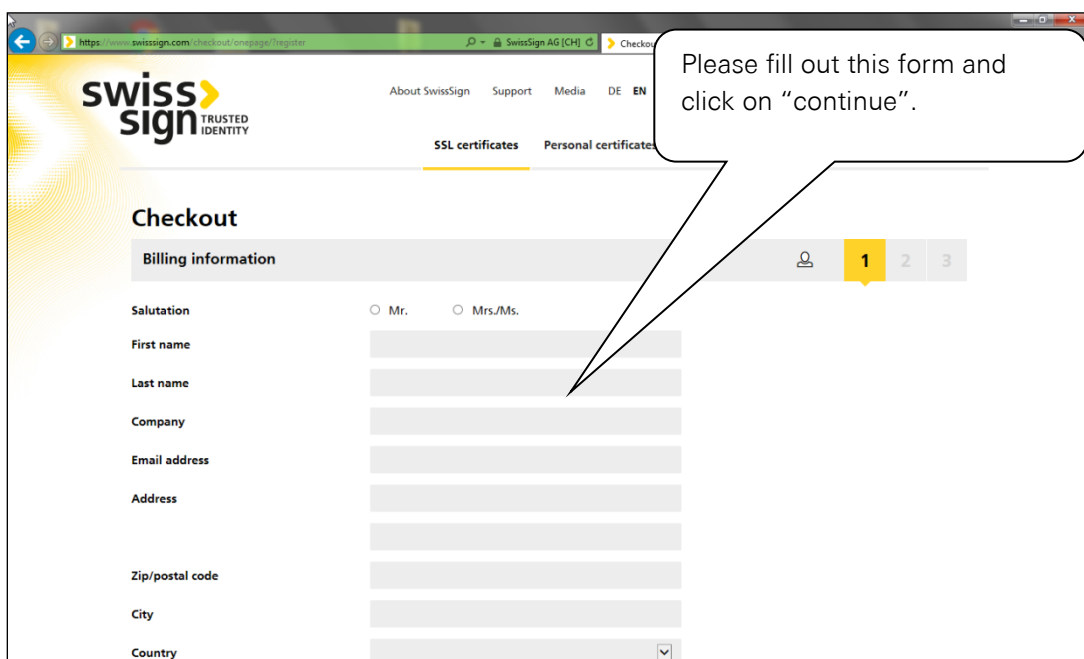
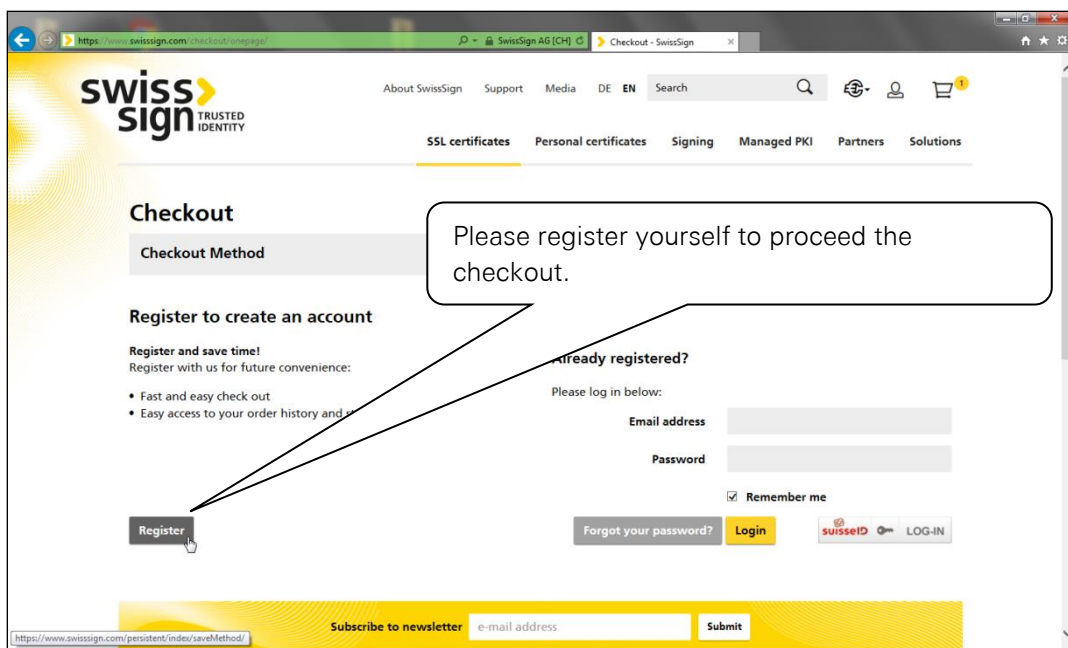
The described certificate is valid for one year and entails costs.



2.1 Requesting a certificate

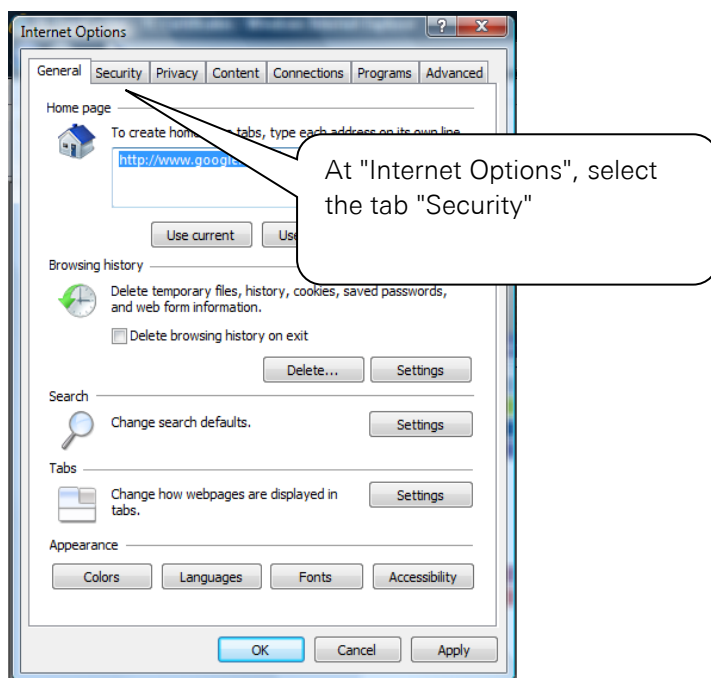
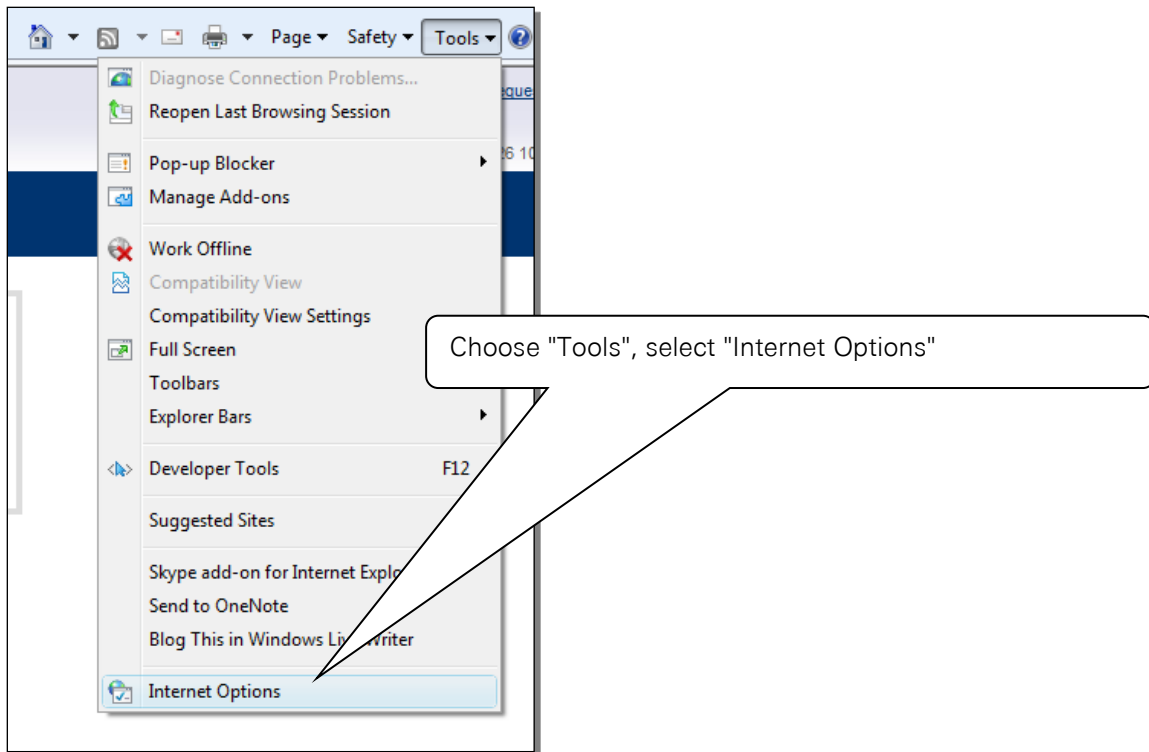
Open the website „https://www.swisssign.com/personenzertifikate/personal-id-silver “

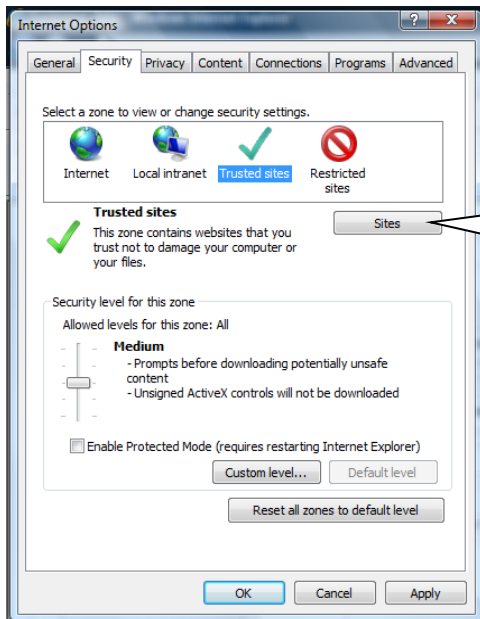




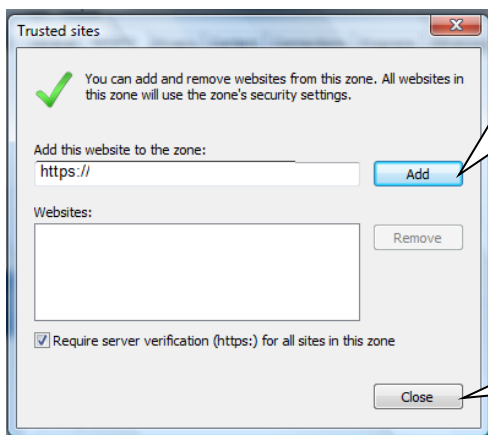
After completing the ordering process, within the following half an hour you will receive an e-mail containing the license code. Follow the steps as described in the following pages to successfully request the certificate by using the license code you just ordered. Depending on your Internet Explorer settings, you might have to follow the steps below to add the SwissSign TrustCenter website to your trusted sites.

First of all please start the Internet Explorer and follow these steps:





Select the item "Trusted sites" and then click "Sites"



Now you can add the website "swissign.net" to the zone. Fill in this address and then click "Add".

Once the website has been added, click "Close" to end the dialogue

Once you have closed the Internet Options dialogue, you can continue to process your order. Please note the following before generating the key:

- Generate the key either with the browser "Mozilla Firefox" or "Internet Explorer".
- Do not perform any new installations of your system or browser before having received and installed the certificate from SwissSign. The private key, which only works with the certificate, will otherwise be lost.

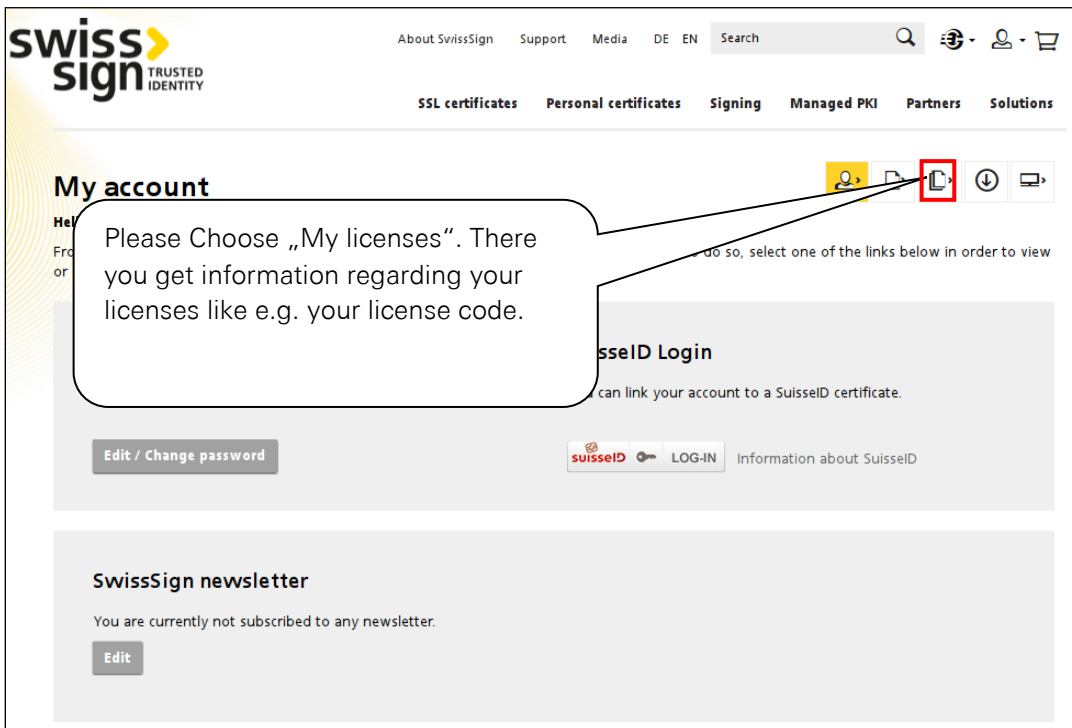
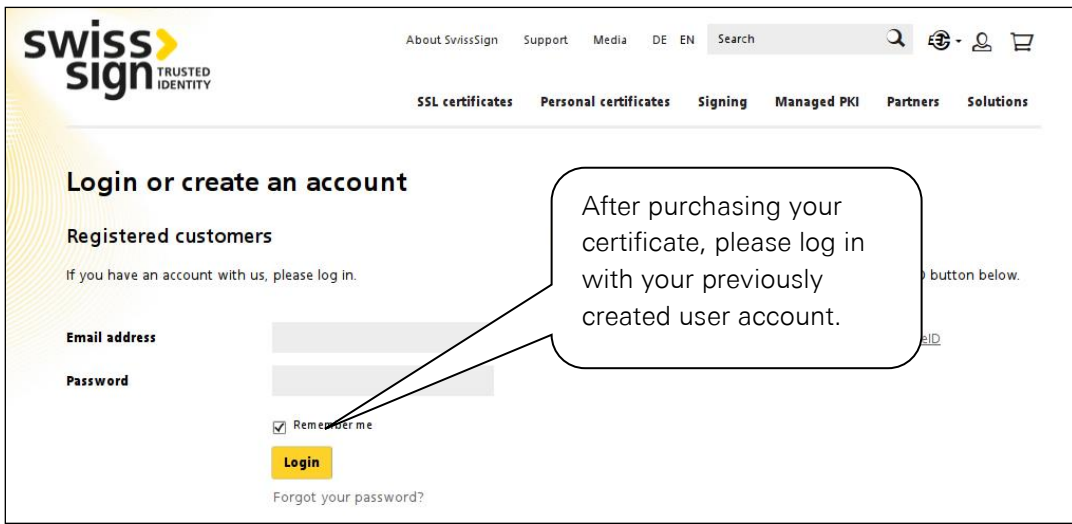


2.2. Creating a certificate

If you received the license code, please move on to chapter 2.2.2. . Otherwise you have to call up the license information. Please follow chapter 2.2.1. to do so.

2.2.1. Obtaining license information

Please open the following Webpage <https://www.swissign.com/en/customer/account/login/>



2.2.2. Create a certificate with your license code

After you ordered your “Personal ID Silver” you receive an e-mail containing your license key. Now, to request your certificate, go to <http://swissign.net> .

Home | Support | Certificate authority | Shop | Revoke certificate | Help

swissign

Search / Manage Certificates

- Public search > Columns
- Account logon

Account

- Logon
- Create

Certificate login

- Logon

New users

- Proceed without account (for quick single certificate request)**
- Create account (for managing several certificates)

Click „Proceed without account“. If you want to manage several certificates, you can create an account.

Home | Support | Certificate authority | Shop | Revoke certificate | Help

swissign

Search / Manage Certificates

Public search > Columns

Certificates

- New**
- Search / Manage

Account

- Logon
- Create

Certificate login

- Logon

Public search

Search text :

Exact search: "O=SwissSign AG"
Wildcard search: Swiss*

License :

Page size :

Search

Click „New“ at „Certificates“

Home | Support | Certificate authority | Shop | Revoke certificate | Help

swissign

New certificate request

License > Submission

Get a license from our Shop

License

* License code :

Proceed

Enter your license code you ordered at the beginning.
Afterwards click “Proceed”



Next are general terms and conditions. Read this and accept the terms if you want to proceed.

Click below on the appropriate button.

Please click "Proceed". If you just want to generate an e-mail certificate, you don't have to fillout the text box named "PKCS#10".

Please enter the e-mail address you want to certify.

Afterwards click on "Proceed"



Personal Silver Certificate
 > License > Validity > EUA > CSR > Email **Contact** > Submission

Contact
 Address used for the notifications related to this request.

* **Email address** :
Overrides the predefined email address above

Preferred language : English Deutsch

Notice :

Free text

Back Proceed

Here you can check and alter your contact information.
Click "Proceed" to continue.

Email > Contact **Submission**

Certificate data

Subject DN	CN	
	emailAddress	
	OU	Email Validated Only
Subject Alternative Name	email	

[A proof of possession mail will be sent to](#)

Key generation
 The generated key will be encrypted with the following password.

For security reasons, SwissSign is unable to recover lost key passwords. Their secure storage is in the sole responsibility of the user.

* **Password** :
 Repeat password :

Back Request certificate

Check your information regarding your certificate.
Additionally choose a password to secure your certificate against unauthorized access (recommended).
Click on "Request certificate" to proceed. You will receive an e-mail to the address you submitted before.

SwissSign - Your certificate request 2997A328A6EF - Nachricht (HTML)

DATEI NACHRICHT

ca@swissign.net
SwissSign - Your certificate request

An
Signiert von ca@swissign.net

Dear customer,
We are pleased to acknowledge your certificate request.

Request identifier 2997A328A6EF
Subject Validated Only

As the legitimate owner of [you can approve](#) your request by yourself.

If needed, you can adjust your certificate request by [withdrawing](#) your request and then submitting a new one.

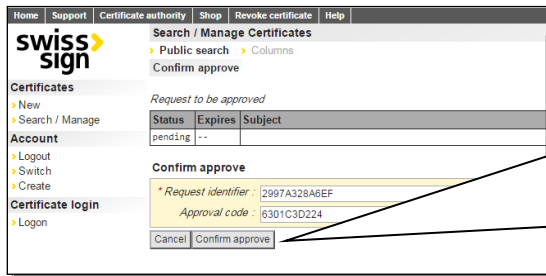
If you suspect that someone is trying to abuse your email and you did not request this certificate, please contact us at registration@swissign.com or fill our [contact form](#).

Do not reply to this automatically generated email.
If you have any questions, contact the helpdesk of your Managed PKI if you have one; otherwise fill our [contact form](#).

Best regards,
Your SwissSign Team

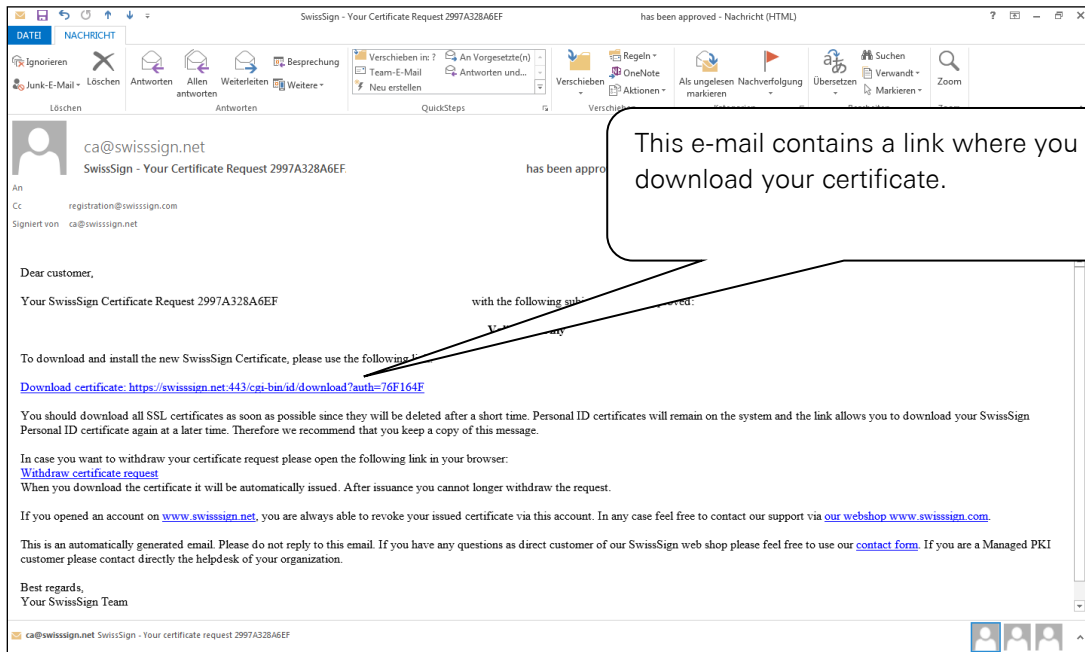
ca@swissign.net SwissSign - Your Certificate Request has been approved

Open the e-mail and click on "approve" to approve your e-mail address

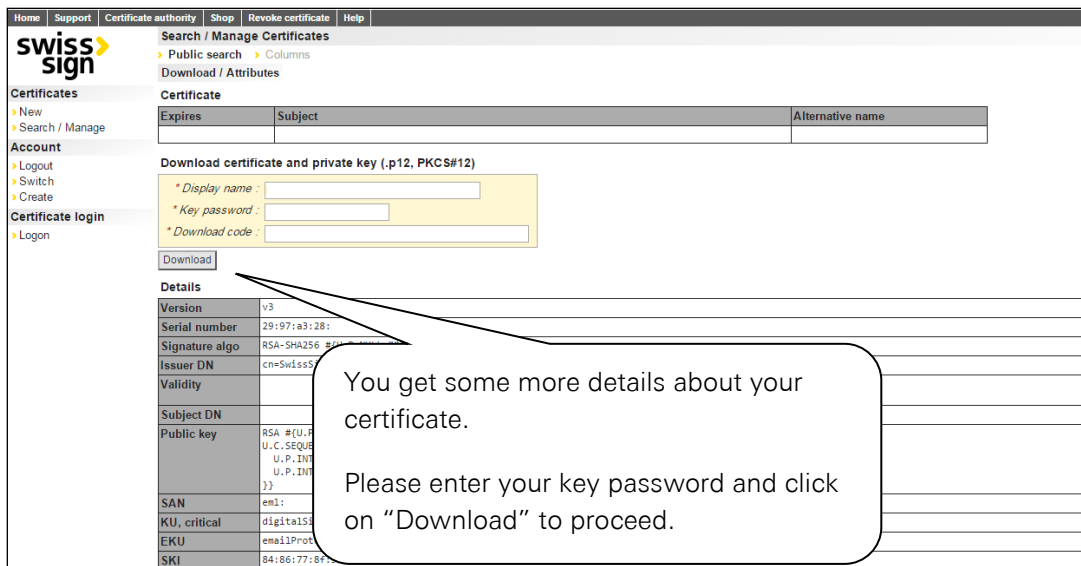


You are linked to "SwissSign.net". Click on "Confirm approve" to finish the approval.

Now your e-mail address is authenticated and you will receive an e-mail containing a link to your certificate.



This e-mail contains a link where you can download your certificate.



You get some more details about your certificate.

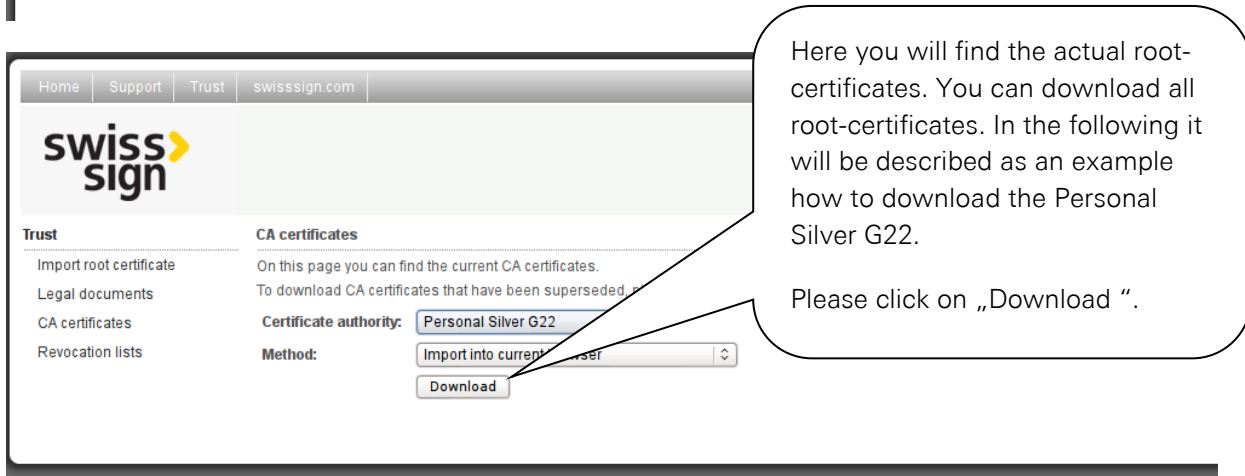
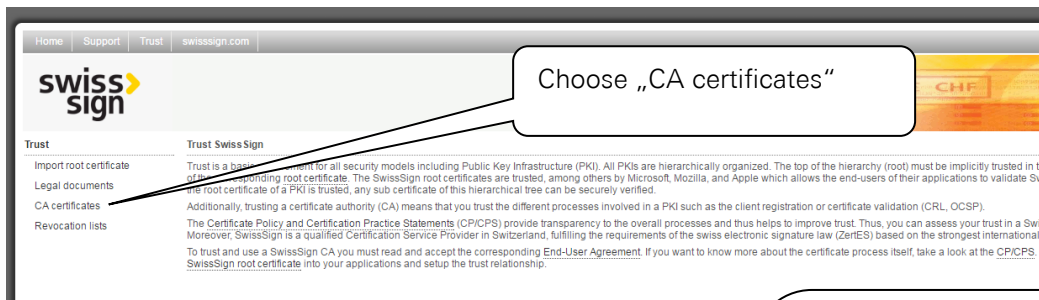
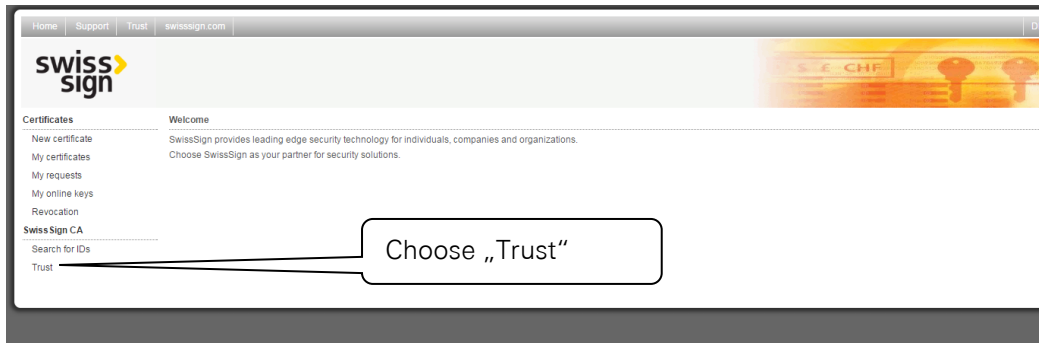
Please enter your key password and click on "Download" to proceed.

After you clicked on "Download" you finished requesting, authenticating and generating your certificate. Your certificate should be in your download folder.

2.3. Installing a certificate

This chapter describes how to install the certificate created in the prior steps. You have to do this step to comfortably communicate encrypted with ALDI by using your Outlook.

At first, install the Root-CAs of the trustcenter SwissSign. For this please open the webpage from SwissSign with the following address: <https://swissign.net/cgi-bin/home>

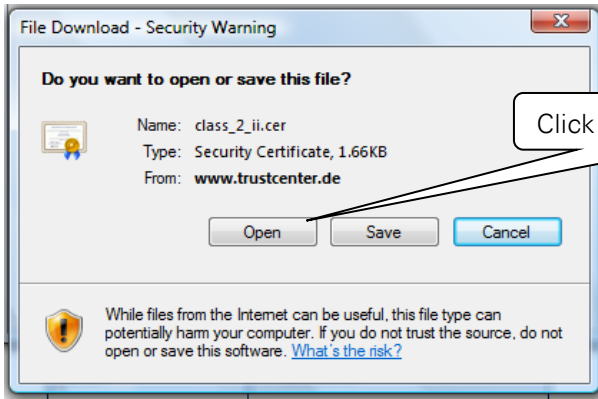


Save the file with the file-extension „.cer“.

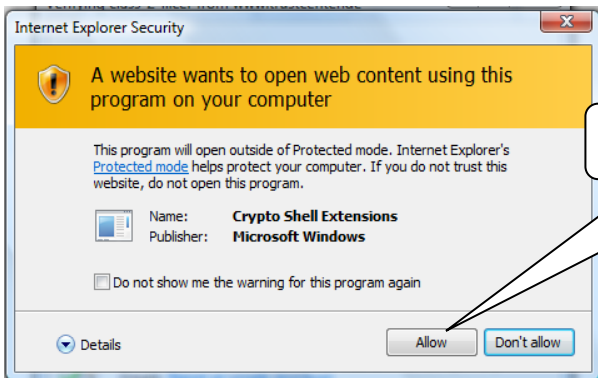
Depending on your Internet browser, you will receive a mask asking you to trust a new certificate authority (CA). Please choose the two options that contain “trust to identify websites” and “trust to identify e-mail user” or words to that effect and click „OK“.

If you don't get that window please open the „.cer“-file.

You may now get one of the following screens. You have to accept them as described:

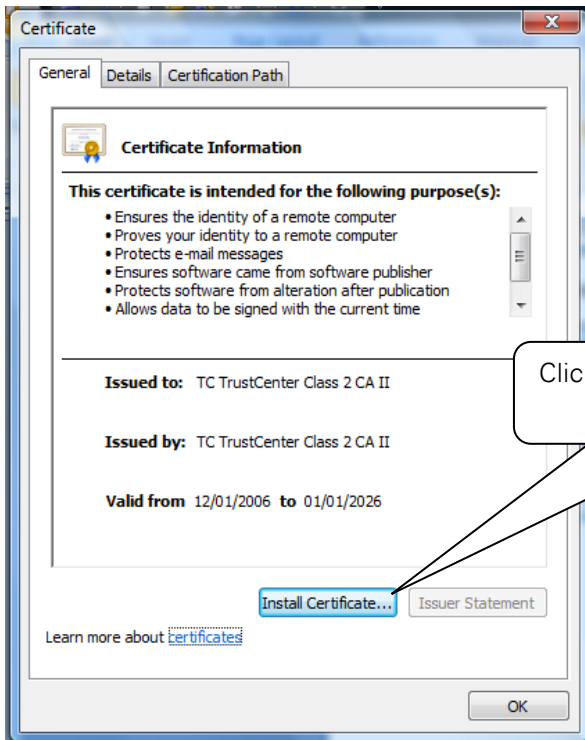


Click „open“



Click "Allow"

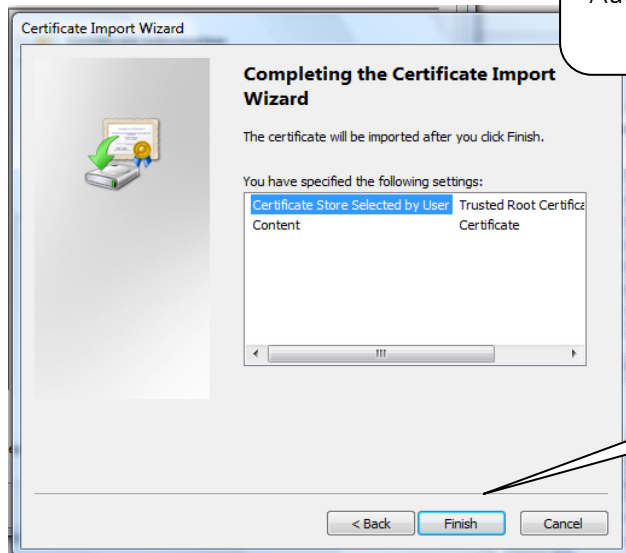
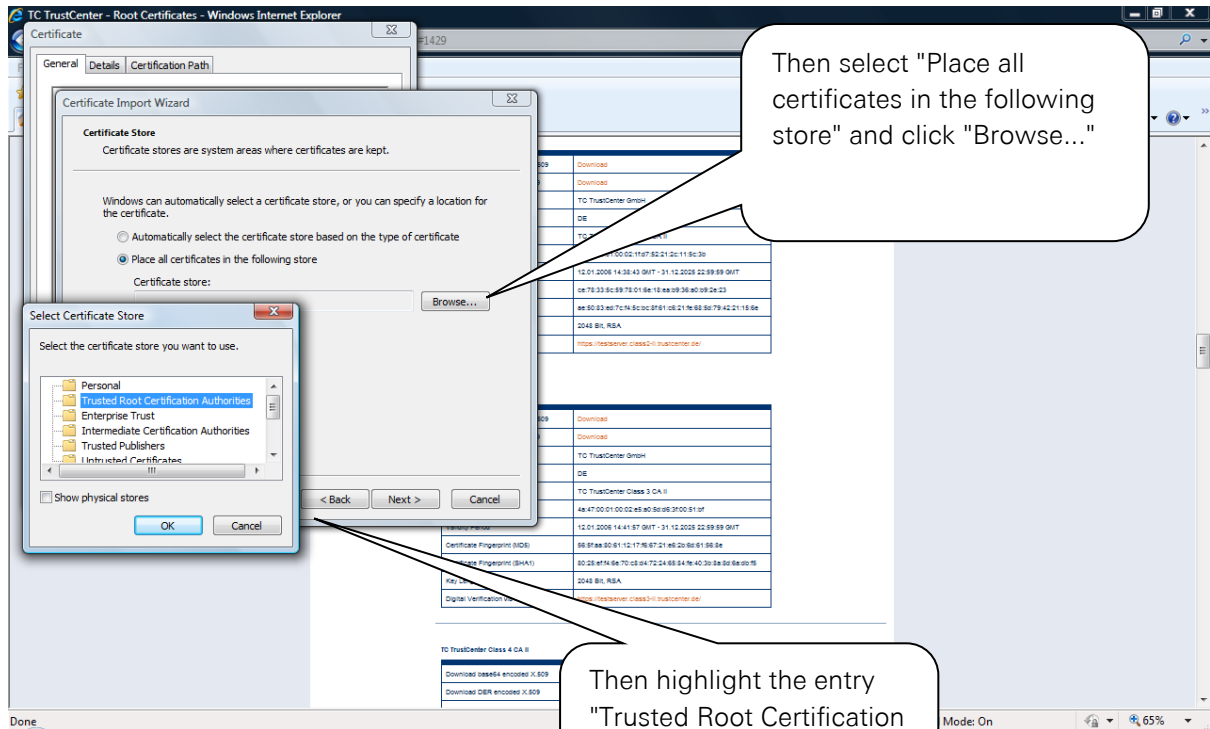
After that you have to install the certificate:



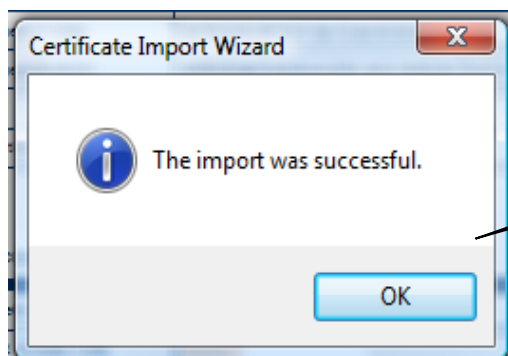
Click "Install Certificate..."



Click "Next >"

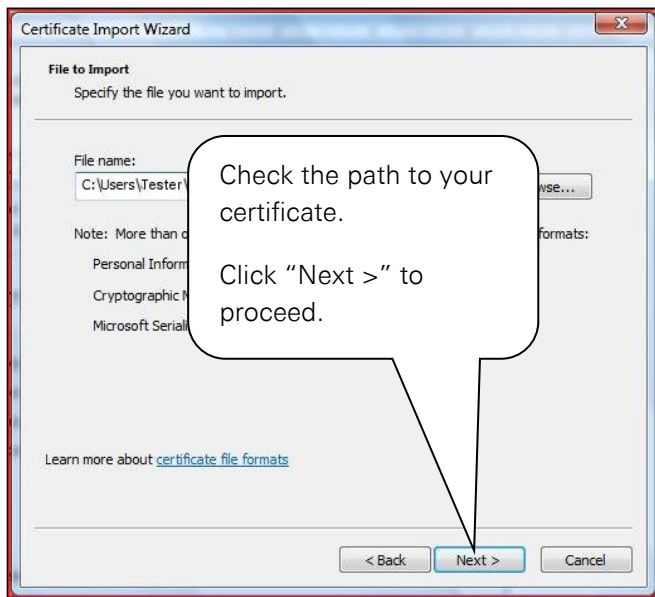
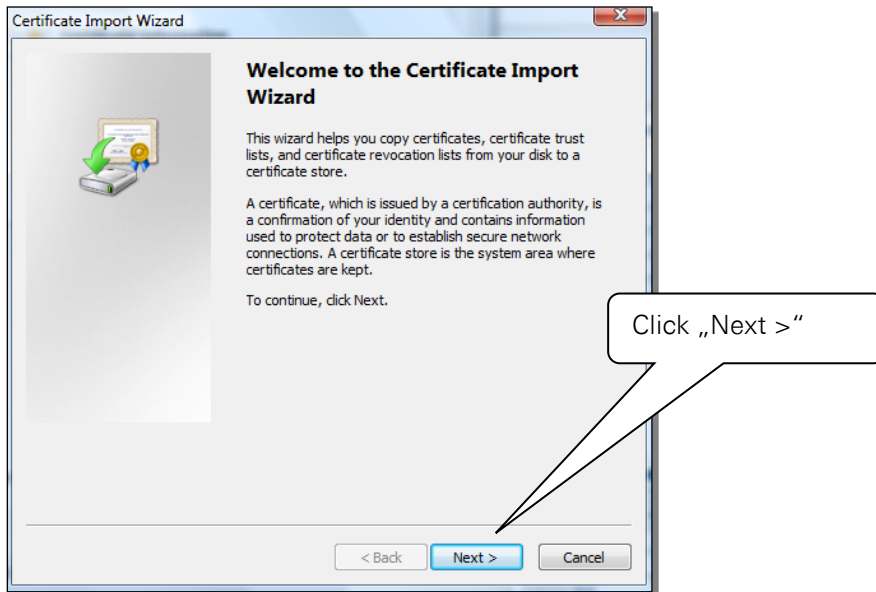


Now you may get a security request concerning the installation of a root certificate. Please confirm with „Yes“:



Click "OK"

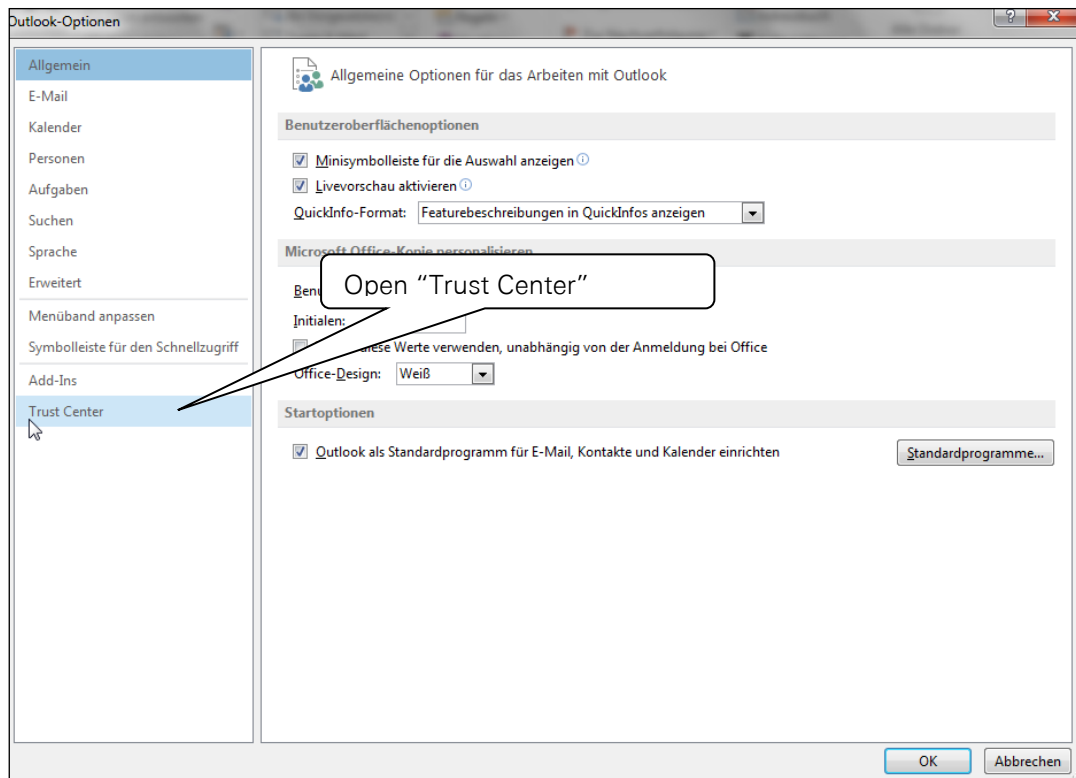
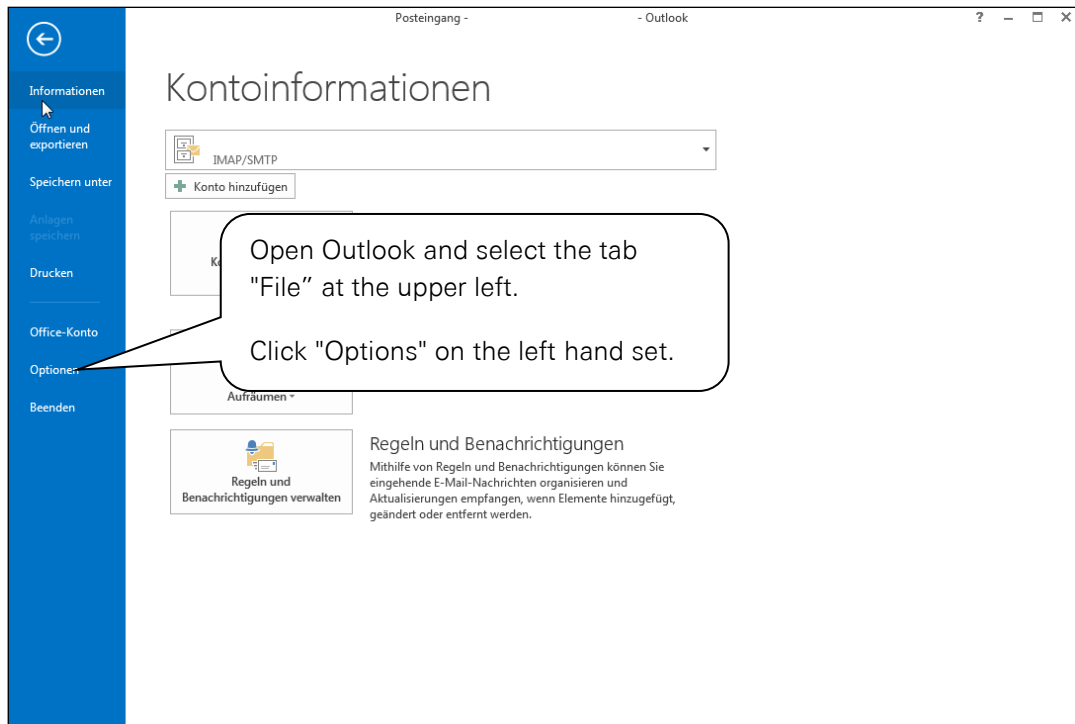
Now install your certificate which you previously downloaded, double-click on the file and open it. Then a “Certificate Import Wizard” opens.

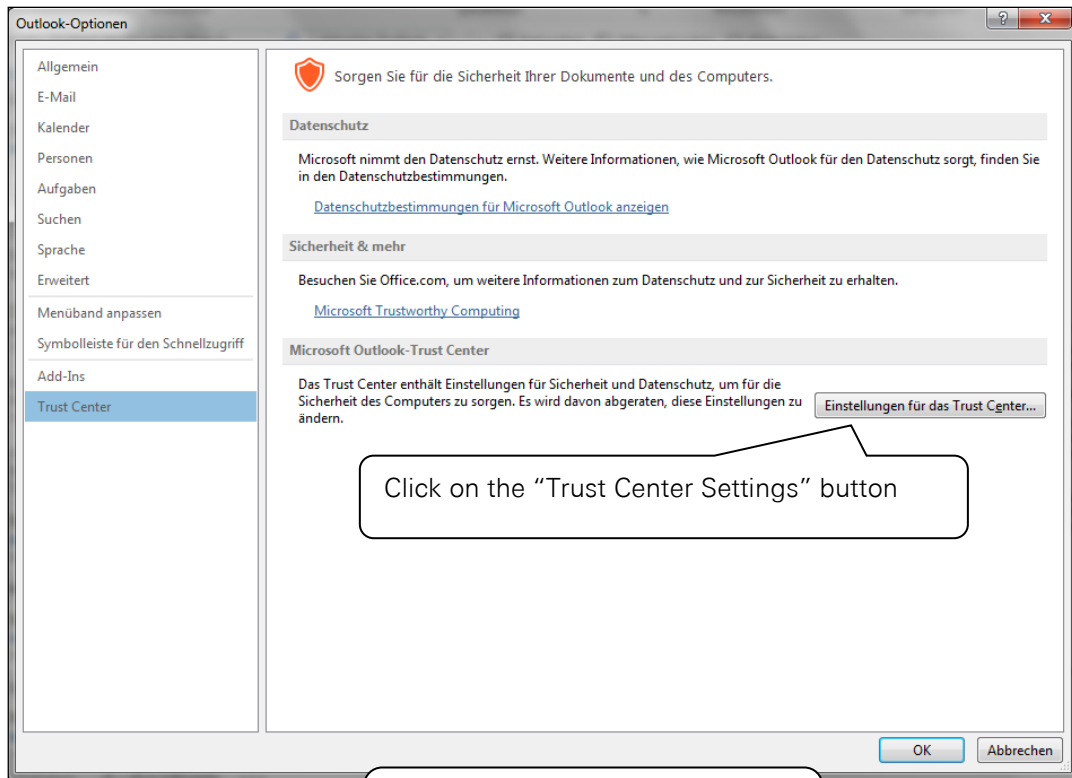




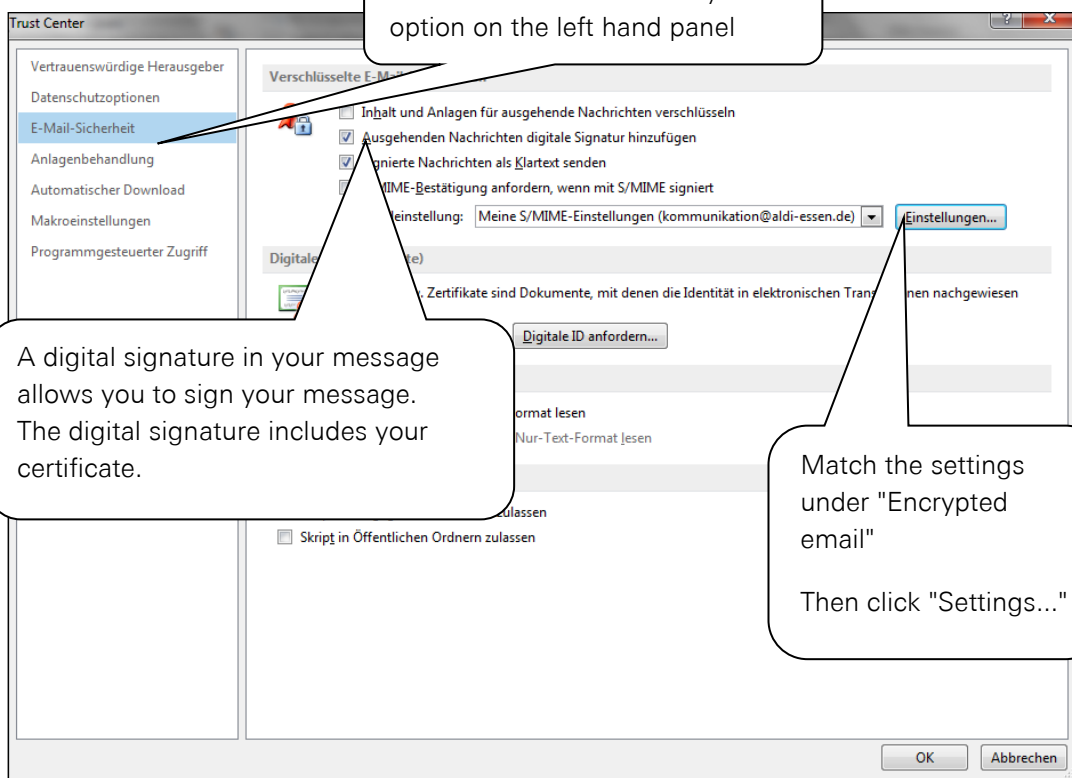
2.4. Setting up the certificate in Outlook

This section explains how to set up your Outlook 2013 to use your certificate as a signature. Start Outlook 2013.





Click on the "Trust Center Settings" button

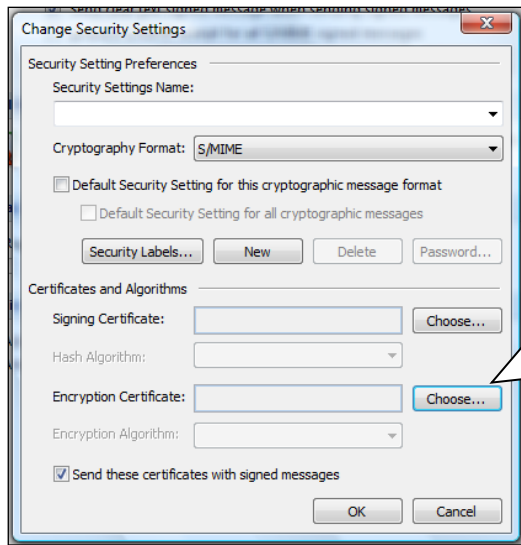


Click on the E-mail Security option on the left hand panel

A digital signature in your message allows you to sign your message. The digital signature includes your certificate.

Match the settings under "Encrypted email"

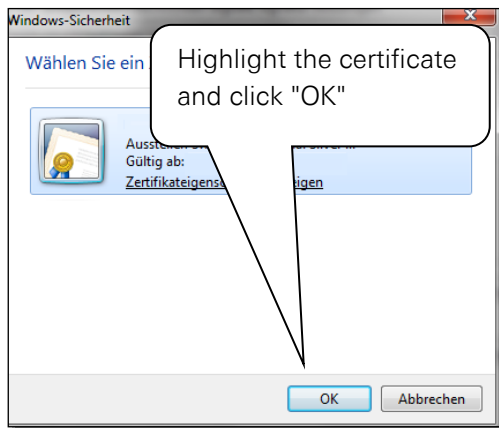
Then click "Settings..."



For encrypted communication, click "Choose..." at "Encryption Certificate"

Depending on the options previously selected, you may also have to select and store a signature certificate.

Now select the requested certificate.



Highlight the certificate and click "OK"

You can choose the Security Settings Name yourself.



Match the settings and then click "OK"

The default settings are now saved. On the next window click "OK" again.

Outlook 2013 is now set up to use your certificate.

2.5. Encryption with Outlook

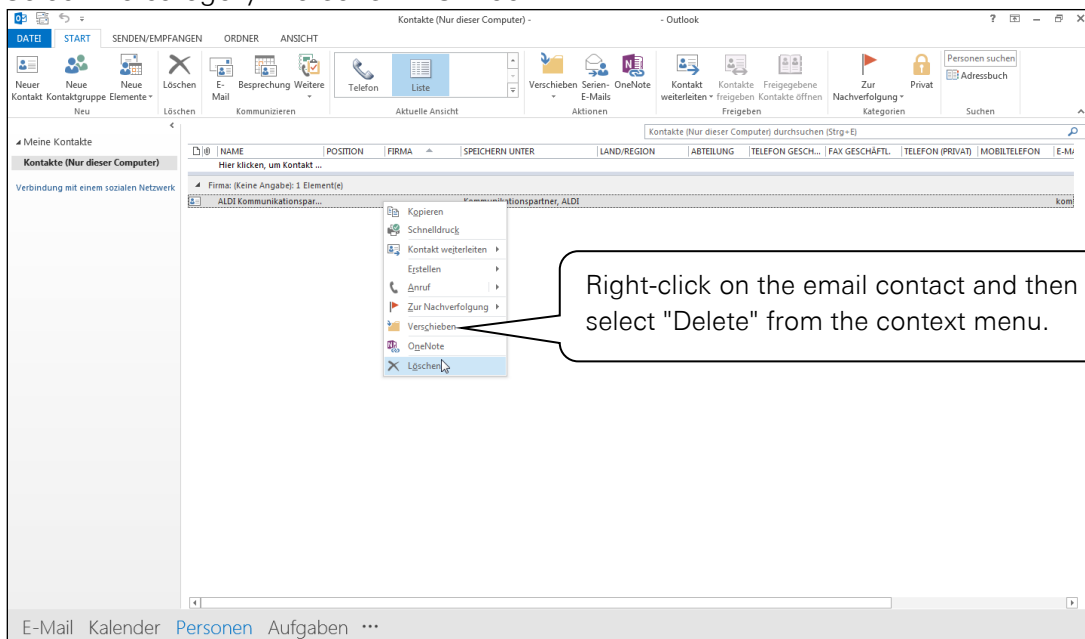
This section explains how to correctly create your ALDI communication partner as a contact for encrypted email communication. Creating a new contact is also required if for example ALDI Nord customizes the name of an email address or if you are asked to do it by an ALDI Nord employee.

Furthermore, the buttons required for encryption in Outlook 2013 are explained.

Deleting the existing contact:

To avoid problems, any contacts of the ALDI Nord communication partner which may already exist must be deleted.

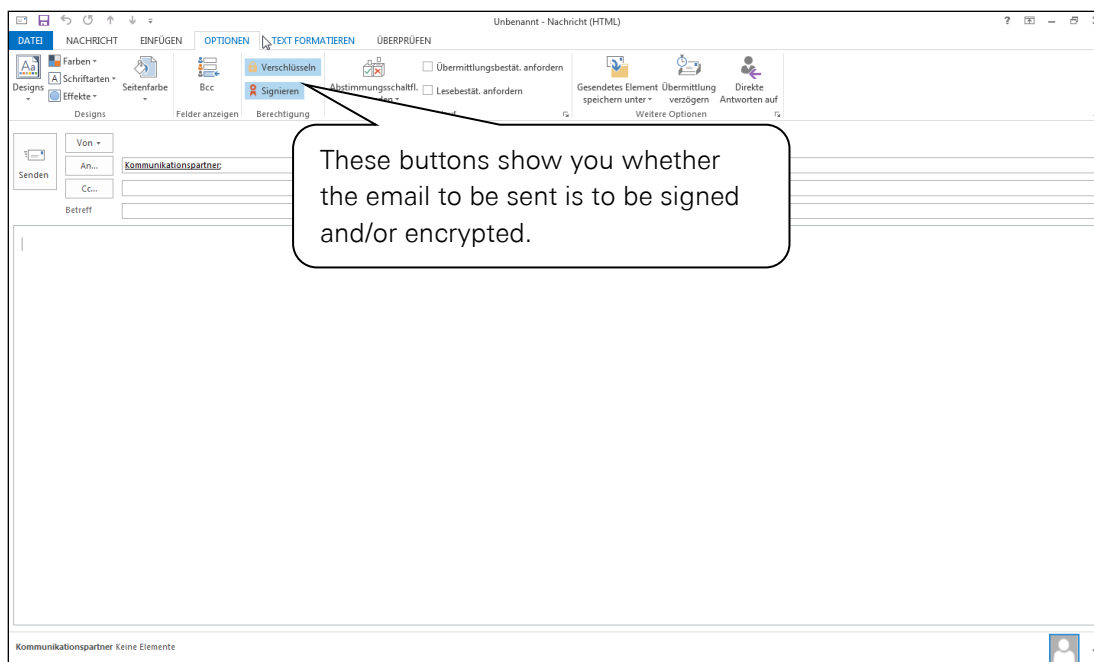
Select the category "Persons" in Outlook.



Creating a new contact:

To set up encrypted communication correctly, the contact of the ALDI Nord address must be set up as explained in section 5.2.. Otherwise, the public certificate of the contact partner is not stored correctly.

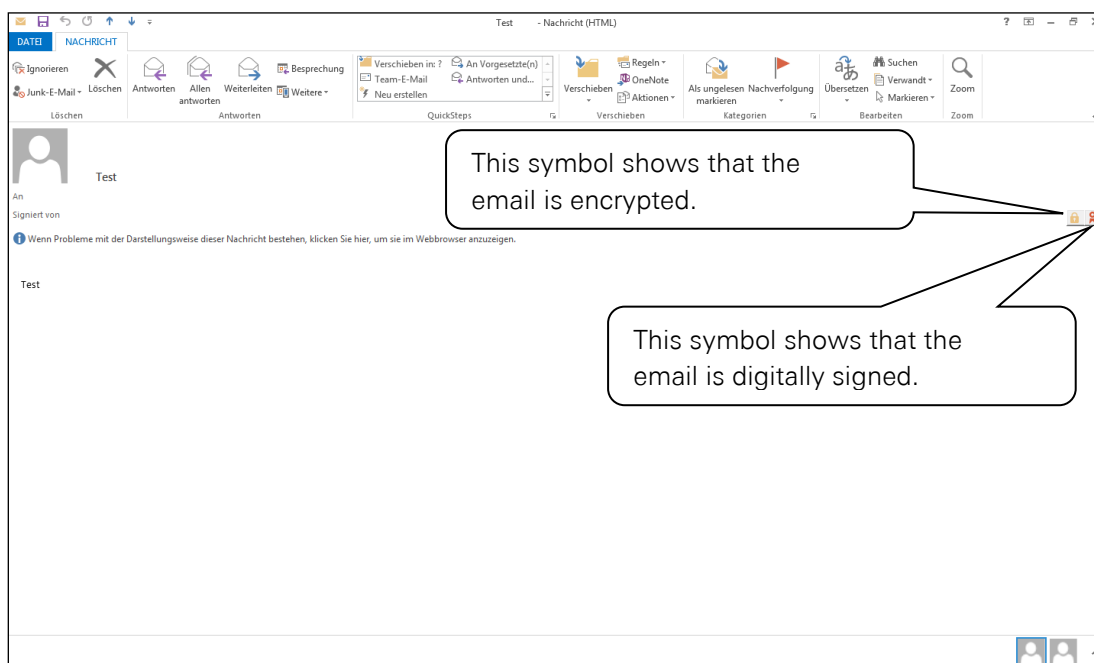
By previously adjusting the settings and installing the certificate, two buttons have been added to the window for a new message.



Before you can send encrypted emails, you must have received a signed email from your ALDI Nord communication partner. It is necessary to publish your public key on the trust center's keyserver (cf. section 2.1) or on the site www.aldi-nord.de/certportal (cf. section 5.3) to let your communication partner send you an encrypted email.

In the appendix of an email sent by your ALDI Nord contact you will receive the signature and the public key of your communication partner.

You can recognize an encrypted and signed email as following:





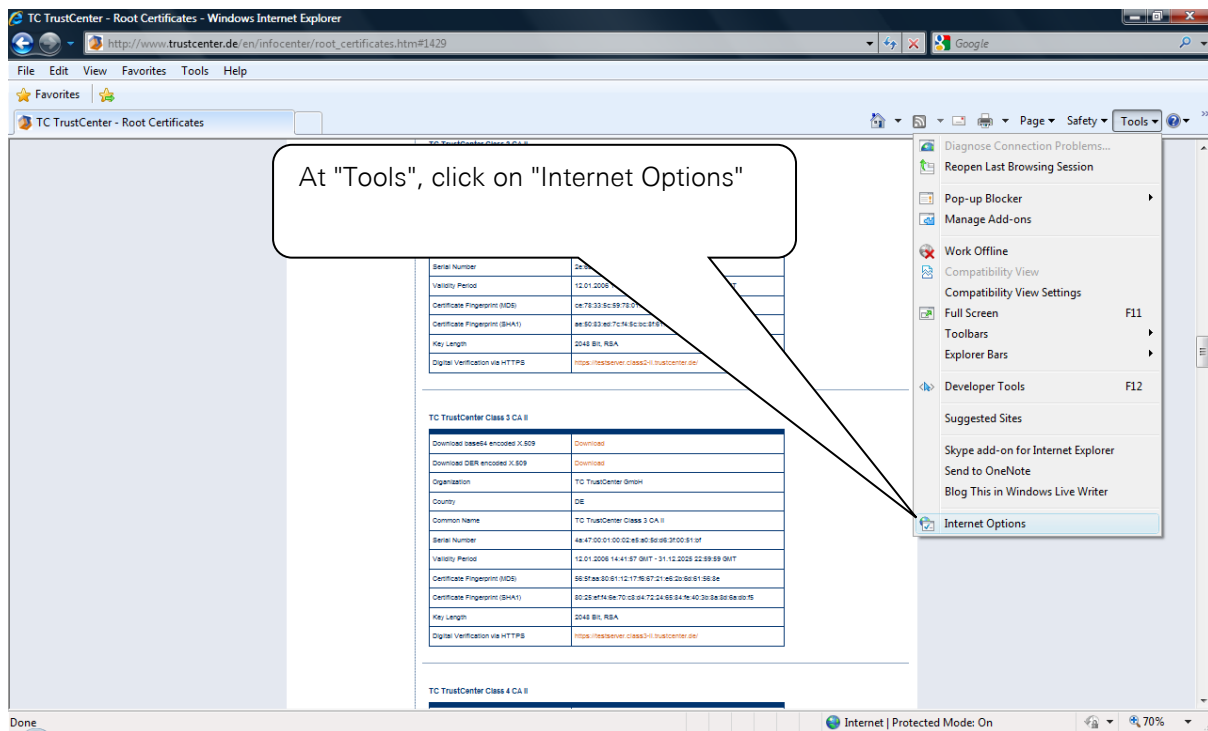
3. Exporting and importing certificates

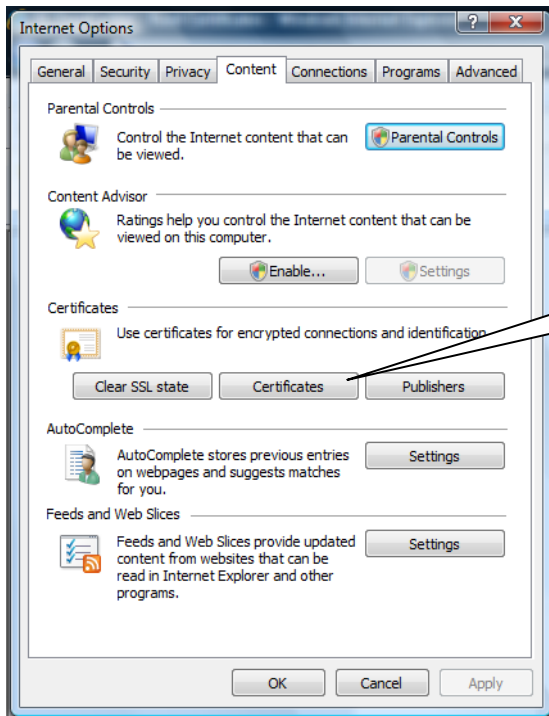
Certificates can be exported and imported so that they can be used on another computer.

3.1 Exporting a certificate

If you would like to use the certificate requested and installed in section 2 on another computer for the email address mentioned above, you have to export the installed certificate from the browser and import it into the browser of the computer to be used in future. This section explains how to do this.

First, open the browser on the computer you have used so far (the browser used in section 2.1 to create the key/certificate).

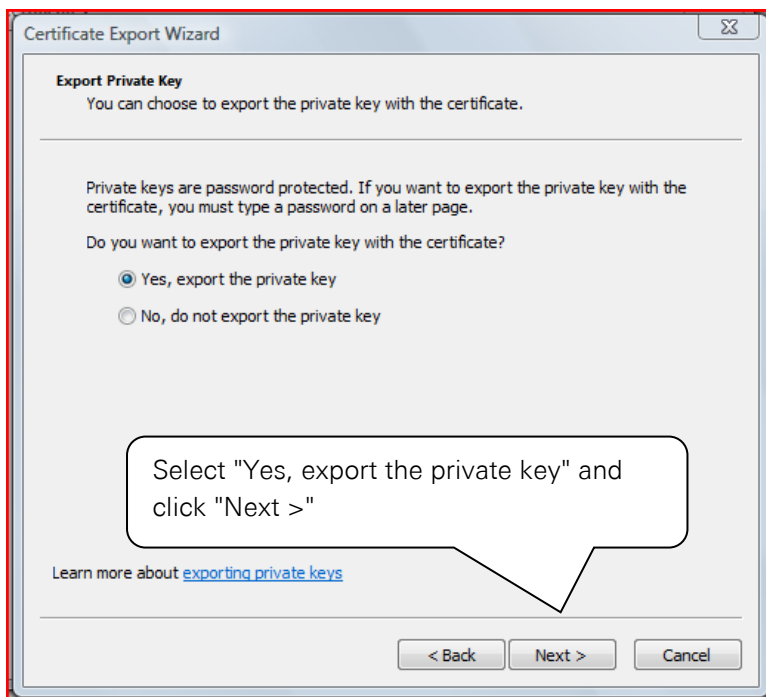




At the tab "Content", click on "Certificates"

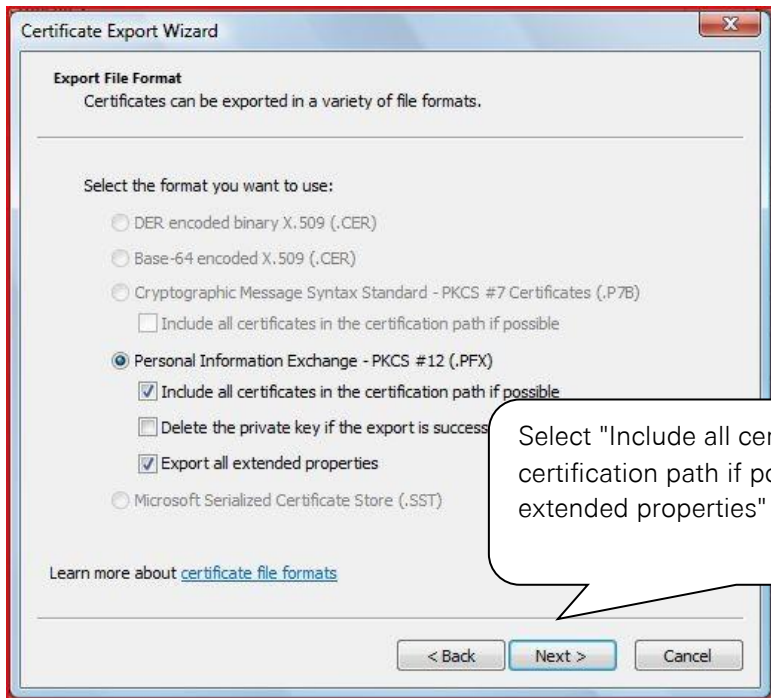


The certificate to be exported (here issued to Rudi Tester) appears under the tab "Personal". Highlight the certificate to be exported and then click on the button "Export..."

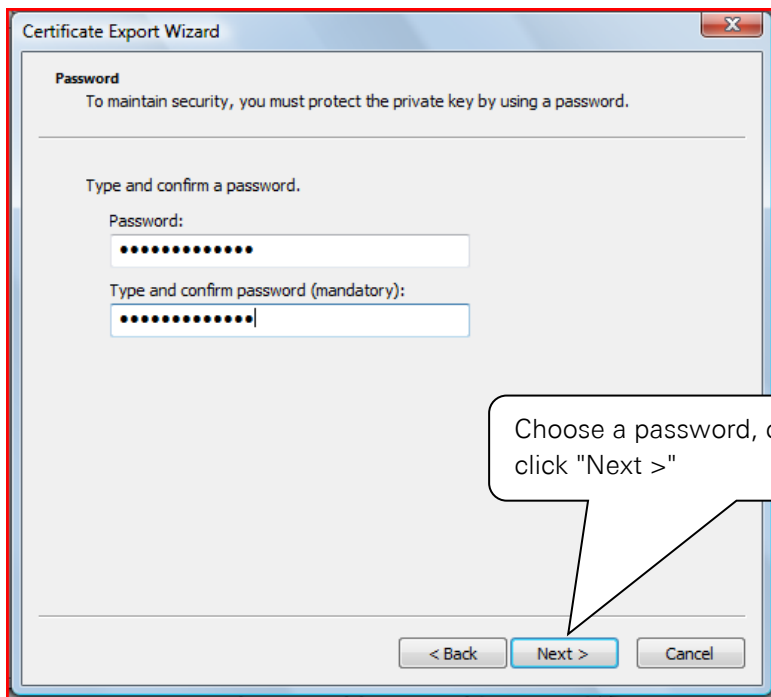


If you proceeded as described in section 2.3 and the option "Yes, export the private key" is greyed out, please check your credentials.

You must be a member of the users group or local administrators group to complete this procedure.



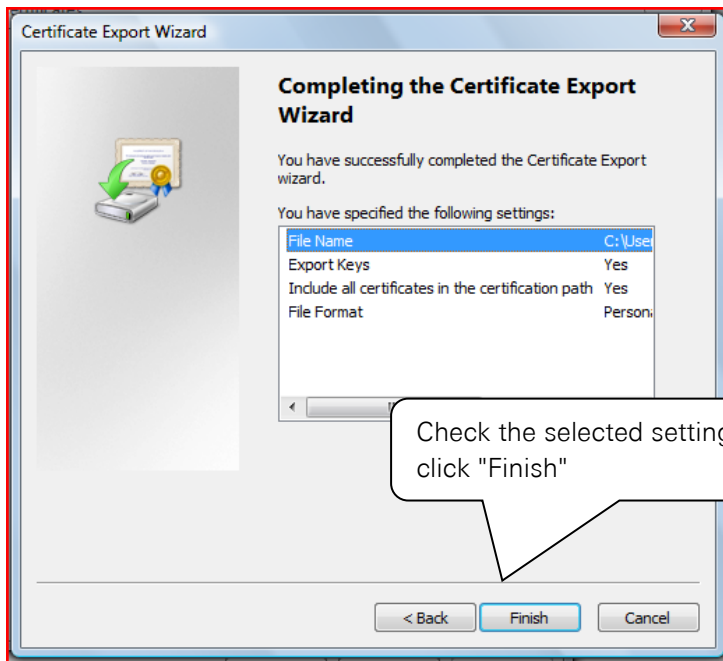
Select "Include all certificates in the certification path if possible" and "Export all extended properties" and click "Next >"



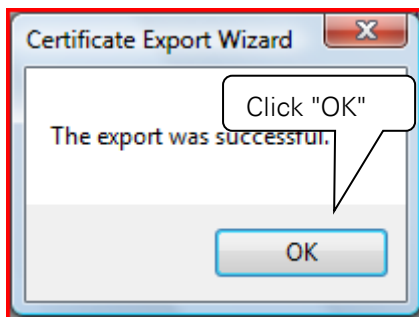
Choose a password, confirm it, and click "Next >"



Choose a file name and store location the key will be exported to and click "Next >"

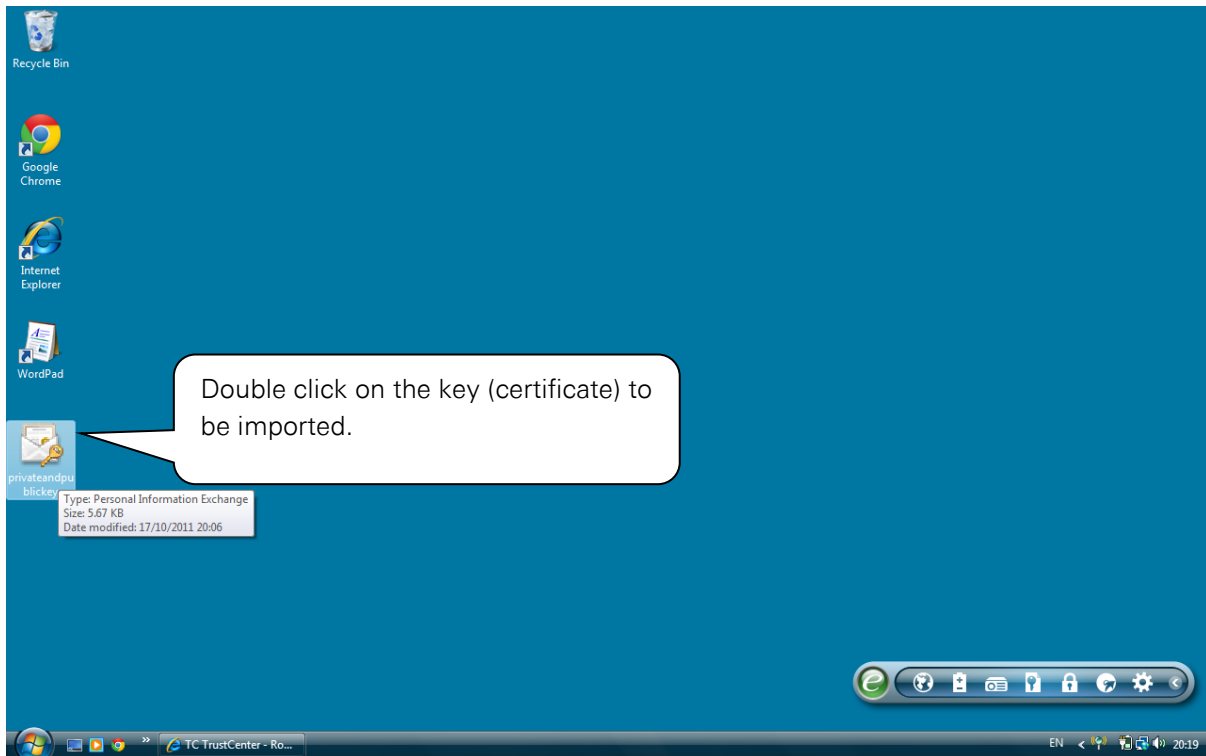


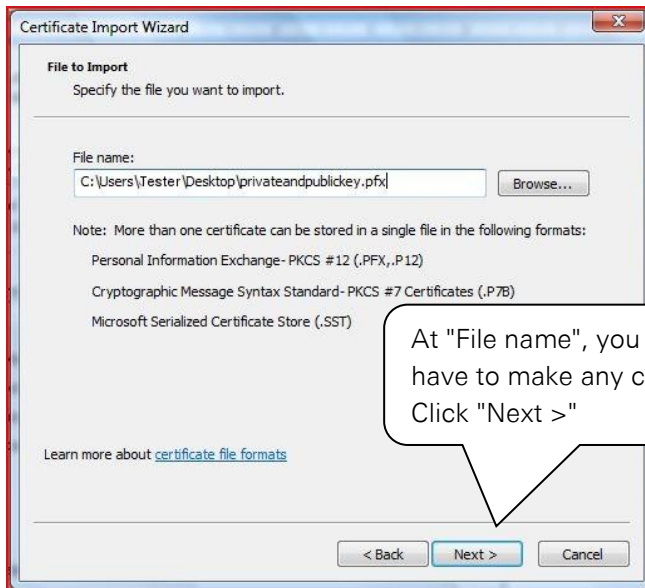
Check the selected settings and click "Finish"



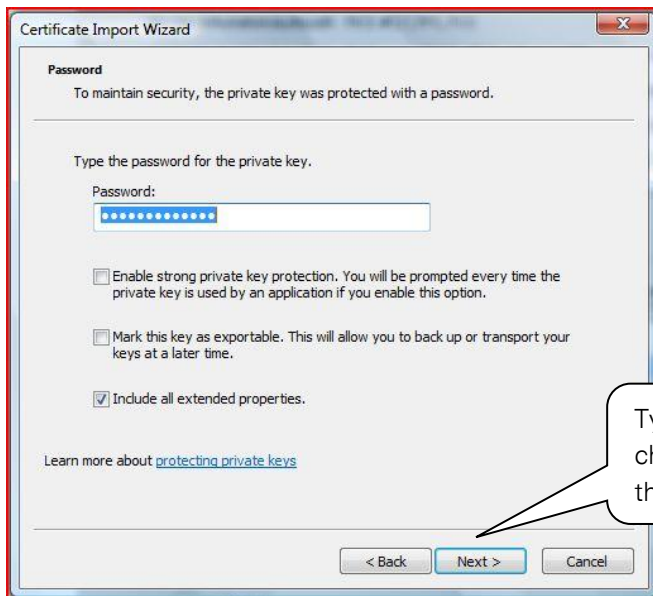
3.2 Importing a certificate

You must import the certificate previously exported on the new computer.
First, open Internet Explorer (or another webbrowser).

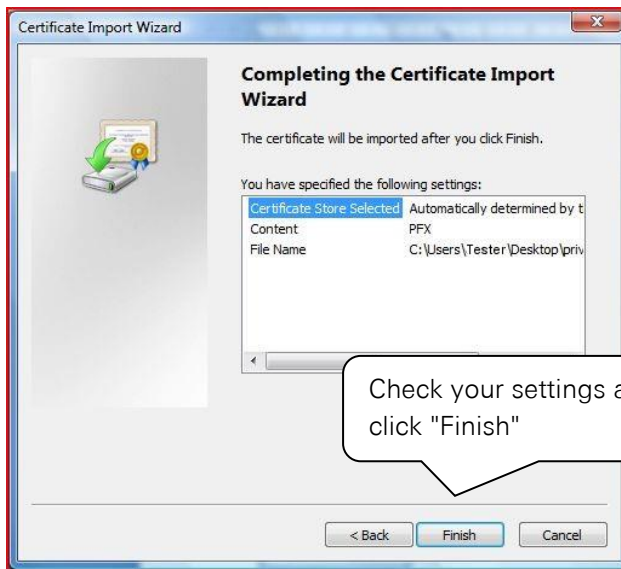
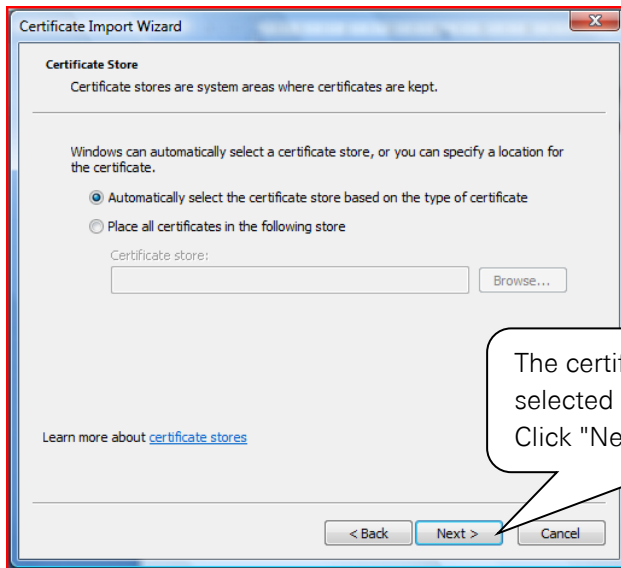




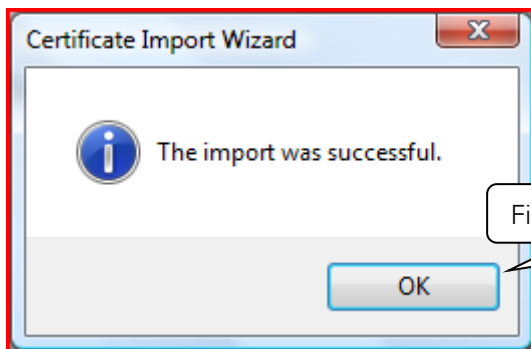
At "File name", you usually do not have to make any changes. Click "Next >"



Type in the password previously chosen for the private key and then click "Next >"



A security warning may then appear. Click "OK" to confirm the message.





4. Installing the ALDI Nord root certificate

With the so-called "Root certificate (CER)" you can check the trust status of the ALDI Nord group user certificates. This means that the system you use can check if the user certificate is really from the ALDI Nord group and if it is still valid. You have three options for receiving the root certificate:

1. You have already received an email from an ALDI employee and thus have access to the web messenger: you can download the root certificate there by clicking "Settings".
2. You can download the root certificate from the website "www.aldi-nord.de/cert".
3. You already have a certificate from one of the trustcenters supported by ALDI Nord and have published your public key on the keyserver. The email from an ALDI Nord employee including the root certificate is sent to you directly.

Installing the root certificate from the website is not different from installing it from the web messenger.

For points 1 and 2, follow the steps below:

Open the website http://www.aldi-nord.de/cert/index_en.html in your Internet Explorer: click on the link "Root certificate" under the heading "The ALDI Nord group root certificate", as shown below.


Welcome to ALDI

Information Root certificate Revocation list English

Secure e-mail communication with ALDI Nord

We are very pleased that you would like to use secure e-mail communication with the ALDI Nord group. We have outlined all of the information required for secure e-mail communication in the documents General Information and Instructions.

To read the documents you will require Adobe Reader®. You can download Adobe Reader® for free from the website www.adobe.co.uk. Please click on the Adobe icon to start the download.



The ALDI Nord group root certificate

To check the trust status of the ALDI Nord group user certificate you will require our root certificate.

Thumbprint S/MIME root certificate

You can check the validity of the ALDI Nord group root certificates with the following thumbprints.

[ALDI Nord Root CA \(from 04.12.2015\) »](#)

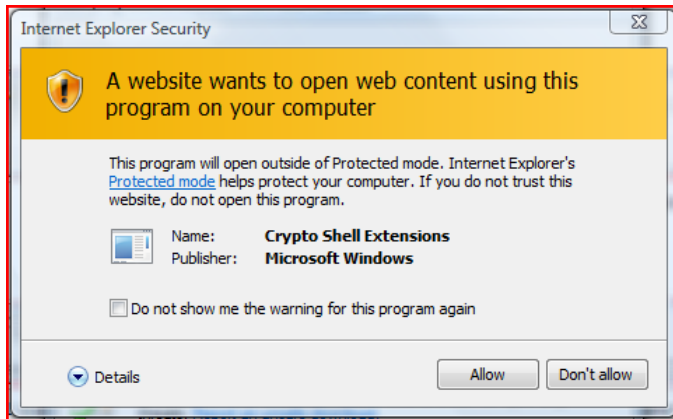
SHA1: a06a c71d b800 e8d9 56c3 c3e5 9ed0 bc3f 0e0 b6d3
MD5: bfd1 22f4 f721 197c 0860 38fc eef2 0752

[ALDI Nord Root CA OLD \(till 06.01.2016\) »](#)

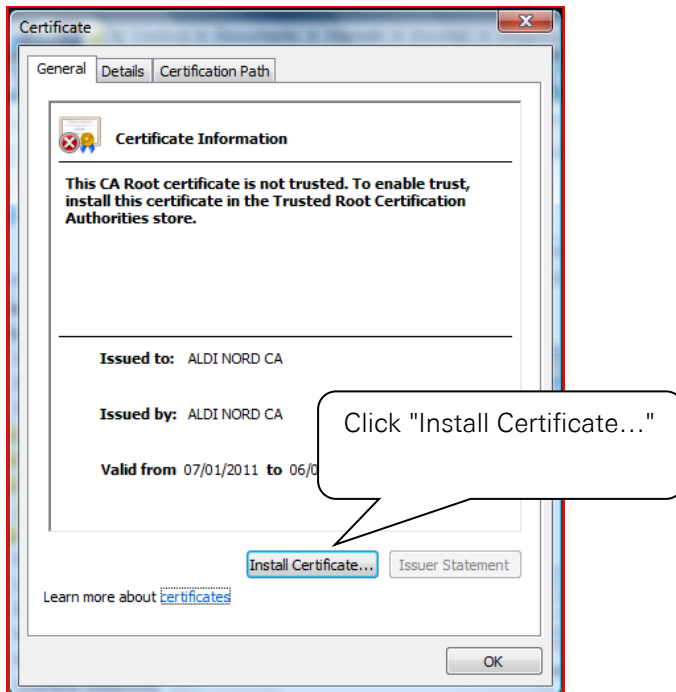
SHA1: e072 577b 2bd8 f68a ee6b eba2 17ca e9b6 b7a6 ba43
MD5: 542b b140 189c 0d0a d146 0007 e677 a6ed

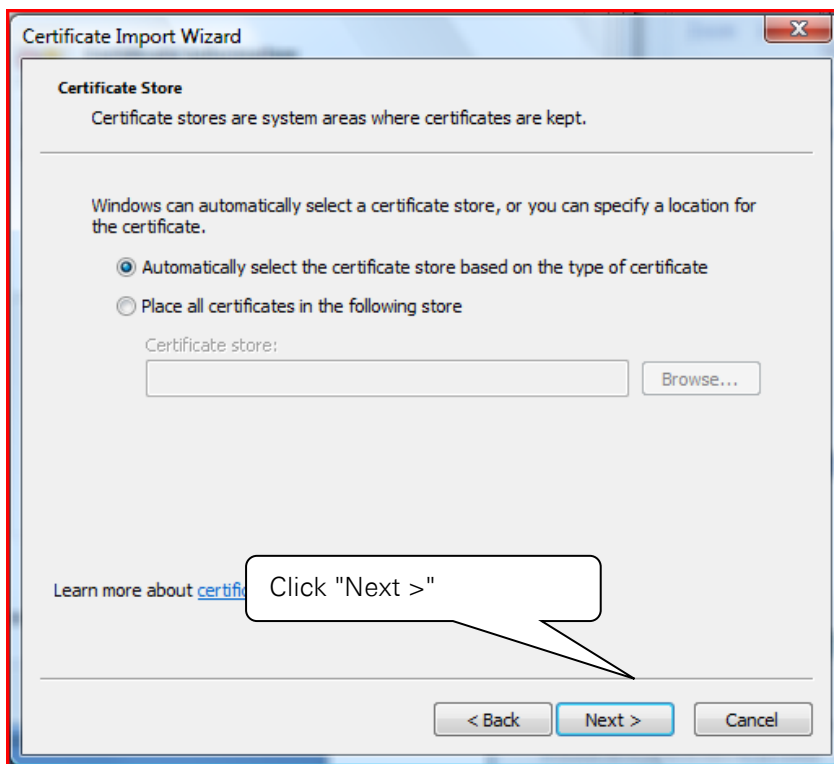
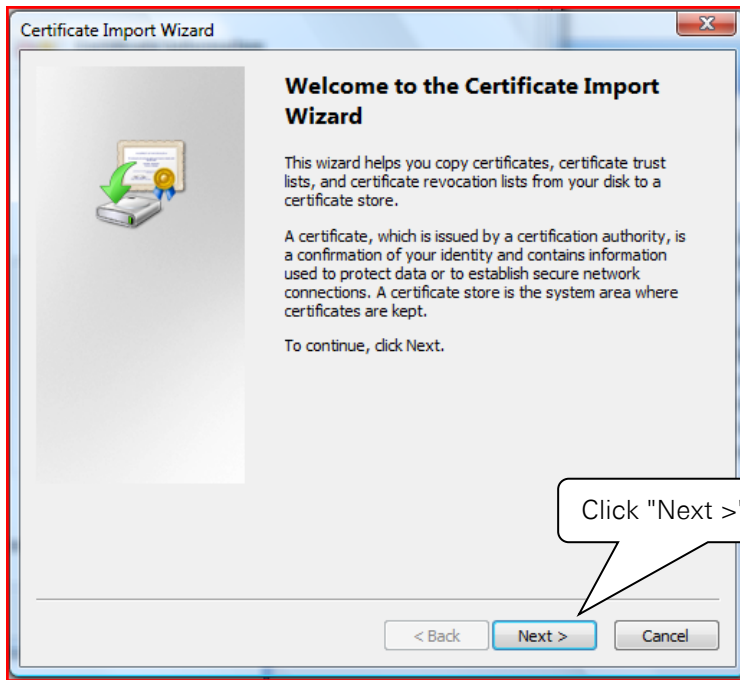
You will then be asked whether you would like to open or save the file. Click "Open".

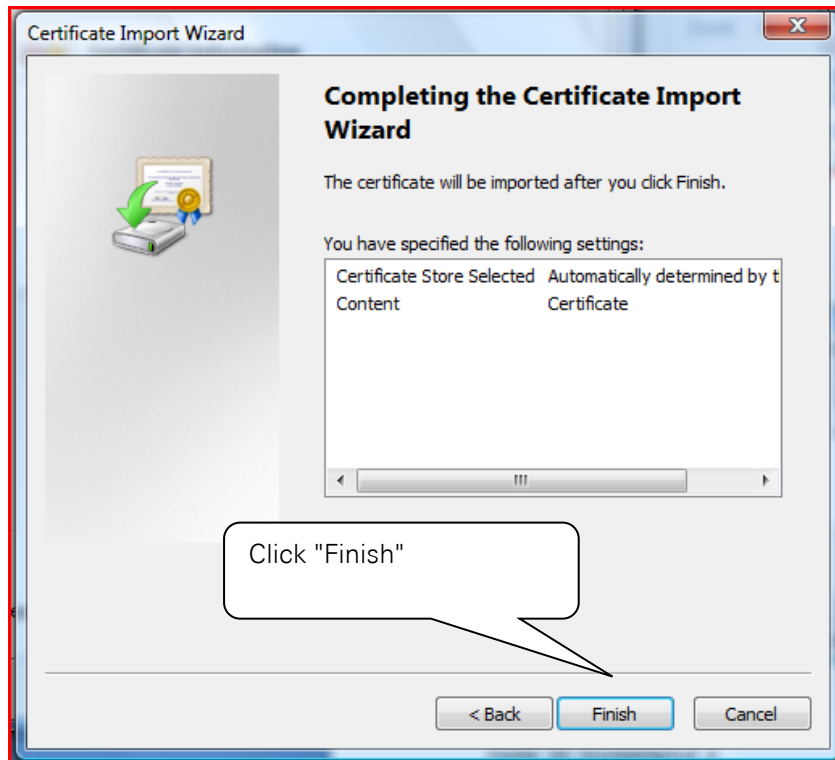
A security warning may appear. Click "Allow" to continue.



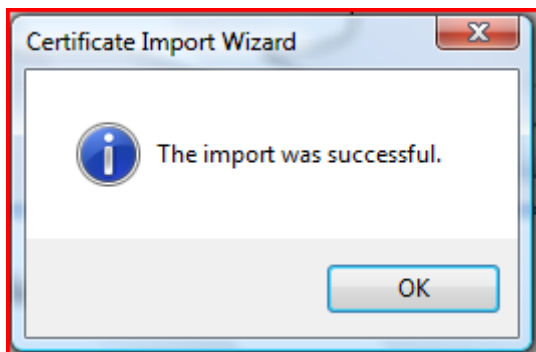
Then, the following messages will appear:





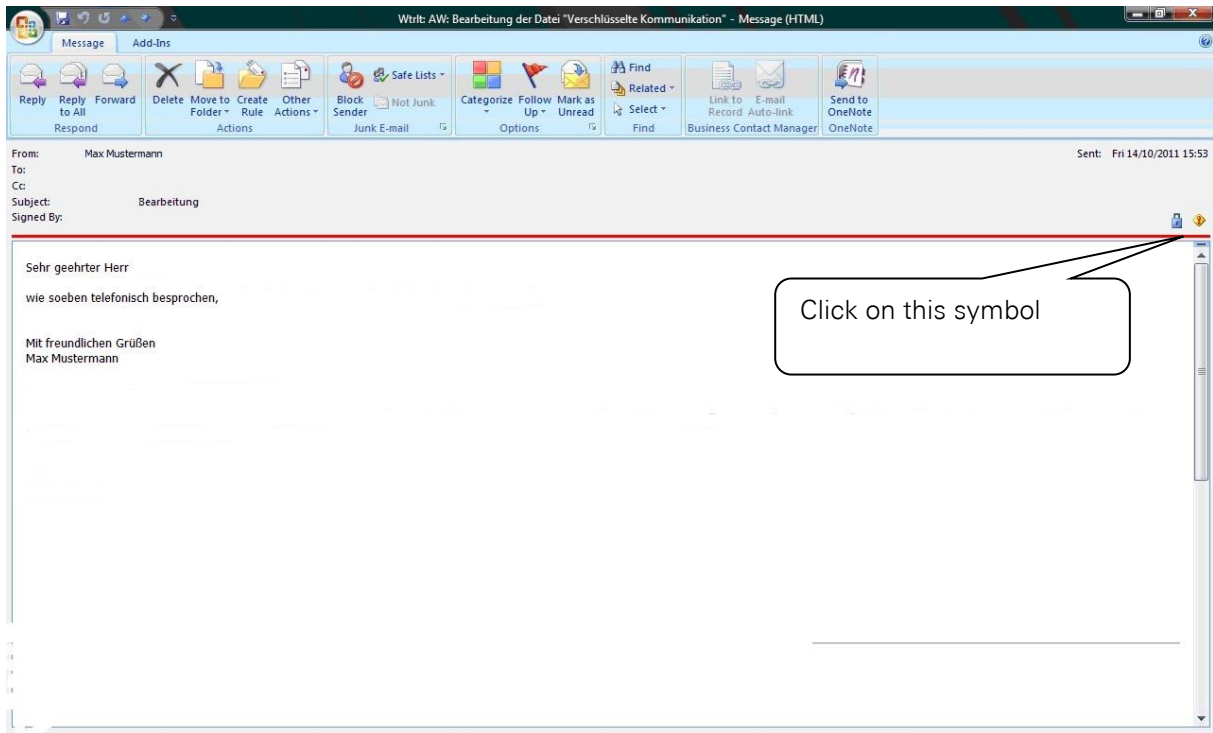


Finally, the following message appears:

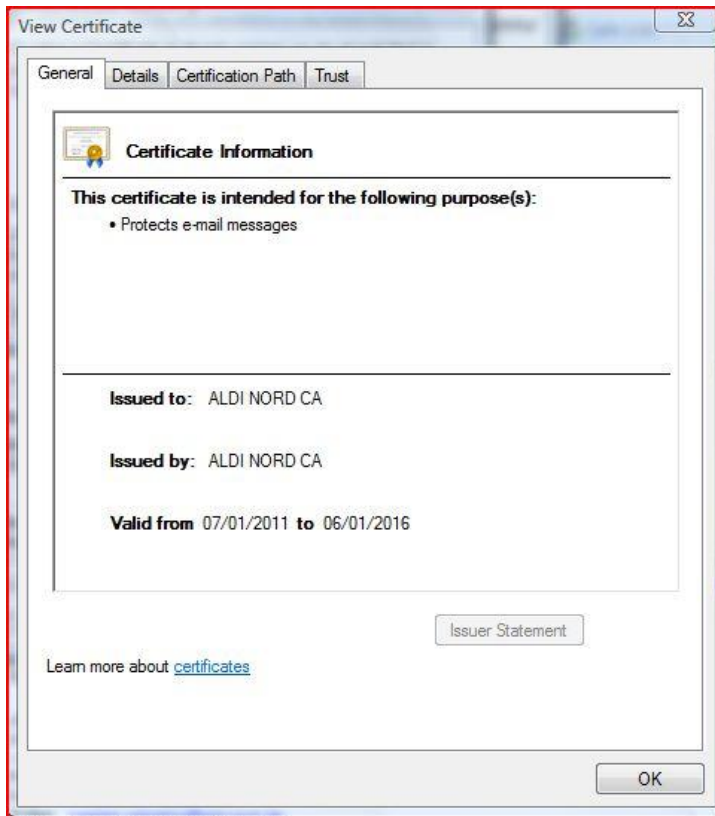


For option 3, follow the steps below:

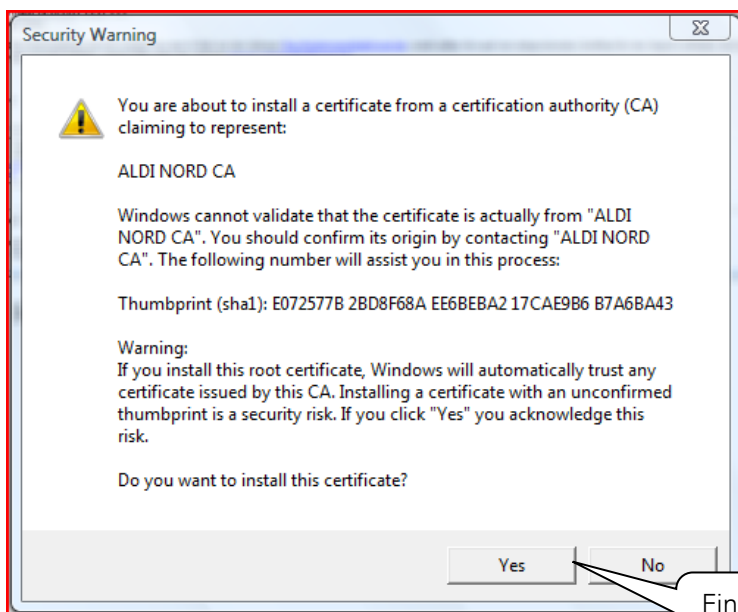
You already have a certificate from one of the TrustCenters supported by ALDI Nord and have published your public key on the keyserver. Your ALDI Nord communication partner has then sent you an email. Open this email with a double-click.



You can also display the certificate.



Before installation a security warning will appear.



The thumbprint of the ALDI Nord root certificate is shown here.

Finally, click "Yes"

After installing the root certificate, you can now communicate encrypted with ALDI Nord.



5. Alternative procedures for receiving and providing certificates

In section 2 setting up for encrypted email communication has been described. Here, the following assumptions were made:

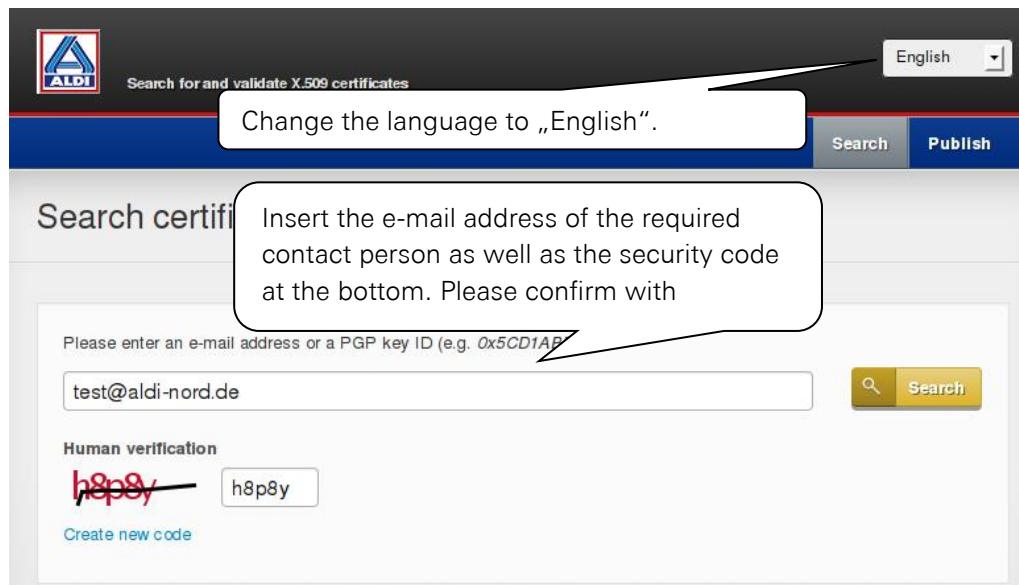
- A suitable certificate has been purchased and provided at the trust center.
- There is an encrypted email from an employee of ALDI Nord, which contains the necessary certificates for encryption in the appendix.

This section describes two alternative ways to exchange keys using the ALDI certportal.

5.1. Downloading a certificate of a communication partner

If the public certificate of an ALDI employee is needed for encrypting email, it can be downloaded from the ALDI certportal.

Follow this link: www.aldi-nord.de/certportal





Now you can see all existing certificates of this person. Click on the entry to get more information.

	test@aldi-nord.de valid from 2013-12-05 until 2023-12-03		
	X.509		
Owner	test@aldi-nord.de	Issued by	ALDI NORD CA ALDI NORD
Signature Algorithm	SHA1WithRSAEncryption		
Algorithm (Key Length)	RSA (2048 bits)		
Fingerprint (SHA1)	4C:31:6E:64:CE:4B:81:88:E9:7		
Serial Number	07:72:72:C6:C4:32:65:BD:8E:73:44:8E:57:A5:F1:B1:DB:44:B1:22		
Key Usage	Data Encipherment, Key Agreement, Key Encipherment		
Valid from	2013-12-05	Expires	2023-12-03

By using this button, you can download the certificate of your contact person.
For encrypted communication you need the certificate with the .cer file extension.

	test@aldi-nord.de valid from 2014-12-14 until 2024-12-12		
--	--	--	--

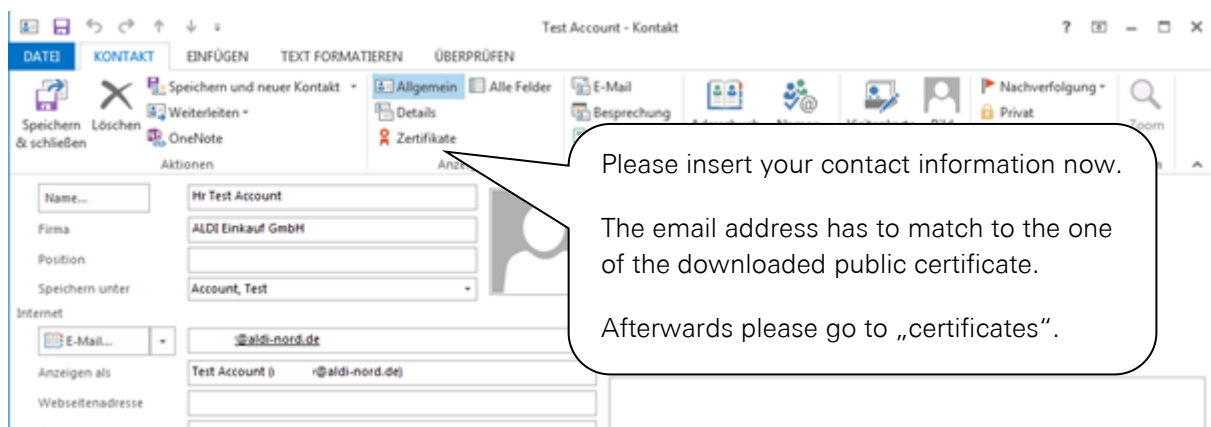
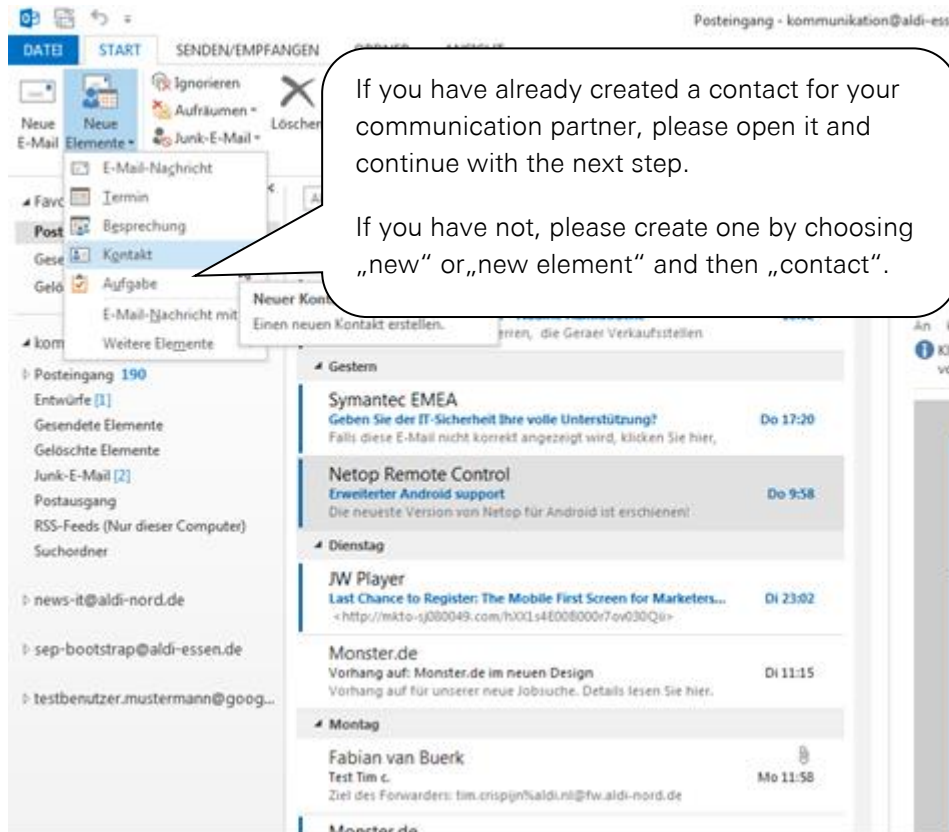
Sometimes there is more than one certificate shown for an email address. Because of that, please check the area "Key Usage". "Data Encipherment" has to be listed for a key to use it for encryption.

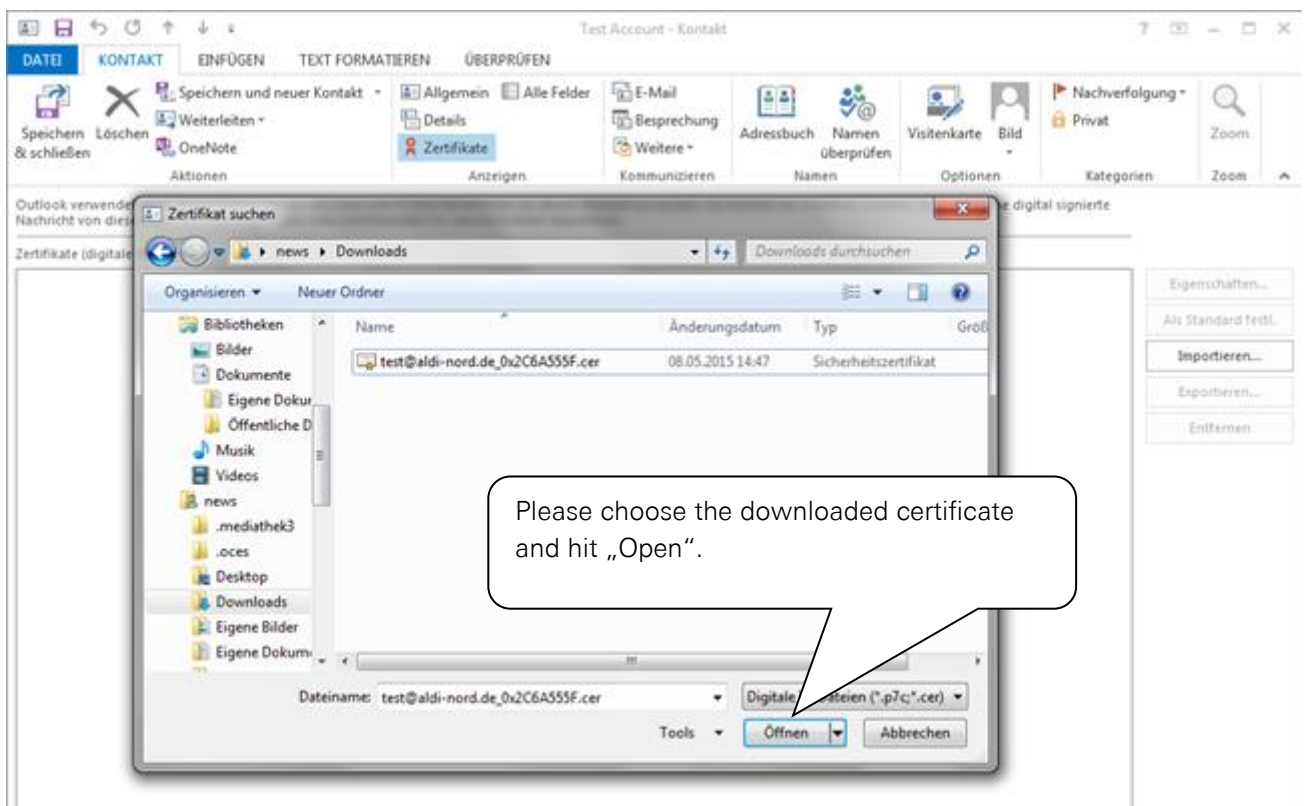
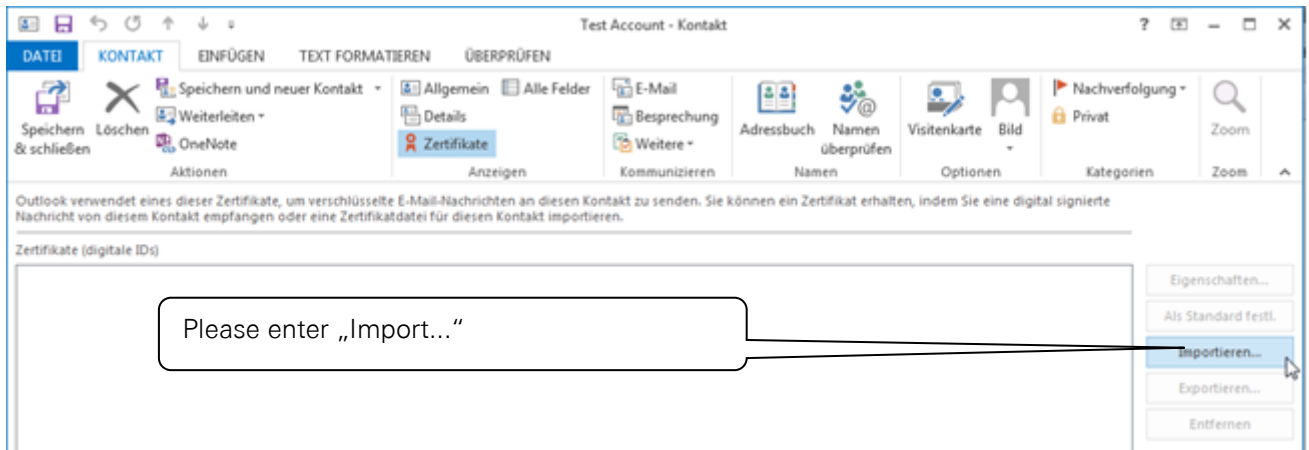


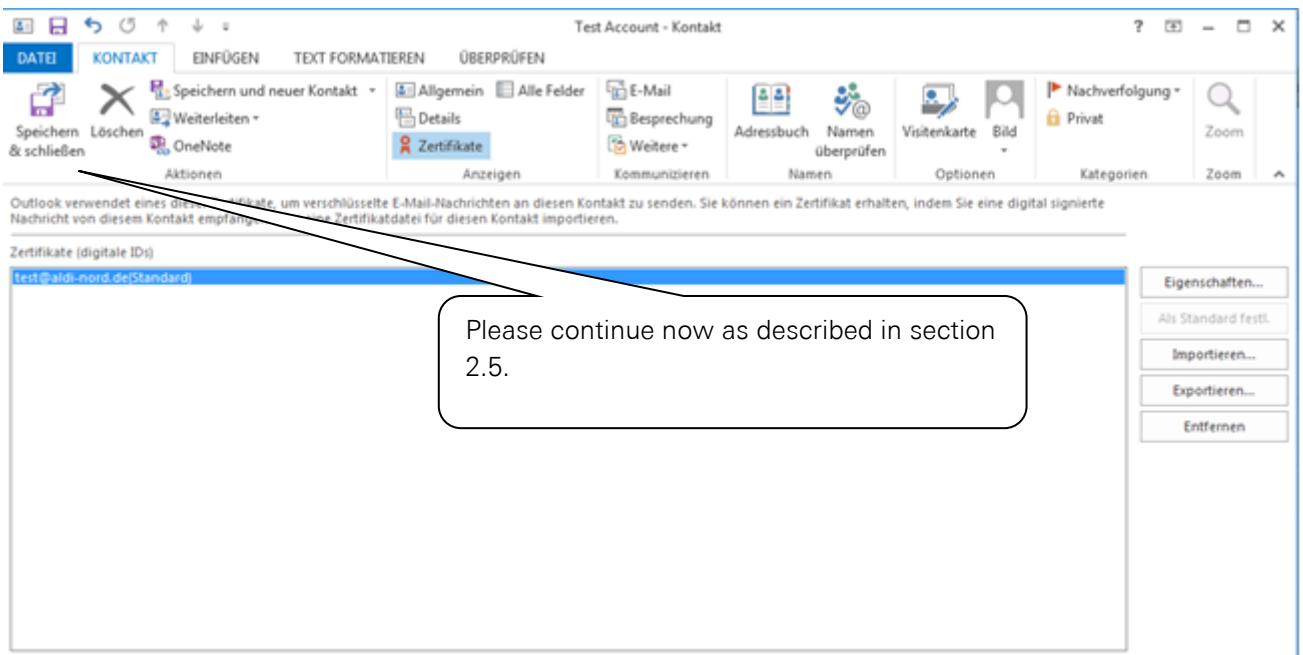
5.2. Matching a downloaded certificate to an Outlook contact

The following describes the way you set up encryption using the certificate you downloaded from “www.aldi-nord.de/certportal”. This step differs from the steps described in section 2.5 because here no signed email from an ALDI Nord employee is needed.

The following screenshots are in german language, please use the respective buttons and options as shown and explained in your client software.



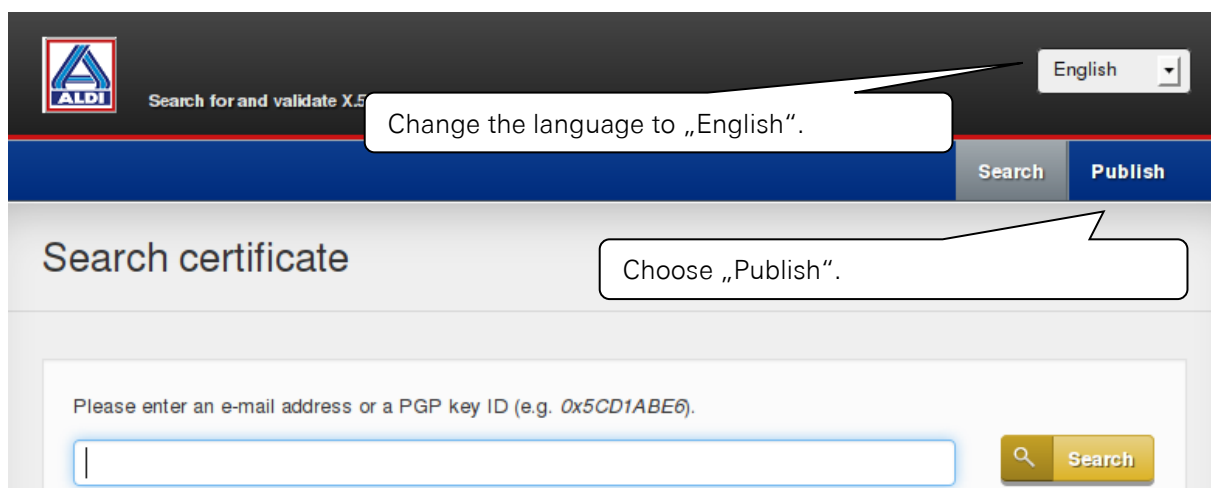




5.3. Uploading own certificates

If you already use certificates for encrypting via S/MIME, but these are not uploaded to the keyserver of the trust center, there is the possibility to upload them to the ALDI certportal.

Follow this link: www.aldi-nord.de/certportal





The screenshot shows the 'Publish' step of the ALDI secure email communication process. At the top, there is a search bar for X.509 certificates. Below it, a callout box contains the instruction: "Move to „user certificate“ and insert your informations. After that, please confirm with „transmit“." The main form has three tabs: "User certificate", "Domain certificate", and "CA certificate". The "User certificate" tab is active. Below the tabs, there is a note: "You can transmit either a X.509 user certificate or a public PGP user key. Before the certificate or key will be published, it has to be checked and approved." The form fields are: "Your name" (Test), "Organization" (Test Company), "Your e-mail address:" (test@test-company.com), "Phone number:" (0123-123-123-123), "Certificate File:" (No file chosen, with a "Browse..." button), and "Human verification:" (7r84d). A "Transmit" button is at the bottom left. A "Mandatory field" label is also present.

To finish this process, please contact your ALDI communication partner so that he can internally release your certificate for use.