

Content

1.	Introduc	ction	2
2.	Request	ting 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	
	2.3.	Installing a certificate	12
	2.4.	Setting up the certificate in Outlook	
	2.5.	Encryption with Outlook	21
3.	Exportir	ng and importing certificates	23
	3.1	Exporting a certificate	23
	3.2	Importing a certificate	
4.	Installin	g the ALDI Nord root certificate	
5.	Alternat	ive procedures for receiving and providing certificates	
	5.1.	Downloading a certificate of a communication partner	
	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. <u>Requesting and setting up a certificate</u>

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"





D https://www.swissign.com/checkout/onepage/	D + @ SwittSign AG [CH] C > Checked - SwitSign ×
swiss> sign image	About SwissSign Support Media DE EN Search Q 😨 Q 🕎 🕯
Checkout Checkout Method	Please register yourself to proceed the checkout.
Register to create an account Register and save time! Register with us for future convenience: • Fast and easy check out • Easy access to your order history and the	Please log in below: Email address
Register	Password ☑ Remember me Forgot your password? Login SUSSetD Om LOG-IN
[https://www.swisssign.com/persistent/indee/saveMethod/]	e to newsletter e-mail address Submit

	About SwissSign Support Media DE EN SSL certificates Personal certificate
Checkout	
Billing information	
Salutation	○ Mr. ○ Mrs./Ms.
First name	
Last name	
Company	
Email address	
Address	
Zip/postal code	
City	
Country	

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:

Encrypted email communication









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

2.2.1. Obtaining license information

Please open the following Webpage https://www.swisssign.com/en/customer/account/login/

	About SvissSign	Support Media DE	EN Search	J €.8 ₽
SIGUIDENTITY	SSL certificates	Personal certificates	Signing Managed PKI	Partners Solutions
Login or create an acco	unt	After pu	rchasing vour	
Registered customers		certifica	te, please log ir	n
If you have an account with us, please log in.		ywith you	ur previously	button below.
		created	user account.	
Email address				EID
Password				
Remember n	ie .			
Login				

	About SvrissSign Su	pport Media DE EN	Search		Q	원·년
SIGUIDENTITY	SSL certificates	Personal certificates	Signing	Managed PKI	Partners	Solutions
My account				<mark>Q,</mark>	<mark>≫'</mark> Ը'	⊕ ⊒`
Please Choose "M ^v you get information licenses like e.g. yo	y licenses". There n regarding your our license code.		do so, sele	ct one of the link	s below in or	der to view
		sselD Log	i n ccount to a	SuisseID certificat	te.	
Edit / Change password		suisselD 🖝 LOO	-IN Inform	nation about Suis	selD	
SwissSign newsletter						
You are currently not subscribed to	any newsletter.					



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 <u>http://swisssign.net</u>.

Home Support Certificat SWISS> SUSS Account > Logon > Create	te authority Shop Revoke certificate Help Search / Manage Certificates Public search > Columns Account logon () An account is optional and is unrelated to the shop at swisssign.com New users
Certificate login → Logon	 Proceed without account (for quick single certificate request Create account (for managing several certificates) Proce Proce without account". If you want to manage several certificates, you can create an account.
Home Support C SWISS SIGN Certificates	Certificate authority Shop Revoke certificate Help Search / Manage Certificates Public search > Columns Public search Click "New" at "Certificates"
New S&)ch / Manage Account > Logon > Create Certificate login > Logon	Exact search: "/O=SwissSign AG" Wildcard search: Swiss* License : Page size : 10 Search



Encrypted email communication



Home Support Certific:	rate authority Shon Devike certificate Heln	
swiss> sign	Personal Silver Certificate License > Validity EUA > CSR > Submission EUA	
 New Search / Manage 	End User Agreement (EUA) for SwissSign Certificates	
Account	As of February, 16th 2016 Want to proceed.	
 Logon Create 	1. General	
Certificate login	SwissSign AG (hereinafter: SwissSign) operates Certific	J
	Back I decline I accept the above conditions	
Home Support C SWISS SIGN	Certificate authority Shop Revoke certificate Help Personal Silver Certificate License > Validity > EUA CSR > Submission CSR	
New	Paste your pkcs#10 Certificate Signing Request (CSR) if you have generated one. Else proceed leaving the field below empty.	
> Search / Manage	DKCS#40 ·	
Account		
 Logon Create 		
Certificate login		
> Logon	Please click "Proceed". If you just war generate an e-mail certificate, you dor have to fillout the text box named "PKCS#10".	וt to ו't

Home Support Certificate	authority Shop Revoke certificate Help
cwie c	Personal Silver Certificate
Sian	> License > Validity > EUA > CSR Email > Contact > Submission
	Email
Certificates	
> New	
Search / Manage	Must be operational
Account	Back Proceed
Logon	
> Create	Please enter the e-mail address you
Certificate login	want to certify.
> Logon	Afterwards click on "Proceed"

ALDI Einkauf GmbH & Co. oHG – Essen Secure email communication



Home Support Certificate Swiss Support Certificates New	authority Shop Revoke co Personal Silver Certif > License > Validity = Contact Address used for the not	rtificate Help cate EUA > CSR > Email Conta fications related to this request.	Here you can check and alter your contact information.
 Search / Manage Account Logon 	* Email address : [c	verrides the predefined email address abo	Click "Proceed" to continue.
 Create Certificate login Logon 	Preferred language : (Notice : Back Proceed	ee text	
Check your i regarding yo Additionally password to certificate ag unauthorized (recommend Certificate" to will receive a address you before.	nformation ur certificate. choose a secure your jainst l access ed). quest o proceed. You in e-mail to the submitted	Email > Contact Submission Certificate data Subject DN Subject Alternativ (1) A proof of poss Key generation The generated key A For security rea Their secure st *Passwor reat passwor Back Request cert	CN emailAddress OU Email Validated Only re Name email ession mail will be sent to will be encrypted with the following password. usons, SwissSign is unable to recover lost key passwords. rarge is in the sole responsibility of the user. d: ificate



Encrypted email communication

page 10 of 43



Home Support Certifie	cate authority Shop Revoke certificate Help Search / Manage Certificates > Public search > Columns	You are linked to "SwissSign.net". Click on
Certificates	Confirm approve	"Confirm approve" to finish the approval.
 New Search / Manage 	Request to be approved Status Expires Subject pending - -	Now your e-mail address is authenticated
> Logout		
> Switch	Confirm approve	and you will receive an e-mail containing a
Certificate login	* Request identifier : 2997A328A6EF	link to your certificate
> Logon	Cancel Confirm approve	
■ 日 ち び ↑ ·	↓	has been approved - Nachricht (HTML) ? 🖂 — 🕫 🗙
DATEI NACHRICHT		
r Ignorieren X Sunk-E-Mail ≠ Löschen	Antworten Allen Weiterer Weiterer Neuerschlung Verschlieben im?	Communication Commun
Loschen	Antworten Quicksteps	
ca@sv	visssign.net	I his e-mail contains a link where you can
An	n - Your Certificate Request 2997A328A6EF. h	download your certificate.
Cc registration@si	wisssign.com	
Signiert von ca@swisssign.r	net	
D i		
Dear customer,		
Your SwissSign Certif	ficate Request 2997A328A6EF with the foll	owing sub-
To download and inst	all the new SwissSign Certificate, please use the following	
Download certificate:	https://swisssign.net:443/cgi-bin/id/download?auth=76F164F	
You should download Personal ID certificate	d all SSL certificates as soon as possible since they will be deleted after a short time. e again at a later time. Therefore we recommend that you keep a copy of this message	Personal ID certificates will remain on the system and the link allows you to download your SwissSign e.
In case you want to w <u>Withdraw certificate r</u> When you download t	ithdraw your certificate request please open the following link in your browser: request the certificate it will be automatically issued. After issuance you cannot longer withd	iraw the request.
If you opened an acco	ount on www.swisssign.net, you are always able to revoke your issued certificate via	this account. In any case feel free to contact our support via our webshop www.swisssign.com.
This is an automaticall customer please contac	ly generated email. Please do not reply to this email. If you have any questions as dir ct directly the helpdesk of your organization.	rect customer of our SwissSign web shop please feel free to use our <u>contact form</u> . If you are a Managed PKI
Best regards, Your SwissSign Team	1	
🚾 ca@swisssign.net SwissSig	gn - Your certificate request 2997A328A6EF	
Home Support Certi	nicate authority Shop Revoke certificate Help Search / Manage Certificates	
swiss> sign	> Public search > Columns Download / Attributes	
Certificates	Certificate	
>New >Search / Manage	Expires Subject	Alternative name
Account		
> Logout	Download certificate and private key (.p12, PKCS#12)	
> Switch > Create	* Display name :	
Certificate login	* Key password :	
> Logon	* Download code :	
	Download	
	Details	
	Version v3	
	Serial number 29:97:a3:28:	
	Signature algo RSA-SHA256 #	
	Validity You get some m	nore details about your

 Serial number
 29:97:83:28:

 Signature algo
 SSA:92:56:00

 Issuer DN
 cn=Ssd:SS

 Validity
 You get some more details about your certificate.

 U.C.SEQUE
 U.C.SEQUE

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

 KU
 estiProt

 KU
 estiProt

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: <u>https://swissSign.net/cgi-bin/home</u>

Home Support Trust swiss	ign.com	DE
swiss> sign		S.E.CHF
Certificates Weld New certificate Swis My certificates Chor	ame Sign provides leading edge security technology for individuals, companies and organizations. se SwissSign as your partner for security solutions.	
My requests My online keys Revocation Swiss Sinn CA		
Search for IDs	Choose "Trust"	
Home Support Trust s	visssign.com	
swiss> sign	Cho	ose "CA certificates"
Trust Import root certificate	rust Swiss Sign rust is a basi The control of the security models including Public Key Infrastructure (PI The control certificate, The SwissSign root certificates are trusted, among c	(I). All PKIs are hierarchically organized. The top of the hierarchy (root) must be implicitly trusted in the thers by Microsoft, Mozilia, and Apple which allows the end-users of their applications to validate Swit
CA certificates Revocation lists	In root central cale of a Prix is fusible, any sub centricate of this interfactional the can be se additionally trusting a certificate autohythy (CA) means that you trust the different process the Certificate Policy and Certification Practice Statements (CPICPS) provide transparer foreover, SwissSign is a qualified Certification Service Provider in Switzerland, fulfilling houst and use a SwissSign CA burn unsite trand and accent the corresponding. Ford Larse	curely vemieo. is involved in a PKI such as the client registration or certificale validation (CRL, OCSP). (y to the overall processes and thus helps to improve trust. Thus, you can assess your trust in a Swiss the requirements of the swiss electronic signature law (ZerES) based on the strongest international s Arcarament flux work to how more about the certificate morces listed thas a look at the CPLPRS Ei
	wissSign root certificate into your applications and setup the trust relationship.	
Home Support	Trust swisssign.com	Here you will find the actual root- certificates. You can download all
swiss		root-certificates. In the following it
sign		how to download the Personal
Trust	CA certificates	Silver G22.
Import root certificate	On this page you can find the current CA certificate	s.
Legal documents	To download CA certificates that have been supers	Please click on "Download".
CA certificates Revocation lists	Method:	
	Download	

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:

Encrypted email communication



File Download - Security Warning
Do you want to open or save this file?
Name: class_2_ii.cer Type: Security Certificate, 1.66KB From: www.trustcenter.de Open Save Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?
A website wants to open web content using this program on your computer
This program will open outside of Protected mode. Internet Explorer's <u>Protected mode</u> helps protect your computer. If you do not trust this website. do not open this roorgam.
Name: Crypto Shell Extensions Publisher: Microsoft Windows
Do not show me the warning for this program again
Details Allow Don't allow



After that you have to install the certificate:



Version 1.9





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



Encrypted email communication



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

Certificate Import Wizard		
	Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area when certificates are kept.	, is re
	To contributy disk nexts	Click "Next >"
		7/
	< Back Next > Car	ncel
Certificate Import Wizard	THE R. LEWIS CO., NAMES IN CO., NAMES INC., NAMES IN CO., NAMES INTERNA IN CO., NAMES INTERNA IN	
File to Import Specify the file you want	to import.	
File name: C:\Users\Tester\ Note: More than o Personal Inform Cryptographic M Microsoft Serial	Check the path to your certificate. Click "Next >" to proceed.	:
Learn more about <u>certificate f</u>	ile formats < Back Next > Car	ncel



Password To maintain security, the private key was protected with a password.	Please enter your key password in here
Type the password for the private key. Password: Enable strong private key protection. You will be prompted every time private key is used by an application if you enable this option. Mark this key as exportable. This will allow you to back up or transport keys at attactive time	the tyour
☑ Include all extended properties.	Mark this option to enable the
Learn more about <u>protecting private keys</u>	export (explained in section 3.1) of your private key afterwards.



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.

\bigcirc	Posteingang Outlook	? – 🗆 X
Control of the second s	Poteingang- -Outlook Contoinformationen Image:	? – 🗆 X
ų		
Dutlook-Optionen	the statement of the st	? ×
Allgemein		
E-Mail	Allgemeine Optionen für das Arbeiten mit Outlook	
Kalender	Benutzeroberflächenoptionen	
Personen	Minisymbolleiste für die Auswahl anzeigen 🛈	
Aufgaben	Livevorschau aktivieren 🛈	
Suchen	Quickunfo-Format: Featurebeschreibungen in Quickunfos anzeigen 💌	
Sprache	Microsoft Office.Konie nersonalisieren	
Erweitert	Bend Open "Trust Center"	





Outlook-Optionen	
Allgemein	Sorgen Sie für die Sicherheit Ihrer Dokumente und des Computers.
E-Mail	
Kalender	Datenschutz
Personen	Microsoft nimmt den Datenschutz ernst. Weitere Informationen, wie Microsoft Outlook für den Datenschutz sorgt, finden Sie in den Datenschutzbestimmungen.
Suchen	Datenschutzbestimmungen für Microsoft Outlook anzeigen
Sprache	Sicherheit & mehr
Erweitert	Besuchen Sie Office.com, um weitere Informationen zum Datenschutz und zur Sicherheit zu erhalten.
Menüband anpassen	Microsoft Trustworthy Computing
Symbolleiste für den Schnellzugriff	Microsoft Outlook-Trust Center
Add-Ins Trust Center	Das Trust Center enthält Einstellungen für Sicherheit und Datenschutz, um für die Sicherheit des Computers zu sorgen. Es wird davon abgeraten, diese Einstellungen zu ändern.
	Click on the "Trust Center Settings" button
	OK Abbrechen
	Click on the E-mail Security
Trust Center	option on the left hand panel
Vertrauenswürdige Herausgeber	
Datenschutzoptionen	Verschlüsselte E-Main
E-Mail-Sicherheit	Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln Q Ausgehenden Nachrichten digitale Signatur hinzufügen
Anlagenbehandlung	vierte Nachrichten als <u>K</u> lartext senden
Automatischer Download	VIME-Bestätigung anfordern, wenn mit S/MIME signiert
Makroeinstellungen	einstending. Meine Symme - Einstendingen (Kommunikationgenur-essen de)
riogrammigestederter zügnin	Digitale
	Zertifikate sind Dokumente, mit denen die Identität in elektronischen Tran
A digital signature i	n your message
allows you to sign y	our message.
The digital signature	e includes your
certificate.	Match the settings
	ulassen under "Encrypted
	Skript in Offentlichen Ordnern zulassen email"
	Then click "Settings"
	OK Abbrechen



Security Setting Preferences	For encrypted communication, click
Cryptography Format: S/MIME	"Choose" at "Encryption Certificate"
Certificates and Algorithms Signing Certificate: Hash Algorithm:	Depending on the options previously selected, you may also have to select and store a signature certificate.
Encryption Algorithm:	
Send these certificates with signed messages OK Cancel	

Now select the requested certificate.



You can choose the Security Settings Name yourself.

ecurity Setting Preferences Security Settings Name:		
Supplier Certificate		-
Cryptography Format:	S/MIME	▼
☑ Default Security Set ☑ Default Security	ing for this cryptographic message Setting for all cryptographic messa	e format ages
Security Labels	New Delete	
ertificates and Algorithms		Match the settings and then click "OK"
Signing Certificate:	Rudi Tester	
Hash Algorithm:	SHA1 🔻	The default settings are now saved. On the next
Encryption Certificate:	Rudi Tester	window click "OK" again.
Encryption Algorithm:	AES (256-bit) -	
Cand these cartificat	es with signed messages	

Outlook 2013 is now set up to use your certificate.

Encrypted email communication



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.

	0 /			
🔮 🗟 🐬 ÷		Kontakte (Nur dieser Computer) -	- Outlook	? E – 8 ×
DATEI START SENDEN/EM	PFANGEN ORDNER ANSICHT			
Neuer Neue Neue Kontakt Kontaktgruppe Elemente * Neu	Löschen Kommunizieren	Liste	Serien- OneNote E-Mails tionen Verleiter verle	n Nachverfolgung* Kategorien Suchen
	٢		Kontakte (Nur dieser Computer) durchsuche	n (Stra+F)
⊿ Meine Kontakte	Die NAME POSTION		LAND/REGION ARTELLING TELECON GESCH	EAV GESCHÄETI TELEFON (RRIVAT) MORTITELEFON E MU
Kontakte (Nur dieser Computer)	Hier klicken, um Kontakt	FIRMA SPECIFICATION CONTER	Analite on observe	
Verbindung mit einem sozialen Netzw	Firma: (Keine Angabe): 1 Element(e)			
reconcioning internet in solution recent	ALDI Kommunikationspar	Communiting tionspartner, ALDI		kom
		Schnellauck Schnellauck Kontak wejereiten → Egstelen → Zur Nachverfolgung → Wersphelen Control Control Lascher	Right-click on the e select "Delete" from	mail contact and then the context menu.
E Mail Kalandar	Dereenen Aufgeben un			
E-IVIAII Kalender	Personen Aufgaben …			

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.

ALDI Einkauf GmbH & Co. oHG – Essen Secure email communication



Unbenant - Nachnicht (HIML)	f 🖽 — 🗗 X
NACHBOCH DNUCKS CPTORES Vereklassen Desmittingibestit androden Sector Escherer Escherer Vereklassen betweitingibestit androden Varie Escherer Vereklassen betweitingibestit androden Vereklassen Varie Escherer Vereklassen betweitingibestit androden Vereklassen Varie Escherer Vereklassen betweitingibestit androden Vereklassen Senter Macheber Escherer Vereklassen betweitingibestit androden Varie Macheber Escherer Vereklassen betweitingibestit androden Betweit Varie Escherer Descherer Vereklassen and/or Betweit Immunikationsaatoe: Immunikationsaatoe: Immunikationsaatoe: and/or encrypted. Immunikationsaatoe: Immunikationsaatoe: Immunikationsaatoe: Immunikationsaatoe: Immunikationsaatoe: Immunikationsaatoe: Immunikationsaatoe: Immunikationsaatoe: Immunikationsaatoe: Immunikationsaatoe: Immunikationsaatoe: Immunikationsaatoe: </td <td></td>	
Kommunikationspartner Keine Elemente	

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:

S (0 ↑ ↓ ÷	Test - Nachricht (HTML)	? 🗈 – 🗗 🗙
DATEI NACHRICHT		
Ignorieren Image: Signorieren Image: Signori	chung Verschieben in: ? G An Vorgesetzte(n) Team-E-Mail Q-Antworten und Werschieben Machweiten mathematicen mathema	
Löschen Antworten	QuickSteps 🕫 Verschieben Kategorien 🕫 Bearbeiten Zoom	^
An Signiert von	This symbol shows that the email is encrypted.	<u> </u>
Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, k	icken Sie hier, um sie im Webbrowser anzuzeigen.	
Test	This symbol shows that the email is digitally signed.	\leq



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).

🥖 TC TrustCenter - Root Certificates - Windows Intern	et Explorer					_ 0 <u>_ ×</u>
📀 🕞 👻 http://www.trustcenter.de/en/infoc	enter/root_certificates.htm#	1429		✓ 47 ×	🚼 Google	۶ -
File Edit View Favorites Tools Help						
🚖 Favorites 🛛 🚔						
TC TrustCenter - Root Certificates				🖄 - 🔊	🔻 🖃 🖶 🔻 Page 🕶 Safety 🕶	Tools 🔻 🔞 🕶 🧼
C InstCenter - Root Certificates	At "Tools",	A standardserbergere 2019 Cellick on "In Encir Numer Vision / Period exertinate Propersion (DOB centrate Pr	Image: Second		Diagnose Connection Problems Reopen Last Browsing Session Pop-up Blocker Manage Add-ons Work Offline Compatibility View Compatibility View Settings Full Screen Toolbars Explorer Bars Developer Tools Suggested Sites Skype add-on for Internet Explorer Send to OneNote Blog This in Windows Live Writer Internet Options	F11 E
		L				
		TC TrustCenter Class 4 CA II				*
Done				Internet Protect	ed Mode: On 🛛 🖓 🔻	🔍 70% 🔻

ALDI Einkauf GmbH & Co. oHG – Essen Secure email communication



Internet Options General Security Privacy Content Connections Programs Advanced Parental Controls	
Control the Internet content that can Parental Controls be viewed. Content Advisor Ratings help you control the Internet content that can be viewed on this computer.	At the tab "Content", click on "Certificates"
Certificates Use certificates for encrypted connections and identification Clear SSL state Certificates Publishers AutoComplete AutoComplete stores previous entries on webpages and suggests matches for you. Feeds and Web Slices Feeds and Web Slices provide updated Content from websites that can be read in Internet Explorer and other programs.	
OK Cancel Apply	X
Intended purpose: <al> Personal Other People Intern Issued To Rudi Tester TC Rudi Tester TC <p< th=""><th>be exported adi Tester) tab ght the kported and button</th></p<></al>	be exported adi Tester) tab ght the kported and button
Import Export Remove	Advanced
Learn more about <u>certificates</u>	Close



Certificate Export Wizard	×
	Welcome to the Certificate Export Wizard
	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
~	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kent
	To continue, dick Next.
Click "Next -	
Click Next >	\sim
Certificate Export Wizard	
Export Private Key You can choose to expor	t the private key with the certificate.
Private keys are passwo certificate, you must typ	rd protected. If you want to export the private key with the e a password on a later page.
Do you want to export th	he private key with the certificate?
Do you want to export the provide the provided to the provided	he private key with the certificate? private key t the private key
Do you want to export the p	he private key with the certificate? private key rt the private key
Do you want to export the goar of the the goar of the goar of the	he private key with the certificate? private key rt the private key
Do you want to export the p Yes, export the p No, do not export Select "Y	he private key with the certificate? private key "t the private key es, export the private key" and
Do you want to export the Yes, export the p No, do not export Select "Y click "Ne:	he private key with the certificate? private key "t the private key es, export the private key" and xt >"
Do you want to export th Yes, export the p No, do not export Select "Ye Click "Ne: Learn more about exporting p	he private key with the certificate? private key rt the private key es, export the private key" and xt >" private keys

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.



Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
💿 Cryptographic Message Syntax Standard - PKCS	#7 Certificates (.P7B)
Include all certificates in the certification path	n if possible
Personal Information Exchange - PKCS #12 (.PF)	X)
📝 Include all certificates in the certification path	n if possible
Delete the private key if the export is succes	Select "Include all certificates in the
Export all extended properties	cortification path if possible" and "Export all
Microsoft Serialized Certificate Store (.SST)	extended properties" and click "Next > "
	extended properties and click Next >
earn more about certificate file formats	
< Back	Next > Cancel
tificate Export Wizard	
ificate Export Wizard Password	
ificate Export Wizard Password To maintain security, you must protect the private key b	by using a password.
ificate Export Wizard Password To maintain security, you must protect the private key t	by using a password.
ificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password.	by using a password.
ificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password:	by using a password.
tificate Export Wizard Password To maintain security, you must protect the private key to Type and confirm a password. Password:	by using a password.
tificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password: Type and confirm account (mandatory);	by using a password.
ificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password: Type and confirm password (mandatory):	by using a password.
ificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password: Type and confirm password (mandatory):	by using a password.
ificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password: •••••••••••• Type and confirm password (mandatory): ••••••••	by using a password.
tificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password: Type and confirm password (mandatory):	by using a password.
tificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password: Type and confirm password (mandatory): Type and confirm password (mandatory):	by using a password.
tificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password: Type and confirm password (mandatory): Type and confirm password (mandatory):	by using a password. Choose a password, confirm it, and click "Next >"
tificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password: Type and confirm password (mandatory): Type and confirm password (mandatory):	by using a password. Choose a password, confirm it, and click "Next >"
tificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password: •••••••• Type and confirm password (mandatory): ••••••••	by using a password. Choose a password, confirm it, and click "Next >"
tificate Export Wizard Password To maintain security, you must protect the private key t Type and confirm a password. Password: •••••••• Type and confirm password (mandatory): ••••••••	by using a password. Choose a password, confirm it, and click "Next >"
tificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password: Type and confirm password (mandatory): ••••••••	by using a password. Choose a password, confirm it, and click "Next >"
tificate Export Wizard Password To maintain security, you must protect the private key b Type and confirm a password. Password: Type and confirm password (mandatory): Type and confirm password (mandatory):	by using a password. Choose a password, confirm it, and click "Next >"



Certificate Export Wizard	
File to Export Specify the name of the f	ile you want to export
File name: privateandpublickey	Browse
	Choose a file name and store location the key will be exported to and click "Next >"
	< Back Next > Cancel
Certificate Export Wizard	×
	Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings:
	Export Keys Yes Include all certificates in the certification path Yes File Format Personi
	Check the selected settings and click "Finish"
	Check the selected settings and click "Finish"



Exporting your	private exchange key
	An application is requesting access to a Protected item.
	Password for: CryptoAPI Private Key Click "OK" OK Cancel Details
Certificate Exp	ort Wizard Click "OK" vas successful.
	ОК



3.2 Importing a certificate

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





File to Import Specify the file you want to import.	
File name:	
C:\Users\Tester\Desktop\privateandpublickey.pfx Browse	
Note: More than one certificate can be stored in a single file in the following formats:	
Personal Information Exchange- PKCS #12 (.PFX,.P12)	
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)	
Microsoft Serialized Certificate Store (.SST) At "File name", y have to make an Click "Next >"	you usually do not ny changes.
Learn more about certificate file formats	
< Back Next > Cancel	
tificate Import Wizard	×
rtificate Import Wizard Password To maintain security, the private key was protected with a password.	
rtificate Import Wizard Password To maintain security, the private key was protected with a password. Type the password for the private key.	
rtificate Import Wizard Password To maintain security, the private key was protected with a password. Type the password for the private key. Password:	
rtificate Import Wizard Password To maintain security, the private key was protected with a password. Type the password for the private key. Password:	
rtificate Import Wizard Password To maintain security, the private key was protected with a password. Type the password for the private key. Password: Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.	
tificate Import Wizard Password To maintain security, the private key was protected with a password. Type the password for the private key. Password: Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option. Mark this key as exportable. This will allow you to back up or transport your keys at a later time.	
rtificate Import Wizard Password To maintain security, the private key was protected with a password. Type the password for the private key. Password: Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option. Mark this key as exportable. This will allow you to back up or transport your keys at a later time. I Include all extended properties.	Type in the password previous
rtificate Import Wizard Password To maintain security, the private key was protected with a password. Type the password for the private key. Password: Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option. Mark this key as exportable. This will allow you to back up or transport your keys at a later time. Mark the all extended properties. Learn more about protecting private keys	Type in the password previousl chosen for the private key and then click "Next >"
rtificate Import Wizard Password To maintain security, the private key was protected with a password. Type the password for the private key. Password: Image: Comparison of the private key protection. You will be prompted every time the private key is used by an application if you enable this option. Image: Mark this key as exportable. This will allow you to back up or transport your keys at a later time. Image: Include all extended properties. Learn more about protecting private keys	Type in the password previousl chosen for the private key and then click "Next >"



Certificate Import Wizard		x	
Certificate Store Certificate stores are system areas	where certificates are kept.		
Windows can automatically select a the certificate.	certificate store, or you can specify a	location for	
Automatically select the certi Olage all applications in the following the fo	ificate store based on the type of certi	ficate	
Certificate store:	liowing store		
		Browse	
	(The certif	icate store can be
Learn more about <u>certificate stores</u>		selected a Click "Ne	automatically. xt >"
	< Back Next >	Cancel	
Certificate Import Wizard			
Con Wiz	npleting the Certificate I zard ertificate will be imported after you clic	mport k Finish.	
You h	ave specified the following settings:		
Cert	tificate Store Selected Automatically d	etermined by t	
Fie	Name C:\Users\Testa	er \Desktop \priv	
•			
	Check you click "Finis	r settings a h"	nd then
	< Back Finish	Cancel	

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

Certificate Import Wizard	
The import was successful.	Finally, click "OK"
ОК	



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

Information Root certificate Revocation list Image: Contract of the second	Welcome to ALDI			
<section-header> 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. Nease cick on the Adobe icon to start the download. Image: Secure e-mail communication with the ALDI Nord group. We have outlined all of the information required for secure e-mail communication. Image: Secure e-mail communication with the ALDI Nord group. We have outlined all of the information required for secure e-mail communication. Image: Secure e-mail communication with the documents General Information and Instructions. Image: Secure e-mail communication with the ALDI Nord group. We have outlined all of the information required for secure e-mail communication with the ALDI Nord group. We have outlined all of the information required for secure e-mail communication with the ALDI Nord group. We have outlined all of the information required for secure e-mail communication with the ALDI Nord group. Image: Secure e-mail communication with the ALDI Nord group rest certificates with the following thumbprints. Image: Secure e-mail communication with the following thumbprints. Image: Secure e-mail communication with the following thumbprints. Image: Secure e-mail communication with the following thumbprints. Image: Secure e-mail communicate e-mail communication with the following t</section-header>	ALDI Information	Root certificate	Revocation list	English 🔻
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. ALD Nord Root CA (from 04.12.2015) » SHA :: 206a C71d 1800 e809 56c3 c3e5 9e40 bc370 e0 b6d3 Lib: bid1 1224 f721 197c 0860 38fc eef2 0752 ALD Nord Root CA OLD (til 06.01.2016) » SHA1:: e072 577b 2bd8 f68a ee6b eba2 17ca e9b6 b7a6 ba43 MDS: 542b b140 189c 0400 ad 146 00007 e677 a6ed	Secure e-mail con	nmunication v	vith ALDI Nord	
To read the documents you will require Adobe Readel [®] . You can download Adobe Readel [®] 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: :06a c71d L800 e8d9 56c3 c3e5 9ed0 bc310 e0 b6d3 MD5: isbd1 22t4 f721 197c 0860 38fc eef2 0752 ALDI Nord Root CA OLD (till 06.01.2016) » SHA1: :072 577b 2bd8 f68a ee6b eba2 17ca e9b6 b7a6 ba43 MD5: 542b b140 189c 040a d146 0007 e677 a6ed	We are very pleased that you would like secure e-mail communication in the docu	o use secure e-mail communi Iments General Information an	cation with the ALDI Nord group. We have d Instructions.	outlined all of the information required for
State: 2020 FREADER 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: 2054 of 71d 1800 e8d9 56c3 c3e5 9ed0 bc310 e0 b6d3 MDS: 5452 total 752 toda f68a ee6b eba2 17ca e9b6 b7a6 ba43 MDS: 5452 total 1854 c00a d146 00007 e677 a6ed	To read the documents you will require A Please click on the Adobe icon to start tl	dobe Reader [®] . You can downlo ne download.	oad Adobe Reader [®] for free from the websit	te www.adobe.co.uk.
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 bc370 e0 b6d3 MD5: std1 22t4 (f721 197c 0860 38fc eef2 0752 ALDI Nord Root CA OLD (till 06.01.2016) » SHA1: e072 577b 2bd8 f88a ee6b eba2 17ca e9b6 b7a6 ba43 MD5: std2 b140 189c 0d0a d146 00007 e677 a6ed				
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 bc31 0 e0 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 040a d146 00007 e677 a6ed	The ALDI Nord group 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 0 e0 b6d3 MD5: btd1 22t4 f721 197c 0860 38fc eef2 0752 ALDI Nord Root CA OLD (till 06.01.2016) » SHA1: e072 577b 2bd8 f58a ee6b eba2 17ca e9b6 b7a6 ba43 MD5: 542b b140 189c 040a d146 00007 e677 a6ed	To check the trust status of the ALDI No	rd group user certificate you wi	ill require our 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 0 MD5: bfd1 22t4 f721 197c 0860 38fc eet2 0752 ALDI Nord Root CA OLD (till 06.01.2016) » SHA1: e072 577b 2bd8 f58a ee6b eba2 17ca e9b6 b7a6 ba43 MD5: 542b bt40 189c 0d0a dt46 0007 e677 a6ed	Thumbprint S/MIME root co	ertificate		
ALDI Nord Root CA (from 04.12.2015) » SHA1: a06a c71d b800 e8d9 56c3 c3e5 9ed0 bc310 e0 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 040a d146 0007 e677 a6ed	You can check the validity of the ALDI N	ord group root certificates with	the following thumbprints.	
SHA1: a06a c71d b800 e8d9 56c3 c3e5 9ead bc310 e0 b6d3 MD5: bfd1 22f4 f721 197c 0860 38fc eef2 0752 ALDI Nord Root CA OLD (till 06.01.2016) » SHA1: e072 577b 2bd8 f58a ee6b eba2 17ca e9b6 b7a6 ba43 MD5: 542b b140 189c 040a d146 00007 e677 a6ed	ALDI Nord Root CA (from 04.12.2	015) »		
ALDI Nord Root CA OLD (till 06.01.2016) » SHA1: e072 577b 2bd8 f68a ee6b eba2 17ca e9b6 b7a6 ba43 MD5: 542b b140 189c 040a d146 0007 e677 a6ed	SHA1: a06a c71d b800 e8d9 56c3 c3e5 MD5: bfd1 22f4 f721 197c 0860 38fc eef2	9ed0 bc3f0;e0 b6d3 0752		
SHA1: e072 577b 2bd8 f68a ee6b eba2 17ca e9b6 b7a6 ba43 MD5: 542b b140 189c 0d0a d146 0007 e677 a6ed	ALDI Nord Root CA OLD (till 06.0	1.2016) »		
	SHA1: e072 577b 2bd8 f68a ee6b eba2 1 MD5: 542b b140 189c 0d0a d146 0007 el	7ca e9b6 b7a6 ba43 677 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.

Internet Exp	plorer Security
	A website wants to open web content using this program on your computer
	This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program. Name: Crypto Shell Extensions Name: Name: Name: Crypto Shell Extensions
	Do not show me the warning for this program again
💽 De	etails Allow Don't allow

Then, the following messages will appear:

0	Certificate	×	
	General Details Certification Path		
	Certificate Information		
	This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.		
	Issued to: ALDI NORD CA		
	Issued by: ALDI NORD CA Click "Install Ce	ertif	icate"
	Valid from 07/01/2011 to 06/0		
	Install Certificate Issuer Statement		
	OK		



Certificate Import Wizard		
	Welcome to the Certificate Import Wizard	
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Next.	
	Click "Next >"	
	< Back Next > Cancel	

Certificate Import Wizard
Certificate Store Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Place all certificates in the following store
Certificate store: Browse
Learn more about certific Click "Next >"
< Back Next > Cancel



Certificate Import Wizard	
	Completing the Certificate Import Wizard
	The certificate will be imported after you click Finish.
	Certificate Store Selected Automatically determined by t
	Content Certificate
	· · · · · · · · · · · · · · · · · · ·
Click	"Finish"
	< Back Finish Cancel
(L	

Finally, the following message appears:

Certificate Import Wizard
The import was successful.
ОК

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.



👧 🚽 9 5 * * 🔹	Wtrlt: AW: Bearbeitung der Datei "Versch	lüsselte Kommunikation" - Message (HTML)	
Message Add-Ins			0
Reply Forward to Reply Forward Respond Respond	Block Not Junk Sender Junk E-mail G Options G	A Find → Related - ↓ Select - Find Subjects Crotal Manager Denvice	
From: Max Mustermann			Sent: Fri 14/10/2011 15:53
To: Cc:			
Subject: Bearbeitung Signed By:			
Sehr geehrter Herr			
wie soeben telefonisch besprochen,		Click on this symbol	
Mit freundlichen Grüßen Max Mustermann			
2 4			
4			
l			

Your message w	thority Information as digitally signed with a	certificate issued b	y a Cert <mark>ificat</mark> e
The signature is vet chosen to tru	invalid because you have	either distrusted	or not
Issued by:	ALDI NORD CA		
Valid From:	07/01/2011 to 06/01	/2016	
dic The certi check th "Trust" sig	ficate appears, e data and click	ou trust mail th	Details
Do you want to t	rust this Certin	ority?	
If you choose Tr dialog that follow	ust, you must also click is to add the certificate t	on the Root Cer o your system.	rtificate Store

You can also display the certificate.



This certificate is intend • Protects e-mail messa	ded for the following purpose(s): ages
Issued to: ALDI NO	DRD CA
Issued by: ALDI NO	DRD CA
Valid from 07/01/20	011 to 06/01/2016
	Issuer Statement

Before installation a security warning will appear.

Security Warning	
You are about to install a certificate from a certification authority (CA) claiming to represent:	
ALDI NORD CA	
Windows cannot validate that the certificate is actually from "ALDI NORD CA". You should confirm its origin by contacting "ALDI NORD CA". The following number will assist you in this process: Thumbprint (sha1): E072577B 2BD8F68A EE6BEBA2 17CAE9B6 B7A6BA43 Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk. Do you want to install this certificate?	The thumbprint of the ALDI Nord root certificate is shown here.
Yes No Fina	ally, click "Yes"
	J

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

Search for and validate X.509 certificates	English
Change the language to "English".	Search Publish
Search certifi Insert the e-mail address of the required contact person as well as the security code at the bottom. Please confirm with Please enter an e-mail address or a PGP key ID (e.g. 0x5CD1AP	
test@aldi-nord.de Human verification h8p8y Create new code	Q Search



Valid certif infor	v you can see all existing cer person. Click on the entry to rmation.	o get more		
✓	test@aldi-nord.de valid from 2013-12-05 until 2023-1	2-03		± ∎ 1
Owner	test@aldi-nord.de	Issued by	ALDI NORD CA ALDI NORD	
Signatur e Algorithm	SHA1WithRSAEncryption	By using this butt	on, you can download	the
Algorithm (Key Length)	RSA (2048 bits)	For encrypted cor	mmunication you need	the
Fingerprint (SHA1)	4C:31:6E:64:CE:4B:81:88:E9:7	certificate with th	e .cer file extension.	
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	
0	test@aldi-nord.de valid from 2014-12-14 until 2024-1	2-12		± =

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.





Encrypted email communication

ALDI Einkauf GmbH & Co. oHG – Essen Secure email communication



	↓ u EINFÜGEN TEXT FORMAT	Tes IEREN ÜBERPRÜFEN	t Account - Kontakt			? 🖭	- □	×
Speichern Löschen	Speichern und neuer Kontakt * Weiterleiten * OneNote	Allgemein Alle Felder Details Zertifikate	E-Mail	Adressbuch Namen überprüfen	Visitenkarte	Nachverfolgung * Privat	Q Zoom	
A	Aktionen	Anzeigen	Kommunizieren	Namen	Optionen	Kategorien	Zoom	^
Zertifikate (digitale IDs)	Please enter "Imp	ort"]		Eige Als S	nschaften tandard fest	 EL
				<u></u>		Eq	portieren	G
						E	ntfernen	



Version 1.9



🗉 🖯 5 (5 f 4 .	Tes	st Account - Kontakt			? 🗈	- 🗆 X
DATE KONTAKT EINFÜGEN TEXT FORMAT	TEREN ÜBERPRÜFEN					
Speichern Löschen & Weiterleiten *	Allgemein Alle Felder	E-Mail Besprechung	Adressbuch Namen überprüfen	Visitenkarte Bild	Nachwerfolgung * Privat	Zoom
Aktionen	Anzeigen	Kommunizieren	Namen	Optionen	Kategorien	Zoom 🔺
Outlook verwendet eines dietsen <u>Frakske</u> , um verschlüssett Nachricht von diesem Kontakt empfänge Zertrifika Zertrifikate (digitale IDs)	e E-Maili-Nachrichten an diesen Ko tdatei für diesen Kontakt importie	ntakt zu senden. Sie i ren.	cönnen ein Zertifikat erhalt	en, indem Sie eine digit	tal signierte	
test@aldi-nord.de(Standard)					Eige	inschaften
		tinuo now	as doscribod ir		Als S	tandard festi.
	2.5.	linue now		1 Section	Im	portieren
					Eq	portieren
)	6	intfernen

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: <u>www.aldi-nord.de/certportal</u>

Search for and validate X.5	Change the language to "English".	Eng	glish 🗾
		Search	Publish
Search certificate	Choose "Publish".		7
Please enter an e-mail address or a	a PGP key ID (e.g. <i>0x5CD1ABE6</i>).	<u>৭</u> s	learch



informa	o "user certificate" and i tions. After that, please	nsert your confirm wit
Publish "transm	nit".	
User certificate Domain	certificate CA certificate	
You can transmit either a X. Before the certificate or key	509 user certificate or a public PGP user k will be published, it has to be checked and	ey. approved.
Your name	Test	
Organization	Test Company	
Your e-mail address [*] :	test@test-company.com	
Your e-mail address : Phone number :	0123-123-123-123	
Your e-mail address': Phone number': Certificate File':	test@test-company.com 0123-123-123-123 No file chosen The supported formats are ASC. PEM. DER and	Browse

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