



Inhalt

1. Einleitung	2
2. Beantragung und Einrichtung eines Zertifikats	2
2.1 Beantragung eines Zertifikats	2
2.2. Erstellen eines Schlüsselpaares	7
2.2.1. Lizenzinformation abrufen	7
2.2.2. Erstellen eines Schlüsselpaares mit Lizenzcode	8
2.3. Installation eines Zertifikats	13
2.4. Einrichten des Zertifikats in Outlook	19
2.5. Verschlüsselung mit Outlook	22
3. Zertifikate ex- und importieren	24
3.1 Zertifikat exportieren	24
3.2 Zertifikat importieren	29
4. Installation des ALDI Nord Stammzertifikats	32
5. Alternatives Vorgehen zum Erhalt und zur Bereitstellung von Zertifikaten	36
5.1. Herunterladen des Zertifikats eines Kontaktpartners	37
5.2. Heruntergeladenes Zertifikat einem Outlook Kontakt hinzufügen	38
5.3. Bereitstellung von eigenen Zertifikaten	40

1. Einleitung

Dieses Dokument stellt eine Anleitung für die Einrichtung einer verschlüsselten Kommunikation mit ALDI Nord aus Sicht eines externen Kommunikationspartners dar. Bei Fragen oder Unklarheiten sprechen Sie bitte mit Ihrem IT-Administrator. Diese Anleitung wurde am 30.08.2016 überprüft. Etwaige Änderungen seitens der Hersteller können ein anderes Verhalten, als das hier beschriebene verursachen.

Auf folgendem System wurde die Anleitung erstellt:

- Windows 7
- Internet Explorer 11
- MS Outlook 2013

Bei abweichenden Systemen kann es unter Umständen zu anderen Ansichten kommen.

2. Beantragung und Einrichtung eines Zertifikats

Dieses Kapitel beschreibt die Beantragung und Einrichtung eines Zertifikats für die verschlüsselte

E-Mail-Kommunikation mit ALDI Nord. Derzeit wird der Zertifizierungsanbieter (Trustcenter) SwissSign von ALDI Nord empfohlen.

Hierdurch wird eine höchstmögliche Kompatibilität zu den von ALDI Nord verwendeten Verschlüsselungsmechanismen gewährleistet.

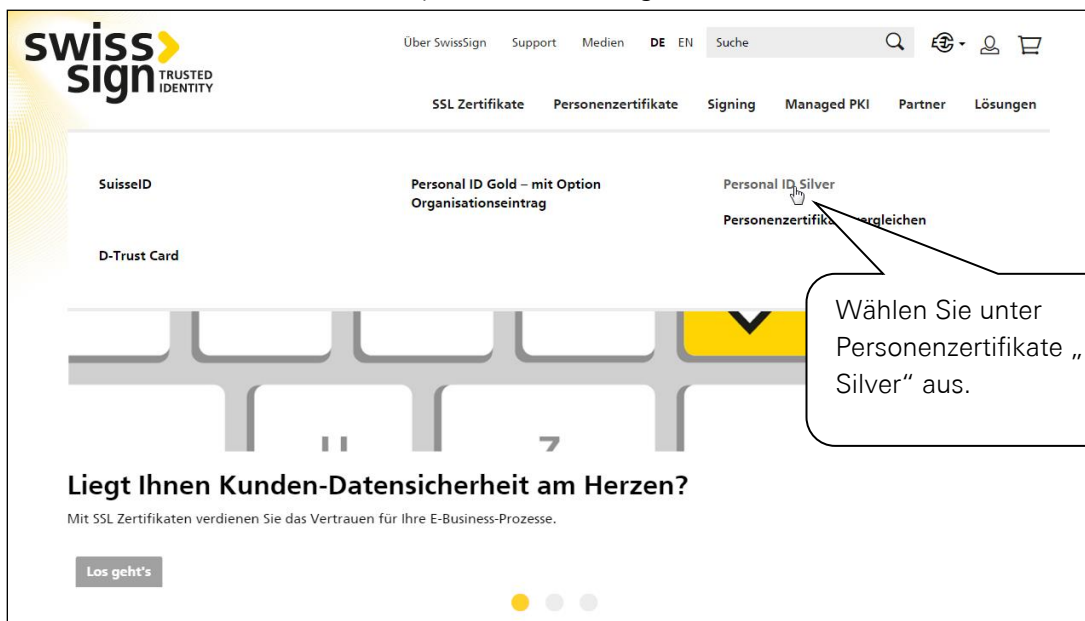
Exemplarisch wird in dem folgenden Kapitel das Produkt „Personal ID Silver“ von SwissSign beantragt.

Bitte beachten Sie, dass das Zertifikat in dem beschriebenen Kapitel für eine E-Mail-Adresse ausgestellt wird und nur mit dieser verwendet werden kann. Der Zugriff auf die E-Mail-Adresse muss mittels Outlook über das Protokoll POP3 oder IMAP erfolgen.

Das beschriebene Zertifikat ist mindestens ein Jahr gültig und ist mit Kosten verbunden.

2.1 Beantragung eines Zertifikats

Öffnen Sie die Internetseite „<http://www.swissign.com/>“



The screenshot shows the SwissSign website interface. At the top, there is a navigation bar with links for 'Über SwissSign', 'Support', 'Medien', and language options 'DE' and 'EN'. A search bar is also present. Below the navigation, there are tabs for 'SSL Zertifikate', 'Personenzertifikate', 'Signing', 'Managed PKI', 'Partner', and 'Lösungen'. The 'Personenzertifikate' tab is active, displaying a grid of certificate options: 'SuissID', 'D-Trust Card', 'Personal ID Gold – mit Option Organisationseintrag', and 'Personal ID Silver'. A mouse cursor is hovering over the 'Personal ID Silver' option. A callout box with a pointer to this option contains the text: 'Wählen Sie unter Personenzertifikate „Personal ID Silver“ aus.' Below the grid, there is a section titled 'Liegt Ihnen Kunden-Datensicherheit am Herzen?' with a subtext 'Mit SSL Zertifikaten verdienen Sie das Vertrauen für Ihre E-Business-Prozesse.' and a button labeled 'Los geht's'.



swiss sign TRUSTED IDENTITY

Über SwissSign Support Medien DE EN Suche

SSL Zertifikate

Home » Personenzertifikate » Personal ID Silver

Personal ID Silver

secured by swiss sign PERSONAL ID SILVER

Preiswe

Mit dem f vertrauen Software-Sekunden Möchten S Managed P

Anzahl Jahre 1 Jahr

EUR 25.00 1 Stk.

In den Warenkorb

MasterCard VISA

Wählen Sie die gewünschte Laufzeit des Zertifikates aus.
Legen Sie es dann mit einem Klick auf „In den Warenkorb“ in den Warenkorb.
Daraufhin öffnet sich der Warenkorb und Sie können mit einem Klick auf „Zur Kasse gehen“ den Bestellvorgang fortsetzen.

swiss sign TRUSTED IDENTITY

Über SwissSign Support Medien DE EN Suche

SSL Zertifikate Personenzertifikate Signing Managed PKI Partner Lösungen

Zur Kasse

Wie möchten Sie zur Kasse gehen?

Registrieren Sie sich, um Ihr anzulegen

Registrieren und Zeit sparen!
Registrieren Sie sich für mehr Komfort bei

- Schneller und einfacher Bestellvorgang
- Einfacher Zugriff auf Ihre bisherigen Be

Passwort

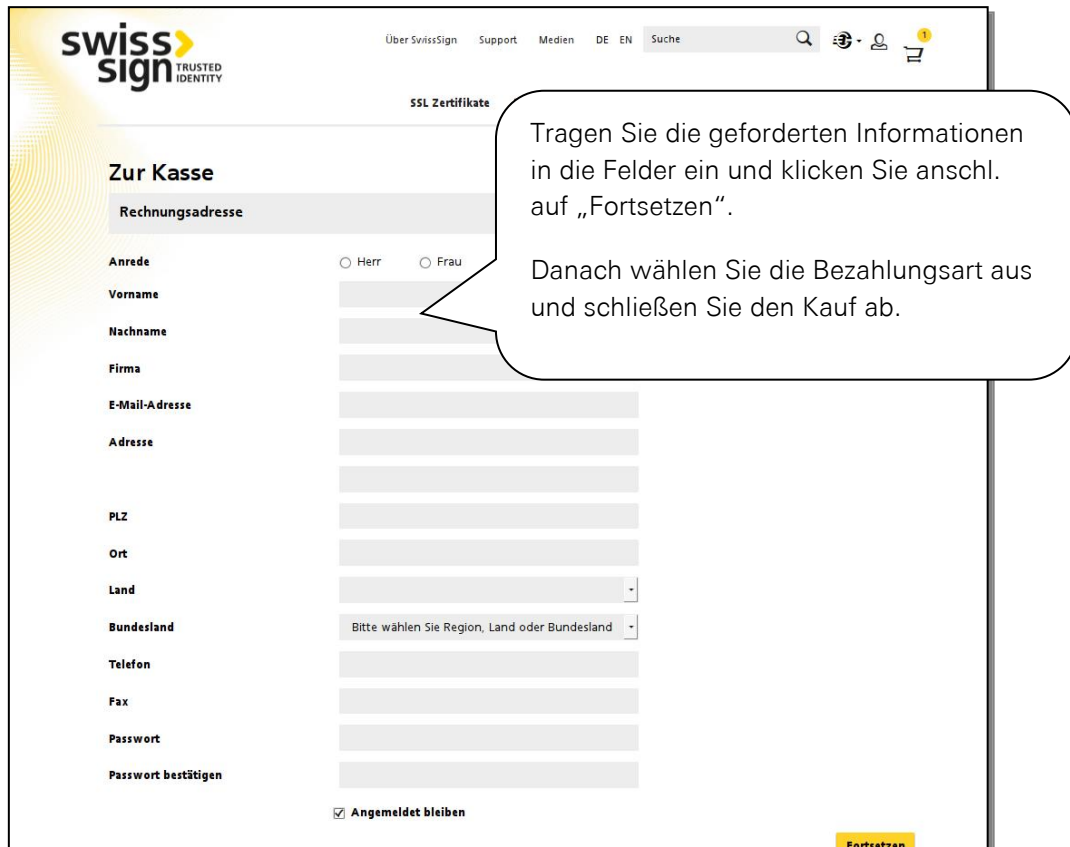
Angemeldet bleiben

Passwort vergessen? Anmelden

suisseID LOG-IN

Registrieren

Sofern Sie noch kein Kunde sind, so registrieren Sie sich mit einem Klick auf „Registrieren“ um den Bestellprozess fortsetzen zu können.



The screenshot shows the 'Zur Kasse' (Checkout) page on the SwissSign website. The page includes a header with the SwissSign logo and navigation links. The main content area contains a form for entering billing information. A callout box with a speech bubble points to the form fields, containing the following text:

Tragen Sie die geforderten Informationen in die Felder ein und klicken Sie anschl. auf „Fortsetzen“.

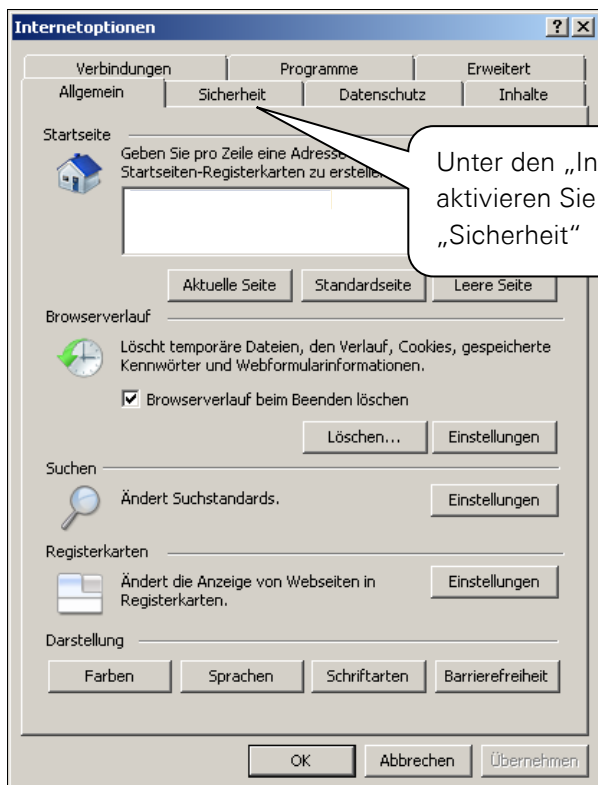
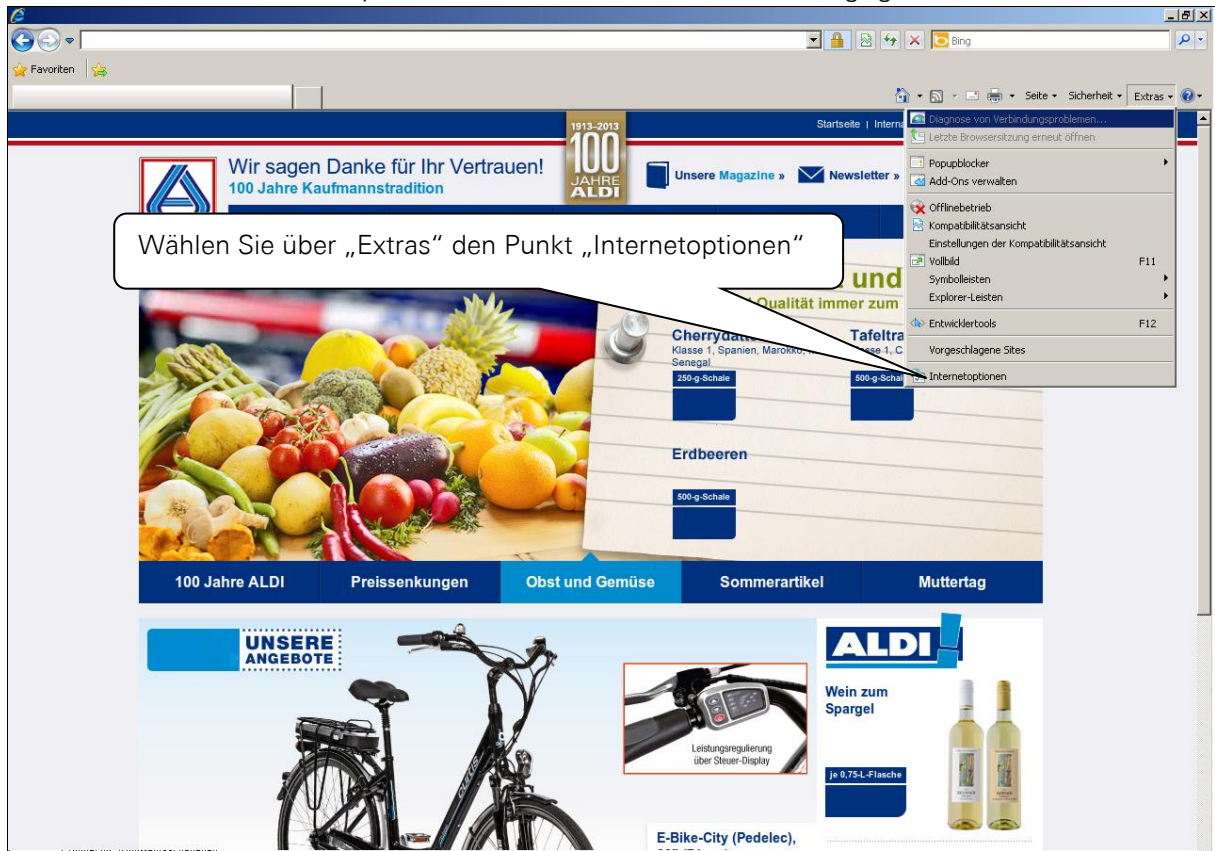
Danach wählen Sie die Bezahlungsart aus und schließen Sie den Kauf ab.

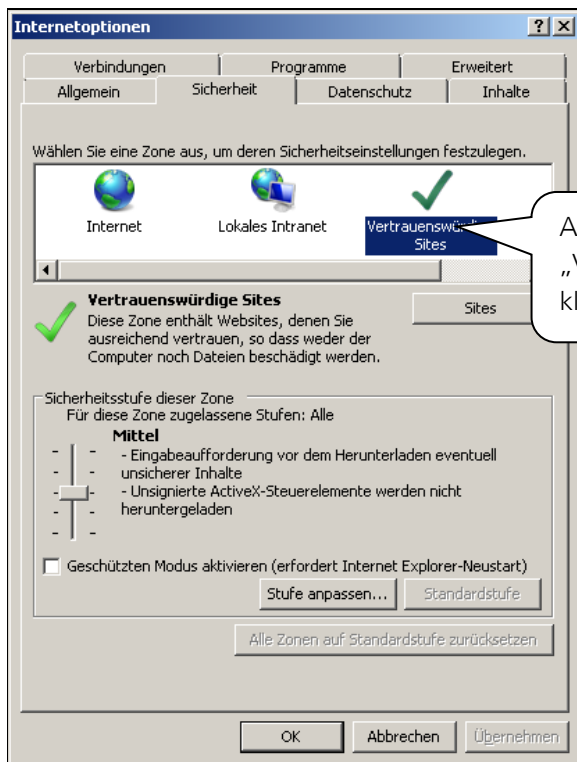
The form fields include: Rechnungsadresse, Anrede (Herr/Frau), Vorname, Nachname, Firma, E-Mail-Adresse, Adresse, PLZ, Ort, Land, Bundesland (with a dropdown menu), Telefon, Fax, Passwort, and Passwort bestätigen. There is also a checkbox for 'Angemeldet bleiben' and a 'Fortsetzen' button at the bottom right.

Nachdem Sie den Bestellvorgang abgeschlossen haben, erhalten Sie innerhalb der nächsten ½ Stunde eine E-Mail mit dem Lizenzcode. Die auf den nachfolgenden Seiten beschriebenen Schritte demonstrieren, wie Sie, nach dem Erhalt eines Lizenzcodes, ein Zertifikat beantragen.

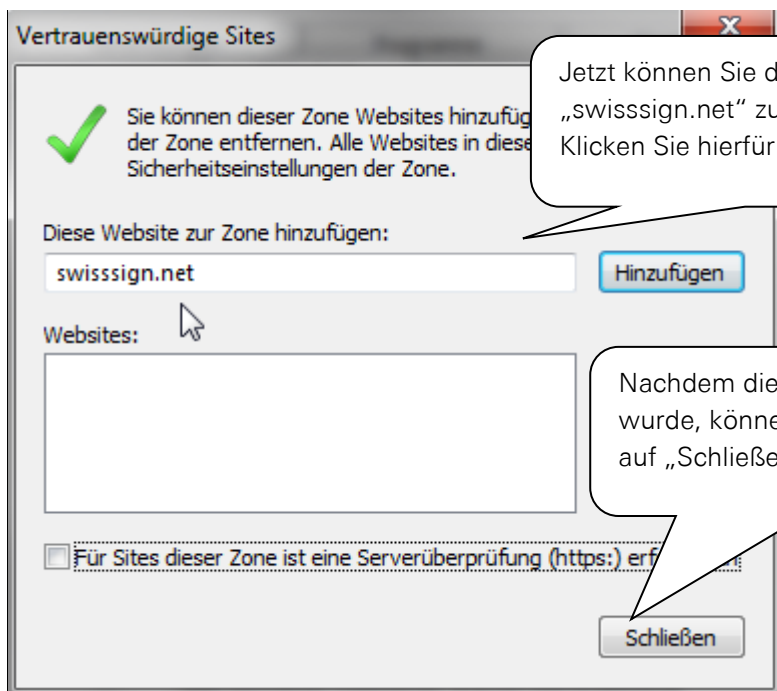


Abhängig von den Einstellungen Ihres Internet Explorers wird die Internetseite als nicht vertrauenswürdig erkannt. In diesem Fall müssen Sie folgende Schritte durchführen und die Trustcenter-Webseite zu den vertrauenswürdigen Webseiten hinzufügen. Hierzu öffnen Sie bitte zuerst den Internet-Explorer und fahren dann wie unten angegeben fort.





Aktivieren Sie bitte den Eintrag „Vertrauenswürdige Sites“ und klicken Sie anschließend auf „Sites“



Jetzt können Sie die Webseite „swissign.net“ zur Zone hinzufügen. Klicken Sie hierfür auf „Hinzufügen“

Nachdem die Seite hinzugefügt wurde, können Sie mit einem Klick auf „Schließen“ den Dialog beenden

Nach dem Sie ebenfalls die Internetoptionen geschlossen haben können Sie den Bestellvorgang fortsetzen. Bitte beachten Sie folgende Hinweise, bevor Sie das Schlüsselpaar erzeugen:

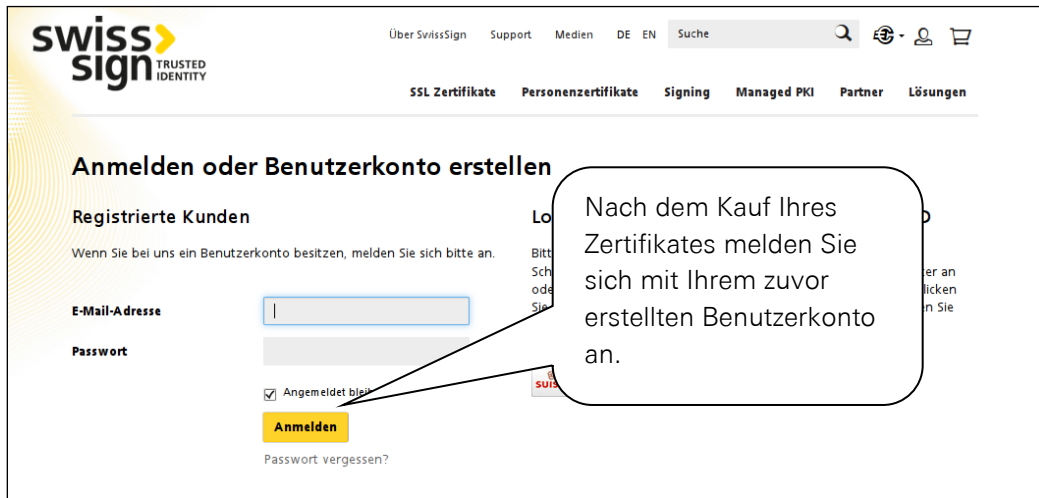
- Erzeugen Sie das Schlüsselpaar entweder mit dem Browser „Mozilla Firefox“ oder „Internet Explorer“.
- Bitte nehmen Sie keine Neuinstallation Ihres Systems oder Browsers vor, bevor Sie das Zertifikat von SwissSign erhalten und installiert haben. Der private Schlüssel, ohne den das Zertifikat nicht funktioniert, ginge sonst verloren.

2.2. Erstellen eines Schlüsselpaars

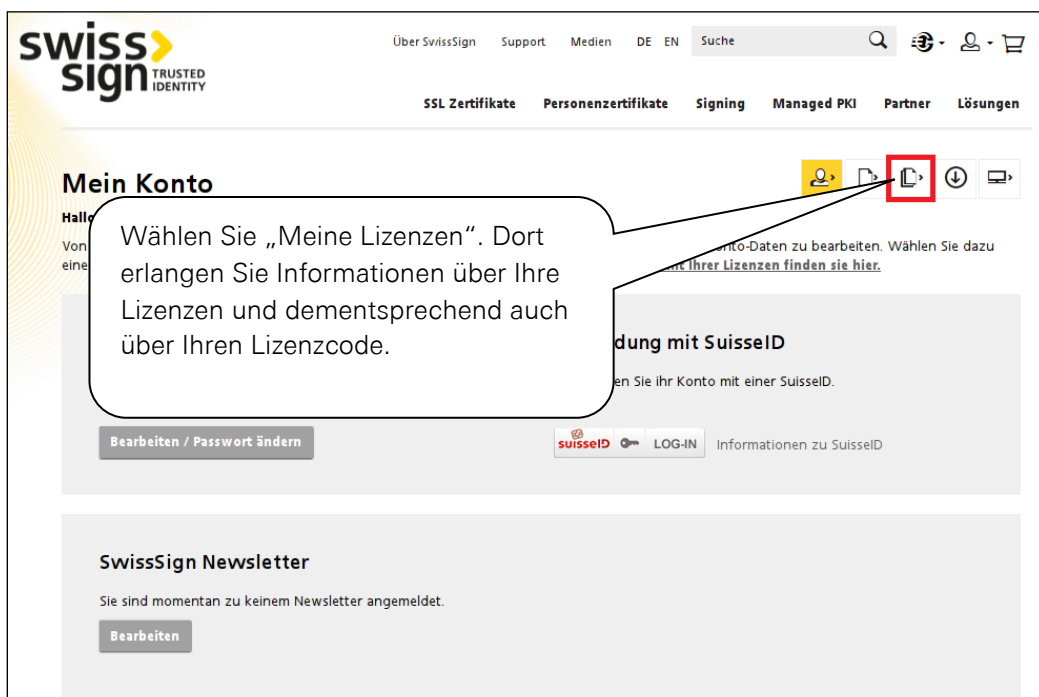
Wenn Sie ein Lizenzcode erhalten haben, fahren Sie bitte mit Kapitel 2.2.2 fort. Ansonsten müssen Sie zuerst den Lizenzcode erlangen. Dazu setzen Sie bitte Kapitel 2.2.1. fort.

2.2.1. Lizenzinformation abrufen

Bitte öffnen Sie die Internetseite <https://www.swissign.com/de/customer/account/login/>



The screenshot shows the SwissSign login page. The header includes the SwissSign logo and navigation links. The main heading is "Anmelden oder Benutzerkonto erstellen". Under "Registrierte Kunden", there is a form with fields for "E-Mail-Adresse" and "Passwort", a checkbox for "Angemeldet bleiben", and an "Anmelden" button. A callout box points to the "Anmelden" button with the text: "Nach dem Kauf Ihres Zertifikates melden Sie sich mit Ihrem zuvor erstellten Benutzerkonto an."



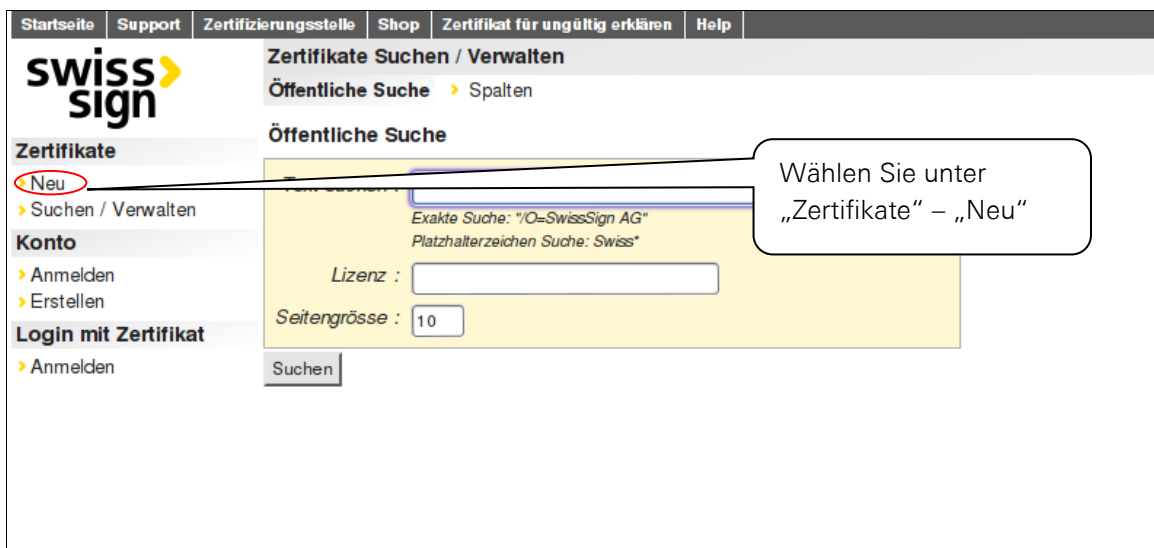
The screenshot shows the "Mein Konto" page. The header is the same as the previous page. The main heading is "Mein Konto". In the top right corner, there is a navigation menu with icons for user profile, licenses, and other account functions. A red box highlights the license icon. A callout box points to this icon with the text: "Wählen Sie „Meine Lizenzen“. Dort erlangen Sie Informationen über Ihre Lizenzen und dementsprechend auch über Ihren Lizenzcode." Below the heading, there is a section for "Anmeldung mit SuisseID" and a "SwissSign Newsletter" section.

2.2.2. Erstellen eines Schlüsselpaars mit Lizenzcode

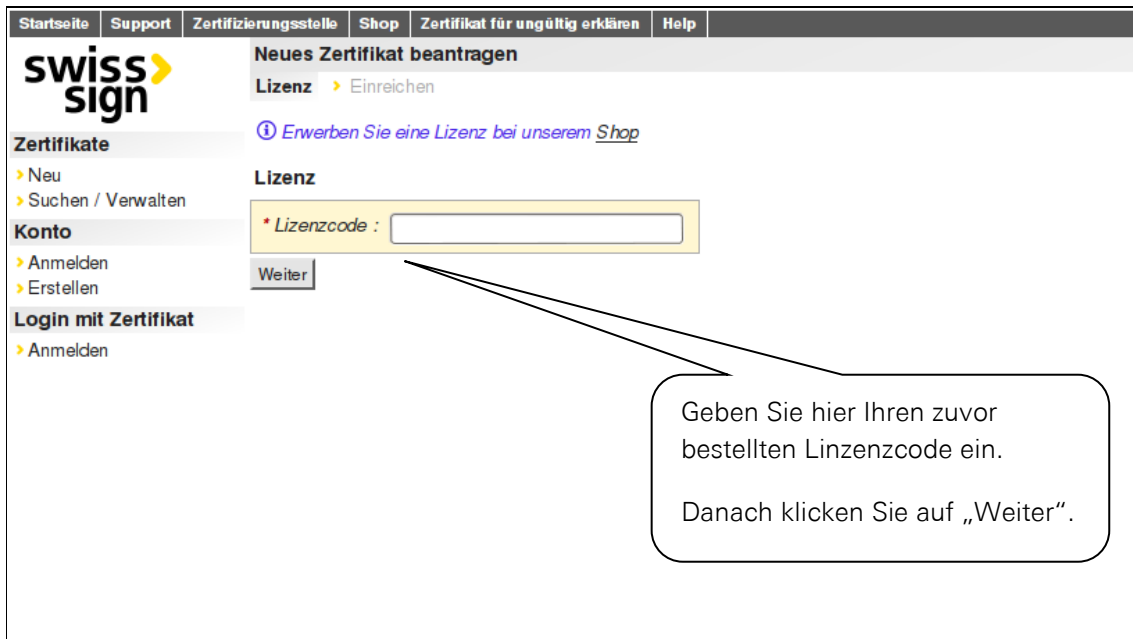
Sobald Sie die „Personal ID Silver“ bestellt haben und den Lizenzcode erhalten haben, können Sie mit dem Lizenzcode ein Zertifikat beantragen. Dazu gehen Sie auf <http://www.swissign.net>



The screenshot shows the swissign website interface. The navigation bar includes 'Startseite', 'Support', 'Zertifizierungsstelle', 'Shop', 'Zertifikat für ungültig erklären', and 'Help'. The main content area is titled 'Zertifikate Suchen / Verwalten' and includes a sidebar with 'Konto' and 'Login mit Zertifikat' sections. The 'Neue Benutzer' section is highlighted, with a red circle around the link 'Weiter ohne Konto (schnelle Einzelzertifikatsanforderung)'. A callout box points to this link with the text: 'Klicken Sie auf „Weiter ohne Konto“. Falls Sie mehrere Zertifikate erstellen und verwalten wollen können Sie sich auch ein Konto erstellen.'



The screenshot shows the swissign website interface, specifically the 'Öffentliche Suche' section. The navigation bar is the same as in the previous screenshot. The main content area is titled 'Zertifikate Suchen / Verwalten' and includes a sidebar with 'Zertifikate' and 'Konto' sections. The 'Neu' link in the 'Zertifikate' section is highlighted with a red circle. A callout box points to this link with the text: 'Wählen Sie unter „Zertifikate“ – „Neu“'. Below the callout, the search form is visible, including fields for 'Lizenz' and 'Seitengröße' (set to 10), and a 'Suchen' button.



Startseite Support Zertifizierungsstelle Shop Zertifikat für ungültig erklären Help

swiss sign

Neues Zertifikat beantragen
Lizenz > Einreichen

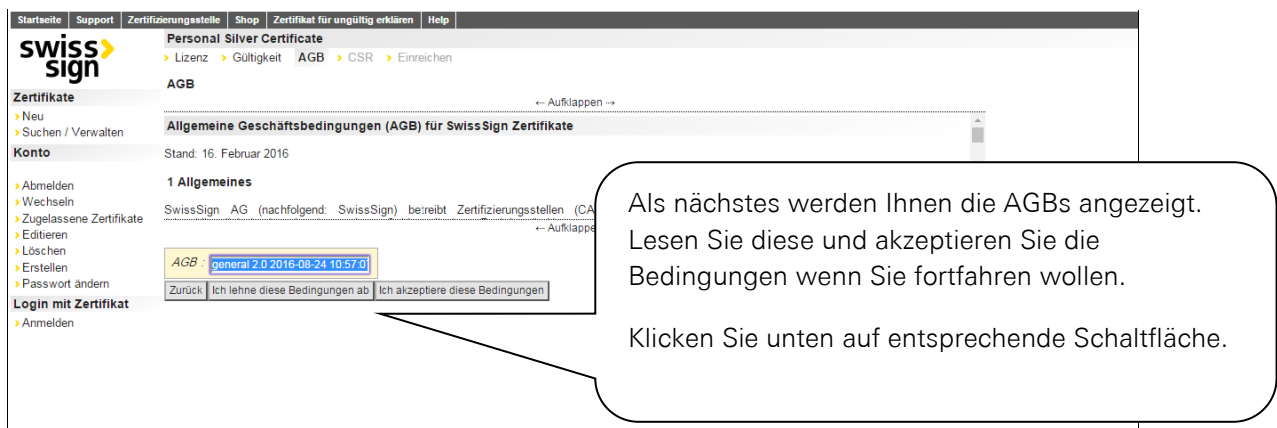
Erwerben Sie eine Lizenz bei unserem Shop

Lizenz

* Lizenzcode :

Weiter

Geben Sie hier Ihren zuvor bestellten Lizenzcode ein.
Danach klicken Sie auf „Weiter“.



Startseite Support Zertifizierungsstelle Shop Zertifikat für ungültig erklären Help

swiss sign

Personal Silver Certificate
Lizenz > Gültigkeit > AGB > CSR > Einreichen

AGB

Allgemeine Geschäftsbedingungen (AGB) für SwissSign Zertifikate

Stand: 16. Februar 2016


1 Allgemeines

SwissSign AG (nachfolgend: SwissSign) betreibt Zertifizierungsstellen (CA)

AGB: general 2.0 2016-08-24 10:57:01

Zurück Ich lehne diese Bedingungen ab Ich akzeptiere diese Bedingungen

Als nächstes werden Ihnen die AGBs angezeigt. Lesen Sie diese und akzeptieren Sie die Bedingungen wenn Sie fortfahren wollen. Klicken Sie unten auf entsprechende Schaltfläche.



Personal Silver Certificate
 > Lizenz > Gültigkeit > AGB > CSR > Einreichen

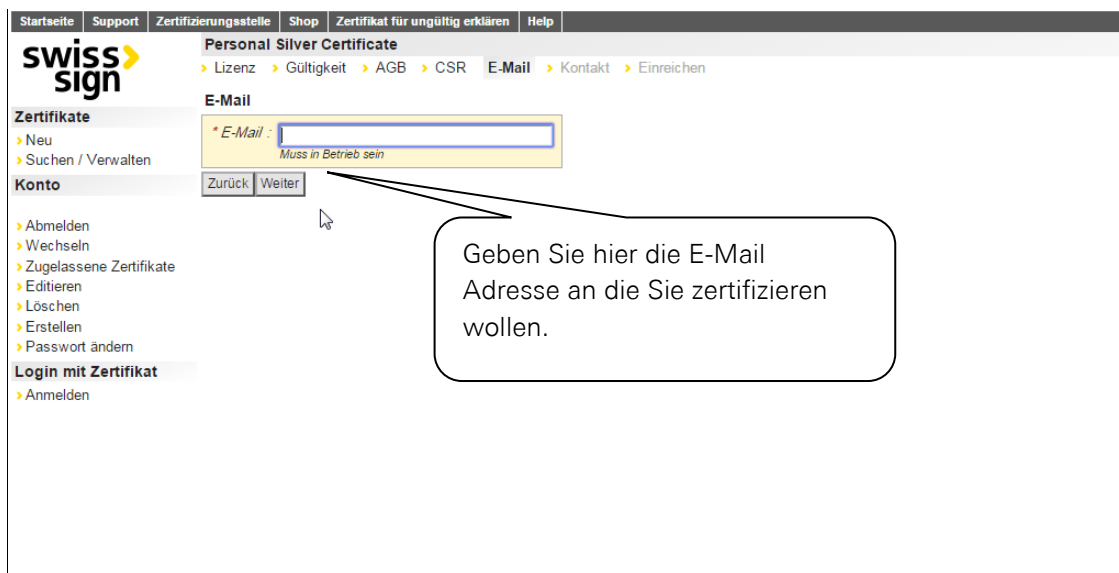
CSR
 Fügen Sie Ihre pkcs#10 Zertifikatsregistrierungsanforderung (CSR) ein, falls Sie eine erstellt haben. Ansonsten lassen Sie das Feld leer und fahren Sie weiter.

PKCS#10 :

Zurück Weiter

Im Standardfall diese Aufforderung freilassen (Nur im Fall von Zertifikatsregistrierungsanforderung ausfüllen).

Klicken Sie auf „Weiter“

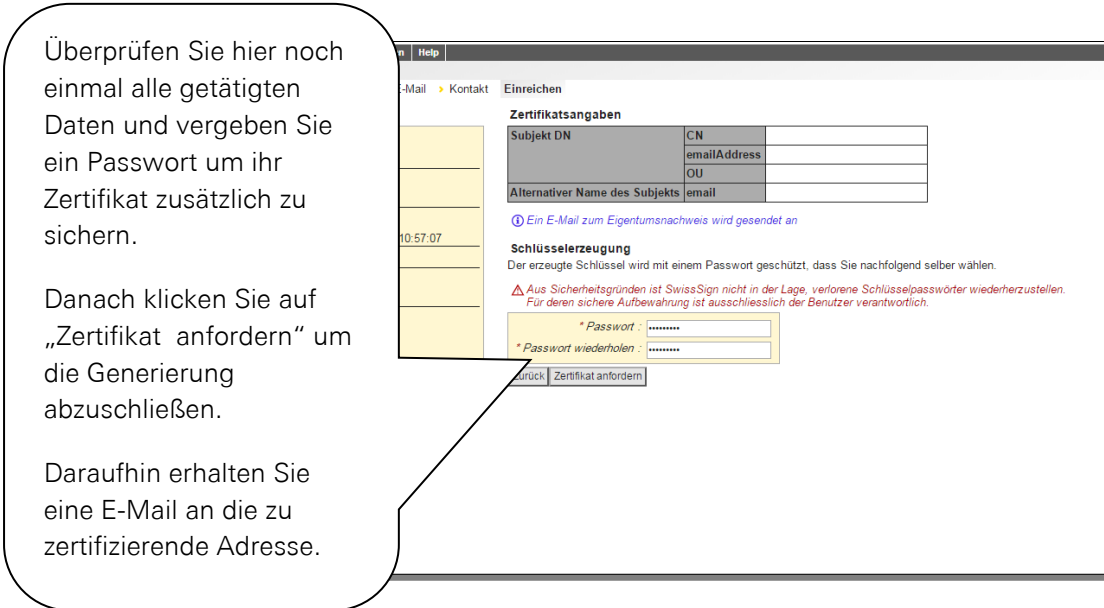


Personal Silver Certificate
 > Lizenz > Gültigkeit > AGB > CSR > E-Mail > Kontakt > Einreichen

E-Mail
 * E-Mail :
Muss in Betrieb sein

Zurück Weiter

Geben Sie hier die E-Mail Adresse an die Sie zertifizieren wollen.



Einreichen

Zertifikatsangaben

Subjekt DN	CN	
	emailAddress	
	OU	
Alternativer Name des Subjekts	email	

Ein E-Mail zum Eigentumsnachweis wird gesendet an

Schlüsselerzeugung
 Der erzeugte Schlüssel wird mit einem Passwort geschützt, dass Sie nachfolgend selber wählen.

⚠ Aus Sicherheitsgründen ist SwissSign nicht in der Lage, verlorene Schlüsselpasswörter wiederherzustellen. Für deren sichere Aufbewahrung ist ausschliesslich der Benutzer verantwortlich.

* Passwort :
 * Passwort wiederholen :

Zurück Zertifikat anfordern

Überprüfen Sie hier noch einmal alle getätigten Daten und vergeben Sie ein Passwort um ihr Zertifikat zusätzlich zu sichern.

Danach klicken Sie auf „Zertifikat anfordern“ um die Generierung abzuschließen.

Daraufhin erhalten Sie eine E-Mail an die zu zertifizierende Adresse.



Mi 24.08.2016 12:59
ca@swissign.net
SwissSign - Ihre Zertifikatsanforderung

An
Signiert von ca@swissign.net

Geme bestätigen
Anforderungsid

Klicken Sie in dieser E-Mail auf den Link „genehmigen“

Validated Only

Als rechtmässiger Inhaber von können Sie Ihre Anforderung selbst [genehmigen](#).

Bei Bedarf können Sie Ihre Zertifikatsanforderung korrigieren, indem Sie Ihre Anforderung [zurückziehen](#) und dann eine neue stellen.

Falls Sie vermuten, dass jemand versucht, Ihre E-Mail Adresse zu missbrauchen, und die Zertifikatsanforderung nicht von Ihnen gestellt wurde, kontaktieren Sie uns bitte unter registration@swissign.com oder über unser [Kontaktformular](#).

Antworten Sie nicht auf dieses automatisch generierte Email.
Bei Fragen wenden Sie sich an das Helpdesk Ihrer Managed PKI, falls Sie eine haben; ansonsten füllen Sie unser [Kontaktformular](#).

Freundliche Grüsse,
Ihr SwissSign Team

Startseite Support Zertifizierungsstelle Shop Zertifikat für ungültig erklären Help EN DE

swissign Zertifikate Suchen / Verwalten

Zertifikate

Zu genehmigende Anforderung

Status	Läuft ab	Subjekt	Alternativer Name	Ungültigerklärungsdatum	Ungültigerklärungsgrund
hängig	--		/OU=Email Validated Only		

Genehmigung bestätigen

*Anforderungsidentifikator :

Genehmigungscode :

Abbrechen | [Genehmigung bestätigen](#)

Sie werden wieder auf „SwissSign.net“ geleitet wo Sie Ihr Zertifikat nun genehmigen können.

Klicken Sie auf „Genehmigung bestätigen“.

Damit gilt diese E-Mail Adresse als Authentifiziert.

Mi 24.08.2016 13:02
ca@swissign.net
SwissSign - Ihre Zertifikatsa

An
Cc registration@swissign.com
Signiert von ca@swissign.net

Ihre SwissSign Zertifikatsanforderung mit folgendem Subjekt wurde genehmigt:
Validated Only

Um das neue SwissSign Zertifikat herunterzuladen und zu installieren, verwenden Sie bitte folgenden Link:
[Zertifikat herunterladen: https://swissign.net.443/cgi-bin/id/download?auth=43E79B084FC6D6AED99D1B0459DE472DC73B6A84&id=7E872BCF363048BE](https://swissign.net.443/cgi-bin/id/download?auth=43E79B084FC6D6AED99D1B0459DE472DC73B6A84&id=7E872BCF363048BE)

SSL Zertifikate sind zeitnah herunterzuladen, da sie anschliessend von der SwissSign Plattform gelöscht werden. Personenzertifikate können Sie mit diesem Link auch zu einem späteren Zeitpunkt erneut herunterladen. Wir empfehlen Ihnen deshalb eine Kopie dieser Nachricht aufzubewahren.

Falls Sie Ihre Zertifikatsanforderung zurückziehen möchten, öffnen Sie bitte folgenden Link in Ihrem Browser:
[Zurückziehung Zertifikatsanforderung](#)
Erst nach dem Herunterladen des Zertifikates wird dieses automatisch ausgestellt und die Zertifikatsanforderung kann nicht mehr zurückgezogen werden.

Sofern Sie ein Konto auf www.swissign.net haben, können Sie hierüber auch das ausgestellte Zertifikat revozieren. Im Zweifelsfalle steht Ihnen unser Support unter Kontakt auf [dem Webshop www.swissign.com](http://dem-Webshop-www-swissign-com) zur Verfügung.

Das ist ein automatisch generiertes Email. Bitte antworten Sie nicht auf dieses Email! Bei Fragen kontaktieren Sie bitte als direkter Webshopkunde unseren [Support](#).
Sofern Sie Ihr Zertifikat über eine Managed PKI bezogen haben, kontaktieren Sie bitte das Benutzer Helpdesk Ihrer Organisation.

Freundliche Grüsse,
Ihr SwissSign Team

Sie erhalten daraufhin eine weitere E-Mail.
Klicken Sie auf den Link „Zertifikat herunterladen“



Startseite Support Zertifizierungsstelle Shop Zertifikat für ungültig erklären Help EN DE

swiss sign Zertifikate Suchen / Verwalten

Suchen Spalten
Herunterladen / Attribute

Zertifikat

Status	Lauf ab	Subjekt	Alternativer Name	Ungültigerklärungsdatum	Ungültigerklärungsgrund
gültig					

Zertifikat und privaten Schlüssel herunterladen (.p12, PKCS#12)

*Anzeigename :
*Schlüsselpasswort :

Herunterladen

Details

Version	v3
Seriennummer	7e18712b:cf36:30:48:bce:c5:a3:a3
Signaturalgo	RSA-SHA256 #[U.P.NULL ***]
Aussteller DN	cn=SwissSign Personal Silver CA 20
Gültigkeit	
Subjekt DN	
Öffentlicher Schlüssel	RSA #[U.P.NULL ***]: #(U.C. SEQUENCE { U.P. INTEGER 004235968d07864c3c413 U.P. INTEGER 01:00:01 })
SAN	eml:
KU, kritisch	digitalSignature, keyEncipherment, dataEncipherment
EKU	emailProtection
SKI	00:62:04:60:75:3f:3b:ab:73:1d:c7:f2:a9:cc:bff
AKI	f0:c7:a3:32:91:b5:eb:ca:b5:58:77:15:a7:4e:be
CRL	<fn = url: http://crl.swissign.net/FRCTA33291856BCA85507715A74EBE1A5D614325> <fn = url: ldap://directory.swissign.net/CN=FRCTA33291856BCA85507715A74EBE1A5D614325%2C=SwissSign%2C=CH/certificateRevocationList?base?objectClass=cRLDistributionP
CP	2.16.756.1.89.1.3.1.6; cps: http://repository.swissign.com/SwissSign-Silver-CP-CPS.pdf

Hier sehen Sie entsprechende Infos zu dem Zertifikat.

Geben Sie hier ihr Schlüsselpasswort ein und klicken Sie daraufhin auf die Schaltfläche „Herunterladen“

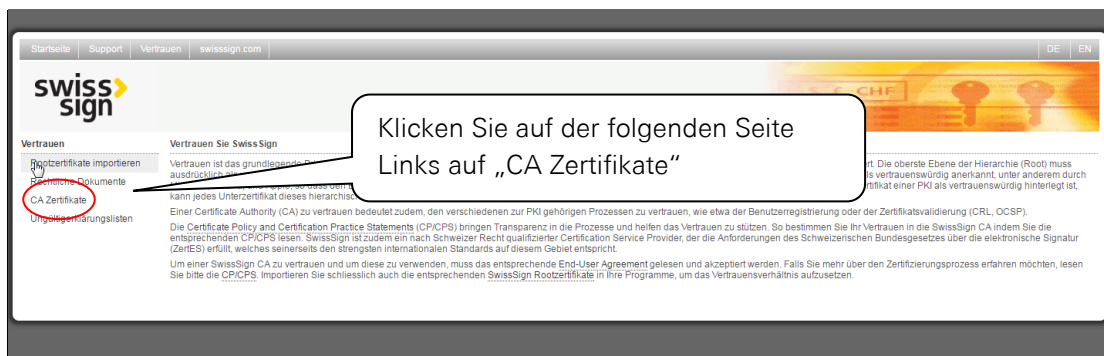
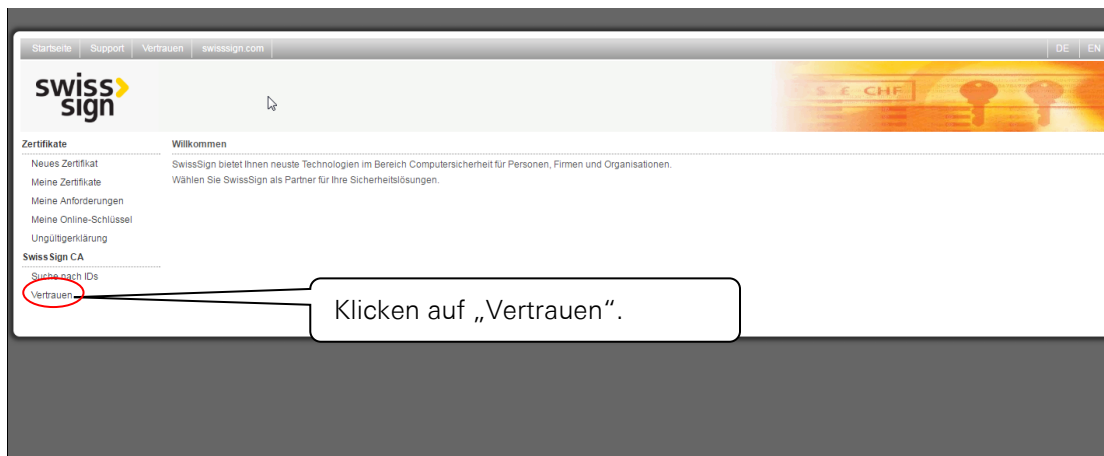
Mit einem Klick auf „Herunterladen“ Beenden Sie die Beantragung, Authentifizierung und Generierung der Zertifikate. Sie sollten das Zertifikat nun in Ihrem Download Ordner vorfinden.

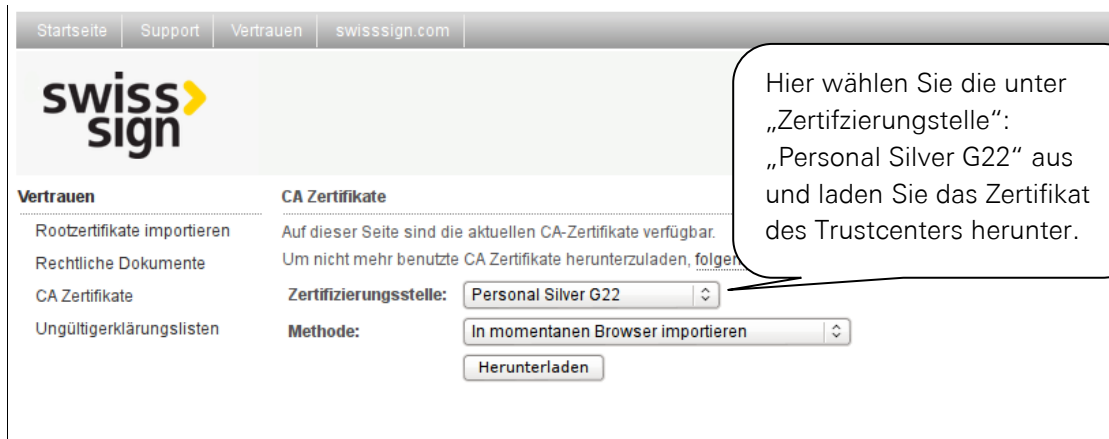
2.3. Installation eines Zertifikats

Dieses Kapitel beschreibt die Installation des zuvor beantragten Zertifikats, damit Sie anschließend sicher und bequem über Outlook mit ALDI Nord verschlüsselt kommunizieren können.

Bevor Sie Ihr eigenes Zertifikat installieren, müssen Sie die Root-CAs des Trustcenters wie folgt installieren:

Rufen Sie die Webseite von SwissSign mit der Adresse: <https://swissign.net/cgi-bin/home> auf.

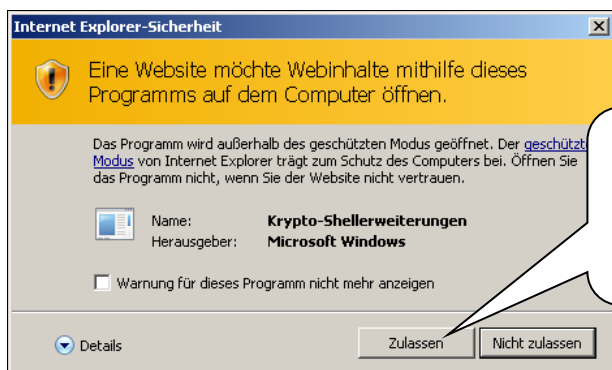




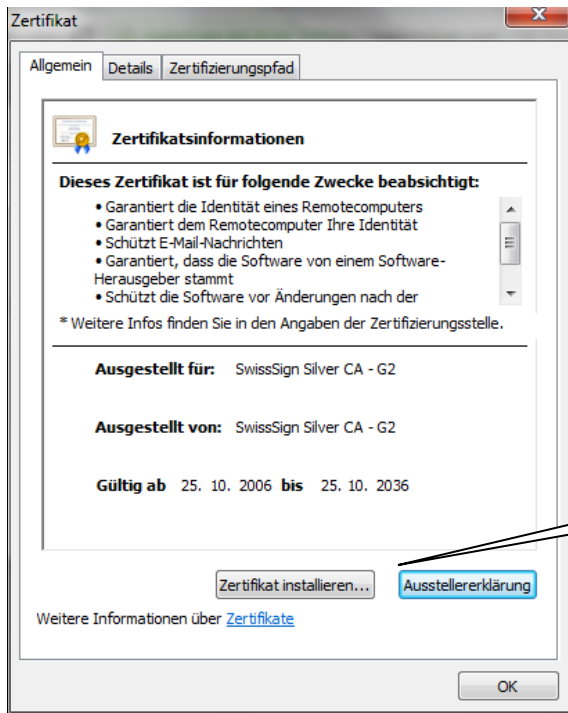
Speichern Sie die Datei mit der Endung „.cer“.

Sollte sich dieses Fenster nicht öffnen, so klicken Sie die heruntergeladene Datei doppelt an bzw. öffnen diese.

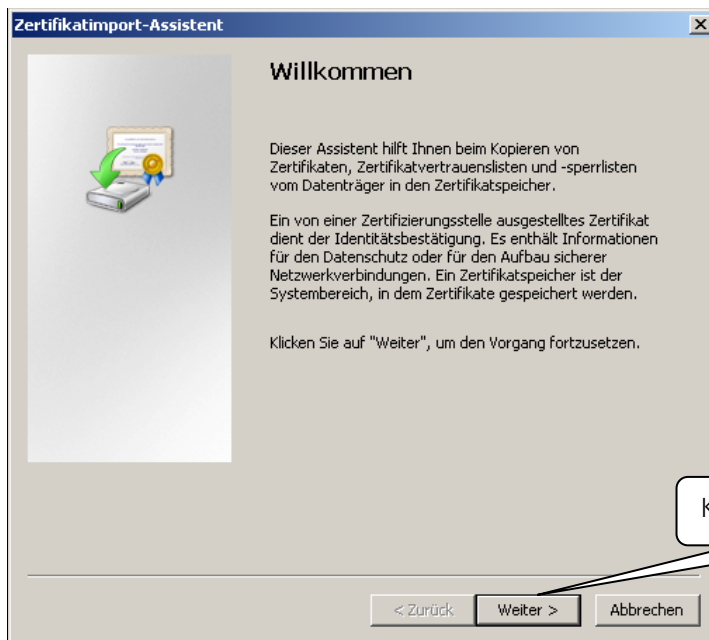
Gegebenenfalls erscheinen die folgenden zwei Sicherheitswarnungen:



Nachdem Sie die Warnungen bestätigt haben fahren Sie wie folgt fort:



Klicken Sie auf „Zertifikat“



Klicken Sie auf „Weiter“

Wählen Sie anschließend den Eintrag „Alle Zertifikate in folgendem Speicher speichern“ und klicken Sie auf „Durchsuchen“

Anschl. markieren Sie den Eintrag „Vertrauenswürdige Stammzertifizierungsstellen“ und klicken auf „OK“

The screenshot shows the 'Zertifikatimport-Assistent' dialog box. The 'Zertifikatspeicher' section has the radio button 'Alle Zertifikate in folgendem Speicher speichern' selected. The 'Zertifikatspeicher auswählen' dialog is open, showing a tree view with 'Vertrauenswürdige Stammzertifizierungsstellen' selected. The background shows a table with certificate details.

base64 encoded X.509	Download
DER encoded X.509	Download
Organization	
Country	DE

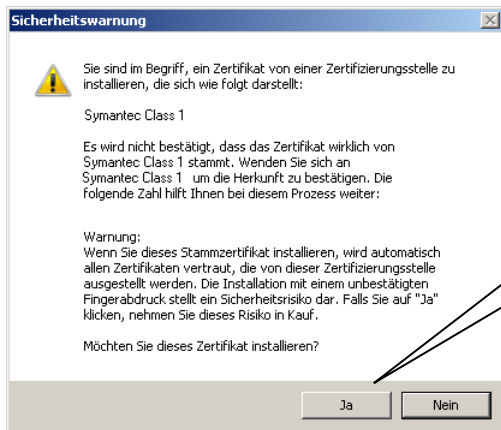
Key Length	
Digital Verification via HTTPS	https://
Organization	TC TrustCenter GmbH
Country	DE

Klicken Sie abschließend auf „Fertig stellen“

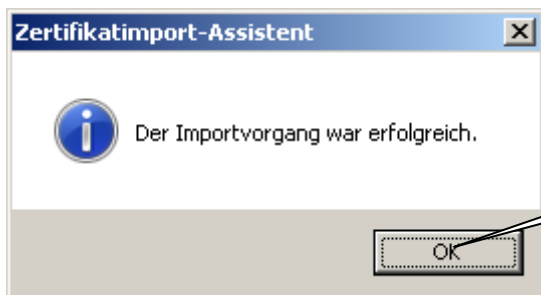
The screenshot shows the 'Fertigstellen des Assistenten' dialog box. It contains a summary of the selected settings: 'Vom Benutzer gewählter Zertifikatspeicher' and 'Vertrauenswürdige Stammzertifizierungsstellen'. The 'Fertig stellen' button is highlighted.

Vom Benutzer gewählter Zertifikatspeicher	Vertrauenswürdige Stammzertifizierungsstellen
Inhalt	Zertifikat

Abhängig vom Betriebssystem erscheint folgende Sicherheitswarnung:



Klicken Sie auf „Ja“

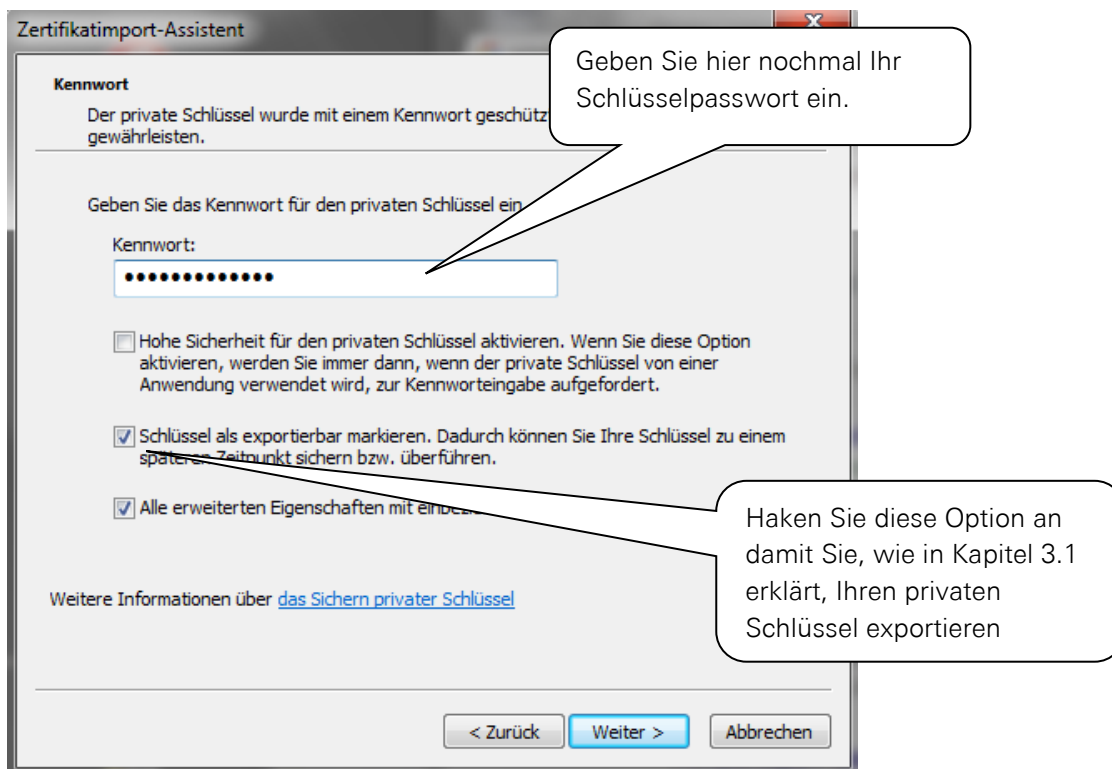
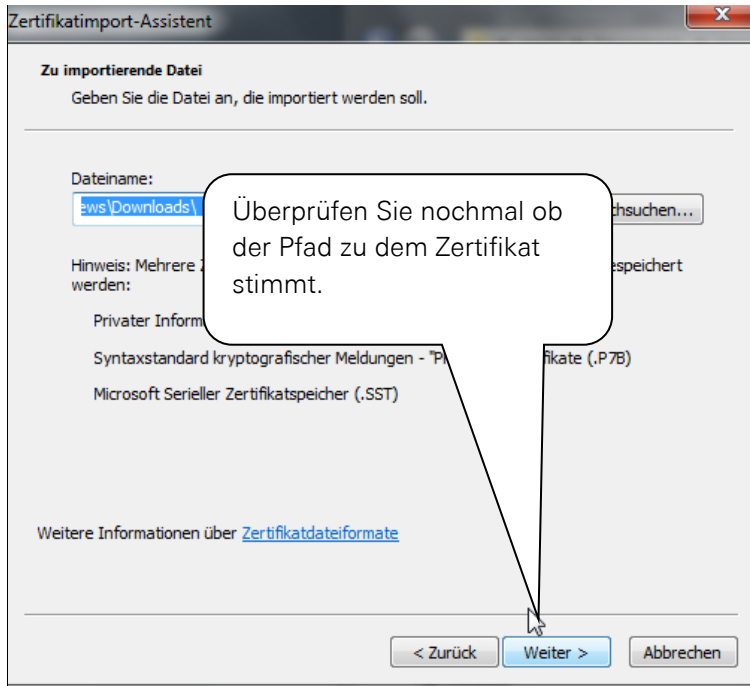


Und auf „OK“

Nun installieren Sie ihr Zertifikat welches Sie zu zuvor Heruntergeladen haben und klicken Sie die Datei doppelt an bzw. öffnen diese. Daraufhin öffnet sich der Zertifikatimport-Assistent



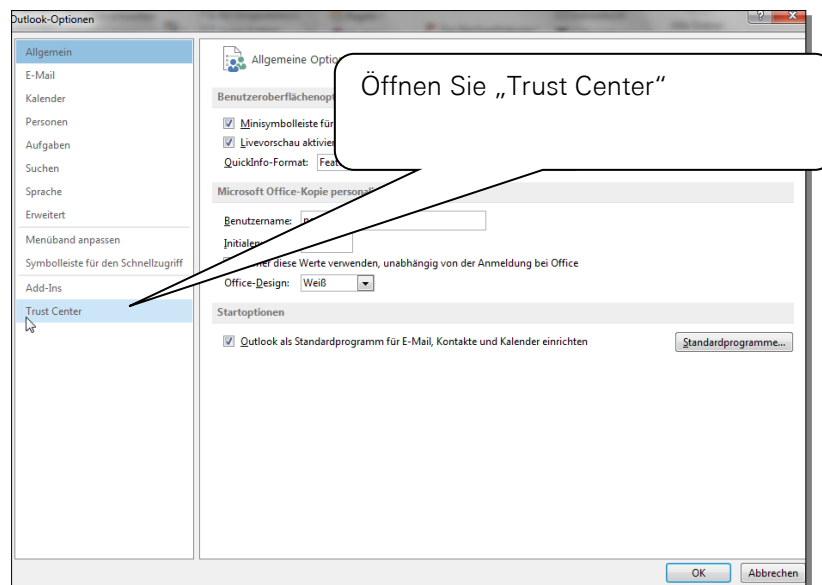
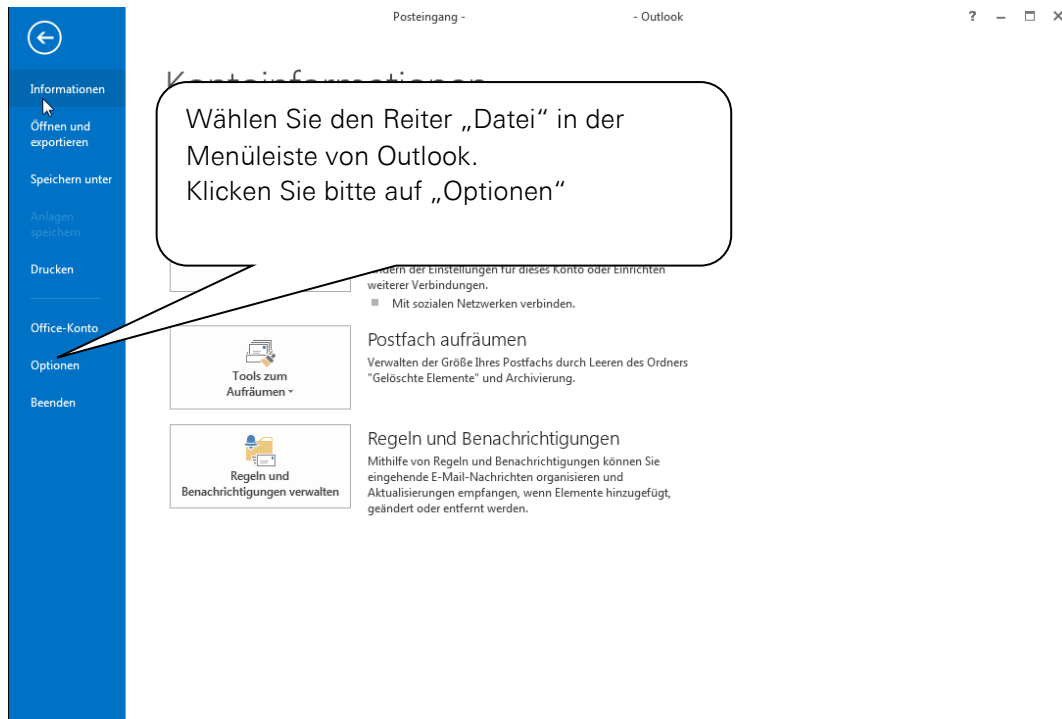
Klicken Sie auf „Weiter >“

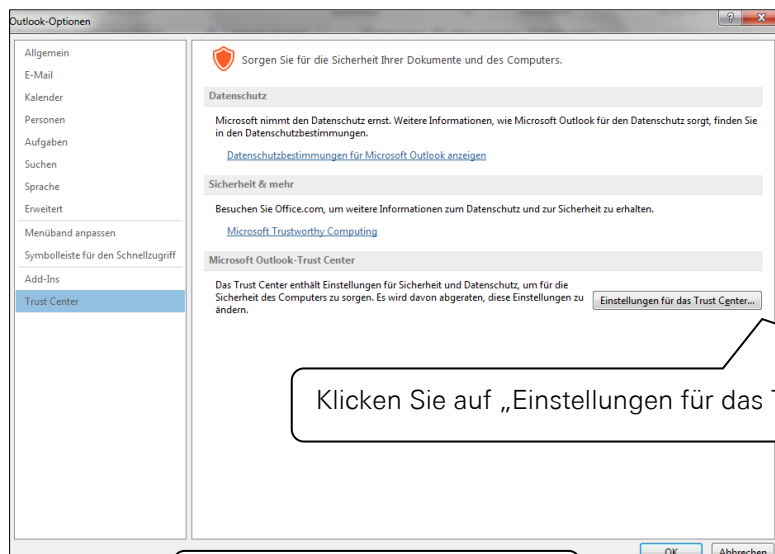


Damit ist Ihr Zertifikat nun auf Ihrem System hinterlegt und steht anderen Programmen zur Verfügung.

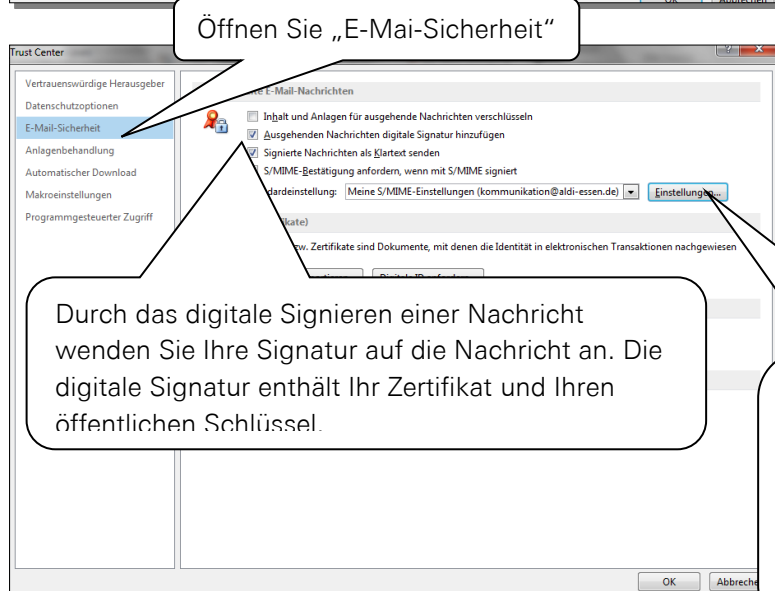
2.4. Einrichten des Zertifikats in Outlook

In diesem Kapitel wird gezeigt, wie Sie Ihr Outlook 2013 einrichten um Ihr Zertifikat zum Signieren zu verwenden. Starten Sie Outlook 2013.





Klicken Sie auf „Einstellungen für das Trust Center ...“

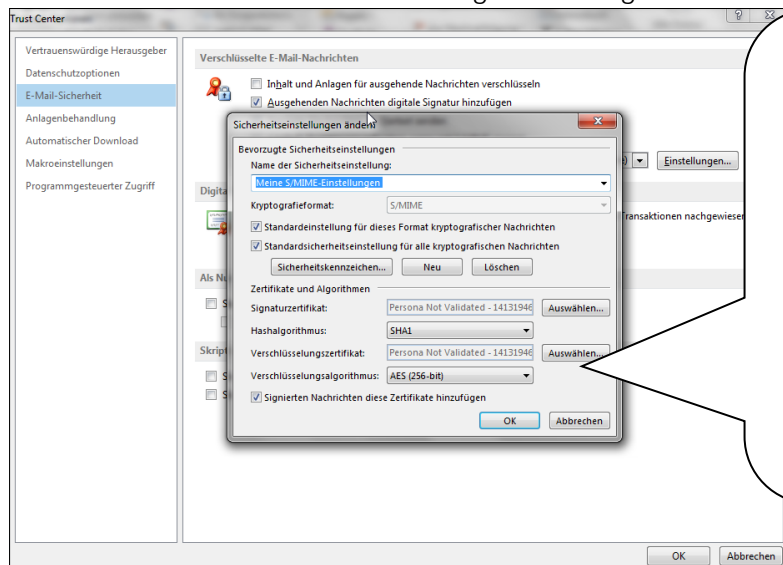


Öffnen Sie „E-Mail-Sicherheit“

Durch das digitale Signieren einer Nachricht wenden Sie Ihre Signatur auf die Nachricht an. Die digitale Signatur enthält Ihr Zertifikat und Ihren öffentlichen Schlüssel.

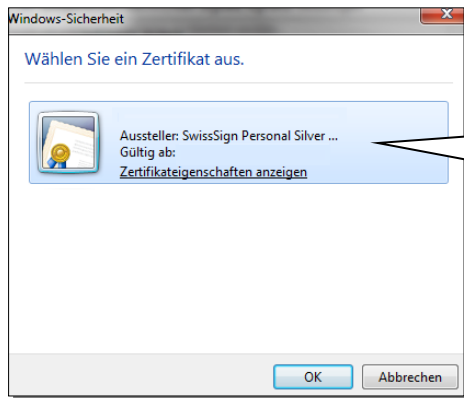
Gleichen Sie die Einstellungen unter „Verschlüsselte E-Mail-Nachrichten“ an und klicken Sie anschl. auf „Einstellungen“

Der Name der Sicherheitseinstellung kann frei gewählt werden.

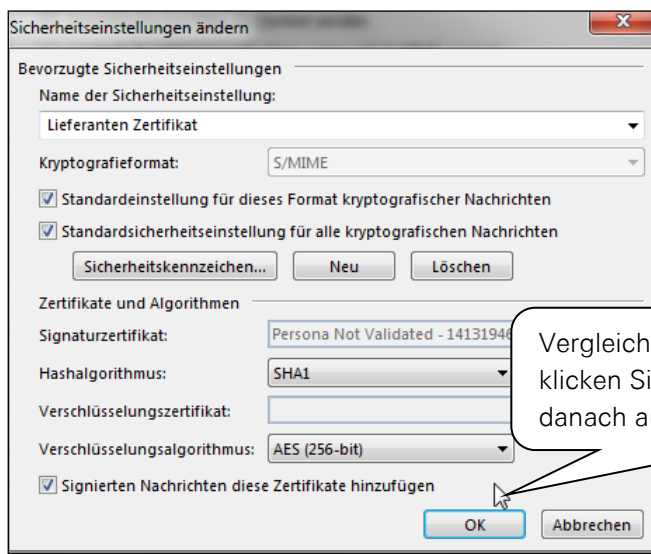


Um verschlüsselt zu kommunizieren, klicken Sie auf „Auswählen“.
Je nachdem welche Auswahl Sie in der vorangehenden Maske getroffen haben, müssen Sie auch ein Signaturzertifikat auswählen und hinterlegen.

Wählen Sie nun das beantragte Zertifikat aus.



Markieren Sie Ihr Zertifikat und klicken Sie unten „OK“.



Vergleichen Sie die Einstellungen und klicken Sie abschließend auf „OK“ und danach auf „schließen“

Outlook 2013 ist jetzt für die Nutzung Ihres Zertifikats eingerichtet.

2.5. Verschlüsselung mit Outlook

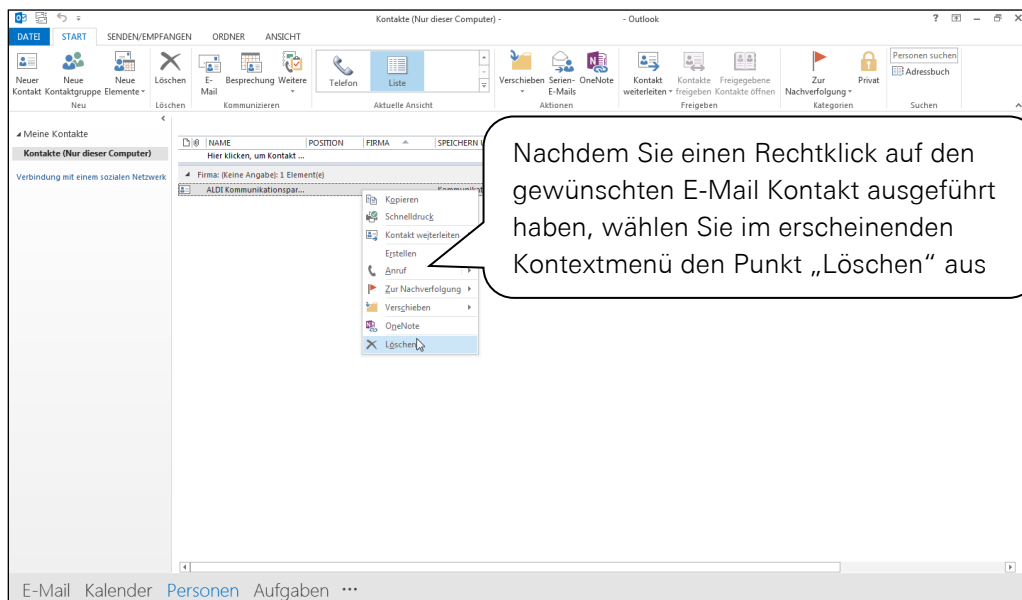
Dieses Kapitel beschreibt die korrekte Anlage eines Kontakts des ALDI Kommunikationspartners für die verschlüsselte E-Mail-Kommunikation. Die Neuanlage ist auch dann notwendig, wenn z. B. der Name einer E-Mail-Adresse durch ALDI Nord angepasst wird oder Sie durch einen Mitarbeiter von ALDI Nord gebeten werden.

Des Weiteren wird anhand von Outlook 2013 exemplarisch auf die zur Verschlüsselung notwendigen Schaltflächen eingegangen. Die Darstellung kann in anderen E-Mail-Programmen abweichen.

Bestehenden Kontakt löschen:

Um Probleme zu vermeiden, muss der eventuell bereits bestehende Kontakt des Kommunikationspartners bei ALDI Nord gelöscht werden.

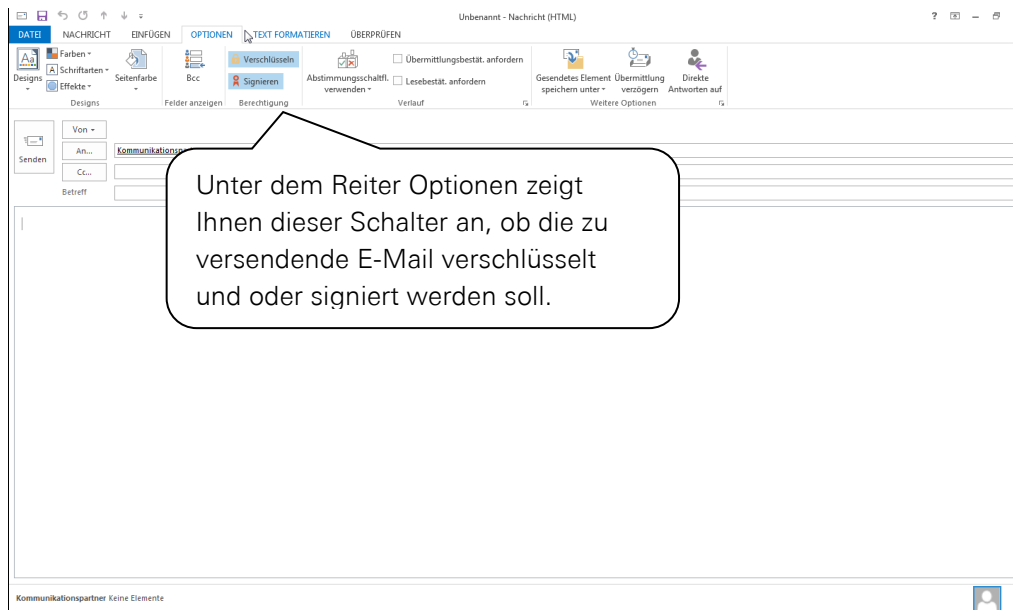
Wählen Sie bitte in Outlook die Kategorie Personen aus und löschen Sie dort den Kommunikationspartner bei ALDI..



Neuen Kontakt anlegen:

Damit die verschlüsselte Kommunikation korrekt funktioniert muss der Kontakt der ALDI Nord Adresse wie vgl. Kapitel 5.2 beschrieben angelegt werden. Andernfalls wird das öffentliche Zertifikat des Kontaktpartners unter Umständen nicht korrekt abgelegt.

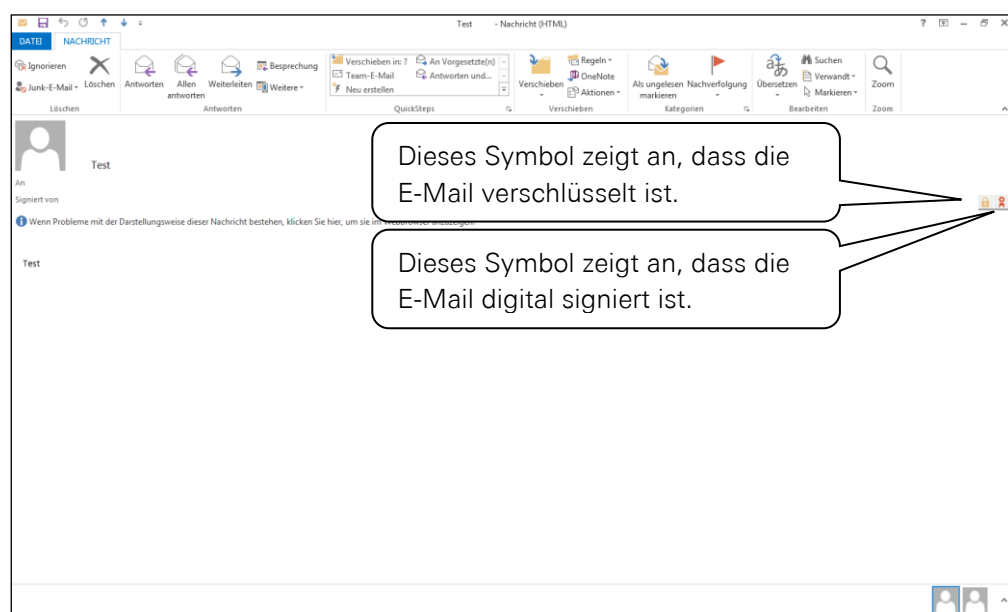
Durch die zuvor festgelegten Einstellungen und durch die Installation des Zertifikats wurden dem Fenster für eine neue Nachricht zwei Schalter hinzugefügt.



Bevor Sie verschlüsselte E-Mails versenden können, müssen Sie entweder eine verschlüsselte E-Mail von Ihrem Kommunikationspartner bei ALDI Nord erhalten haben oder Sie importieren das Zertifikat ihres Kommunikationspartner über die Seite www.aldi-nord.de/certportal (vgl. Kapitel 5.1)

Damit Ihr Kommunikationspartner bei ALDI Nord Ihnen eine verschlüsselte E-Mail zusenden kann, ist das Publizieren Ihres öffentlichen Schlüssels auf dem Keyserver des Trustcenters erforderlich (vgl. Kapitel 2.1). Alternativ können Sie Ihren öffentlichen Schlüssel auch auf der Seite www.aldi-nord.de/certportal bereitstellen (vgl. Kapitel 5.3).

Sie erkennen eine erhaltene verschlüsselte und signierte E-Mail wie folgt:



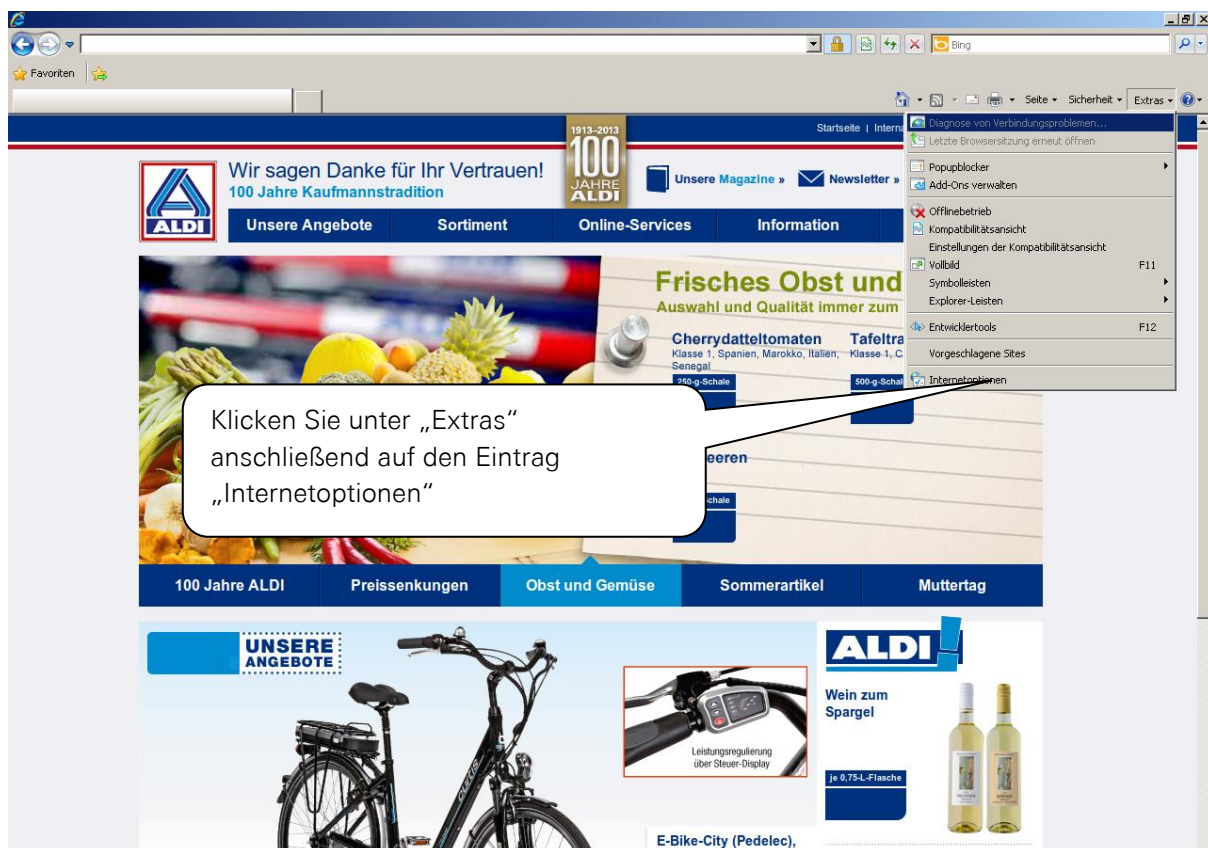
3. Zertifikate ex- und importieren

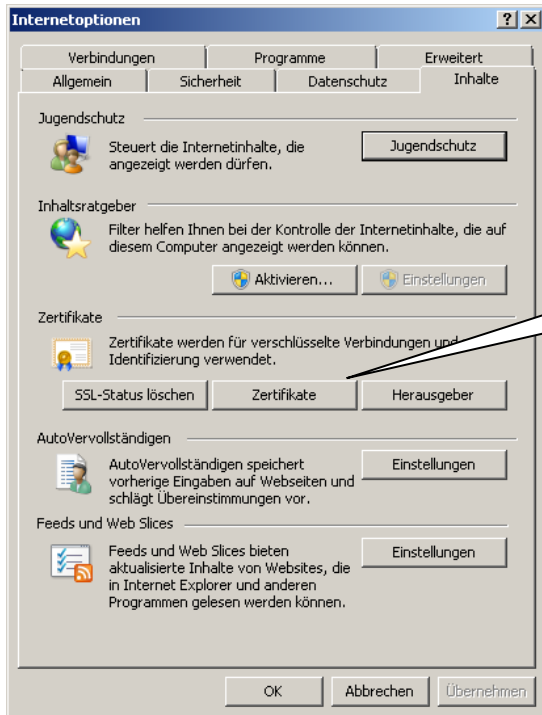
Zertifikate können exportiert und importiert werden, damit diese auf einem anderen PC genutzt werden können.

3.1 Zertifikat exportieren

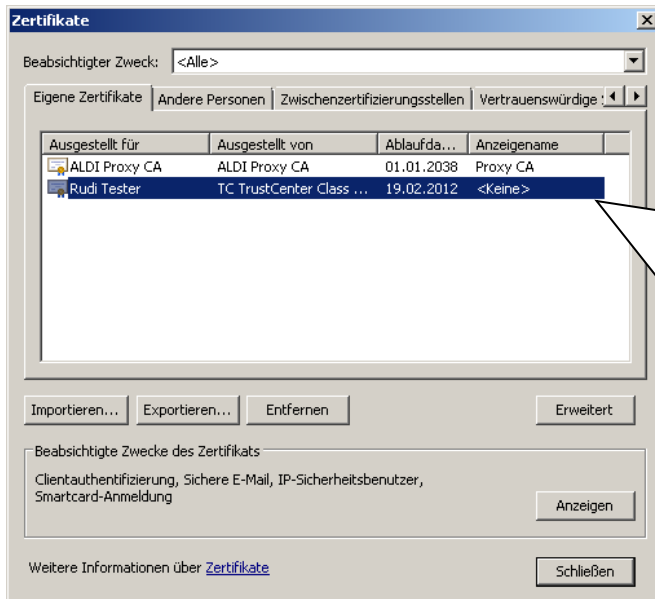
Falls Sie für die o. a. E-Mail-Adresse das unter Punkt 2 beantragte und installierte Zertifikat auf einem anderen PC nutzen möchten, müssen Sie das installierte Zertifikat aus dem Browser exportieren und in den Browser des zukünftigen PCs importieren. Dieses Kapitel beschreibt das Vorgehen.

Öffnen Sie zunächst den Browser auf dem bisherigen PC (der Browser mit dem Sie die unter Punkt 2.1 generierten Schlüsselpaare/Zertifikat erzeugt haben).





Klicken Sie unter dem Reiter „Inhalte“ die Schaltfläche „Zertifikate“ an



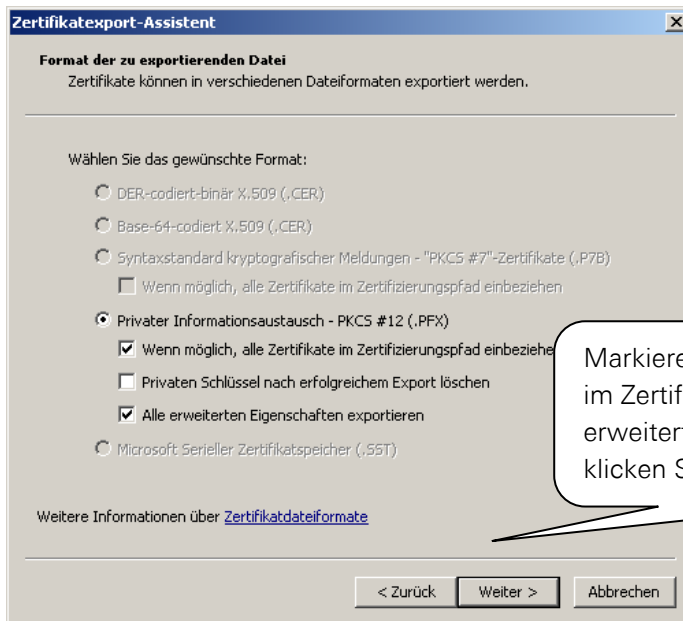
Unter dem Reiter „Eigene Zertifikate“ erscheint das zu exportierende Zertifikat (hier Rudi Tester). Markieren Sie das zu exportierende Zertifikat und klicken Sie anschließend auf die Schaltfläche „Exportieren...“



Wenn Sie wie unter Kapitel 2.3 verfahren sind und sollten Sie an diesem Punkt die Option „Ja, privaten Schlüssel exportieren“ ausgegraut vorfinden, überprüfen Sie nochmals ihre Berechtigung.

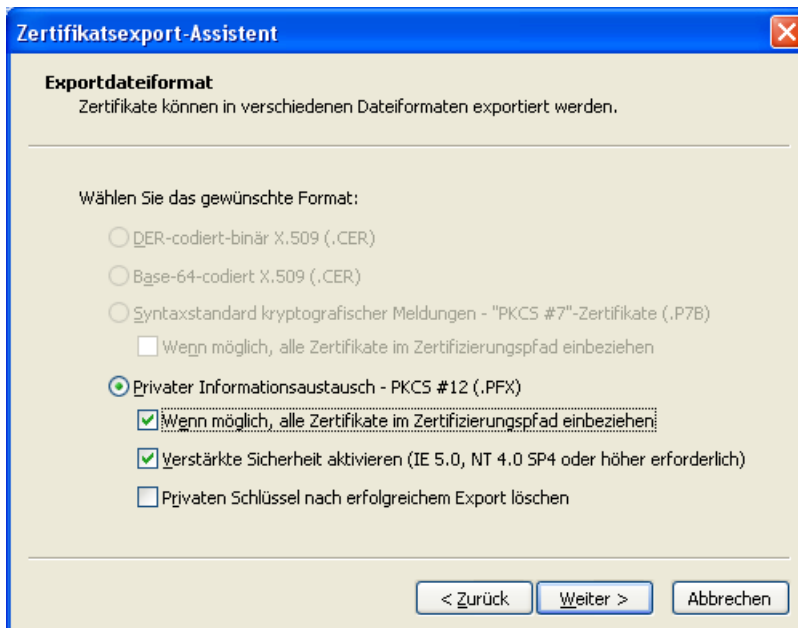
Sie müssen mindestens Mitglied der Gruppe Benutzer oder Lokale Administratoren sein, um dieses Verfahren ausführen zu können.

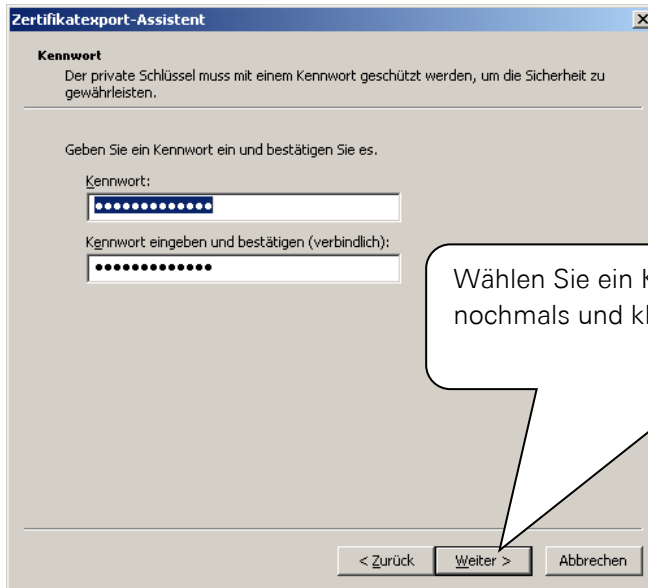
Windows 7:



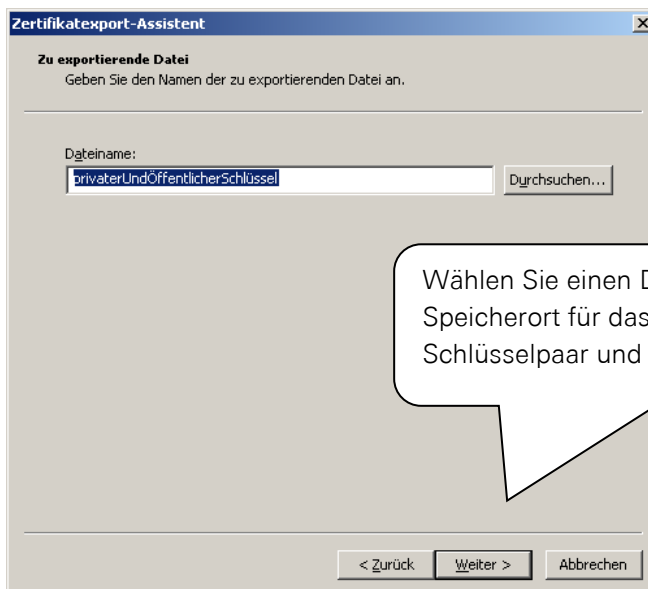
Markieren Sie „Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen“ und „Alle erweiterten Eigenschaften exportieren“ und klicken Sie auf „Weiter >“

Windows XP:

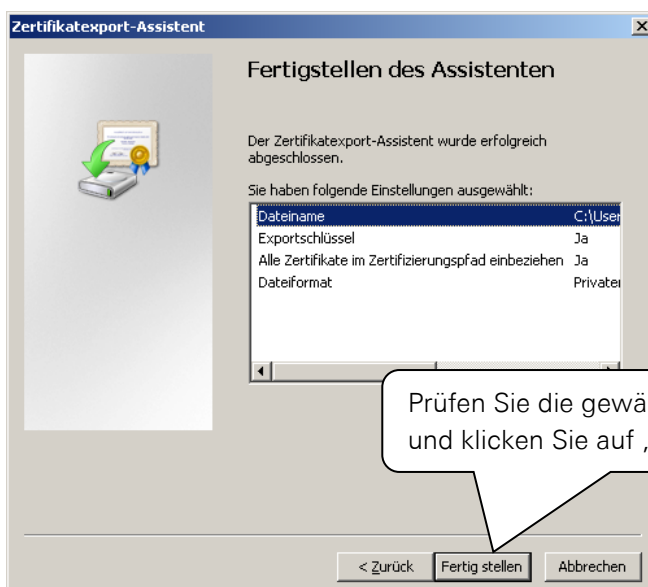




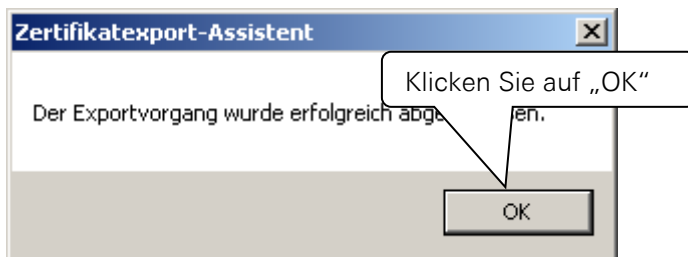
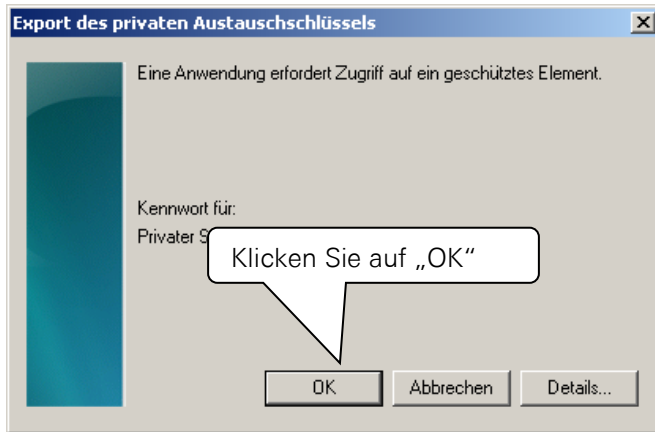
Wählen Sie ein Kennwort, bestätigen Sie dieses nochmals und klicken Sie auf „Weiter >“



Wählen Sie einen Dateinamen und einen Speicherort für das zu exportierende Schlüsselpaar und klicken Sie auf „Weiter >“

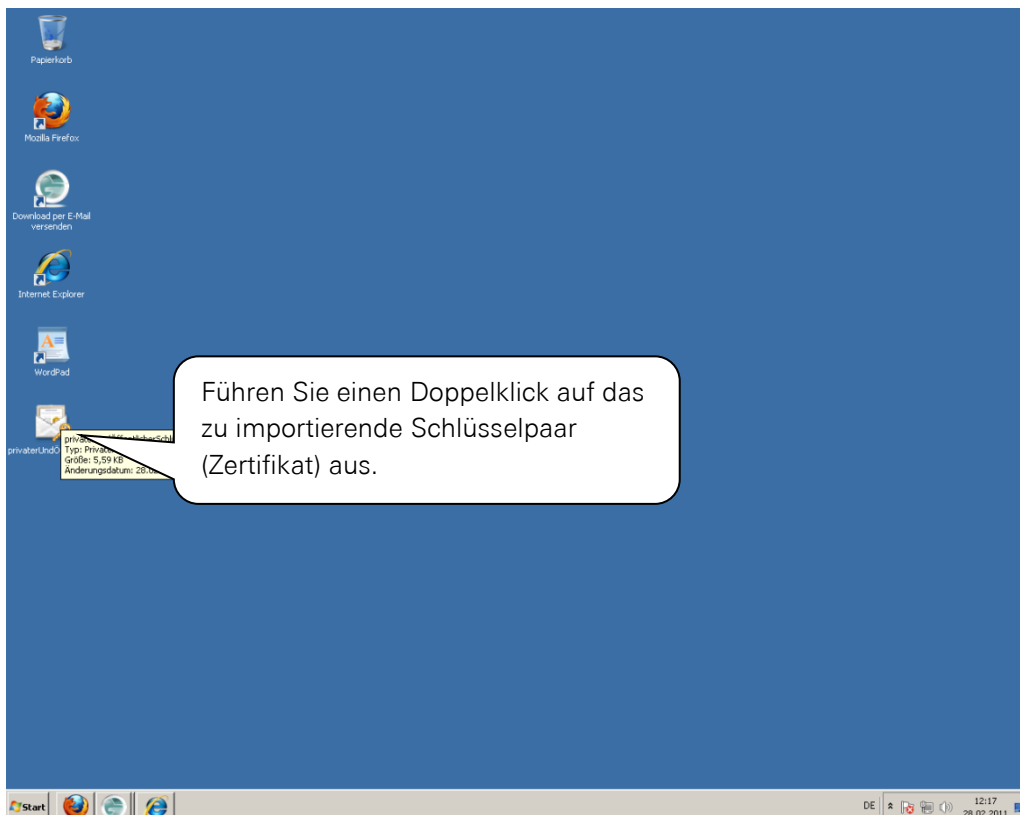


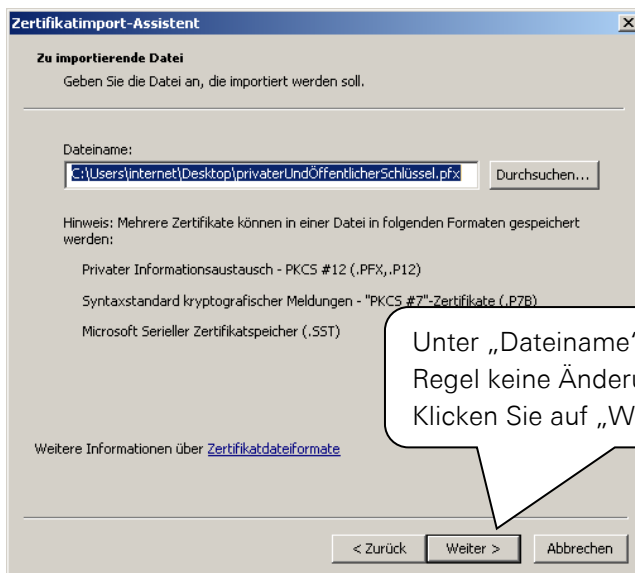
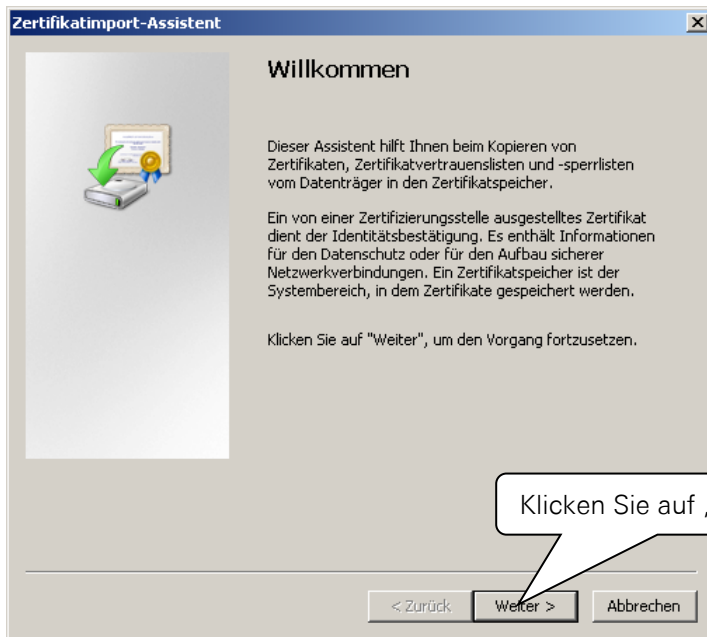
Prüfen Sie die gewählten Einstellungen und klicken Sie auf „Fertig stellen“



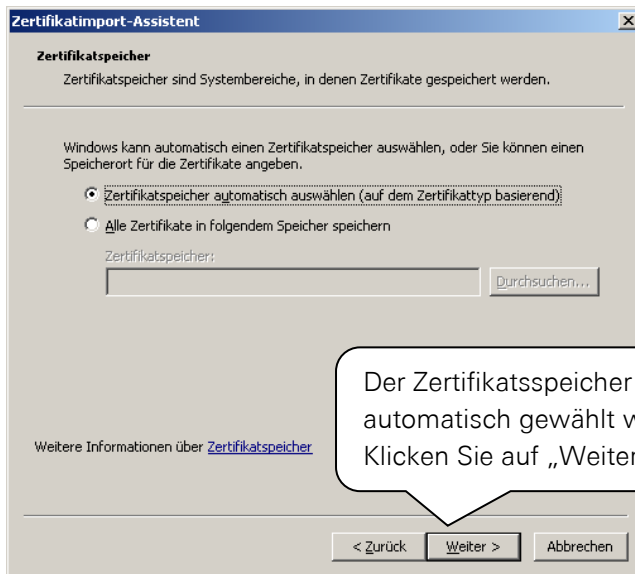
3.2 Zertifikat importieren

Das zuvor exportierte Zertifikat müssen Sie auf den neuen PC importieren.

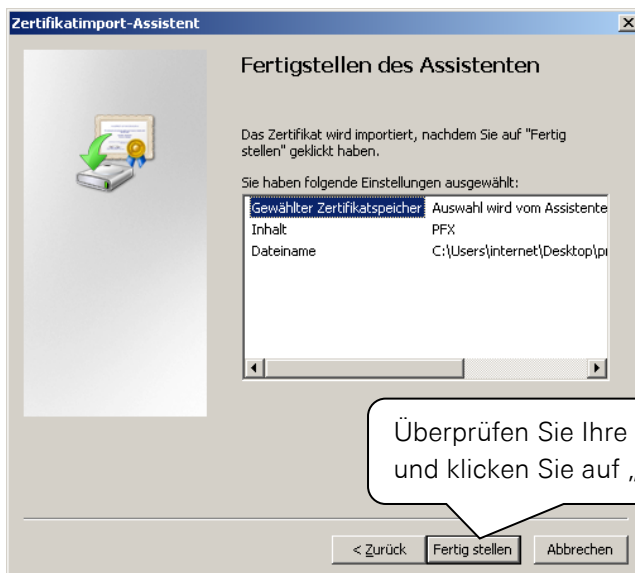




Handelt es sich um ein kennwortgeschütztes Zertifikat, so ist im nachfolgenden Dialog das entsprechende Kennwort für das Zertifikat einzutragen. Bitte bestätigen Sie mit „Weiter“.

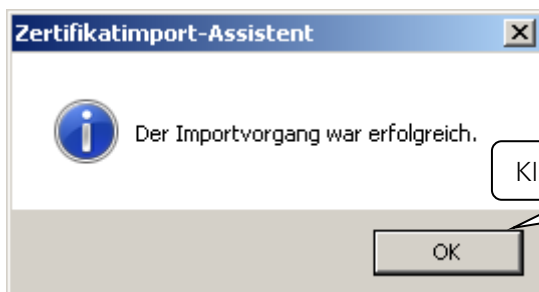


Der Zertifikatsspeicher kann automatisch gewählt werden. Klicken Sie auf „Weiter >“



Überprüfen Sie Ihre Einstellungen und klicken Sie auf „Fertig stellen“

Anschließend erhalten Sie evtl. noch einen Sicherheitshinweis, den Sie bestätigen können.



Klicken Sie abschließend auf „OK“



4. Installation des ALDI Nord Stammzertifikats

Mit dem sogenannten Stammzertifikat („Root certificate (CER)“) kann der Vertrauensstatus der Benutzerzertifikate der Unternehmensgruppe ALDI Nord überprüft werden. Das bedeutet, dass Ihr eingesetztes System überprüfen kann, ob das Benutzerzertifikat wirklich von der Unternehmensgruppe ALDI Nord ist und ob es noch gültig ist. Für den Bezug des Stammzertifikats stehen drei Optionen zur Auswahl:

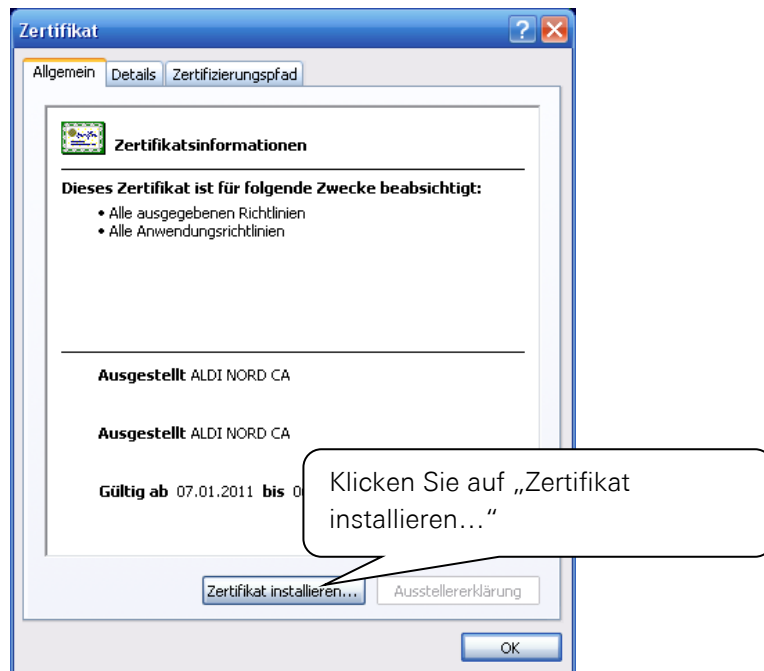
1. Sie haben bereits eine E-Mail von einem ALDI Mitarbeiter erhalten und verfügen somit über einen Zugang zum Webmessenger: Dort können Sie über den Punkt „Einstellungen“ das Stammzertifikat herunterladen.
2. Unter der Seite „www.aldi-nord.de/cert“ steht Ihnen das Stammzertifikat zum Download zur Verfügung.
3. Sie verfügen bereits über ein Zertifikat von einem von ALDI Nord unterstützten Trustcenter und haben Ihren öffentlichen Schlüssel auf dem Keyserver publiziert. Die E-Mail eines ALDI Nord Mitarbeiters wird Ihnen inkl. Stammzertifikat direkt zugestellt.

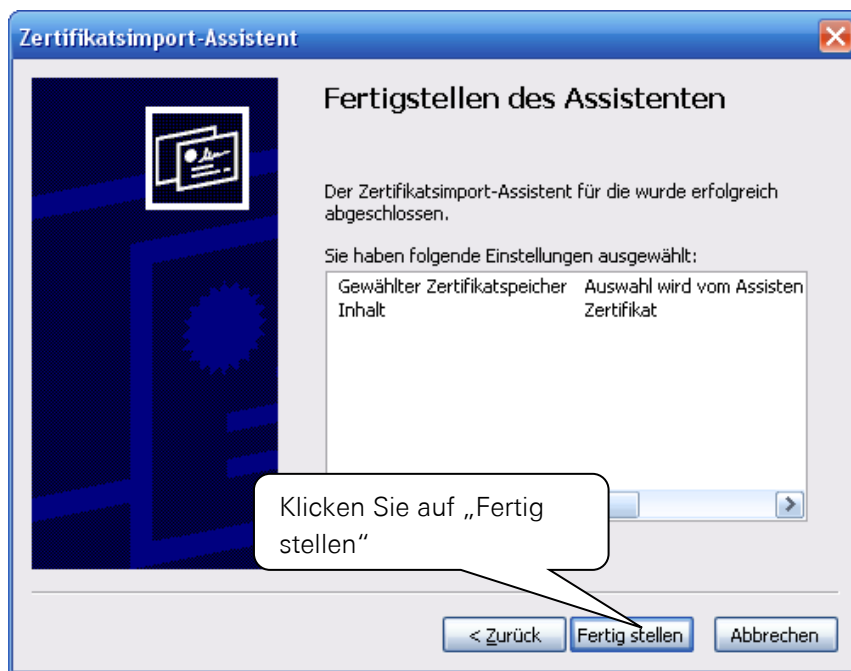
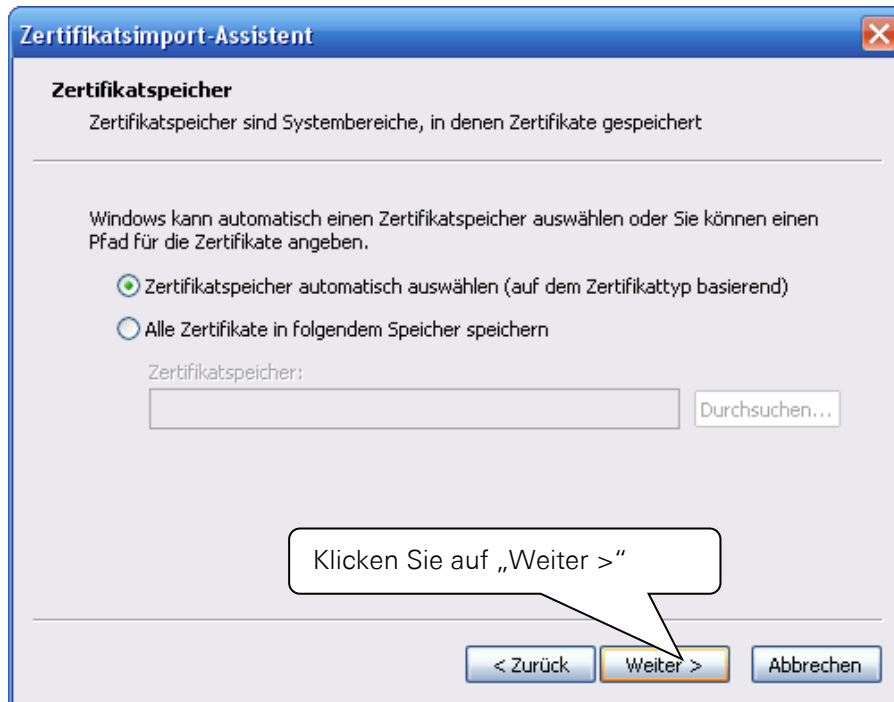
Die Installation des Stammzertifikats über die Webseite unterscheidet sich nicht durch die Installation aus dem Webmessenger.

Führen Sie für Punkt 1 und Punkt 2 bitte folgende Schritte aus:

Öffnen Sie bitte die Seite www.aldi-nord.de in Ihrem Internet Explorer und klicken Sie auf den Menüeintrag „Stammzertifikat“. Anschließend werden Sie gefragt, ob Sie die Datei öffnen oder speichern möchten. Klicken Sie auf „öffnen“.

Nachdem Sie „öffnen“ gewählt haben, erhalten Sie folgende Abbildungen:



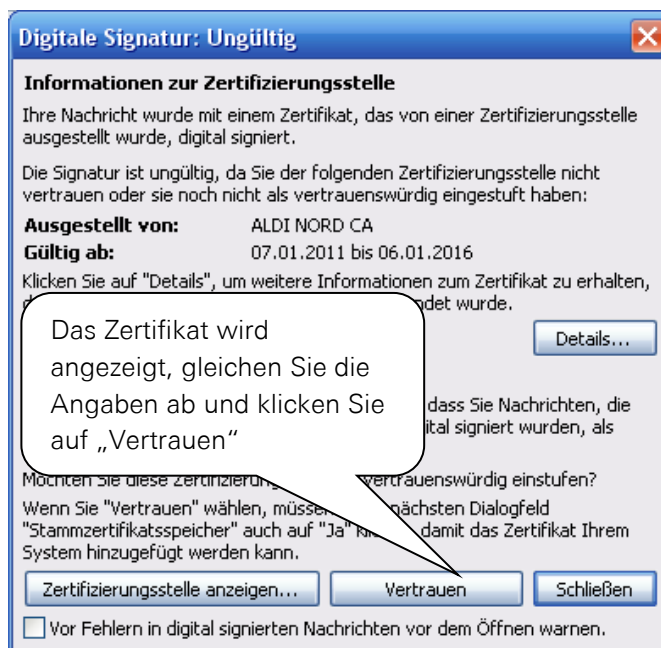
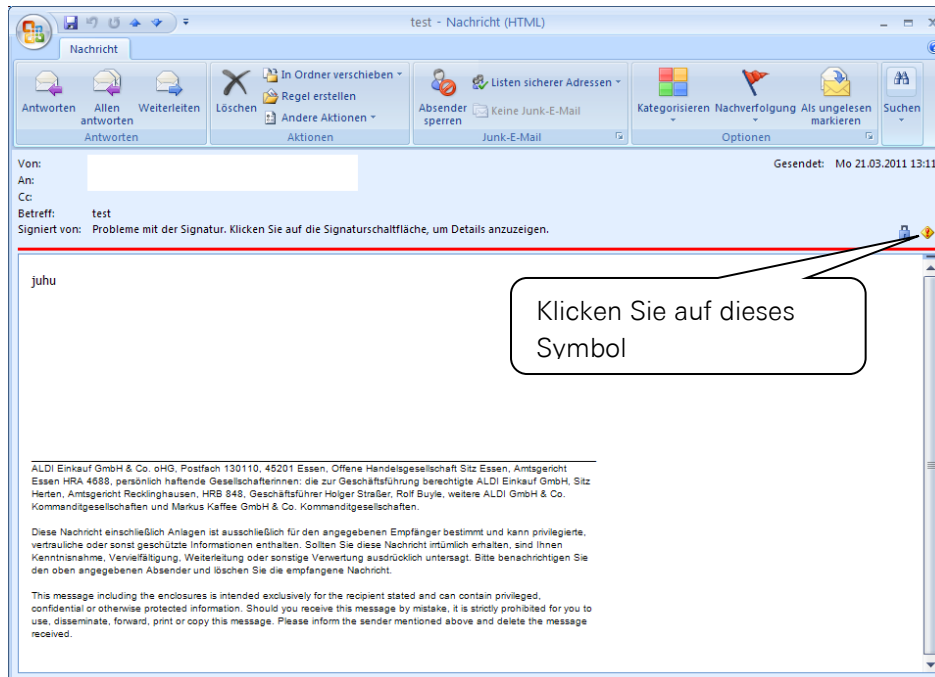


Abschließend erhalten Sie folgende Meldung:

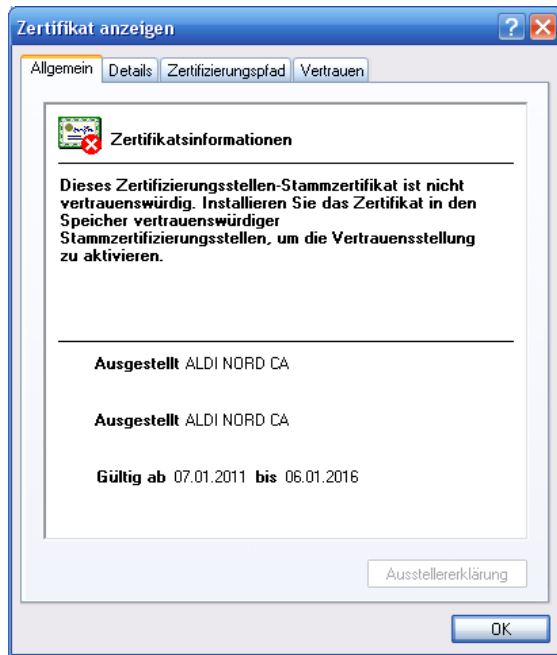


Führen Sie für Punkt 3 bitte folgende Schritte aus:

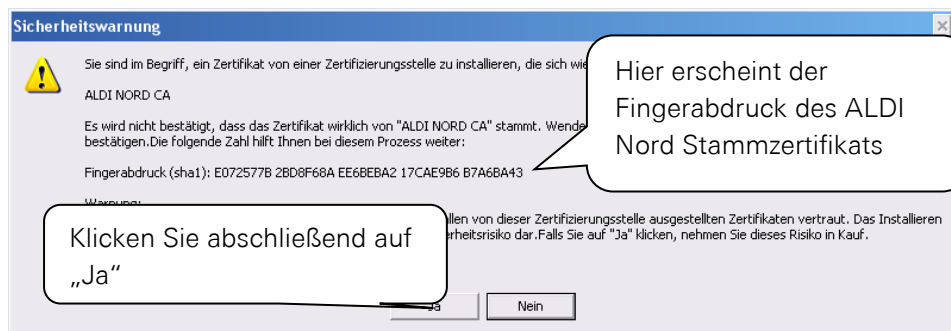
Sie verfügen bereits über ein Zertifikat von einem von ALDI Nord unterstützten Trustcenter und haben Ihren öffentlichen Schlüssel auf dem Keyserver publiziert. Anschließend hat Ihnen Ihr ALDI Nord Kommunikationspartner eine verschlüsselte E-Mail gesendet. Öffnen Sie diese E-Mail mittels Doppelklick.



Sie können sich das Zertifikat durch einen Klick auf „Details“ auch anzeigen lassen.



Vor der Installation wird eine Sicherheitswarnung angezeigt.



Nachdem Sie das Stammzertifikat installiert haben ist alles zur verschlüsselten Kommunikation vorbereitet. Sie können nun mit ALDI-Nord verschlüsselt kommunizieren.

5. Alternatives Vorgehen zum Erhalt und zur Bereitstellung von Zertifikaten

In Kapitel 2 wurde die Einrichtung der Zertifikate zur verschlüsselten E-Mail-Kommunikation beschrieben. Hierbei wurden die folgenden Annahmen getroffen:

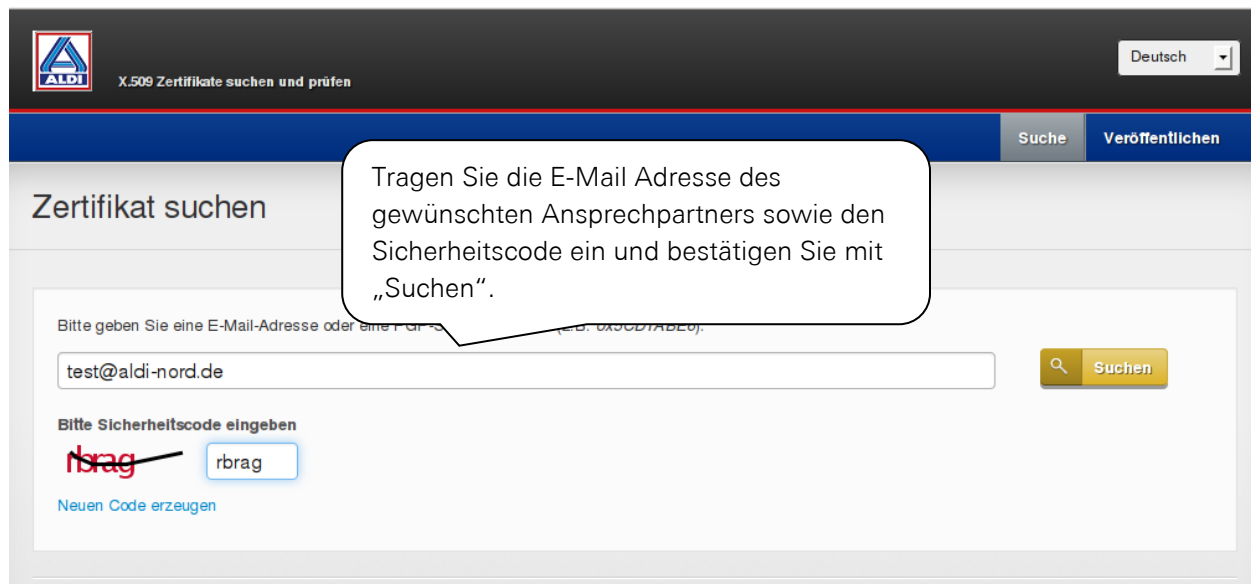
- Es wurde ein geeignetes Zertifikat erworben, und auf dem Trustcenter zur Verfügung gestellt.
- Es liegt eine verschlüsselte E-Mail eines Kontaktpartners der ALDI Unternehmensgruppe vor, welche die benötigten Zertifikate zur Verschlüsselung an den Kontaktpartner im Anhang enthält.

Dieses Kapitel beschreibt zwei alternative Vorgehensweisen zur Durchführung des Schlüsselaustauschs über das ALDI Zertifikatsportal (www.aldi-nord.de/certportal).

5.1. Herunterladen des Zertifikats eines Kontaktpartners

Sofern zur E-Mail-Verschlüsselung das öffentliche Zertifikat eines Mitarbeiters der ALDI Nord unternehmensgruppe benötigt wird, kann dieses über das ALDI Zertifikatsportal abgerufen werden.

Rufen Sie die Internetseite www.aldi-nord.de/certportal auf.



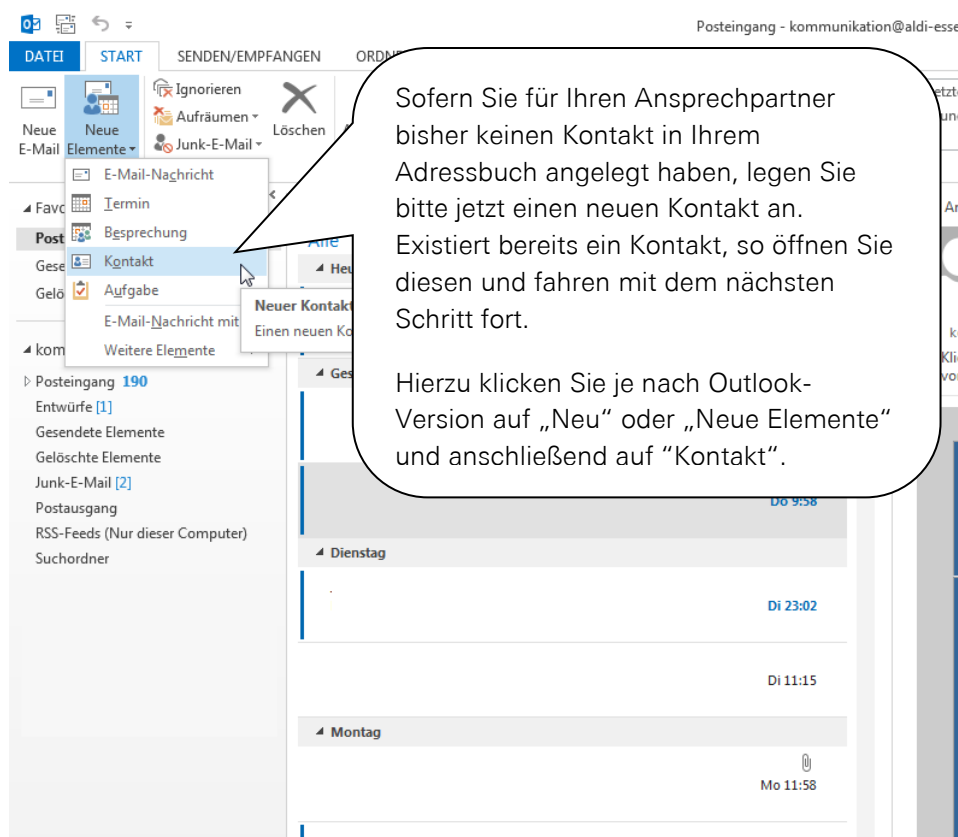
Gültige Zertifikate	
  X.509	test@aldi-nord.de gültig ab 2013-12-05 bis 2023-12-03
Besitzer	test@aldi-nord.de
Herausgegeben von	ALDI NORD CA ALDI NORD CA
Signaturalgorithmus	SHA1WithRSAEncryption
Algorithmus (Schlüssellänge)	RSA (2048 bits)
Fingerabdruck (SHA1)	4C:31:6E:64:CE:4B:81:88:E9:7B:C9:51:F...
Seriennummer	07:72:72:C6:C4:32:65:BD:8E:73:44:8E:57:A5:F1:B1:DB:44:B1:22
Schlüsselbenutzung	Datenverschlüsselung, Schlüsselvereinbarung, Schlüsselverschlüsselung
Gültig ab	2013-12-05
Gültig bis	2023-12-03

Unter Umständen werden für eine E-Mail-Adresse mehrere Zertifikate angezeigt. Daher ist der Bereich Schlüsselbenutzung vor dem Herunterladen zu prüfen. Damit ein Zertifikat zur

Verschlüsselung genutzt werden kann, muss unter Schlüsselbenutzung der Eintrag „Datenverschlüsselung“ aufgeführt werden.

5.2. Heruntergeladenes Zertifikat einem Outlook Kontakt hinzufügen

Nachfolgend wird beschrieben, wie Sie ein über die Internetseite www.aldi-nord.de/certportal erhaltenes öffentliches Zertifikat Ihres ALDI Kontaktpartners zur Verschlüsselung einrichten. Dieser Schritt weicht von den in Punkt 2.5 beschriebenen Schritten ab, da hier keine (signierte) E-Mail durch den ALDI-Ansprechpartner benötigt wird.



Posteingang - kommunikation@aldi-esse

DATEI START SENDEN/EMPFANGEN ORD...

Neue E-Mail Elemente

E-Mail-Nachricht

Aktionen

Ignorieren

Aufräumen

Junk-E-Mail

Löschen

Besprechung

Kontakt

Aufgabe

E-Mail-Nachricht mit

Weitere Elemente

Neuer Kontakt

Einen neuen Ko...

Posteingang 190

Entwürfe [1]

Gesendete Elemente

Gelöschte Elemente

Junk-E-Mail [2]

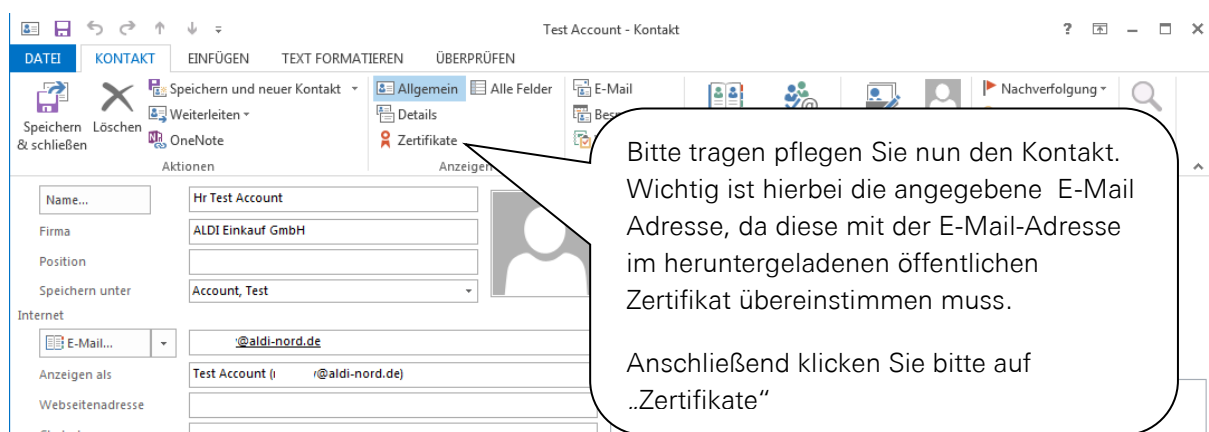
Postausgang

RSS-Feeds (Nur dieser Computer)

Suchordner

Sofern Sie für Ihren Ansprechpartner bisher keinen Kontakt in Ihrem Adressbuch angelegt haben, legen Sie bitte jetzt einen neuen Kontakt an. Existiert bereits ein Kontakt, so öffnen Sie diesen und fahren mit dem nächsten Schritt fort.

Hierzu klicken Sie je nach Outlook-Version auf „Neu“ oder „Neue Elemente“ und anschließend auf „Kontakt“.



Test Account - Kontakt

DATEI KONTAKT EINFÜGEN TEXT FORMATIEREN ÜBERPRÜFEN

Speichern und neuer Kontakt

Speichern & schließen

Löschen

Weiterleiten

OneNote

Aktionen

Anzeigen

Name... Hr Test Account

Firma ALDI Einkauf GmbH

Position

Speichern unter Account, Test

Internet

E-Mail... @aldi-nord.de

Anzeigen als Test Account (i @aldi-nord.de)

Webseitenadresse

Chatadresse

Alle Felder

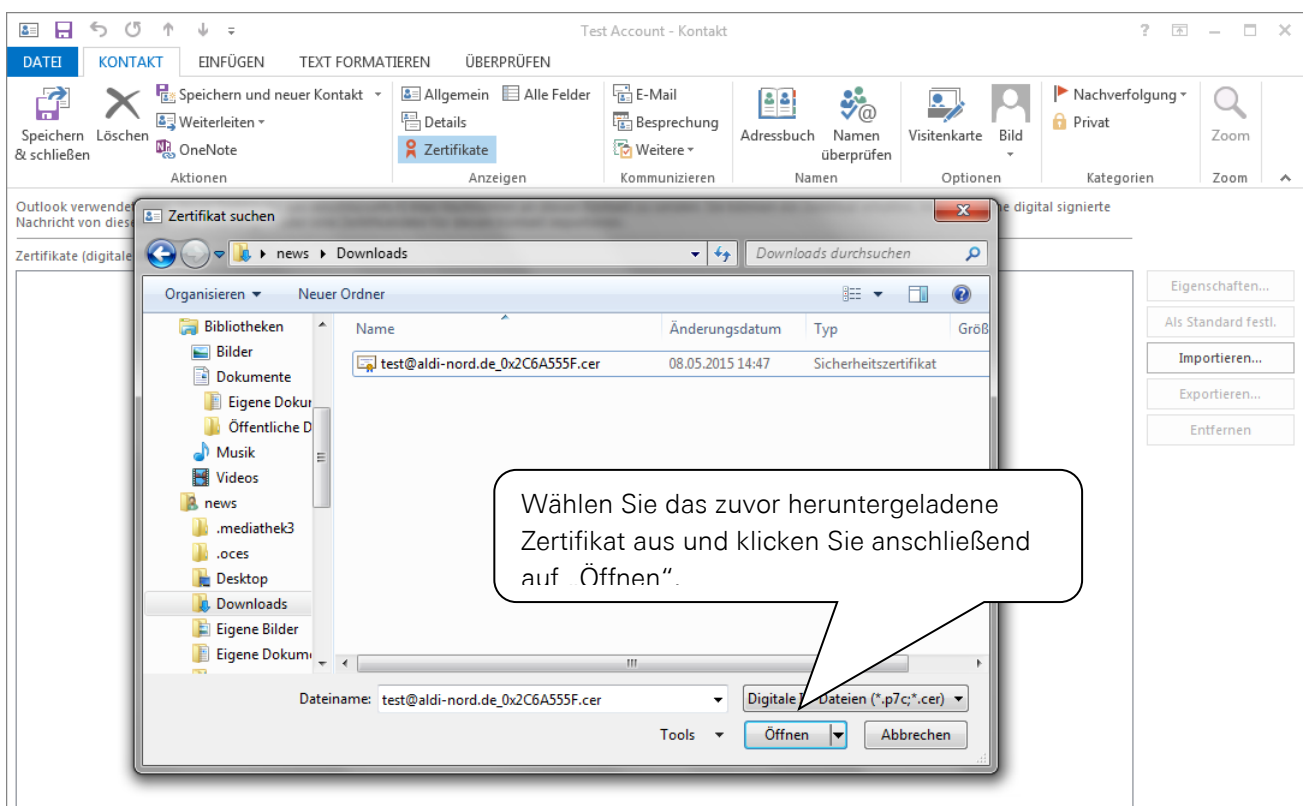
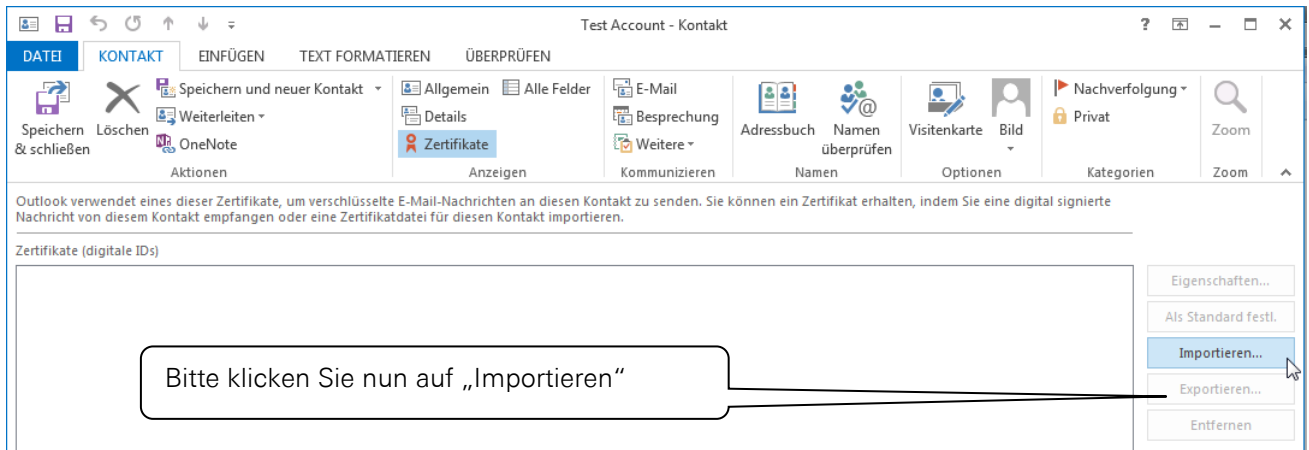
Details

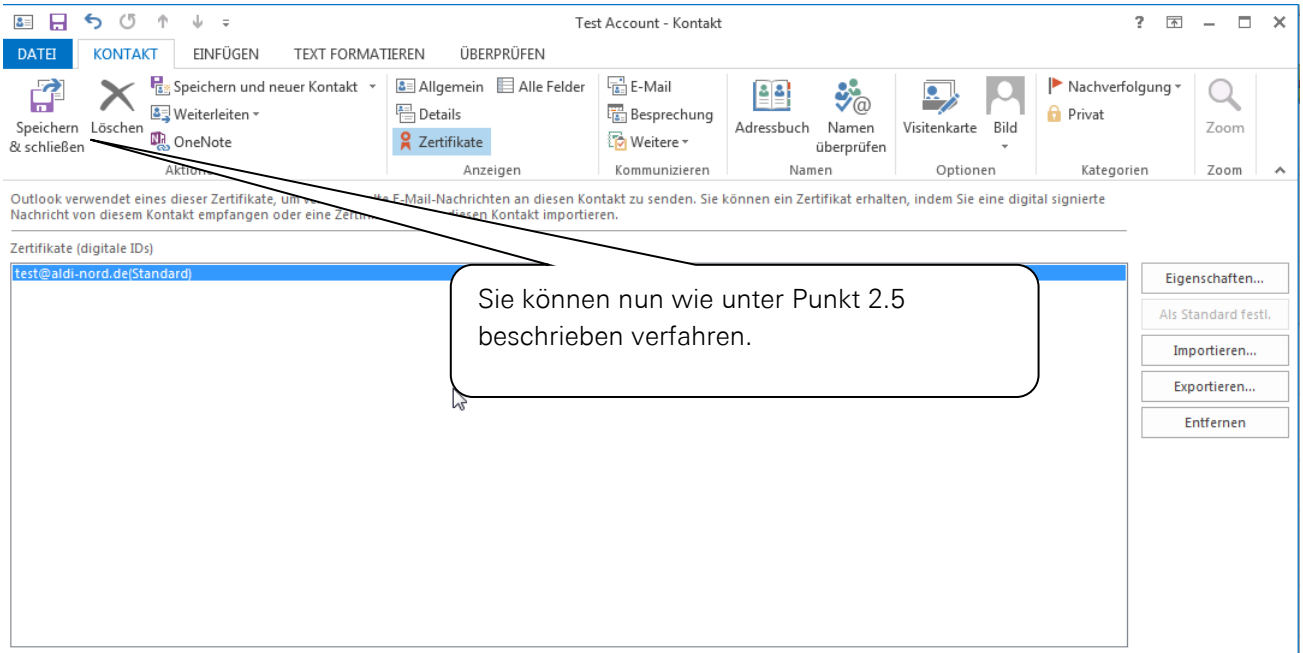
Zertifikate

Nachverfolgung

Bitte tragen pflegen Sie nun den Kontakt. Wichtig ist hierbei die angegebene E-Mail Adresse, da diese mit der E-Mail-Adresse im heruntergeladenen öffentlichen Zertifikat übereinstimmen muss.

Anschließend klicken Sie bitte auf „Zertifikate“

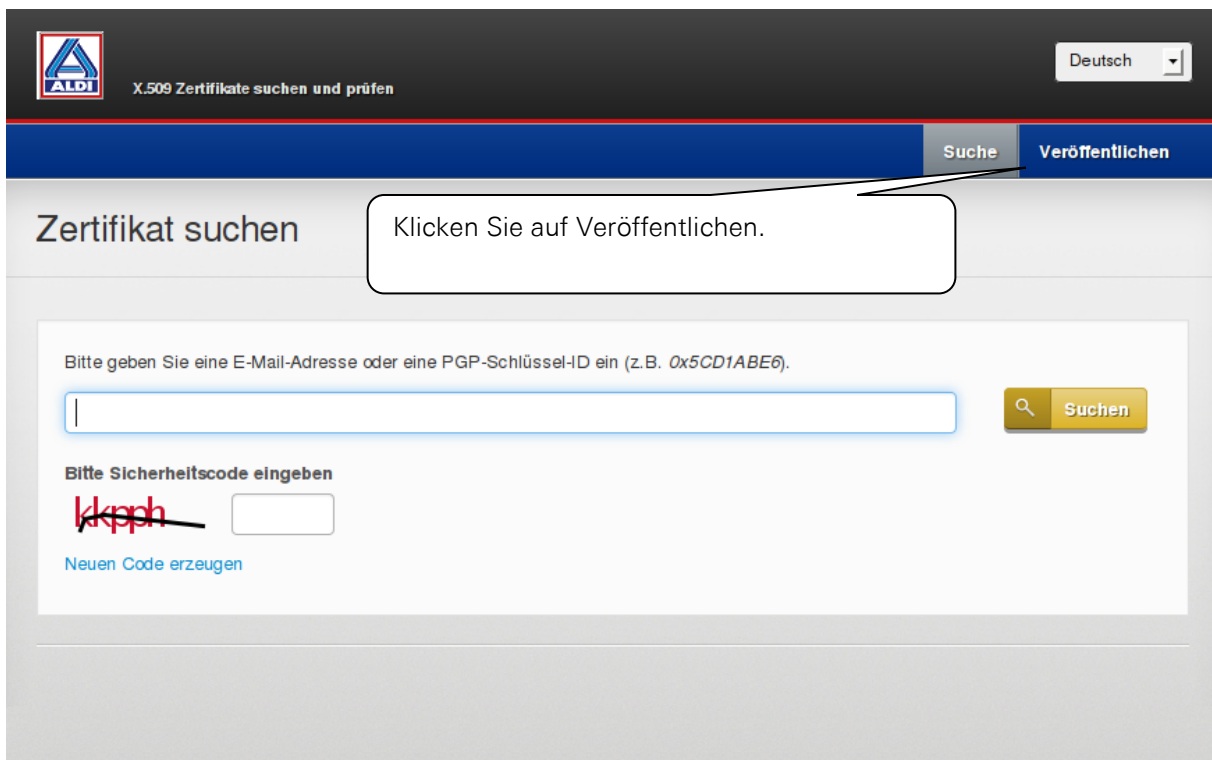




5.3. Bereitstellung von eigenen Zertifikaten

Sofern Sie bereits Zertifikate zur E-Mail-Verschlüsselung mittels S/MIME nutzen, diese jedoch nicht auf den unterstützten Trustcentern zur Verfügung stehen, besteht die Möglichkeit diese Zertifikate über das ALDI Zertifikatsportal bereitzustellen.

Rufen Sie die Internetseite www.aldi-nord.de/certportal auf.





Klicken Sie auf Benutzerzertifikat und tragen Sie Ihre Daten ein. Anschließend bestätigen Sie mit „Übermitteln“.

Zertifikat veröffentlichen

Benutzer-Zertifikat | Domain-Zertifikat | CA-Zertifikat

Übermitteln Sie ein **X.509**-Benutzer-Zertifikat oder einen öffentlichen **PGP**-Benutzer-Schlüssel. Die Veröffentlichung erfolgt ggf. nach Prüfung und Freigabe.

Ihr Name:

Organisation:

Ihre E-Mail-Adresse*:

Telefon*:

Zertifikatsdatei*:

Die unterstützten Formate sind ASC, PEM, DER und CER

Bitte Sicherheitscode eingeben*:

*Pflichtfeld

Als abschließenden Schritt wenden Sie sich bitte an Ihren ALDI Ansprechpartner, damit dieser Ihr Zertifikat intern zur Nutzung freigeben kann.