Einrichtung der Verschlüsselung für Signaturportal

Verschlüsselung wird mit Hilfe von sogenannten Zertifikaten erreicht. Diese ermöglichen eine sichere Kommunikation zwischen Ihnen und dem Signaturportal. Benutzen sie für die Installation bitte ausschließlich den **Windows Internet Explorer**.

Vorab: Anlegen eines Users mit Hilfe der Empfängerbetreuung

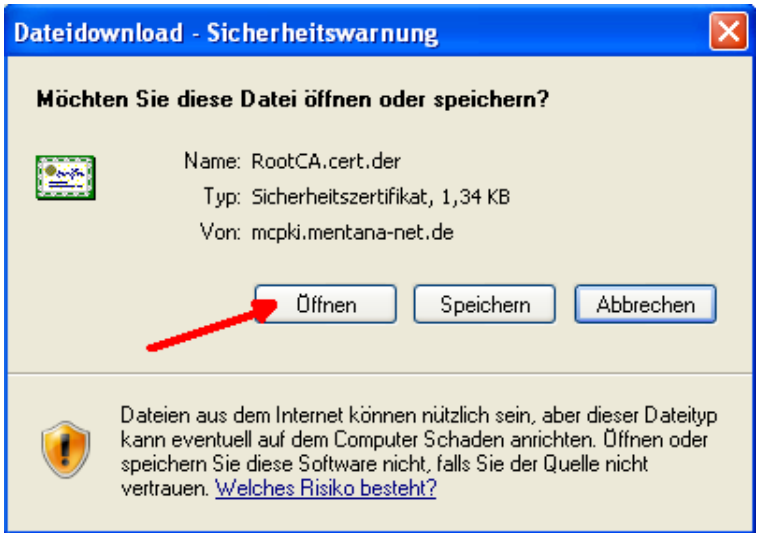
1. Loggen Sie sich in ihr Signaturportal ein.
2. Überprüfen Sie unter Einstellungen/Postfach/Rechnungsausgang/Empfängerverifikation ob Sie den Punkt „Empfänger Verifikationsprotokoll übersenden“ aktiviert haben.
3. Nun müssen Sie dem Empfänger, mit dem Sie verschlüsselt kommunizieren wollen, über ihr Sigmail-Postfach eine Email schicken. Fügen Sie dazu eine Testrechnung bei, die noch unverschlüsselt übertragen werde kann er.
4. Die Empfängerbetreuung legt automatisch für jede (unbekannte) Emailadresse ein neues Postfach im Signaturportal an.
5. Ihr Empfänger bekommt vom System die Zugangsdaten übermittelt.
6. Ihr Empfänger muss sich einloggen und seine Daten ergänzen, damit eine Verschlüsselungszertifikat erstellt werden darf.
7. Wenn Ihr Empfänger den Login bestätigt kann es losgehen, und er ist im LDAP eingetragen.

Anleitung Schritt für Schritt

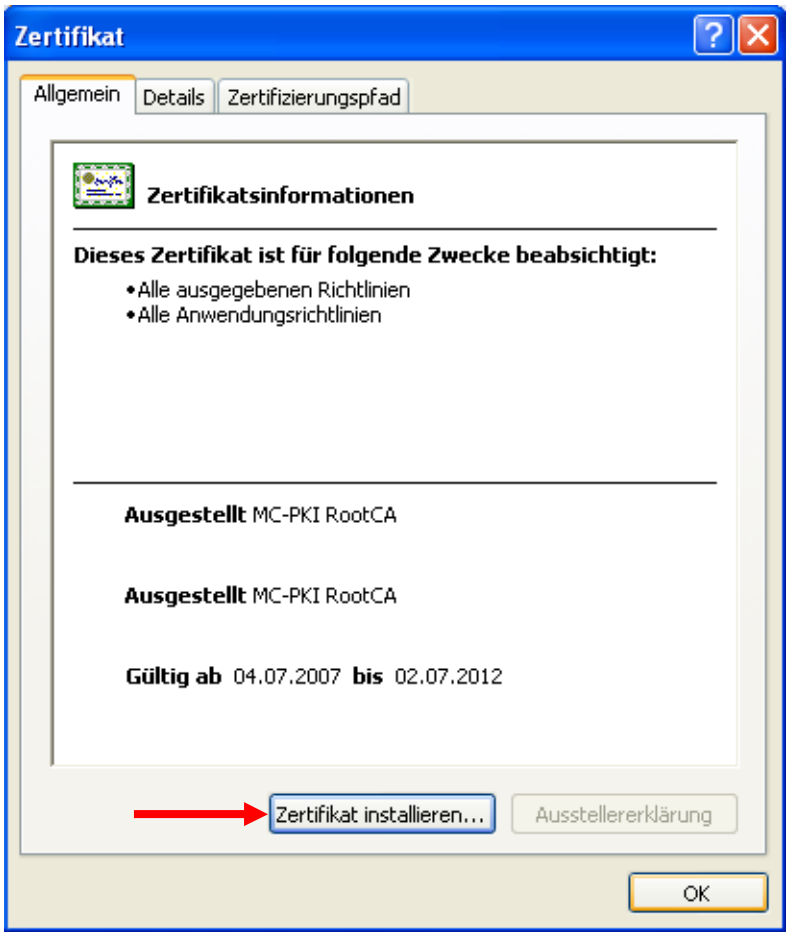
Schritt 1: Installation der Root-Zertifikate

8. Loggen Sie sich auf ihrem Signaturportal ein. Im „Adressbuch“ finden sie den Kartenreiter „PKI“ und den Unterpunkt „Root-Zertifikate“. Klicken sie auf den Link „Zertifikat RootCA installieren“, um die Installation des ersten Zertifikats zu beginnen.

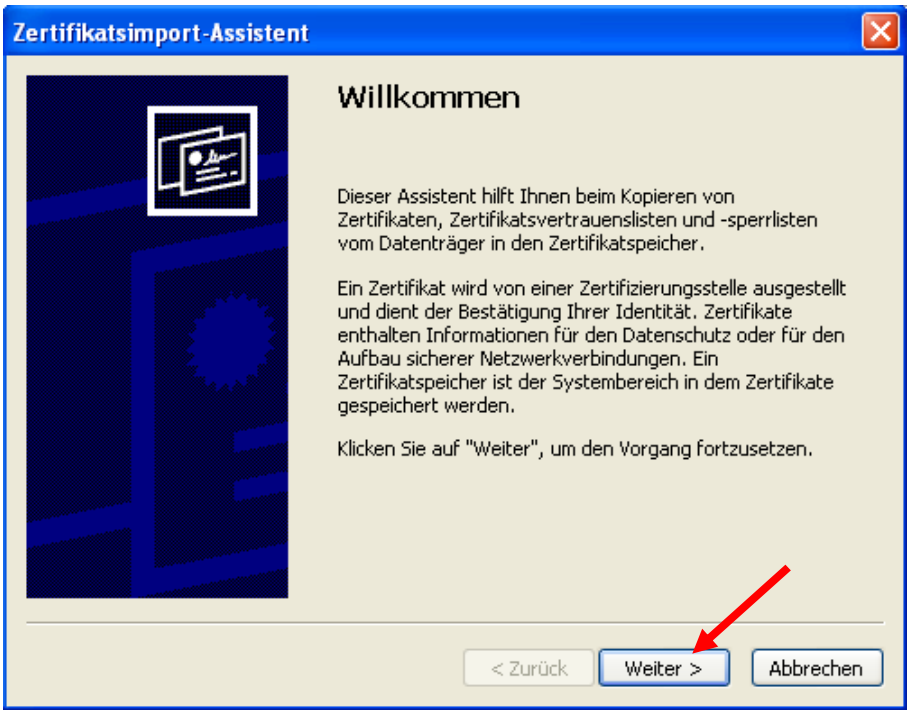
9. Das folgende Fenster (siehe Abbildung) öffnet sich, bestätigen Sie den Download indem sie „Öffnen“ betätigen.



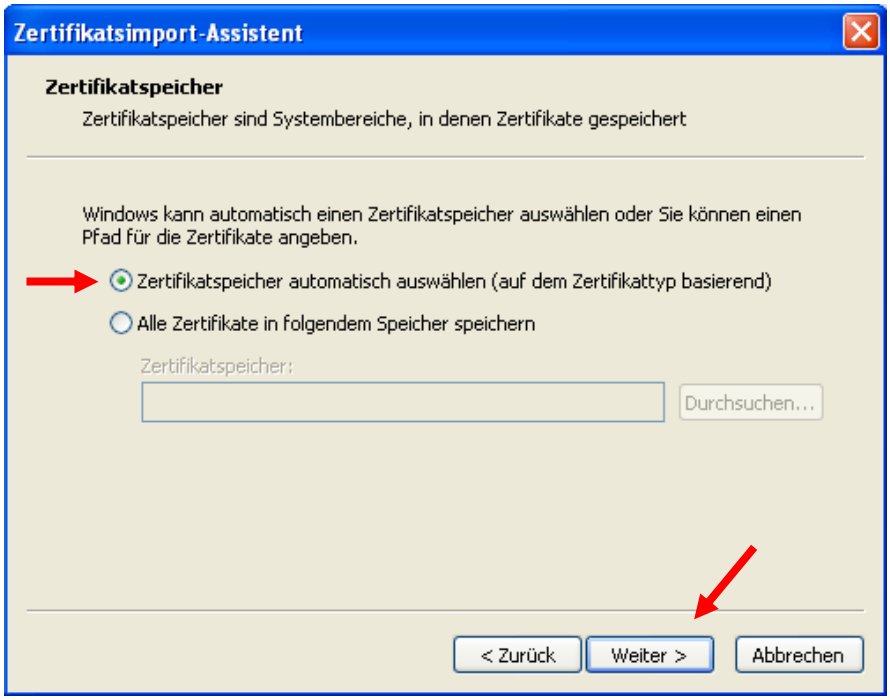
10. Im Fenster „Zertifikat“ bestätigen Sie die Installation indem Sie „Zertifikat installieren“ betätigen.



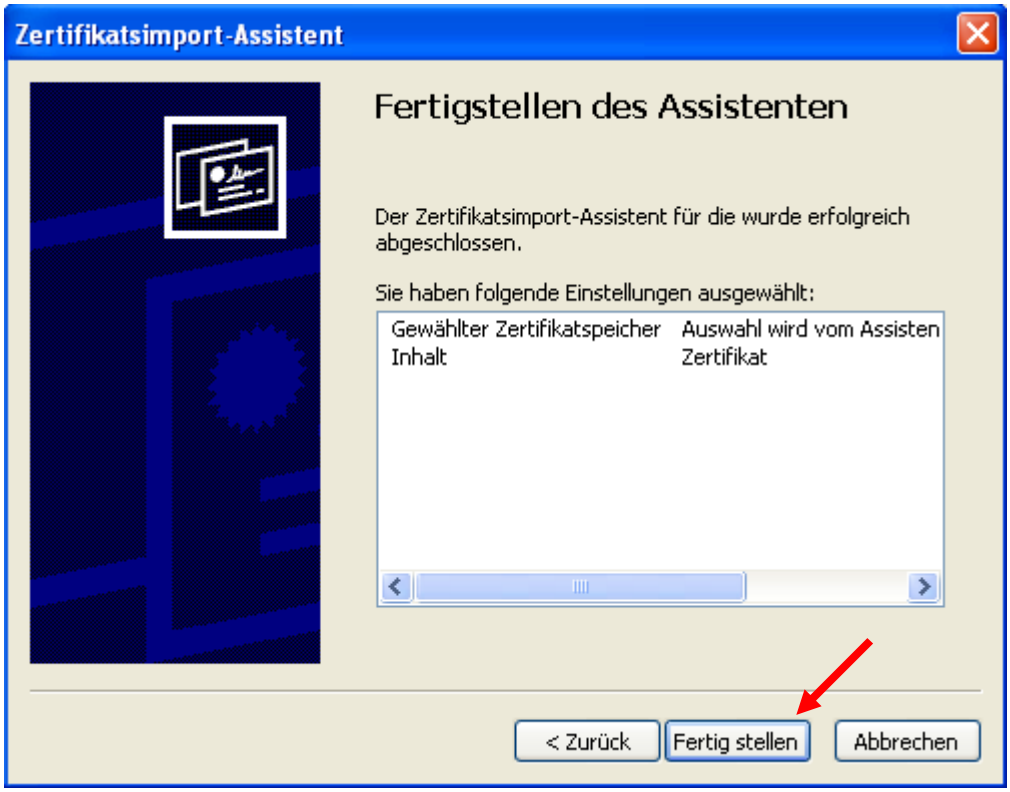
11. Bestätigen Sie im „Zertifikatsimport-Assistent“ das Willkommensfenster mit „Weiter“.



12. Im folgenden Fenster wird nach dem Speicherort des Zertifikats gefragt. Wählen sie den Punkt „Zertifikatsspeicher automatisch auswählen (auf den Zertifikattyp basierend)“ aus, und bestätigen Sie mit „Weiter“.



13. Schließen Sie die Installation im folgenden Fenster ab, indem Sie „Fertig stellen“ drücken.



WICHTIG: Um verschlüsselte Nachrichten problemlos Empfangen und versenden zu können führen Sie die vorbeschriebenen Schritte 1 bis 6 für folgende Root-Zertifikate durch.

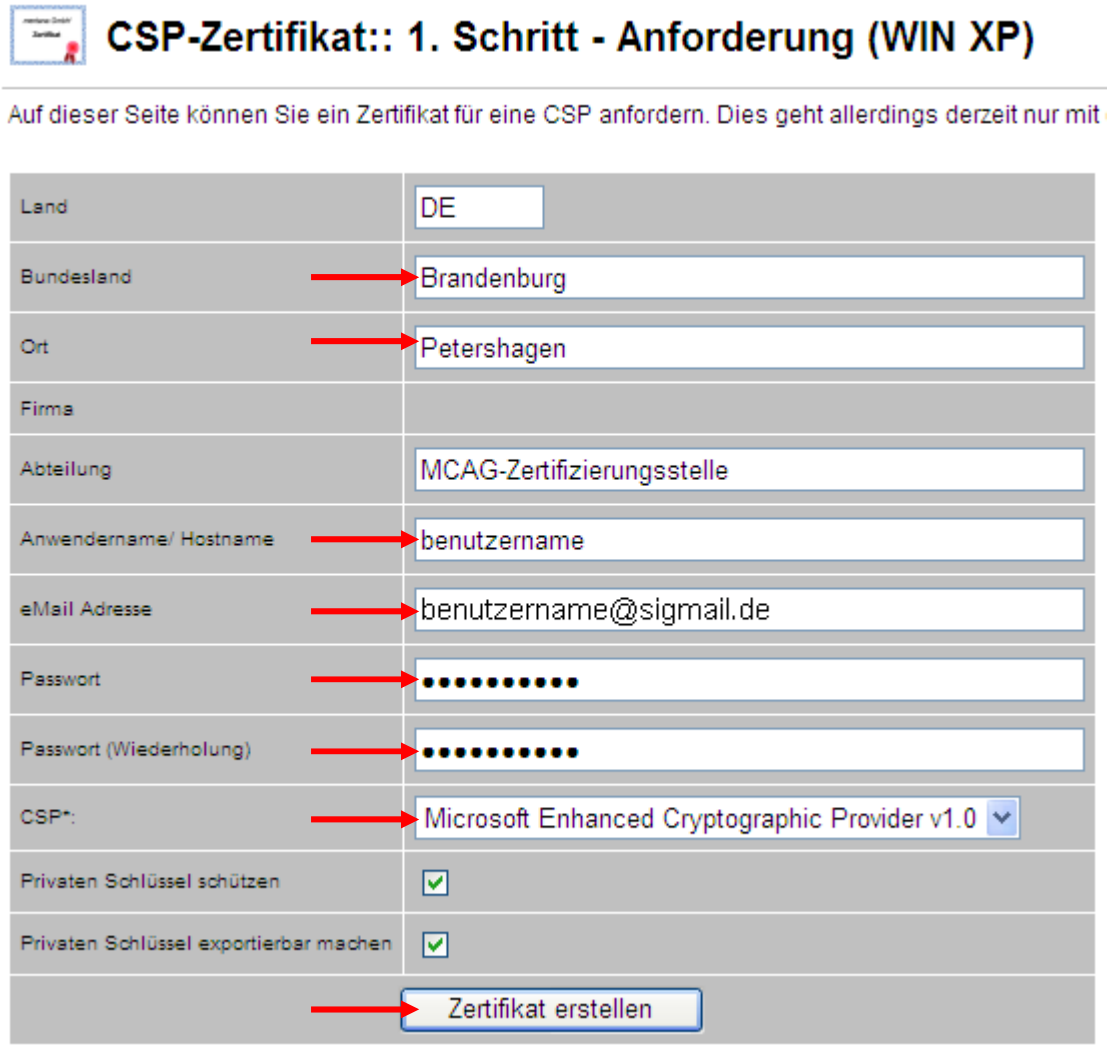
- **RootCA**
- **Signaturportal_UserCA**
- **OCSPCA**
- **Class1-CA**

Die Root-Zertifikate finden sie im Adressbuch Kartenreiter „PKI“ Unterpunkt Root-Zertifikate (siehe Punkt 1). Die Installation der weiteren Zertifikate ist optional möglich um auch Empfänger dieser Domains zu erreichen.

Damit ist die Installation der Root-Zertifikate (Schritt 1) abgeschlossen.

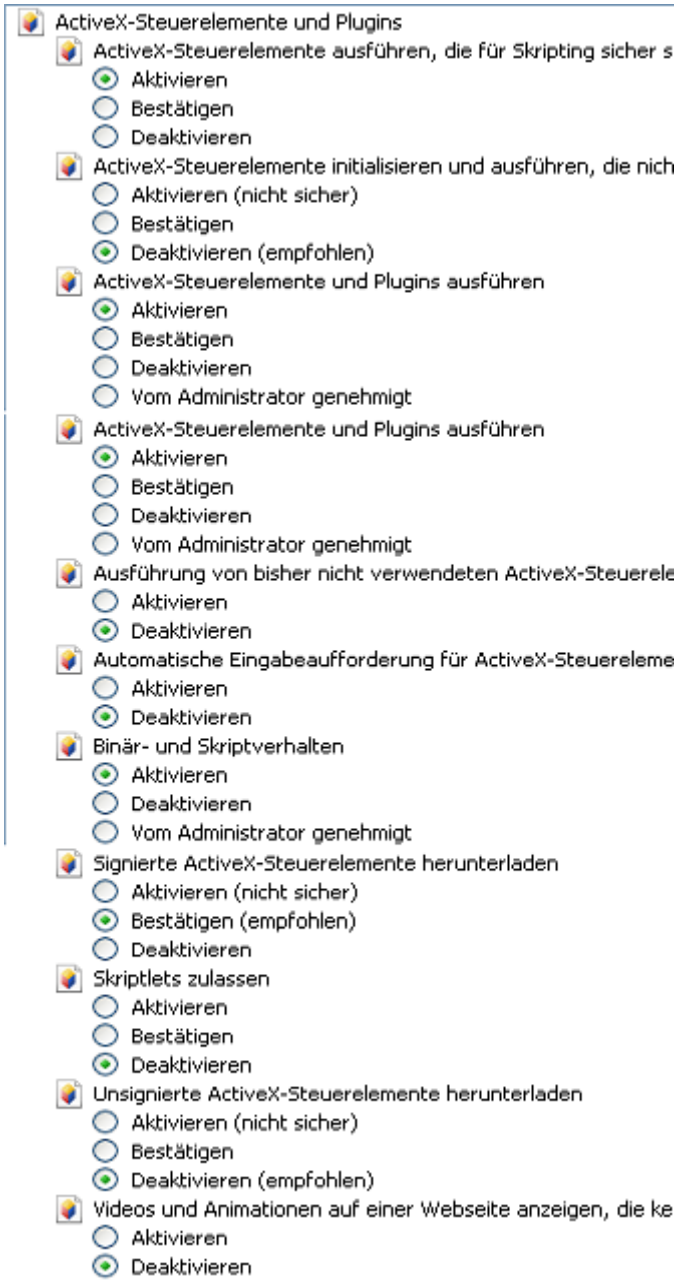
Schritt 2: Erstellung eines eigenen E-Mail- Zertifikates für die Verschlüsselung

14. Als nächster Schritt muss ein E-Mail- Zertifikat für Sie erzeugt werden. Öffnen Sie dazu den Menüpunkt „Adressbuch“/ Kartenreiter „PKI“ / „E-Mail-Zertifikat“. Füllen Sie die Felder Bundesland, Ort und Passwort entsprechend aus. Wählen Sie in der Auswahlbox „CSP“ den **„Microsoft Enhanced Cryptographic Provider v1.0“.** Prüfen Sie ihre Angaben nochmals (siehe Abbildung) und betätigen Sie anschließend „Zertifikat erstellen“.

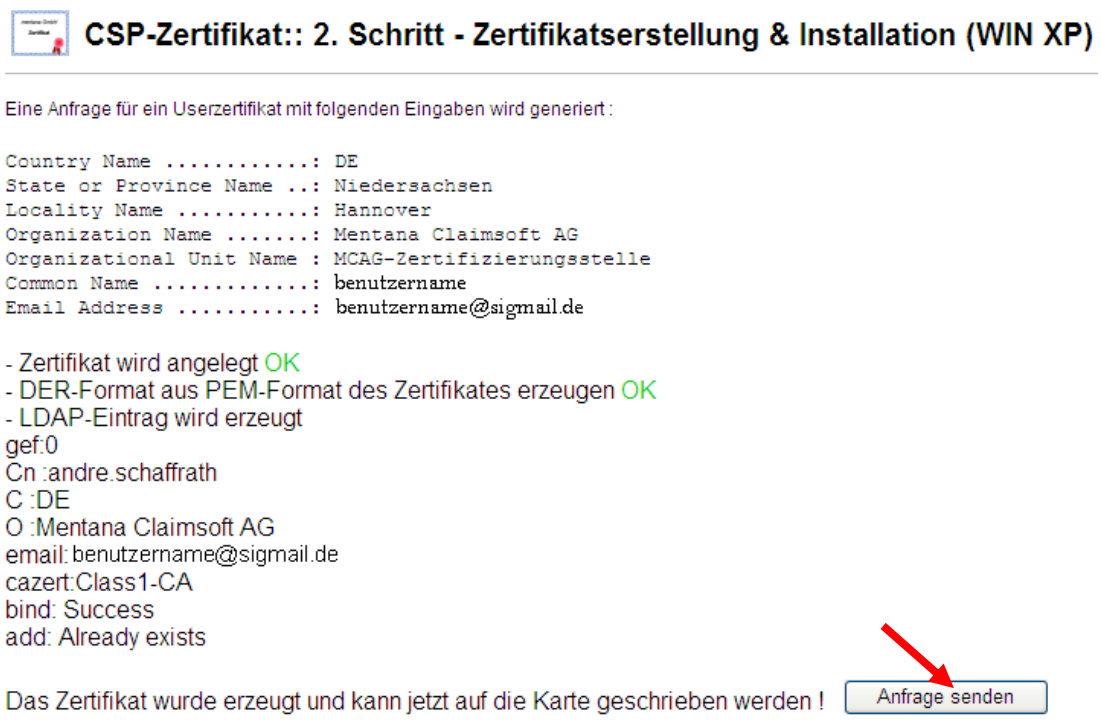


Hinweis:

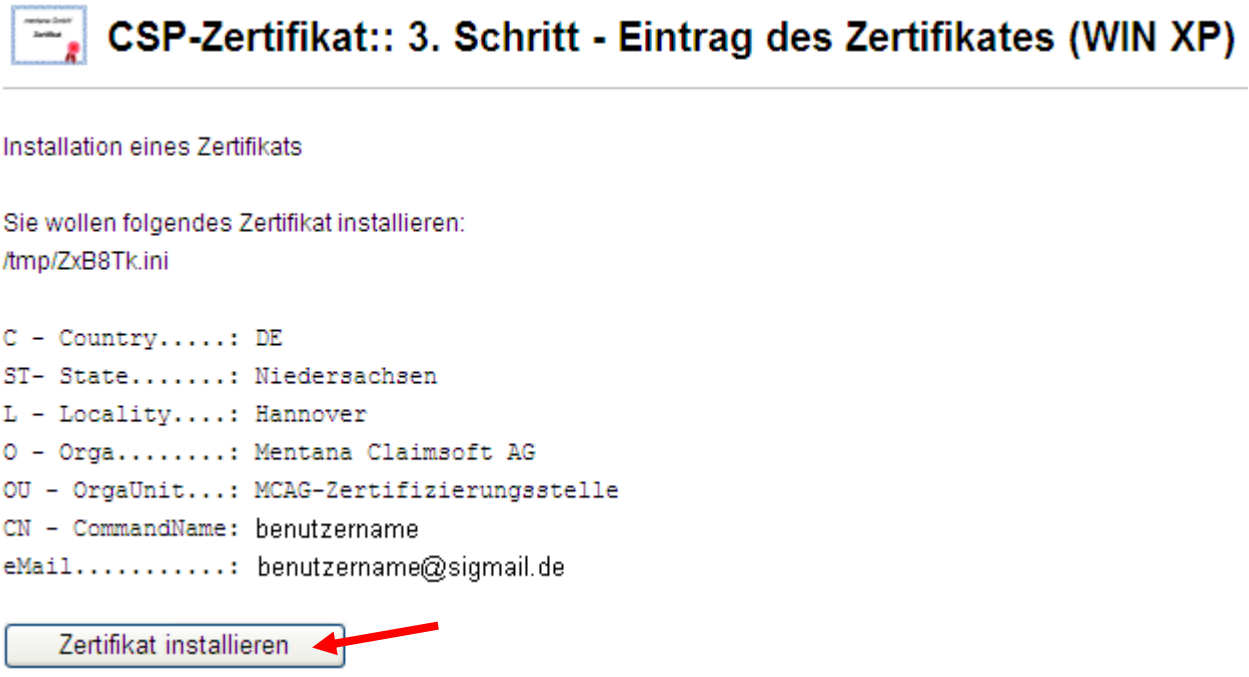
Falls Sie im Feld „CSP“ keine Auswahl treffen können, ist es notwendig, dass Sie in ihrem Browser die ActiveX-Steuerelemente zulassen. Diese Einstellungen finden Sie in ihrem Internet Explorer in dem Menüpunkt „**Extras“/ „Internetoptionen“/ Sicherheit.**. Unter der Registerkarte „Sicherheit“ können Sie die Sicherheitsstufe ihres Browsers anpassen (betätigen sie den Button „Stufe anpassen“). Ihre Einstellungen sollten wie folgt aussehen:



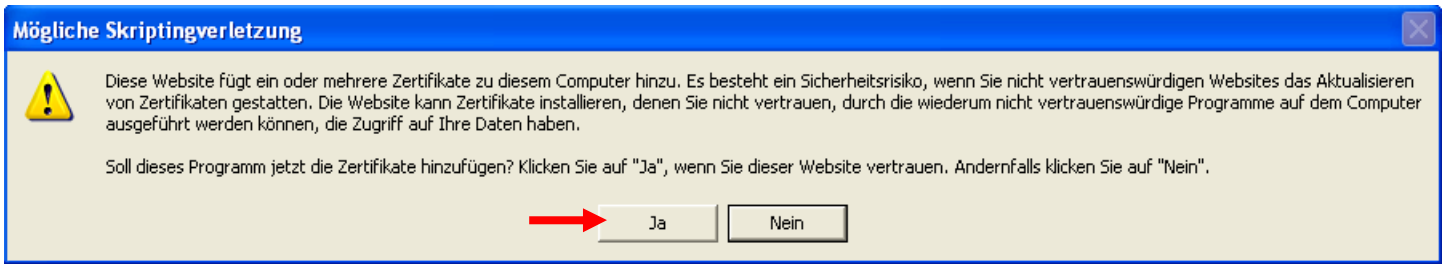
15. Ein neues Fenster öffnet sich, bitte überprüfen Sie hier noch einmal ihre Daten. Bestätigen Sie die Anfrage dann indem Sie „Anfrage senden“ betätigen.



16. Nun wird ihr Zertifikat erstellt, nach wenigen Sekunden sollten Sie folgendes sehen (siehe Abbildung). Betätigen sie „Zertifikat installieren“.



17. Je nach Einstellung ihrer Sicherheitsoptionen erhalten Sie nun eine Warnung. Bestätigen Sie diese mit „ja“.

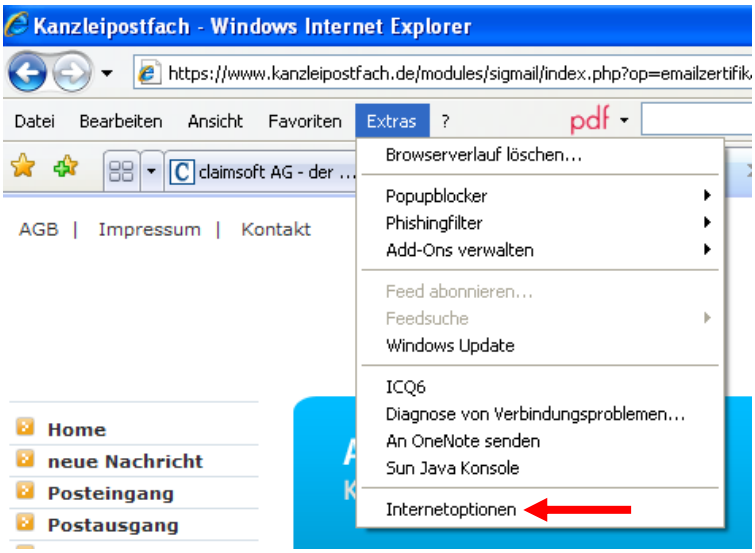


18. Anschließend werden Sie über die erfolgreiche Installation informiert. Klicken sie auf „OK“.

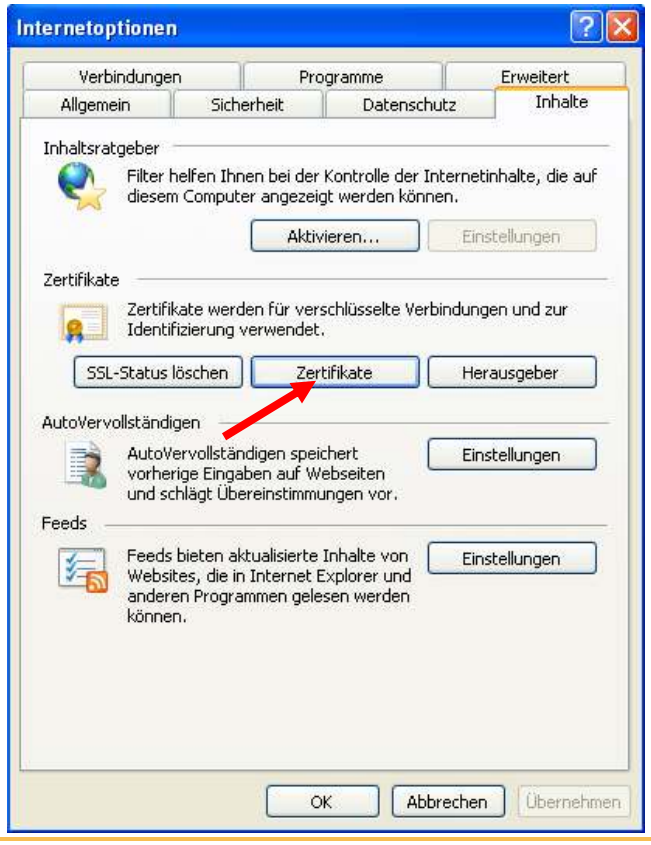
Das Zertifikat ist nun erstellt und kann im nächsten Schritt exportiert werden.

Schritt 3: Export des erstellten Zertifikats

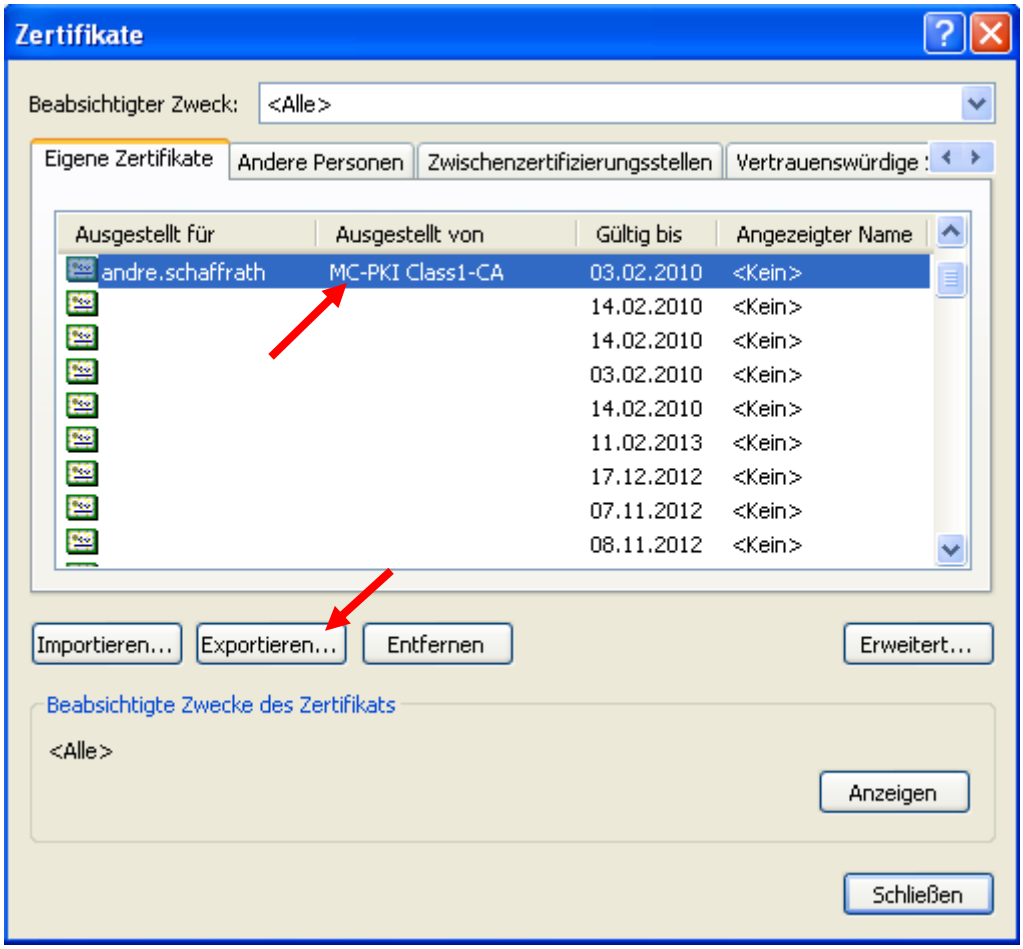
19. Das installierte Zertifikat muss nun aus dem Internet Explorer exportiert werden, um es anschließend im Outlook verwenden zu können. Unter „Extras“ finden Sie die „Internetoptionen“ ihres Internet Explorers.



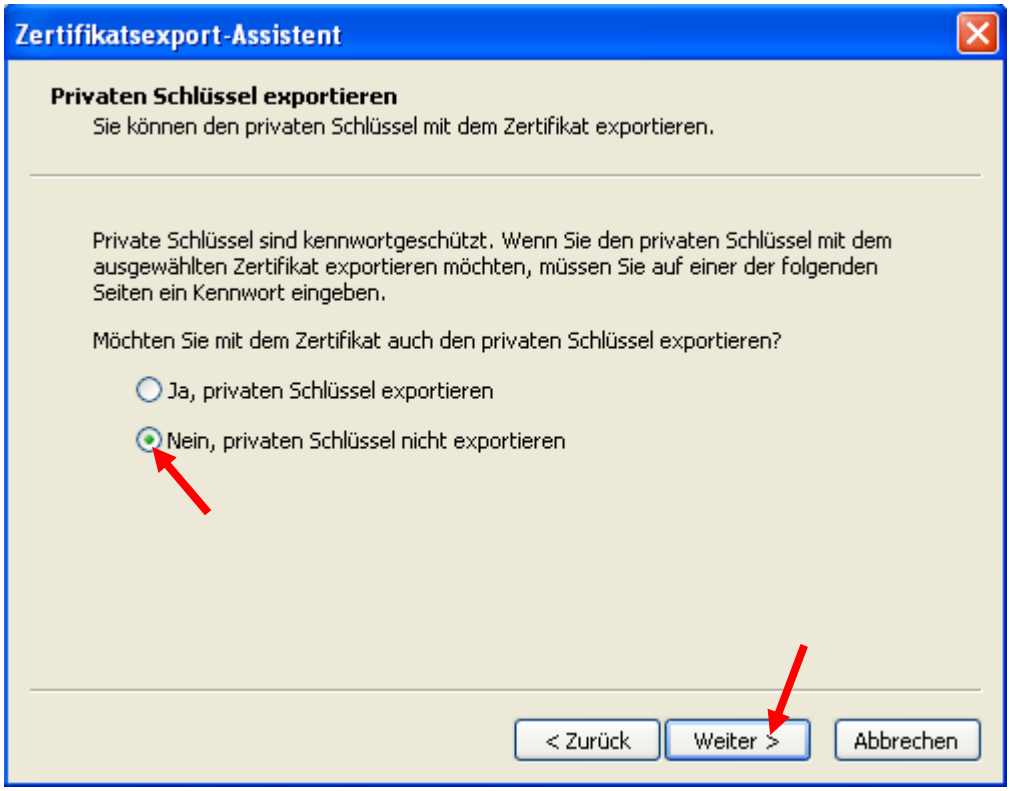
20. Öffnen sie nun den Kartenreiter „Inhalte“.
    Um sich ihre Zertifikate anzusehen, betätigen sie „Zertifikate“.



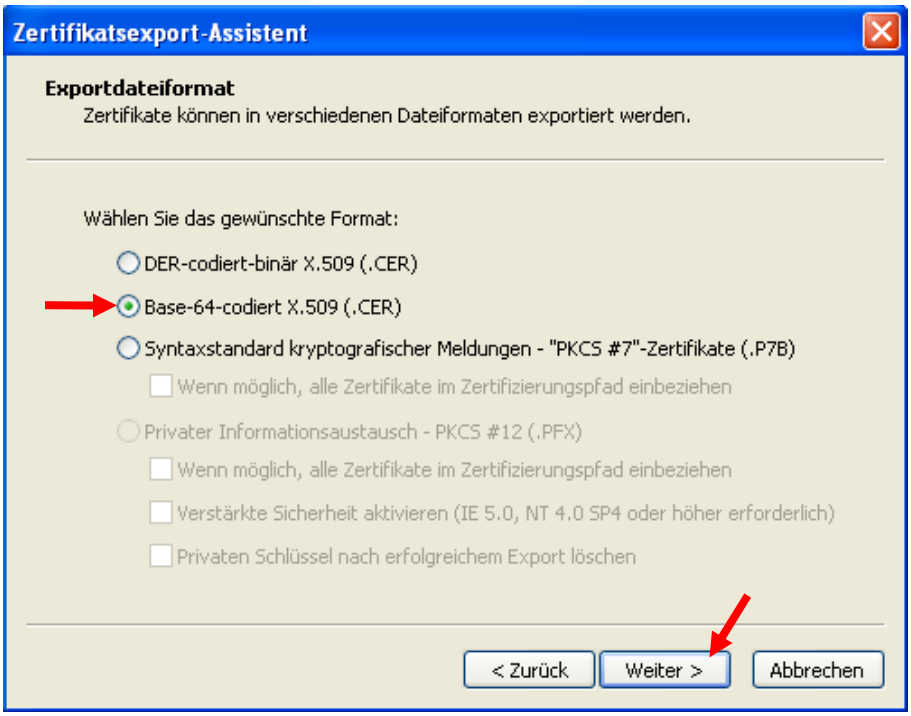
21. Suchen Sie sich aus der folgenden Liste ihr erstelltes Zertifikat heraus. Achten Sie auf den richtigen Namen (Ausgestellt für), sowie den richtigen Aussteller (MC-PKI Class1-CA). Betätigen Sie anschließend „Exportieren“.



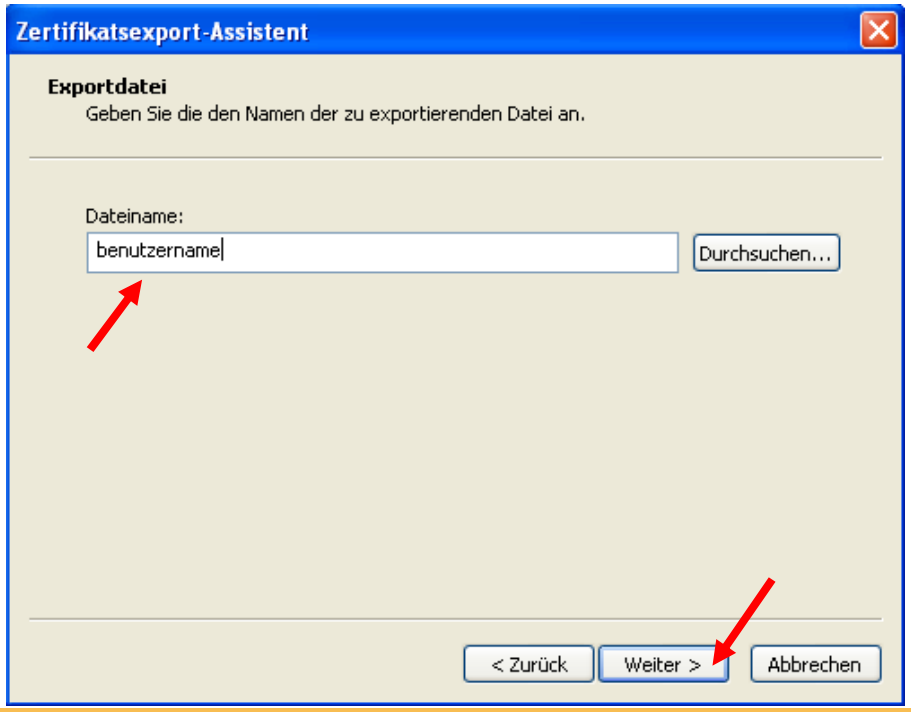
22. Es öffnet sich der Zertifikatsexport-Assistent. Das Willkommensfenster bestätigen Sie indem Sie „Weiter“ drücken. Im nächsten Fenster werden Sie gefragt ob sie ihren privaten Schlüssel exportieren möchten. Wählen Sie „Nein, privaten Schlüssel nicht exportieren“, und bestätigen Sie anschließend ihre Wahl mit „Weiter“.



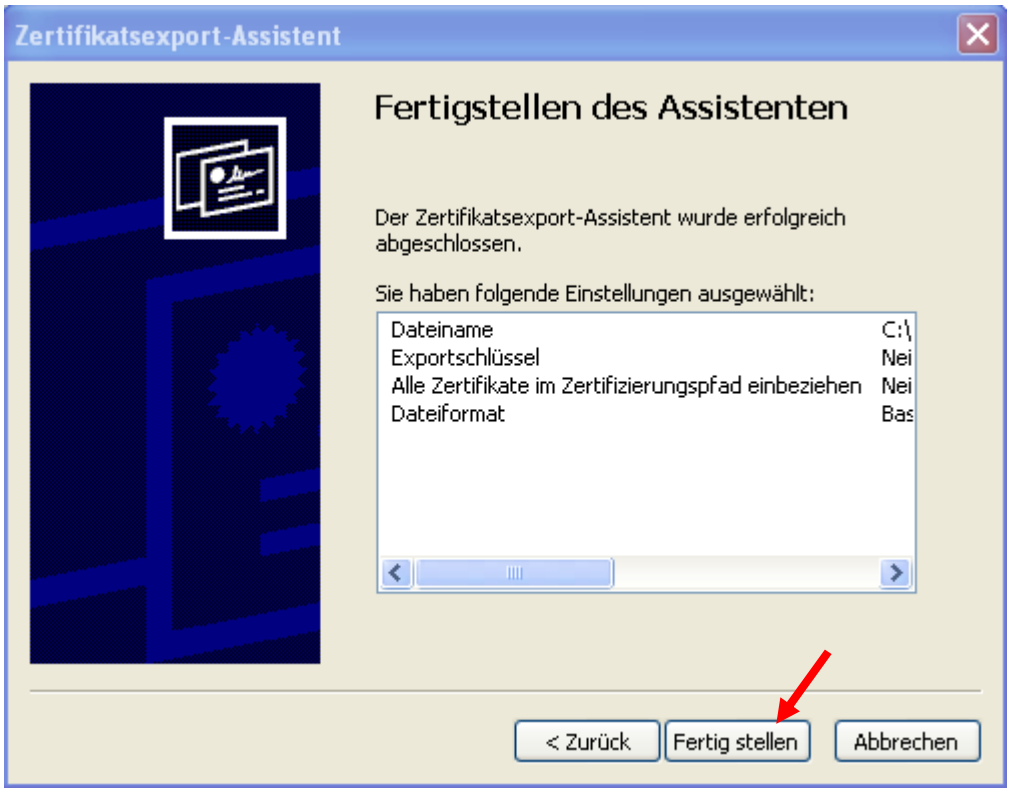
23. Im folgenden Fenster müssen Sie das Dateiformat festlegen, mit welchem das Zertifikat exportiert werden soll. Wählen Sie hier „Base-64-codiert X.509 (.CER)“ aus und bestätigen Sie ihre Auswahl mit „Weiter“.



24. Nun werden Sie aufgefordert einen Namen für die zu exportierende Datei einzugeben. Verwenden Sie hier am besten ihren Benutzernamen aus Schritt 5, dies erleichtert die spätere Zuordnung. Bestätigen Sie ihre Eingaben mit „Weiter“.



25. Überprüfen Sie ihre Angaben im folgenden Fenster und bestätigen Sie diese durch drücken von „Fertig stellen“.



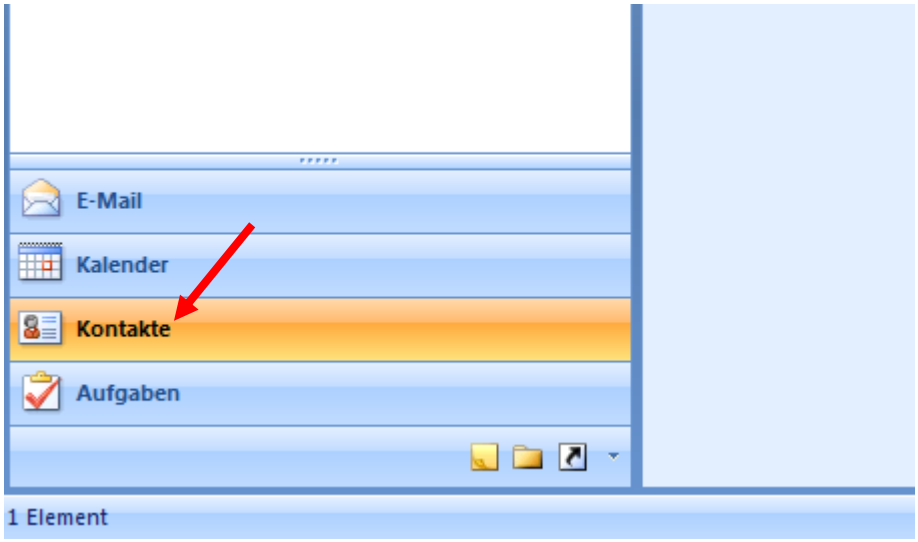
26. Sie erhalten eine Meldung wenn die Datei erfolgreich exportiert wurde.

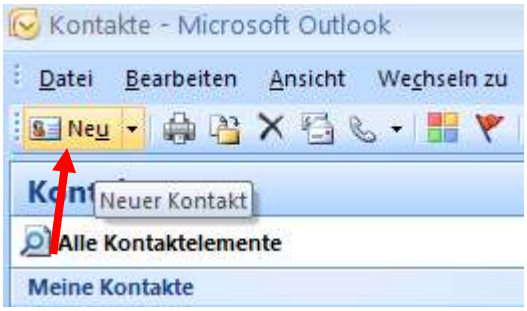
Das Zertifikat wurde erfolgreich exportiert und kann nun in Outlook eingefügt werden.

Schritt 4: Einbinden des Zertifikats in Outlook 2007

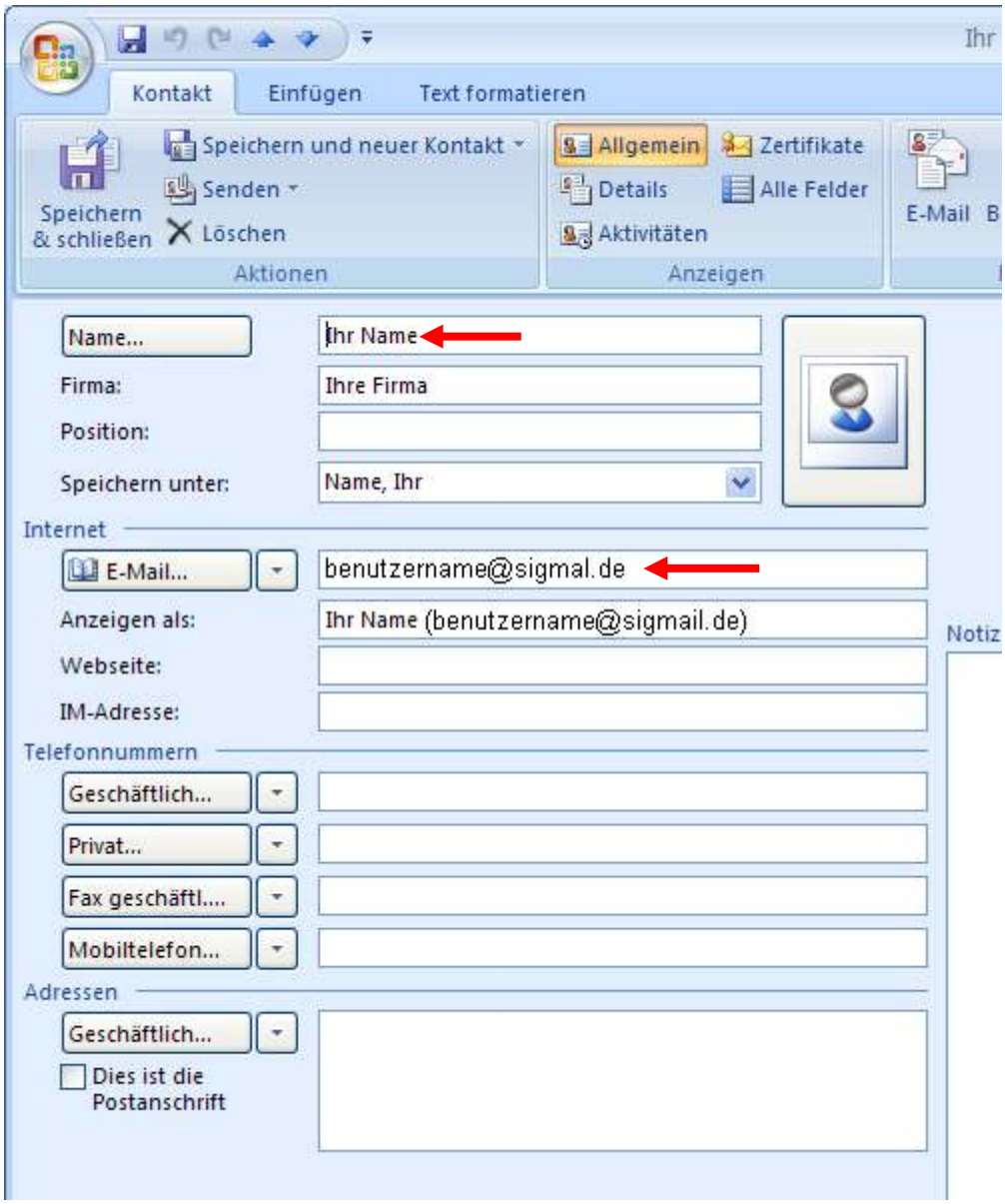
Es wird davon ausgegangen, dass Sie sich bereits ein Konto (für ihr Signaturportal) im Outlook angelegt haben, und dieses fehlerfrei funktioniert.

27. Öffnen Sie ihr Outlook 2007, und legen Sie einen neuen Kontakt an. Wählen Sie die Rubrik Kontakte und betätigen Sie den Button „Neu“.



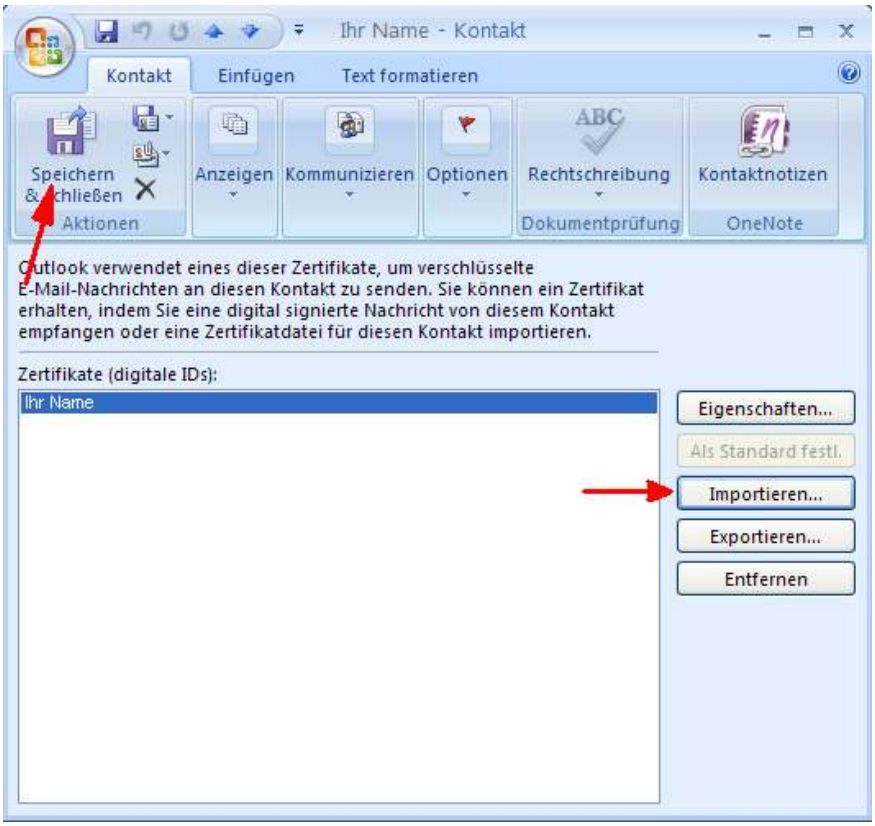


28. Geben Sie nun in den folgenden Feldern Ihre Daten ein. Achten Sie darauf, dass Sie die E-Mail-Adresse ihres Signaturportals (Benutzername@sigmail.de) in das Feld „E-Mail“ eintragen.



29. Betätigen Sie den Button für Zertifikate innerhalb ihres neu erstellten Kontakts.

30. Importieren Sie nun das von ihnen erstellte und exportierte Zertifikat. Betätigen Sie dafür „Importieren“, und wählen Sie Ihr Zertifikat aus. Bestätigen Sie ihre Auswahl, und speichern Sie anschließend die Kontaktdaten (betätigen Sie dazu „Speichern & Schließen“).



31. Schließen Sie nun ihr Outlook (dadurch werden die neuen Daten übernommen).

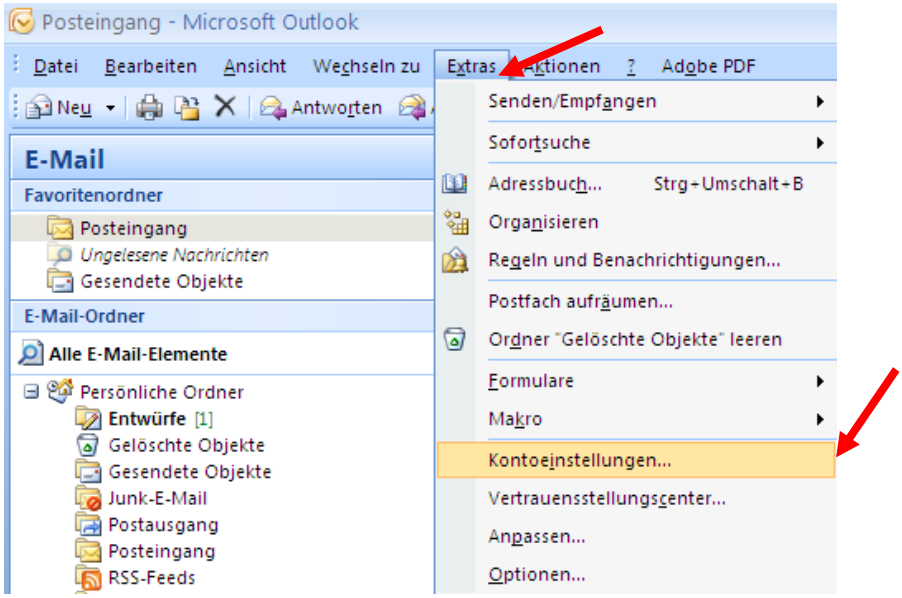
Mit dem Neustart von Outlook ist die Vorbereitung für die Verschlüsselung abgeschlossen.

Schritt 5: Einrichten eines LDAP-Adressbuches

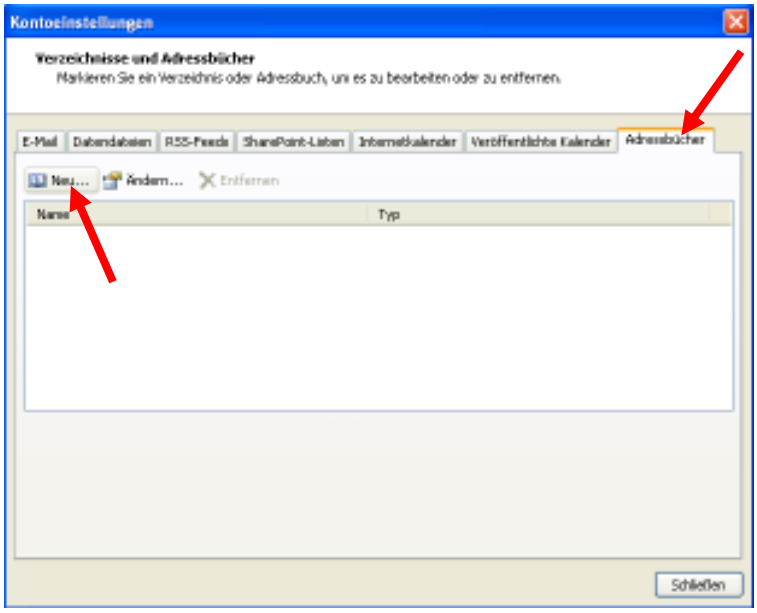
Signaturportal.de stellt die Adressen der Gerichte und Kollegen über ein Online abrufbares Adressbuch (LDAP) zur Verfügung. Nachfolgend wird beschreiben wie dieses einzurichten ist.

Outlook 2007

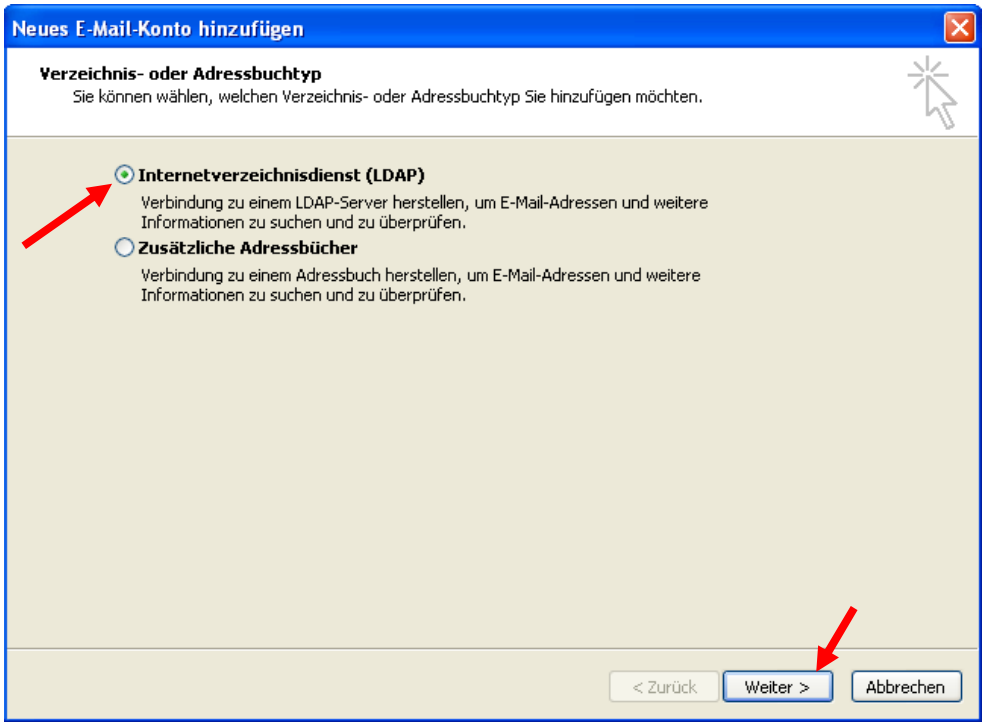
32. Öffnen sie unter dem Menüpunkt „Extras“ die „Kontoeinstellungen“.



33. Wählen Sie dort den Kartenreiter „Adressbücher“ aus. Betätigen Sie „Neu“ um ein neues LDAP-Verzeichnis anzulegen.

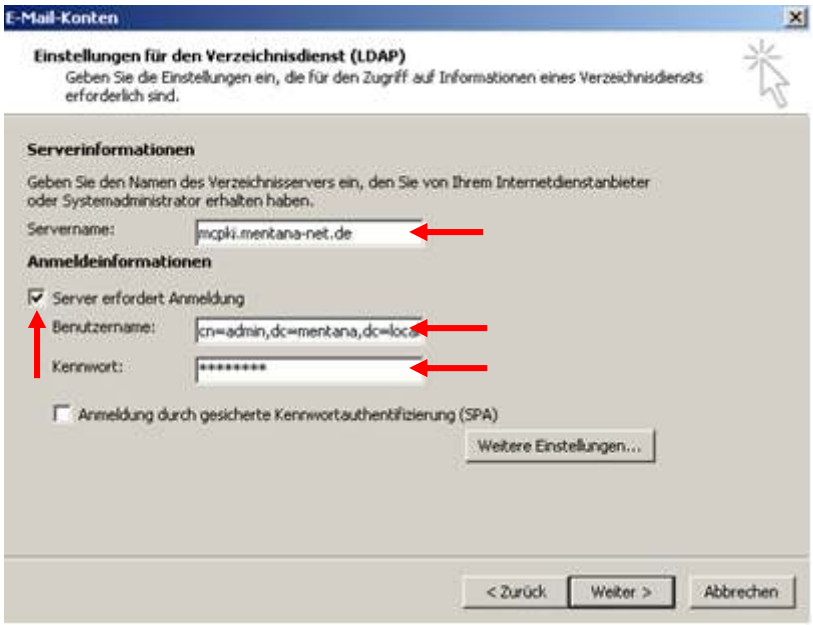


34. Nun wählen Sie den Punkt „Internetverzeichnisdienst (LDAP)“ und bestätigen mit „Weiter“.

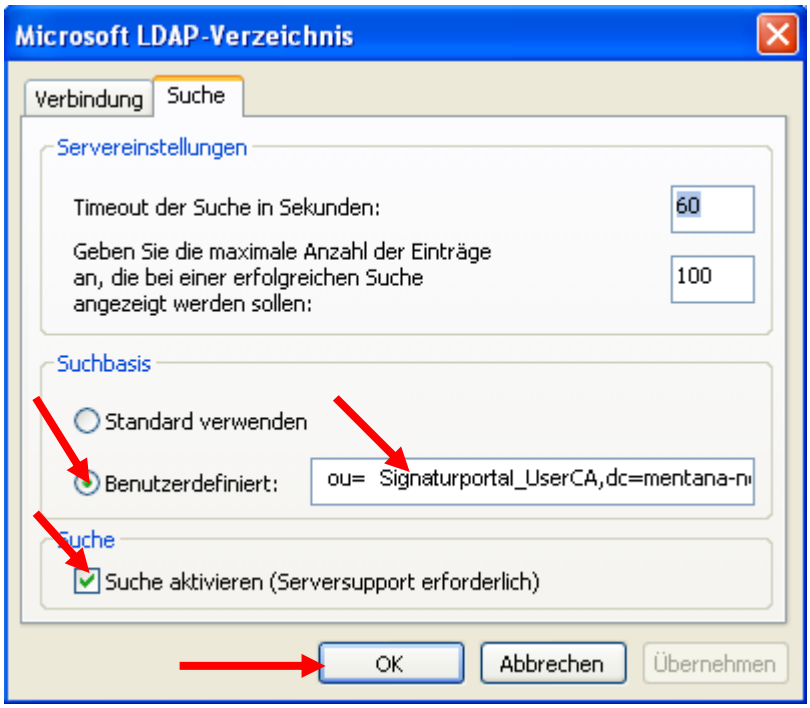


35. Unter Serverinformationen tragen Sie als „Servername“ **„mcpki.mentana-net.de“** ein.

36. Unter Anmeldeinformationen setzten Sie ein Häkchen bei „Server erfordert Anmeldung“. Dann tragen Sie als „Benutzername“ die Base DN **(cn=mentuser,dc=mentana-net,dc=de)** ein. Das Kennwort finden Sie in Ihrem Signaturportal unter Adressbuch, Kartenreiter LDAP-Verzeichnisdienst. Klicken Sie nun auf „Weitere Einstellungen“.



37. Wählen Sie in diesem Fenster die Registerkarte „Suchen“ aus. Wählen Sie im Abschnitt Suchbasis „**Benutzerdefiniert“** und tragen sie **(ou=Signaturportal_UserCA,dc=mentana-net,dc=de)** ein. Setzen Sie im Abschnitt Suche einen Haken bei „Suche aktivieren“, und bestätigen Sie anschließend mit „OK“.



38. Bestätigen Sie nun die Erstellung des LDAP-Verzeichnisses indem Sie auf „Weiter“ klicken. Wählen Sie im folgenden Fenster „Fertig stellen“ aus um die Erstellung abzuschließen.

Schließen Sie nun Outlook und starten Sie es neu damit die Daten richtig Übernommen werden.

39. Wenn Sie nun ihr Outlook wieder öffnen, ist ihr Konto bereit verschlüsselte Nachrichten zu versenden. Aktivieren Sie dazu das Symbol zur E-Mail-Verschlüsselung bei versenden von E-Mails über ihr Signaturportal.

Haben Sie weitere Fragen?
Bitte nutzen Sie zunächst den Hilfe – Bereich auf www.Signaturportal.de

Oder nutzen Sie einen der nachfolgenden Kontakte:

Hotline: **01805/ 691188** (12 Cent/min.) Mo.- Sa. 9.00 Uhr bis 17.00 Uhr

Notfall-Hotline: 0160 / 173 14 17 täglich bis 22 Uhr

E- Mail: support@Signaturportal.de