1. Zertifikatsinstallation und Anbindung an das Mailkonto

Das beantragte persönliche Zertifikat wird standardmäßig in den Zertifikatspeicher des Browsers abgelegt, mit dem es beantragt wurde.

Hinweis: Wurde zum Beantragen des persönlichen Zertifikates und zum Importieren des Benutzerzertifkates der Internet Explorer als Browser genutzt, erübrigen sich die Arbeitsschritte 1 bis 7 dieses Abschnittes, da das persönliche Zertifikat bereits an der richtigen Stelle im Zertifikatspeicher vorliegt. In diesem Fall geht es bei Punkt 8 mit der Anbindung des Zertifikates an das Mailkonto weiter.

Um das persönliche Zertifikat in **Outlook 2010** zu installieren, muss es als Datei im **PKCS#12-Format**, dies entspricht den Dateitypen **pfx** beziehungsweise **p12**, vorliegen. Dazu muss es aus dem Browser exportiert werden, mit dem es beantragt wurde. Das Exportieren von Zertifikaten aus Browsern wird unter dem folgenden Link beschrieben:

Die Installation des persönlichen Zertifikates erfolgt in 13 Arbeitsschritten:

- « Lokaler Datenträger (C:) > tmp 44 tmp durchsuchen Q • Datei Bearbeiten Ansicht Extras ? 0 Organisieren 🔻 In Bibliothek aufnehmen 🔻 Freigeben für 🔻 >> 1 . Name Änderungsdatum Computer 😒 xmustercertkey.pfx 15.04.2008 18:16 Lokaler Datenträger (C:) Benutzer Download MSOCache Office 2010 Developer R PerfLogs ProgramData Programme savwsa tmp 111 1 Element Status: 🎎 Freigegeben
- Im Windows Explorer wird das Zertifikat "xmustercertkey.pfx", das in dem Verzeichnis C:\tmp liegt doppelt angeklickt.

2. Es startet der "Zertifikatsimport-Assistent" der mit "Weiter" zum nächsten Dialogfenster führt.

| Zertifikatimport-Assistent | | × |
|----------------------------|---|-----|
| | Willkommen | |
| | Dieser Assistent hilft Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und -sperrlisten vom Datenträger in den Zertifikatspeicher. Ein von einer Zertifizierungsstelle ausgestelltes Zertifikat dient der Identitätsbestätigung. Es enthält Informationen für den Datenschutz oder für den Aufbau sicherer Netzwerkverbindungen. Ein Zertifikatspeicher ist der Systembereich, in dem Zertifikate gespeichert werden. Klicken Sie auf "Weiter", um den Vorgang fortzusetzen. | |
| | | |
| | < Zurück Weiter > Abbred | hen |

3. Im Eingabefeld **"Dateiname:"** erscheint die zu importierende Datei mit vollständiger Pfadangabe (**hier:** C:\tmp\xmustercertkey.pfx). Über **"Weiter >"** startet das nächste Dialogfenster.

| Zertifikatimport-Assistent | | | | | |
|---|--|--|--|--|--|
| Zu importierende Datei | | | | | |
| Geben Sie die Datei an, die importiert werden soll. | | | | | |
| Dateiname: | | | | | |
| C:\tmp\xmustercertkey.pfx Durchsuchen | | | | | |
| Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden: | | | | | |
| Privater Informationsaustausch - PKCS #12 (.PFX,.P12) | | | | | |
| Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B) | | | | | |
| Microsoft Serieller Zertifikatspeicher (.SST) | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Weitere Informationen über Zertifikatdateiformate | | | | | |
| | | | | | |
| | | | | | |
| < <u>Z</u> urück Weiter > Abbrechen | | | | | |

4. Im Eingabefeld "Kennwort:" wird das Passwort verlangt, das beim Export des Zertifikates vergeben wurde. Zusätzlich empfiehlt es sich, die Optionsfelder "Schlüssel als exportierbar markieren...." und "Alle erweiterten Eigenschaften mit einbeziehen." auszuwählen. Zum Schluss wird die Schaltfläche "Weiter >" angeklickt.

| Zertifikatimport-Assistent | |
|---|--|
| Kennwort | |
| Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten. | |
| Geben Sie das Kennwort für den privaten Schlüssel ein. | |
| Kennwort- | |
| Hohe Sicherheit f ür den privaten Schl üssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schl üssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert. | |
| chlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen. | |
| IIIe erweiterten Eigenschaften mit einbeziehen. | |
| Weitere Informationen über <u>das Sichern privater Schlüssel</u> | |
| < <u>Z</u> urück Weiter > Abbrechen | |

5. Der "Zertifikatsimport-Assistent" öffnet das Fenster "Zertifikatspeicher". Hier ist der Optionspunkt "Zertifikatspeicher automatisch auswählen... " zu markieren. Mit "Weiter >" startet der nächste Bildschirm des Assistenten.

| Zertifikatimport-Assistent |
|--|
| Zertifikatspeicher Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden. |
| Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben. |
| Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend) |
| Zertifikatspeicher: |
| <u>D</u> urchsuchen |
| |
| |
| |
| Weitere Informationen über <u>Zertifikatspeicher</u> |
| |
| < <u>Z</u> urück Weiter > Abbrechen |

6. Der "Zertifikatsimport-Assistent" zeigt jetzt noch einmal die getroffenen Einstellungen. Der Import des Zertifikates wird über "Fertig stellen" gestartet.

| Zertifikatimport-Assistent | | × |
|----------------------------|---|---|
| | Fertigstellen des A | ssistenten |
| | Das Zertifikat wird importiert, stellen" geklickt haben. | nachdem Sie auf "Fertig |
| | Sie haben folgende Einstellung | gen ausgewählt: |
| | Gewählter Zertifikatspeicher Inhalt Dateiname | Auswahl wird vom Assistente PFX C:\tmp\xmustercertkey.pfx |
| | ٠ III | • |
| | | |
| | < <u>Z</u> urück | Fertig stellen Abbrechen |

7. Das letzte Bild des "Zertifikatimport-Assistenten" bestätigt den erfolgreichen Importvorgang und wird mit "OK" bestätigt.



 Das Zertifikat muss nun an das persönliche E-Mail-Konto (hier: Max Musterfrau) gebunden werden.
 Dazu wird nach dem Start von Outlook 2010 auf der Karteikarte "Datei" der

Menüpunkt "**Optionen...** " aufgerufen. Im linken Fenster wird das "**Sicherheitscenter**" selektiert. Im rechten Fenster wird die Schaltfläche "**Einstellungen für das Sicherheitscenter**" angeklickt.

| Outlook-Optionen | 8 |
|-------------------------------------|--|
| Allgemein E-Mail | Sorgen Sie für die Sicherheit Ihrer Dokumente und des Computers. |
| Kalender | Datenschutz |
| Kontakte | Microsoft nimmt den Datenschutz ernst. Weitere Informationen, wie Microsoft Outlook für den Datenschutz sorgt, finden Sie in den Datenschutzbestimmungen |
| Notizen und Journal | Datenschutzbestimmungen für Microsoft Outlook anzeigen |
| Durchsuchen | Programm zur Verbesserung der Benutzerfreundlichkeit |
| Mobiltelefon | Sicherheit & mehr |
| Sprache Erweitert | In Office.com finden Sie weitere Informationen zum Datenschutz und zur Sicherheit. |
| Menüband anpassen | Microsoft Trustworthy Computing |
| Symbolleiste für den Schnellzugriff | Microsoft Outlook-Sicherheitscenter |
| Add-Ins Sicherheitscenter | Das Sicherheitscenter enthält Einstellungen für Sicherheit und Datenschutz, um für die Sicherheit des Computers zu sorgen. Es wird |
| | OK Abbrec |

 Im linken Fenster wird "E-Mail-Sicherheit" ausgewählt. Im rechten Teil des Dialogfensters wird in der Kategorie "Verschlüsselte E-Mail_Nachrichten" die Schaltfläche "Einstellungen" selektiert.

| Sicherheitscenter | |
|--|---|
| Vertrauenswürdige Herausgeber DEP-Einstellungen Datenschutzoptionen E-Mail-Sicherheit Anlagenbehandlung Automatischer Download Einstellungen für Makros Programmgesteuerter Zugriff | Verschlüsselte E-Mail-Nachrichten Inhalt und Anlagen für ausgehende Nachrichten verschlüsse Ausgehenden Nachrichten digitale Signatur hinzufügen Signierte Nachrichten als Klartext senden S/MIME-Bestätigung anfordern, wenn mit S/MIME signiert Standardeinstellung: Digitale IDs (Zertifikate) Digitale IDs (Zertifikate) Importieren/Exportieren Digitale ID szw. Zertifikate sind Dokumente, mit denen die Identinachgewiesen werden kann. Importieren/Exportieren Digitale ID anfordern |
| | Skript in Ordnern Skript in freigegebenen Ordnern zulassen Skript in Öffentlichen Ordnern zulassen |

 Im Dialogfenster "Sicherheitseinstellungen ändern" wird in der Kategorie "Zertifikate und Algorithmen" neben dem Eingabefeld "Signaturzertifikat:" die Schaltfläche "Auswählen..." angeklickt.

| Sicherheitseinstellungen ändern | |
|---|--|
| Bevorzugte Sicherheitseinstellunge Name der Sicherheitseinstellung | en |
| Kryptografieformat: | s/MIME v |
| Standardeinstellung für dies | es <u>F</u> ormat kryptografischer Nachrichten |
| Stan <u>d</u> ardsicherheitseinstellu | ng für alle kryptografischen Nachrichten |
| Sicherheitskennzeichen | Neu Löschen Kennwort |
| Zertifikate und Algorithmen | |
| Signaturzertifikat: | Auswählen |
| Hashalgorithmus; | |
| Verschlüsselungszertifikat: | Auswählen |
| Verschlüsselungsalgorithmus; | |
| 🔽 Signierten Nachrichten diese | Zertifikate hinzufügen |
| | OK Abbrechen |

11. In dem Dialogfenster **"Zertifikat bestätigen"** wird das persönliche Zertifikat selektiert (hier: PN: Xaver Muster) und mit **"OK"** bestätigt.

| Windows-Sicher | heit | × |
|--|--|----|
| Zertifikat b Bestätigen Sie nicht um das r | estätigen dieses Zertifikat, indem Sie auf "OK" klicken. Wenn es si ichtige Zertifikat handelt, klicken Sie auf "Abbrechen". | ch |
| | PN: Xaver Muster Aussteller: Uni-Osnabrueck RZ-CA Gültig ab: 15.04.2008 bis 15.04.2011 Zertifikateigenschaften anzeigen Gültig ab: 15.04.2008 bis 15.04.2011 | |
| | OK Abbrech | en |

12. Das Dialogfenster "Sicherheitseinstellungen ändern" zeigt die zuvor ausgewählten Zertifikate an. Das Eingabefeld "Name der Sicherheitseinstellung:" erwartet einen beliebigen Bezeichner (hier: Max Musterfrau) Der Gesamtdialog wird über "OK" beendet.

| Sicherheitseinstellungen ändern | 1 | — |
|---------------------------------------|--|-----------|
| Bevorzugte Sicherheitseinstellunge | en | |
| Name der Sicherheitseinstellung | j: | |
| Xaver Muster | | - |
| Kryptografieformat: | S/MIME | |
| 🔲 Standardeinstellung für dies | es <u>F</u> ormat kryptografischer Nachrichten | |
| Stan <u>d</u> ardsicherheitseinstellu | ng für alle kryptografischen Nachrichten | |
| Sigherheitskennzeichen | <u>N</u> eu <u>L</u> öschen <u>K</u> | ennwort |
| Zertifikate und Algorithmen | | |
| Signaturzertifikat: | PN: Xaver Muster | uswählen |
| Hashalgorithmus: | SHA1 | |
| Verschlüsselungszertifikat: | PN: Xaver Muster | uswählen |
| Verschlüsselungsalgorithmus: | AES (256-bit) | |
| 🔽 Signierten Nachrichten diese | e <u>Z</u> ertifikate hinzufügen | |
| | ОК | Abbrechen |

Das Zertifikat ist jetzt (Arbeitsschritt 8 -12) an das persönliche E-Mail-Konto (**hier:** Xaver Muster) gebunden.

2. Signieren von E-Mails mit Outlook 2010

Nachdem das persönliche Zertifikat importiert wurde, können E-Mails beim Versenden mit einer Signatur versehen werden. Das folgende Beispiel beschreibt, wie der fiktive Benutzer Xaver Muster der fiktiven Benutzerin Yvonne Muster eine signierte E-Mail zusendet.

2.1 Erzeugen einer E-Mail mit persönlicher Signatur

Nach dem Starten von Outlook wird über "**Neu...**" und dann "**Neue E-Mail-Nachricht**" eine neue E-Mail erzeugt. Um diese Nachricht zu signieren, wird auf der Registerkarte "**Optionen**" auf die Schaltfläche "**Signieren**" (rot eingekreist) geklickt.

Hinweis: Outlook 2010 kann so konfiguriert werden, dass für jede neue E-Mail automatisch eine Signatur vergeben wird. (**siehe:** Installation des persönlichen Zertifikates Bild 10 --> hier ist ein Häkchen in das Optionsfeld "**Ausgehenden Nachrichten digitale Signatur hinzufügen**" zu setzen.)

| ê 🖬 🖬 🕊 |) U 🎄 🕈 | Ŧ | eine signierte | Mail Na | chricht (HTML) | |) <u>5</u> 3 |
|-------------------|----------------|---|--|------------------|---|---|--------------|
| Datei | Nachricht | Einfügen | Optionen | Text format | ieren Überprüfer | 1 | ۵ 🕜 |
| Designs | Bcc | Berechtigung | 🛃 Verschlüsse <section-header> Signieren</section-header> | eln 👬 Verlauf | Gesendetes Element speichern unter * | 칠 Übermittlung verzögern ዲ Direkte Antworten auf | 0 |
| F | elder anzeigen | Bere | chtigung | | Weiter | e Optionen 5 | |
| Senden Hallo Y | An | <u>ymuster@uni-os</u> eine signierte l | <u>snabrueck.de</u> Mail | | | | |
| | | | | | | | |
| 2 | Vonne Muster | | | | | 2 | 2 ^ |

2.2 Prüfen der Signatur einer empfangenen E-Mail

Das folgende Beispiel beschreibt, wie die fiktive Benutzerin Yvonne Muster die Signatur einer E-Mail prüft, die sie von Xaver Muster erhalten hat. Voraussetzung dafür ist, dass Yvonne Muster die Root-Zertifikate der ausstellenden Zertifizierungsinstanzen in Outlook eingefahren hat. (Zertifikate und Installationsanleitung siehe zweiter Absatz: Einrichten eines E-Mailkontos unter Outlook 2010 beziehungsweise Einrichten eines Mailkontos unter Outlook 2010 von zu Hause)

 Nach dem Start von Outlook 2010 wird im Posteingang von Yvonne Muster die E-Mail von Xaver Muster geöffnet. In der E-Mail befindet sich das Signatur-Symbol (rot eingekreist), das anzeigt, dass die E-Mail signiert wurde. Durch Klicken auf das Signatur-Symbol werden die Informationen zur Signatur des Absenders (hier: Xaver Muster) angezeigt.

| ن ات 🔜 ا 🖂 | 5 🛧 🌩 - | eine signierte Mail Na | chri | icht (HTML) | | - | - |
|---------------------------|---|-----------------------------|------|-------------|------------|------------|---|
| Datei Na | achricht | | | | | | |
| ि X & + Löschen | Antworten Allen antworten | Drafts An Vorgesetzte(n) | 4 F | Verschieben | Kategorien | Bearbeiten | 1 |
| Löschen | Antworten | QuickSteps | Fai | | | | 7 |
| Betreff: Signiert von: | eine signierte Mail xmuster@uni-osnabrueck | .de | | | | | |
| Hallo Yvoni | ne, | | | | | | |
| | | | | | | | |

• Es öffnet sich das Dialogfenster "Digitale Signatur: Gültig", das alle Informationen zur Signatur von Xaver Muster auflistet.

| Digitale Signatur: Gültig | | | | | |
|--|--|--|--|--|--|
| Betreff: Von: Signiert von: | eine signierte Mail Xaver Muster xmuster@uni-osnabrueck.de | | | | |
| 유 | Die digitale Signatur dieser Nachricht ist gültig und vertrauenswürdig. Klicken Sie auf "Details", um weitere Informationen zum Zertifikat zu erhalten, das für die digitale Signatur der Nachricht verwendet wurde. | | | | |
| Details Vor Fehlern in digital signierten Nachrichten vor dem Öffnen warnen. Schließen | | | | | |

3. Verschlüsseln von E-Mails mit Outlook 2010

E-Mails werden immer mit dem "öffentlichen Schlüssel" aus dem persönlichen Zertifikat des Empfängers verschlüsselt.

Wenn beispielsweise Xaver Muster eine verschlüsselte E-Mail an Yvonne Muster senden will, benötigt er dazu den "öffentlichen Schlüssel" des persönlichen Zertifikates von Yvonne Muster.

3.1 Öffentlichen Schlüssel des Empfängers verfügbar machen

Wie kommt Xaver Muster an den "öffentlichen Schlüssel" aus dem persönlichen Zertifikat von Yvonne Muster?

Es gibt verschiedene Methoden, "öffentliche Schlüssel" verfügbar zu machen. Hier wird ein möglicher Weg für Outlook 2010 beschrieben.

 Xaver lässt sich eine signierte E-Mail von Yvonne zusenden. Nach dem Öffnen der signierten E-Mail wird die Adresse des Absenders (hier: Yvonne Muster [ymuster@uni-osnabrueck.de]) zu den Outlook-Kontakten hinzugefügt. Dazu wird die rechte Maustaste gedrückt, wenn sich der Mauszeiger über der E-Mail-Adresse von Yvonne Muster befindet. Aus dem Kontextmenü wird der Untermenüpunkt "Zu Outlook-Kontakten hinzufügen..." ausgewählt.



 Der öffentliche Schlüssel von Yvonnes persönlichem Zertifikat kann jetzt über "Anzeigen" --> "Zertifikate" --> "Eigenschaften" eingesehen werden. Yvonne Musters E-Mail-Adresse und der öffentliche Schlüssel werden über das Symbol "Speichern und schließen" als neuer Kontakt in Outlook 2010 hinterlegt.

| 💁 🛃 🍠 🥶 🖉 🗢 🗇 ╤ Yvonne Muster - Kontakt | | | | | | | |
|---|---|--|-----------|---------------|-----------------------------------|---------------|-------------------|
| Datei Kontakt | Einfügen | Text formatieren | Überpi | rüfen | | | |
| Speichern & schließen | Speichern ur Weiterleiten OneNote Aktionen | nd neuer Kontakt 👻 | Anzeigen | Kommunizieren | Namen | Optionen • | K ategor |
| Outlook verwendet ein senden. Sie können eir Kontakt empfangen od Zertifikate (digitale IDs) | nes dieser Zertifi n Zertifikat erha Jer eine Zertifika): | ikate, um verschlüsse Iten, indem Sie eine atdatei für diesen Ko | Allgemeir | Details | tivitäten tifikate e Felder | itakt zu 1 | |
| PN: Yvonne Muster(Sta | andard) | | | Anzeigen | | - (| Eigens |
| | | | | | | | A <u>I</u> s Star |
| | | | | | | | Imp <u>o</u> |
| | | | | | | | Expo |
| | | | | | | | Ent |
| | | | | | | | |
| Yvonne Mus | ter | | | | | | |

3.2 Erzeugen einer verschlüsselten E-Mail

Xaver Muster besitzt jetzt den **"öffentlichen Schlüssel"** des persönlichen Zertifikates von Yvonne Muster. Er muss ihn benutzen, um eine verschlüsselte E-Mail an Yvonne zu schicken.

Nachdem Xaver Muster eine E-Mail an Yvonne Muster verfasst hat, wird sie mit dem öffentlichen Schlüssel von Yvonne verschlüsselt. Dazu wird auf die Schaltfläche **"Verschlüsseln"** (rot eingekreist) geklickt. Anschließend wird die E-Mail versendet.

| 👔 🖪 🛱 🏦 👘 👘 🖛 eine verschlüsselte Mail - Nachricht (HTML) 🛛 🗖 | | | | | | | |
|---|-------------------|---|-----------------------------|--------------------|---|-----|--|
| Datei | Nachricht | Einfügen Optione | en Text format | ieren Überprüfen | | ۵ 🕜 | |
| Designs | | Berechtigung 🛃 Signi | hlüsseln eren Verlauf | Gesendetes Element | 칠 Übermittlung verzögern 옳 Direkte Antworten auf | | |
| | Felder anzeigen | Berechtigung | | Weiter | e Optionen 🛛 🕞 | | |
| Sender | Von • An Cc | xmuster@uni-osnabrued ymuster@uni-osnabruedk | :k.de . <u>de</u> | | | | |
| | Betreff: | eine verschlüsselte Mail | 9 | | | | |
| Hallo | Yvonne, | | | | | | |
| 2 | | | | | | | |
| 2 | Yvonne Muster | | | | 2 | ۲ ^ | |

Hinweis: Die E-Mail-Adresse des Empfängers muss exakt so geschrieben werden, wie sie im persönlichen Zertifikat des Empfängers enthalten ist. Ansonsten funktioniert das Verschlüsseln nicht.

3.3 Lesen einer verschlüsselten E-Mail

Öffnet Yvonne die E-Mail von Xaver, wird sie automatisch entschlüsselt. Dazu benutzt Outlook den "privaten Schlüssel" des persönlichen Zertifikates von Yvonne Muster. Das Schloss-Symbol zeigt an, dass die E-Mail vom Absender (hier: Xaver Muster) verschlüsselt wurde.



4. Bekannte Probleme

4.1 Einige Mail-Klienten können unter Outlook 2010 verschlüsselte E-Mails nicht entschlüsseln

Unter **Outlook 2010** verschlüsselte E-Mails können nicht von allen Mail-Klienten entschlüsselt werden. Im Rechenzentrum betraf dieses Problem besonders den Mail-Klienten **"Thunderbird".** Genaue Informationen finden sich unter dem folgenden Link "Some email clients unable to decrypt email sent from Outlook 2010".