Anwenderinformation
des Referats Informationstechnologie

EVANGELISCHE LANDESKIRCHE
IN WÜRTTEMBERG

Thema	**E-Mail-Verschlüsselung**			
Betroffene Software	Outlook 2010			
betroffener Anwenderkreis	Anwenderinnen und Anwender im IT-Verbund des Evangelischen Oberkirchenrats Stuttgart			
Stand	November 2014	Version	1	Erstellt von	Referat Informationstechnologie

Evangelischer Oberkirchenrat | Gänsheidestraße 4 | 70184 Stuttgart | Bei Rückfragen wenden Sie sich bitte an folgende Nummer: 0711 2149-533

1 Vorwort

Entsprechend der Datenverschlüsselungsverordnung vom 20. Dezember 2000 (AZ 87.00 Nr. 67) und der Verordnung zur Änderung der Datenverschlüsselungsverordnung vom 18. November 2003 (AZ 87.00 Nr. 71) dürfen seit Anfang 2005 E-Mails mit personenbezogenen Daten nur noch verschlüsselt übertragen werden. Als weitergehende Information finden Sie diese unter http://www.kirchenrecht-wuerttemberg.de/.

E-Mails sind quasi wie eine **Postkarte**. Sie können – wenn auch mit gewissem technischen Aufwand – von Dritten eingesehen und/oder manipuliert werden.

- E-Mails mit personenbezogenen Daten müssen **verschlüsselt** werden, damit sie auch wirklich nur vom berechtigten Empfänger gelesen werden können.

Eine zusätzliche **Signatur** dient dazu, Veränderungen zu erkennen und die Echtheit des Senders zu gewährleisten.

Für die Verschlüsselung und die Signierung einer E-Mail benötigen die kommunizierenden Parteien ein sogenanntes **Zertifikat**. Dieses ist für jede E-Mail-Adresse einzigartig. E-Mail-Empfänger, die in das EDV-System des Oberkirchenrats integriert sind, erfüllen automatisch die Voraussetzung, verschlüsselte und signierte E-Mails zu empfangen.

In diesem Handbuch haben wir beschrieben, wie E-Mails **verschlüsselt** und **signiert** versendet werden können.

2 Umgang mit sicheren E-Mails

2.1 Ziele der Verschlüsselung und Signierung

Durch die Verschlüsselung und Signierung (Digitale Signatur) von E-Mails sollen drei Ziele erreicht werden:

- **Verschlüsselung**
  Durch die Verschlüsselung einer E-Mail wird sichergestellt, dass kein Außenstehender die Daten in der E-Mail lesen kann. D. h. nur ein bestimmter Empfänger mit dem richtigen Zertifikat kann eine E-Mail wieder entschlüsseln.

- **Authentifizierung**
  Durch die Signatur einer E-Mail wird sichergestellt, dass die E-Mail wirklich von dem Absender kommt, von dem sie zu sein scheint.

- **Integrität**
  Durch die Signatur einer E-Mail wird ebenfalls sichergestellt, dass der Inhalt der E-Mail nach der Signierung nicht mehr unbemerkt verändert werden kann. D. h. niemand kann eine signierte E-Mail fälschen, ohne dass Sie es bemerken.

2.2 Sender und Empfänger benötigen ein Zertifikat

Wenn Sie eine verschlüsselte E-Mail versenden, muss auch der Empfänger entsprechend berechtigt sein. Mitarbeiter des Evangelischen Oberkirchenrats in Stuttgart und die der angeschlossen Dienststellen, d.h. alle, deren Rechner bzw. Postfach vom Referat IT betreut wird, besitzen automatisch ein solches Zertifikat. Auch gibt es einige externe E-Mail-Adressen, die bei der Zertifizierungsstelle der Evangelischen Landeskirche Württemberg (https://pki.elk-wue.de/) registriert sind und somit ein Zertifikat haben.

Der sichere Austausch funktioniert ebenso mit allen, die ein Postfach über PC im Pfarramt benützen.
Dies jedoch nur zu Ihrer Information. In der Anwendung brauchen Sie sich hierüber keine Gedanken zu machen, denn das System kümmert sich um die entsprechende Prüfung (s. weiter unten).

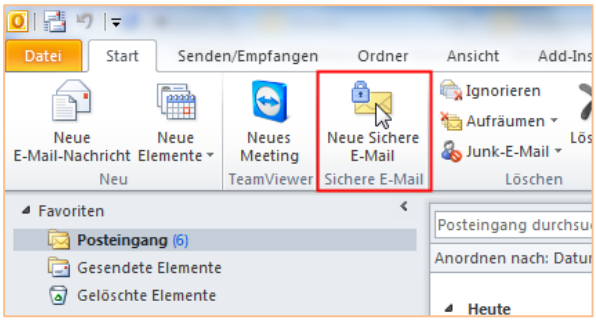
Grundsätzlich können E-Mails nur an Empfänger aus der Globalen Adressliste (GAL) im Outlook sicher versendet werden.

2.3 Senden von verschlüsselten und signierten E-Mails

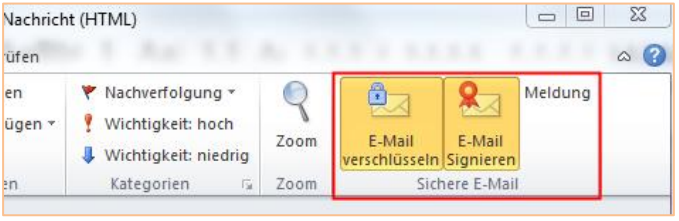
Die Betreffzeile wird **nicht** verschlüsselt.
Deshalb hier keine personenbezogenen Daten eintragen.

Gehen Sie wie beschrieben vor:

Öffnen Sie ein neues E-Mail-Formular über den Button ***Neue Sichere E-Mail***.

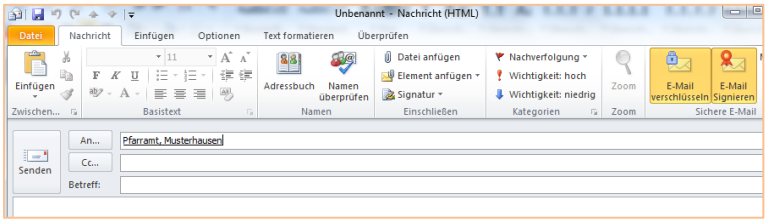


Sie erkennen, dass es sich um eine verschlüsselte und signierte E-Mail handelt, da die beiden Schaltflächen ***E-Mail verschlüsseln*** und ***E-Mail signieren*** aktiv sind (gelb hinterlegt).



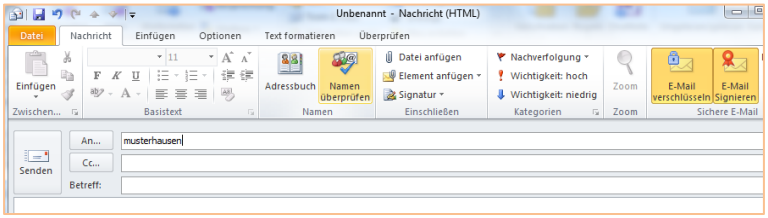
Bei einer „normalen“ E-Mail können die beiden Funktionen auch im Nachhinein aktiviert bzw. deaktiviert werden.

Tragen Sie im Feld ***An:*** den Empfänger ein.
Klicken Sie auf die Schaltfläche
Namen überprüfen

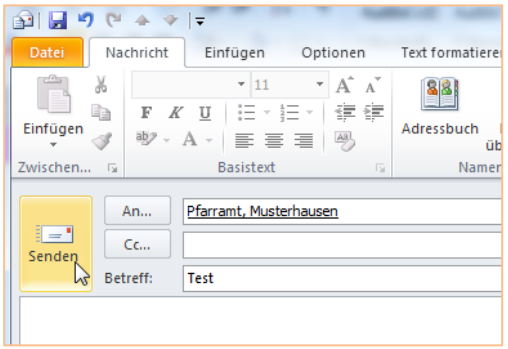


Der Name wird aufgelöst.

Oder wählen Sie den Empfänger aus der Globalen Adressliste aus



Das war's schon:
Klicken Sie nun auf ***Senden***.



2.4 Was passiert jetzt?

Das System überprüft nun, ob die ausgewählten Empfänger berechtigt sind, die E-Mail zu entschlüsseln.

- Falls ***ja***, wird die Nachricht versendet und alles ist erledigt. Es gibt keine extra Bestätigung des Systems.
- Falls ***nein***, wird die Nachricht NICHT versendet und Sie erhalten eine Rückmeldung vom System mit dem Betreff: „JULIA MailOffice Status FAILURE“. Im E-Mail gibt es eine Begründung (Es konnte kein Empfängerschlüssel geladen werden) und die Nennung der E-Mail-Adresse ohne gültigen Schlüssel.

Dies funktioniert natürlich auch dann, wenn Sie mehrere Empfänger ausgewählt haben. Es wird dann pro Empfänger überprüft, ob für die E-Mail-Adresse ein gültiger Schlüssel vorliegt. Bei Vorliegen des Schlüssels erfolgt die Zustellung, bei Nicht-Vorliegen erfolgt keine Zustellung, jedoch die schon erwähnte Fehlermeldung.

D. h. Bei Versand über den Button ***Neue Sichere E-Mail*** stellt das System für Sie sicher, dass die E-Mail nur an Empfänger versandt wird, die auch berechtigt sind, diese zu lesen. Ist diese Berechtigung nicht vorhanden, erhalten Sie vom System eine entsprechende E-Mail.

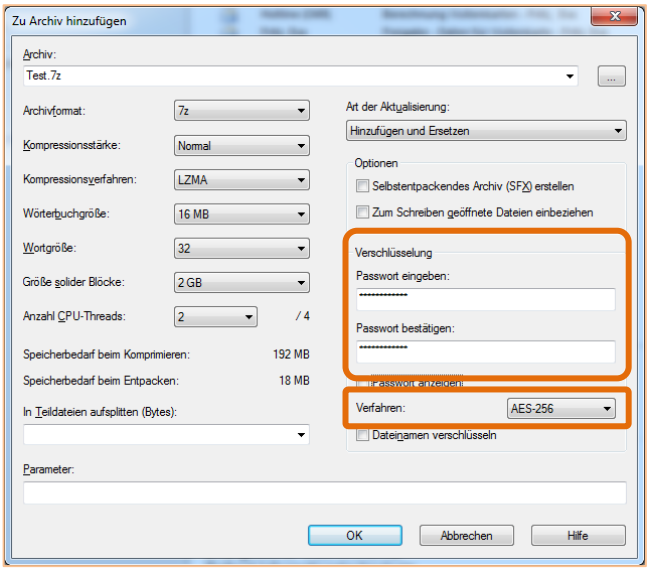
3 Mögliche Alternativen

- Sie können natürlich nach wie vor die Daten auch auf dem ***Postweg*** versenden.

- Eine ***elektronische Alternative*** wäre, unter Zuhilfenahme eines Packprogramms, die Datei zu packen und dabei zu verschlüsseln.

  Es handelt sich dabei um das Programm ***7-Zip***, das auf jedem OKR-Rechner installiert ist.

  Hierzu gehen Sie folgendermaßen vor:
  - Sie erstellen eine Datei (Word, Excel…) mit den zu schützenden Inhalten.
  - Diese Datei speichern Sie auf dem Filesystem (Desktop oder einem Ihrer Laufwerke).
  - Mit der rechten Maustaste wählen Sie ***7-Zip*** und ***Zu einem Archiv hinzufügen…*** bzw. ***add to archive…***.
  - Im folgenden Fenster vergeben Sie ein ***Passwort***.
    Als Verfahren wählen Sie unbedingt ***AES-256*** aus. Damit ist eine gültige Verschlüsselung gewährleistet.



  Mit ***OK*** wird eine neue Datei erstellt, die dann ***als Anhang*** versendet werden kann.

  - Teilen Sie dem Empfänger Ihr vergebenes Passwort unbedingt gesondert mit (z. B. per Telefon).

4 FAQ

Was, wenn ich etwas falsch mache?
Sofern Sie über „Neue sichere E-Mail“ versenden, können Sie gar nichts falsch machen, da sich das System um den sicheren Versand kümmert.

Was, wenn ich den falschen Adressaten ausgewählt habe?
Dies kann leider auch das beste System nicht abfangen. Deshalb sollten Sie vor dem Versand sensibler Daten immer noch einmal genau die Liste der Empfänger kontrollieren. Speziell die automatische Ergänzung/Vorschlag von E-Mailadressen kann hier zu unerwünschten Einträgen führen.

Kann ich auch mehrere Adressaten auswählen?
*Natürlich. Die Berechtigten erhalten die Nachricht verschlüsselt. Sind Empfänger ohne Zertifikat dabei, so erfolgt an diese keine Zustellung. Für jede nicht zugestellte E-Mail erhalten Sie dann vom System eine Nachricht. Hier steht je der Grund (*Es konnte kein Empfängerschlüssel geladen werden*) und der Empfänger, an den die E-Mail nicht versendet wurde.*

Was kann ich machen, wenn der Adressat kein Zertifikat besitzt?
Eine sichere E-Mail an diesen Empfänger ist damit nicht möglich.
Alternative: Sie verschlüsseln die Datei extra mithilfe des Programms 7-Zip und fügen die verschlüsselte und passwortgesicherte Datei als Anhang der E-Mail hinzu (s. Punkt 3 Alternative).

Muss ich vorher überprüfen, ob der Empfänger ein Zertifikat besitzt?
Nein, sobald Sie über „Neue sichere E-Mail“ versenden, kümmert sich das System darum.

Was, wenn ich eine verschlüsselte E-Mail nicht lesen kann?
Dafür dürfen Sie gerne bei der Hotline anrufen.

Wie kann ich nachträglich überprüfen, ob ich die E-Mail verschlüsselt versendet habe?
Sollte dies benötigt werden, dürfen Sie sich auch hiermit gerne an die Hotline wenden.
Dies geht jedoch nur, sofern die gesendete E-Mail noch vorhanden ist.

5 Kontakt

Bei Problemen steht Ihnen die IT-Hotline des Evangelischen Oberkirchenrats zur Verfügung.

Sie erreichen diese wie folgt:

Telefonisch: 0711 2149-533
E-Mail: Hotline@elk-wue.de

Montag bis Donnerstag	07:30 Uhr – 12:00 Uhr 13:00 Uhr – 16:30 Uhr	Freitag	07:30 Uhr – 12:00 Uhr 13:00 Uhr – 15:00 Uhr