

Einrichtung einer E-Mail-Verschlüsselung mit S/MIME-Zertifikaten in Outlook für die Kommunikationspartner von Hamburg Airport oder seiner Tochterunternehmen

Um die aktuellen Datenschutzaufgaben gem. Artikel 32 EU-DSGVO zu erfüllen, müssen E-Mail-Nachrichten mit personenbezogenen Daten verschlüsselt übertragen werden. Grundsätzlich handelt es sich bei personenbezogenen Daten um alle Angaben, die sich einer bestimmten bzw. bestimmbaren natürlichen Position zuordnen lassen. Die genaue Definition kann Artikel 4 Ziffer 1 DSGVO entnommen werden.

Dafür muss der Absender die E-Mail-Nachricht mit dem öffentlich zugänglichen Schlüssel des Empfängers verschlüsseln. Ausschließlich der Empfänger kann die Nachricht dann mit seinem persönlichen Schlüssel wieder entschlüsseln.

Am Hamburg Airport wird dafür das S/MIME-Verfahren verwendet, welches als sehr sicher gilt. Zudem wird dieses von den meisten gängigen E-Mail-Clients unterstützt.

Diese Anleitung bezieht sich im Wesentlichen auf die Verwendung des E-Mail-Clients Microsoft Outlook in der Microsoft Windows Umgebung. Bei diesem ist das S/MIME-Verfahren bereits vollständig integriert und erfordert keine weitere zusätzliche Software oder Erweiterungen. Sie benötigen lediglich Ihr persönliches S/MIME-Zertifikat, welches die beiden Schlüssel enthält. Wie Sie ein solches Zertifikat erhalten, klären Sie mit Ihrer IT-Abteilung bzw. Ihrem zuständigen IT-Dienstleister.

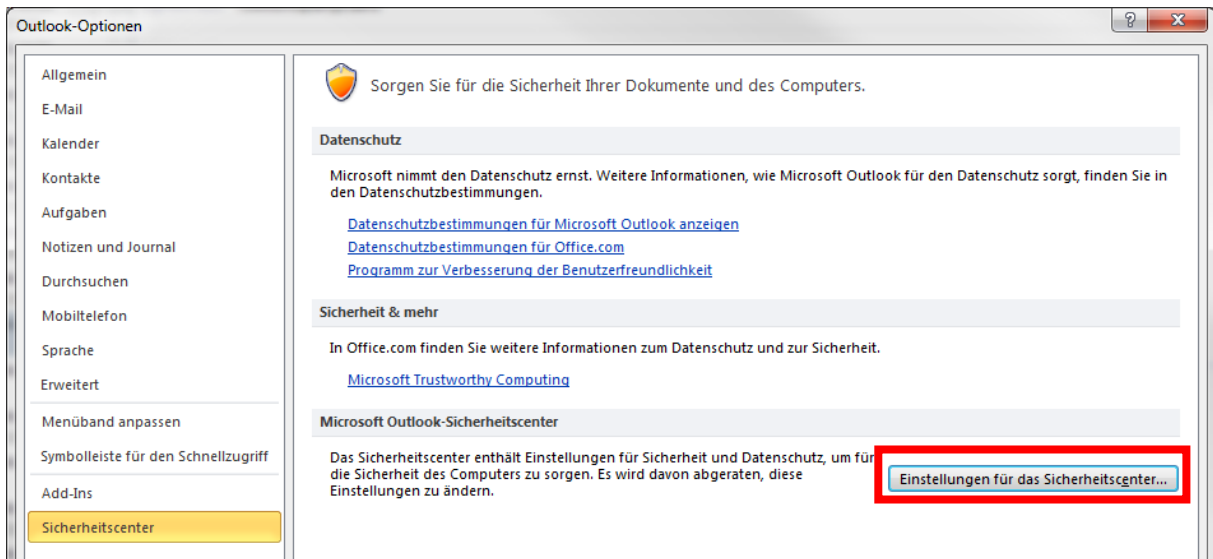
Wenn Sie einen alternativen E-Mail-Client nutzen, informieren Sie sich bitte im Internet über dessen Einrichtung für dieses Verschlüsselungsverfahren oder wenden Sie sich auch hierfür an Ihre IT-Abteilung oder Ihren IT-Dienstleister.

ZERTIFIKAT IN OUTLOOK INSTALLIEREN

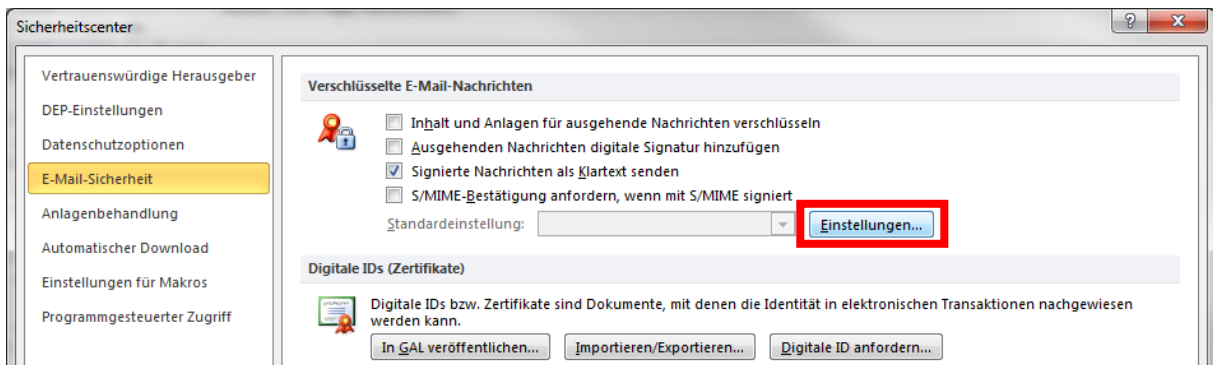
Wenn Sie bereits ein persönliches Zertifikat erhalten haben, können Sie dieses durch einen Doppelklick auf die Datei in Windows installieren. Dabei wählt Windows automatisch die richtigen Einstellungen aus und legt das Zertifikat in dem persönlichen Zertifikatsspeicher ab.

Um die Installation in Outlook vorzunehmen, gehen Sie wie folgt vor:

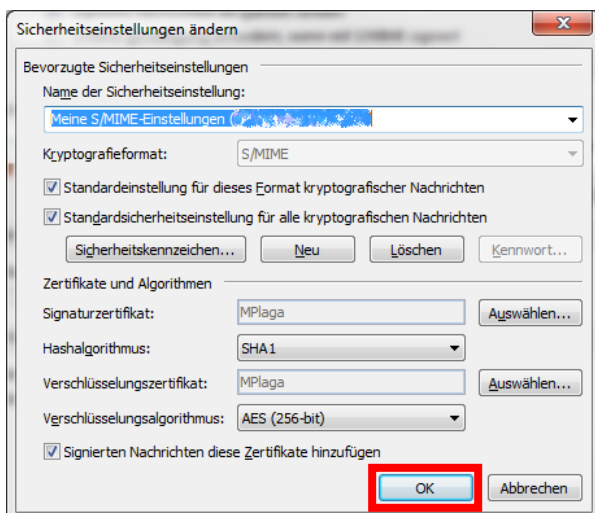
Datei > Optionen > Sicherheitscenter oder **Trust Center** und dort **Einstellungen für das Sicherheitscenter (Trust Center)**.



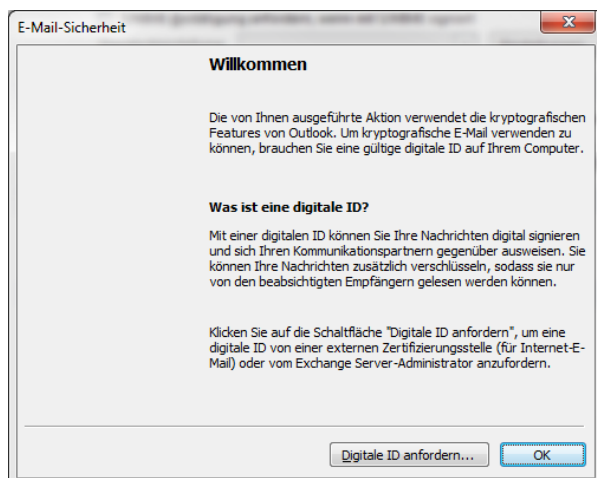
In dem sich dann öffnenden Fenster, gehen Sie auf den Menüpunkt **E-Mail Sicherheit** und klicken dort im Bereich „Verschlüsselte E-Mail-Nachrichten“ auf **Einstellungen**.



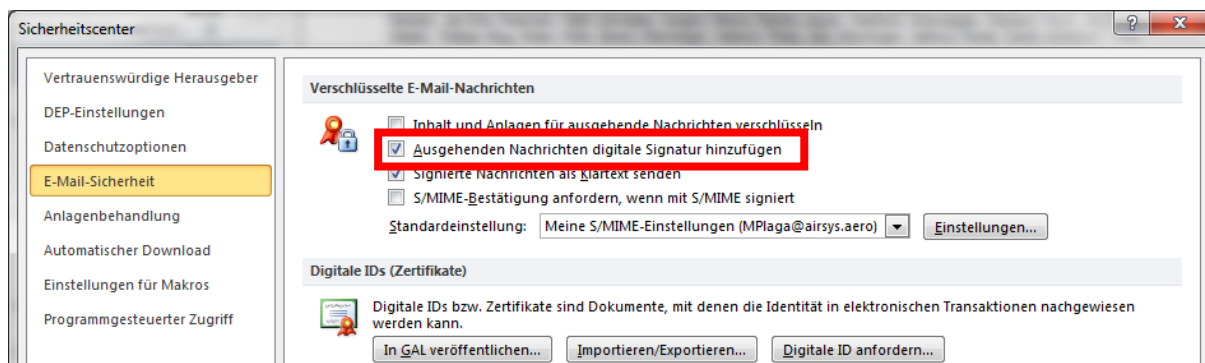
Outlook wählt dann automatisch das richtige Zertifikat aus dem Zertifikatsspeicher aus und zeigt dieses an. Mit einem Klick auf **OK** wird das Zertifikat dann in Outlook übernommen.



Sollten Sie hingegen nachfolgendes Fenster erhalten, ist Ihr Zertifikat noch nicht erfolgreich in Ihrem Benutzerprofil hinterlegt worden. In diesem Fall kontaktieren Sie bitte Ihre IT-Abteilung oder Ihren IT-Dienstleister.



Da das S/MIME-Verfahren einen vorherigen Austausch der Signaturen erfordert, ist es ratsam seine Signatur bei seinen Kommunikationspartnern zu streuen. Dazu empfehlen wir allen ausgehenden Nachrichten die digitale Signatur hinzuzufügen. Dazu setzen Sie noch einen Hacken bei „**Ausgehenden Nachrichten digitale Signatur hinzufügen**“. Abschließend können Sie die restlichen Dialogfelder mit **OK** bestätigen. Damit ist Outlook nun für die E-Mailverschlüsselung eingerichtet.

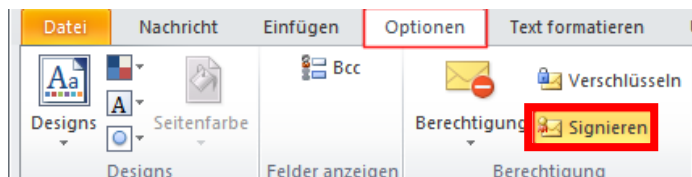


SIGNIERTE UND VERSCHLÜSSELTE NACHRICHTEN VERSENDEN

Um eine verschlüsselte Nachricht versenden zu können, benötigen Sie zunächst das öffentlich zugängliche Zertifikat des Empfängers. Dazu muss Ihnen der Empfänger vorab eine signierte E-Mail-Nachricht senden, deren Signatur seinen öffentlichen Schlüssel enthält.

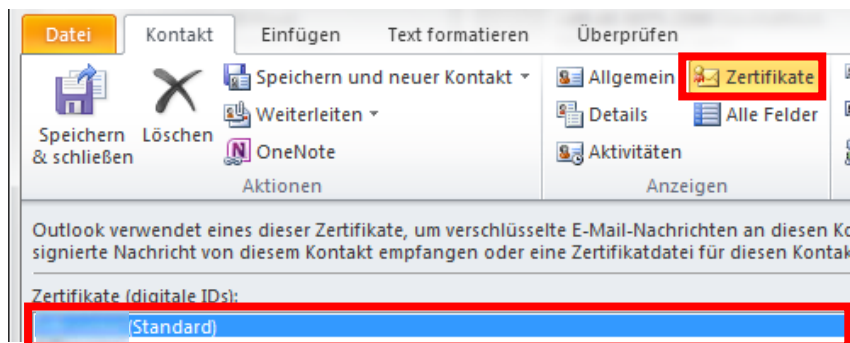
In Outlook können Sie eine signierte Nachricht versenden, indem Sie im Fenster für eine neue E-Mail-Nachricht unter dem Reiter **Optionen** die Funktion **Signieren** markieren. Beim Senden wird diese Nachricht dann automatisch signiert und somit Ihr öffentliches Zertifikat mitgesendet. Da Sie bei der Einrichtung die Funktion

aktiviert haben, ausgehenden Nachrichten Ihre digitale Signatur zuzufügen, ist der Punkt „Signieren“ bei Ihnen auch ohne Ihr Zutun immer automatisch aktiviert.

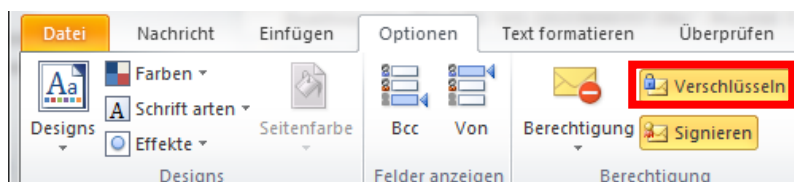


Wenn Sie eine signierte Nachricht eines Kommunikationspartners erhalten haben, mit dem Sie zukünftig verschlüsselte Nachrichten austauschen möchten, so klicken Sie zunächst mit der rechten Maustaste auf den Absender der Nachricht. Aus dem Kontextmenü wählen Sie dann den Menüpunkt **Zu Outlook-Kontakten hinzufügen** und bestätigen das folgende Fenster dann mit **Speichern**. Bei einem bereits bestehenden Kontakt fragt Outlook nach, ob Sie diesen aktualisieren wollen. Auch dies können Sie bestätigen. Das öffentliche Zertifikat wird dann automatisch in dem Kontakt hinterlegt. Zukünftig können Sie dann an diesen Kontakt verschlüsselte E-Mail-Nachrichten senden.

Überprüfen, ob ein Zertifikat korrekt im Kontakt hinterlegt ist, können Sie durch das Öffnen des jeweiligen Kontakts per Doppelklick. Unter der Registerkarte **Kontakt** können Sie dann auf das Feld **Zertifikate** klicken. In diesem sollte dann das Mail-Zertifikat angezeigt werden.



Um nun verschlüsselte E-Mail-Nachrichten an den Empfänger zu versenden, müssen Sie nur noch eine neue E-Mail-Nachricht an den Empfänger erstellen und unter der Registerkarte **Optionen**, zusätzlich die Funktion **Verschlüsseln** aktivieren.



Sollte ein ungültiges oder kein Zertifikat im Kontakt hinterlegt sein, so gibt Outlook eine Warnmeldung beim Versenden der Nachricht aus. In diesem Fall müssen Sie sich nochmal mit Ihrem Kommunikationspartner und/oder Ihrer IT-Abteilung oder Ihrem IT-Dienstleister für eine Problemanalyse in Verbindung setzen.