

eGovernment@School

Senatsverwaltung für Bildung, Jugend und Familie



ZSVU-Useranleitung

Einbinden eines E-Mail-Zertifikats in MS Outlook 2016





Einbinden eines E-Mail-Zertifikats in MS Outlook 2016

Zusammenfassung	
Kategorie	Anleitung
In dieser Anleitung wir 2016 einbinden könne Mails verschicken. Dur gegenüber eindeutig u Sie wirklich der Absend nach dem Versand nich entschlüsseln und lese Daten sichergestellt. Wir empfehlen, dass a	d Ihnen gezeigt, wie Sie E-Mail-Zertifikate in Ihrem Mailkonto in MS Outlook n. Mit diesen E-Mail-Zertifikaten können Sie verschlüsselte und signierte E- ch eine signierte E-Mail weisen Sie sich dem Empfänger der E-Mail nd vertrauenswürdig aus. Durch das Signieren ist für ihn sichergestellt, dass der der E-Mail sind. Zudem wird technisch sichergestellt, dass die E-Mail nt verändert wurde. Verschlüsselte E-Mails kann nur der Empfänger n bzw. den Anhang öffnen. Damit wird die Vertraulichkeit und Integrität der utomatisch alle E-Mails signiert versendet werden.

Inhalt

1.	Einbi	nden eines E-Mail-Zertifikats in MS Outlook 2016	. 3
	1.1	Speichern der Zertifikatsdateien aus einer E-Mail-Anlage	. 3
	1.2	Starten des Zertifikatimport-Assistenten	. 4
	1.3	Der Zertifikatimport-Assistent Schritt-für-Schritt	. 5
2.	Einste	ellungen zur E-Mail-Sicherheit im Outlook Trust Center	. 6



X

für Bildung, Jugend und Familie

1. Einbinden eines E-Mail-Zertifikats in MS Outlook 2016

Outlook 2016 ist ein E-Mail-Client und Organisationstool von Microsoft, das Ihnen auf dem Schuldesktop in der Zentralen Schulverwaltungsumgebung (ZSVU) zur Verfügung gestellt wird.

Das E-Mail-Zertifikat besteht aus zwei Komponenten:

- zwei Zertifikatsdateien (ein Zertifikat zum Signieren von E-Mails und ein Zertifikat zum • Verschlüsseln von E-Mails), die Sie vom SSZB (Absenderadresse: PKI@SenBJF.Berlin.de) erhalten haben und
- einem PIN-Brief, der Ihnen vom SSZB über die Fachpost zugestellt wurde. •

Speichern der Zertifikatsdateien aus einer E-Mail-Anlage 1.1

Speichern Sie beide Zertifikatsdateien (vgl. Abb. 1), erkennbar an der Endung .p12, an einem Ort auf den nur Sie bzw. die berechtigten Personen Zugriff haben, bspw. unter M:\Schulleitung\Zertifikate\E-Mail\20XX, ab.



Abb. 1: Speichern einer Zertifikatsdatei in MS Outlook 2016

Hinweis: Falls Sie ein Zertifikat einbinden möchten, das sich bereits in Ihrer Arbeitsumgebung befindet, können Sie diesen Schritt überspringen und mit Punkt 1.2 fortfahren.





1.2 Starten des Zertifikatimport-Assistenten

Öffnen Sie im Windows-Explorer den (in 1.1 gewählten) Speicherort für die E-Mail-Zertifikate und starten Sie den Zertifikatsimport-Assistenten durch *Doppelklicken* auf eine der beiden Zertifikatsdateien. Bestätigen Sie das erste Fenster des Zertifikatimport-Assistenten mit *Weiter* (vgl. Abb. 2).

Organisieren 🔻	Freigeben für 🔻	Neuer Ordner		
▲ ☆ Favoriten ■ Desktop ● Downloa ● Zuletzt b	ids esucht	Name	-Signatur -Verschluesselung	Änderu 21.11.20 21.11.20
	Zertifikatimport-Assi Willkommen	stent		
	Dieser Assistent hilft ihnen I -sperilisten vom Datenträge Ein von einer Zertifizerungs Es enthäl: Informationen für Netzwerkorenindungen. Ein gespeichert werden. Speicherort Aktueller Benutzer I koleier Computer	zein Kopieren von Zertifikaten, Zei rin den Zertifikatspeicher. stelle ausgestelltes Zertifikat dent den Datenschutz oder für den Au Zertifikatspeicher ist dei Systembe	rtifikatvertrauenslisten und der Identtätsbestätigung. fbau sicherer rech, in dem Zertifikate	
	Klicken Sie auf "Weiter", um	den Vorgang fortzusetzen.	Weite: Abbrecher	

Abb. 2: Aufrufen des Zertifikatimport-Assistenten





1.3 Der Zertifikatimport-Assistent Schritt-für-Schritt

Bestätigen Sie den nächsten Schritt (*Zu importierende Datei*) zunächst mit *Weiter*. Beim Schritt *Kennwort* geben Sie bitte das Kennwort auf Ihrem PIN-Brief ein, das Sie für die E-Mail-Zertifikate erhalten haben und bestätigen Sie dieses Fenster ebenfalls mit *Weiter* (vgl. Abb. 3).

Certifikatimport-Assistent	tifikatimport-Assistent
Zu importierende Datei Geben Sie die Datei an, die importiert werden soll.	Kennwort Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.
Dateiname: E1 Signatur.p12 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)	Geben Sie das Kennwort für den privaten Schlüssel ein. Kennwort: Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert. Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen. V Alle erweiterten Eigenschaften mit einbeziehen.
Weitere Informationen über Zertifikatdateiformate	Weitere Informationen über das Sichern privater Schlüssel
< Zurück Weiter > Abbrechen	< Zurück Weiter >

Abb. 3: Dateiimport und Kennwortabfrage im Zertifikatimport-Assistenten

Die nachfolgende Abfrage (*Zertifikatspeicher*) bestätigen Sie ebenfalls mit *Weiter* und beenden den Assistenten mit einem Klick auf *Fertig stellen* (vgl. Abb. 4). Bestätigen Sie das Dialogfenster zum erfolgreichen Importvorgang mit *OK*.

ertifikatimport-Assistent	Zertifikatimport-Assistent
Zertifikatspeicher Zertifikatspeicher sind Systembereiche, in denen Zertifikate gespeichert werden.	Fertigstellen des Assistenten
Windows kann automatisch einen Zertifikatspeicher auswählen, oder Sie können einen Speicherort für die Zertifikate angeben. © Zertifikatspeicher automatisch auswählen (auf dem Zertifikattyp basierend) © Alle Zertifikate in folgendem Speicher speichern Zertifikatspeicher: Durchsuchen	Das Zertifikat wird importiert, nachdem Sie auf "Fertig stelen" geliddt haben. Sie haben folgende Enstellungen ausgewählt: Gewählter Zertifikatspecifier Inhalt PFX Dateiname E: Signatur.p
Weitere Informationen über Zertifikatspeicher	< >
< Zurück Weiter > Abbrechen	 Zurück Fertig stell



Wiederholen Sie nun die Schritte 1.2 und 1.3 für das zweite E-Mail-Zertifikat



BERLIN

X

2. Einstellungen zur E-Mail-Sicherheit im MS Outlook Trust Center

1. Nach dem Import der E-Mail-Zertifikate müssen in MS Outlook verschiedene Sicherheitseinstellungen vorgenommen werden. Klicken Sie hierfür in MS Outlook auf die Registerkarte Datei und wählen Optionen aus (vgl. Abb. 5).



Abb. 5: Aufrufen der Einstellungsoptionen in Outlook

2. Im neu geöffneten Fenster Outlook–Optionen wählen Sie auf der linken Seite den letzten Eintrag Trust Center aus und klicken rechts auf die Schaltfläche Einstellungen für das Trust Center (vgl. Abb. 6).



Abb. 6: Öffnen des Trust Centers in Outlook



BERLIN

X

3. Klicken Sie nun links auf E-Mail-Sicherheit und wählen rechts in den Einstellungen unter Verschlüsselte E-Mail-Nachrichten die Einträge Ausgehende Nachrichten digitale Signatur hinzufügen und Signierte Nachrichten als Klartext senden durch Setzen eines entsprechenden Hakens aus. Klicken Sie anschließend auf die Schaltfläche Einstellungen... (vgl. Abb. 7).



Abb. 7: Einstellungen zur E-Mail-Sicherheit im Trust Center

A C H T U N G: Sofern mehr als ein E-Mail-Account in Outlook verwendet wird, wählen Sie Ausgehenden Nachrichten digitale Signatur hinzufügen nicht aus, da es zu Komplikationen kommen kann, wenn nicht für alle E-Mail-Adressen Zertifikate vorhanden sind!

4. Das Fenster Sicherheitseinstellungen ändern bietet im unteren Fensterbereich zwei Schaltflächen zum Auswählen der Zertifikate. Wählen Sie dort die neuen E-Mail-Zertifikate, die Sie verwenden möchten, aus. Wenn bereits mehrere Zertifikate installiert wurden, können Sie sich zur Auswahl des richtigen Zertifikats am Gültigkeitszeitraum orientieren. Bestätigen Sie die Auswahl jeweils mit OK. Stellen Sie nun im Fenster Sicherheitseinstellungen ändern den Hashalgorithmus auf SHA256 und den Verschlüsselungsalgorithmus auf AES (256-bit) und schließen Sie das Fenster mit OK (vgl. Abb. 8).

Name der Sicherheitseinstellun	ig:		
Einstellung			
Kryptografieformat:	S/MIME		
Sicherheitskennzeichen	Neu	Löschen	Kennwort
Zertifikate und Algorithmen	cianati ir		Augurählen
Signatal zer ankat.	Signatur		Addition
Hashalgorithmus:	SHA256		
Verschlüsselungszertifikat:	verschluesselung		Auswählen
	AES (256-bit)	~	

Abb. 8: Sicherheitseinstellungen im Trust Center ändern