

# S/MIME Zertifikate

## Bestellung – Installation – Backup

Die S/MIME E-Mail Zertifikate erlauben den Versand von kryptierten und / oder digital signierten E-Mails. Damit kann der Empfänger Ihrer Nachricht davon ausgehen, dass der Absender auch wirklich der Absender der Nachricht ist. Zudem können Sie sicher sein, dass Ihre Nachricht während der Übermittlung inhaltlich nicht abgeändert wurde. Bei kryptierten (verschlüsselten) E-Mails können Sie zudem sicher sein, dass auch nur die eindeutig zuordenbare Person Ihre Nachricht lesen kann.

## S/MIME Zertifikat / Bestellablauf

---

Der Admin Ihres Unternehmens bestellt ein S/MIME Zertifikat für ihre E-Mail Adresse über unseren EPKI Management Tool. Als Bestätigung für die Bestellung erhalten Sie als End-User sowie der Admin eine Bestätigung vom Absender Comodo. Der darin enthalte Link öffnen Sie mit dem passenden Browser:

Windows  
Mac (iOS)

Internet Explorer  
Firefox

Dear [REDACTED]

Your System Administrator requests you to apply for a Corporate Secure Email Certificate to allow you to encrypt and digitally sign your emails.

The Corporate Secure Email Certificate will integrate into your existing email client.

Please click the button below to begin your application.  
[Begin Corporate Secure Email Certificate Application]

If the above button does not work, please navigate to <https://secure.comodo.net/products/CorporateSecureEmail>.  
Your Certificate Password is: [REDACTED]

This email message was sent on behalf of your System Administrator. Should you have any questions regarding your Corporate Secure Email Certificate application, please contact your System Administrator.

Kind Regards,

Comodo Security Services  
[noreply\\_support@comodo.com](mailto:noreply_support@comodo.com)

Secorio AG  
Idyllweg 4  
CH-Hergiswil NW

Tel: +41 41 514 31 31  
Fax: +41 41 560 83 83  
[info@secorio.com](mailto:info@secorio.com)



# Bestellung / Installation / Backup von S/MIME

In der zu öffnenden Seite tragen Sie Ihre E-Mail Adresse und Passwort aus der vorangegangenen Nachricht ein.

## Corporate Secure Email Certificate Center

### User Details:

Please enter the following details:

Email Address

Certificate Password

Anschliessend erhalten Sie eine E-Mail mit einem neuen Link und einem neuen Passwort für das Herunterladen des S/MIME Zertifikate.

Dear Jeffrey Keiser,

Your Corporate Secure Email Certificate has now been issued and is ready to be collected.

Please click the button below to begin collection.  
[Begin Corporate Secure Email Certificate Collection]

If the above button does not work, please navigate to <https://secure.comodo.net/products/CorporateSecureEmail>.  
Your Certificate Password is [REDACTED]

This email message was sent on behalf of your System Administrator. Should you have any questions regarding your Corporate Secure Email Certificate application, please contact your System Administrator.

Kind Regards,

Comodo Security Services  
[noreply\\_support@comodo.com](mailto:noreply_support@comodo.com)

Zu 95% wird das Zertifikat automatisch über den Browser installiert und in Ihren Downloads abgelegt. In einem weiteren Schritt müssen Sie das Zertifikat im Outlook zuordnen.

Weiterführende Informationen finden Sie auf

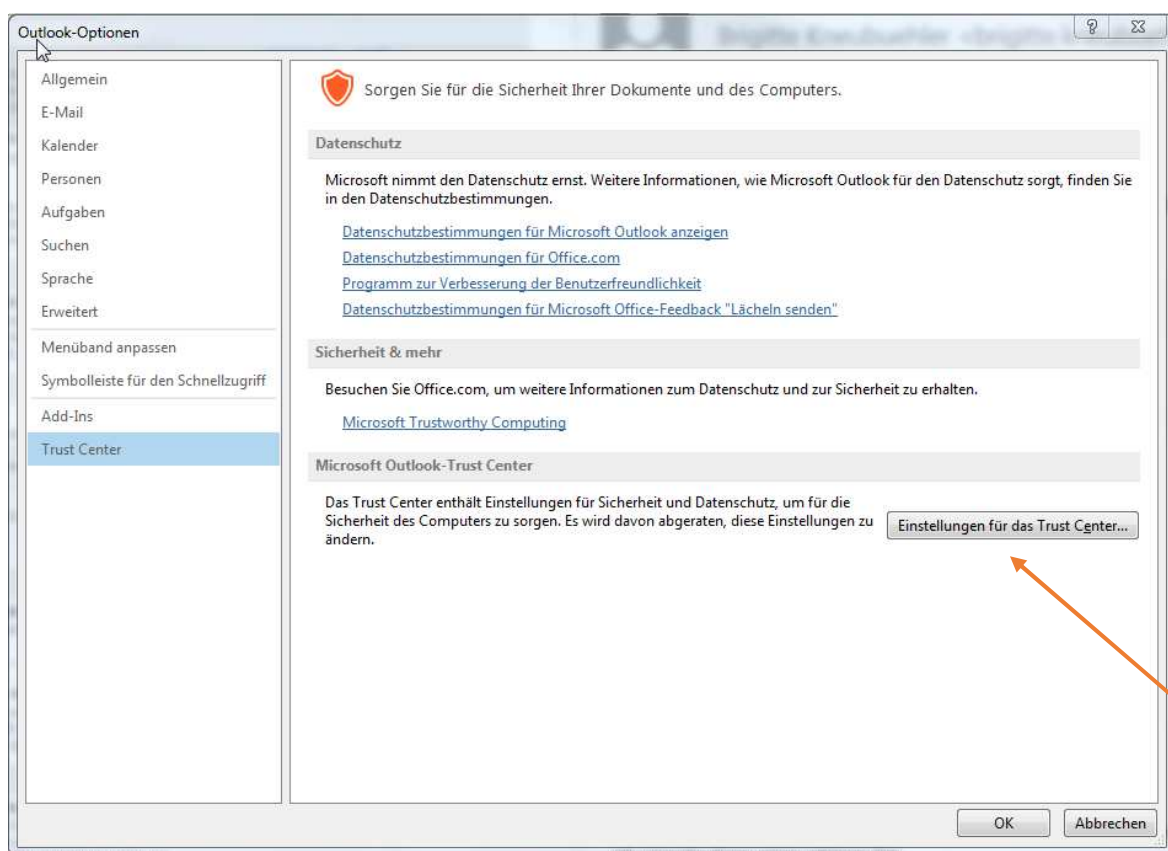
<https://support.comodo.com/index.php?/Knowledgebase/List/Index/18/email-smime>



## Outlook für automatisches Signieren konfigurieren

Die S/MIME Zertifikate bieten einer signierten E-Mail die Sicherheit für den Empfänger, dass der Absender auch wirklich der Absender ist und der Inhalt auf dem Transportweg nicht verändert wurde. In Outlook können Sie einstellen, dass E-Mails immer signiert werden. Für den E-Mail Empfänger ist es kein Problem, wenn er kein eigenes Zertifikat besitzt. Sie können dann aber keine kryptierte E-Mail Kommunikation führen.

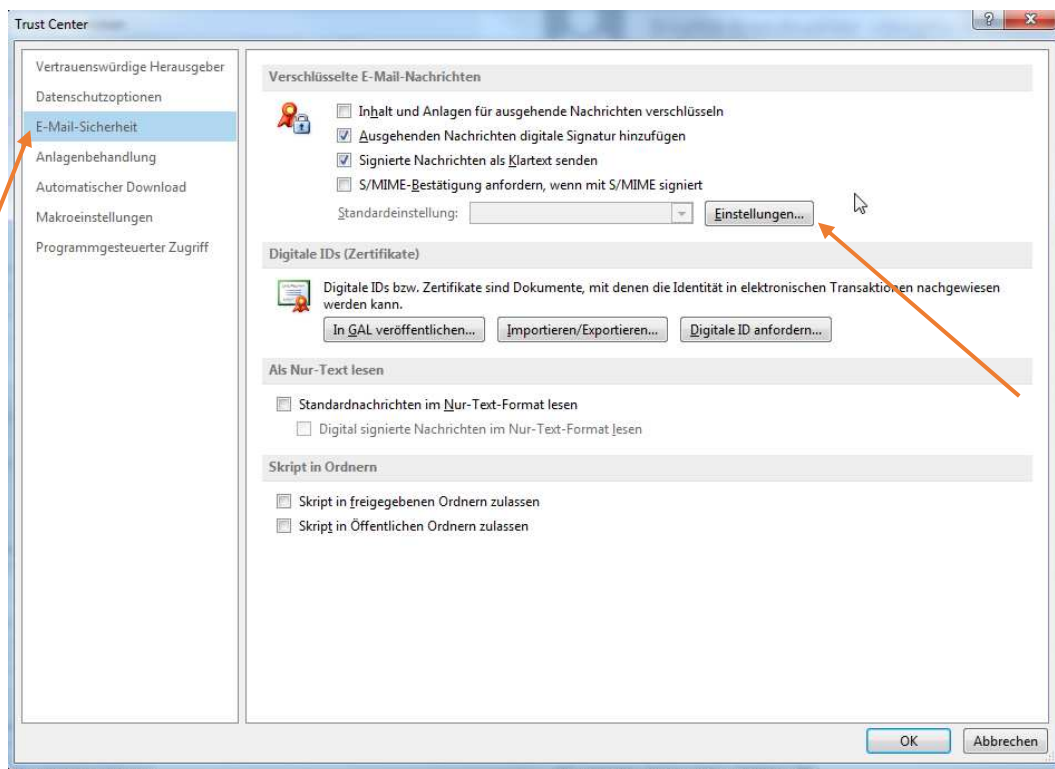
In den Screenshots wird Outlook 2013 verwendet. In den neuen Outlook 2013 & 2016 Versionen heisst es neu "Trust-Center". In vorigen Outlookversionen heisst der Menüpunkt "Sicherheitscenter".



Sie erreichen das Einstellungsmenü über **Datei / Einstellungen** und anschliessend auf der linken Seite im Menü **Trust Center**. Im Interface wählen Sie auf der rechten Seite "**Einstellungen für das Trust Center**".



# Bestellung / Installation / Backup von S/MIME

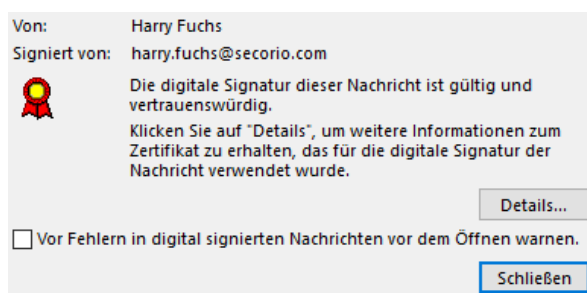


Um nun alle E-Mails zukünftig automatisch signiert zu versenden, wählen Sie **"Ausgehende Nachrichten digitale Signatur hinzufügen"** aus und klicken auf **"OK"**. Unter Einstellungen ordnen Sie das Zertifikat dem zugehörigen E-Mail Account zu.

Beim Empfänger wird das Symbol rechts in der Mail angezeigt, wenn das E-Mail von Ihnen signiert wurde. Mit einem Klick auf das angezeigte Symbol, öffnet sich eine Detailansicht des Zertifikates.



## Verschlüsselte E-Mail versenden

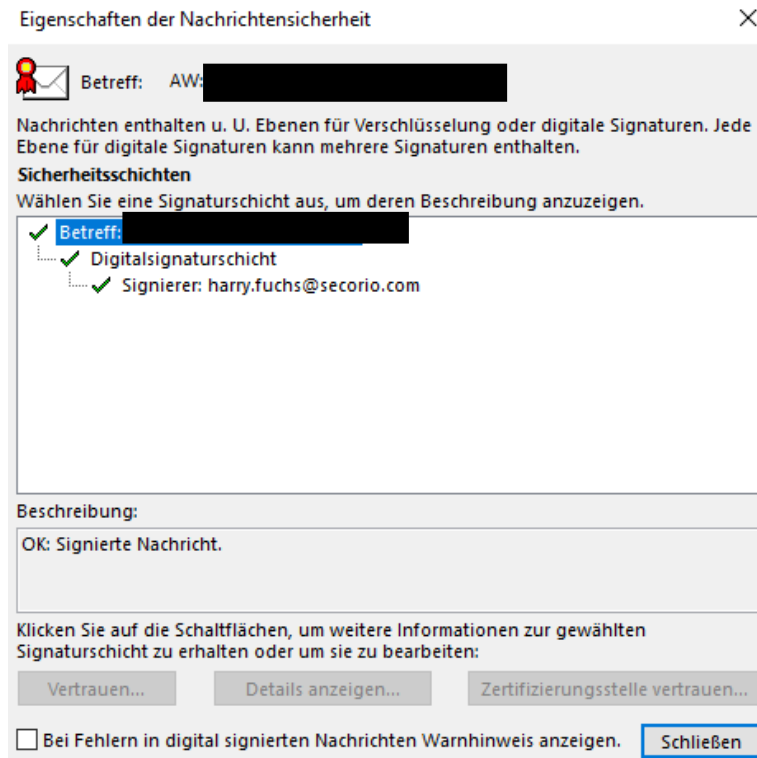


Um eine E-Mail verschlüsselt / kryptiert zu versenden, ist es notwendig, dass man mind. einmal öffentlichen Schlüssel der Person lokal installiert hat. Diesen erhalten Sie automatisch mit einer signierten E-Mail mit. Schicken Sie sich gegenseitig eine signierte E-Mail, ab sofort können Sie sämtliche Nachrichten kryptiert versenden.

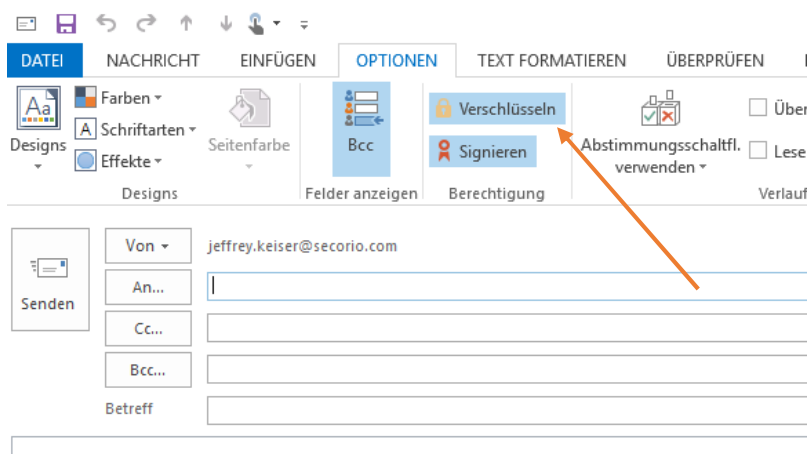


# Bestellung / Installation / Backup von S/MIME

Sie sehen nun dass es sich um eine **Digitale Signatur** handelt, und das Zertifikat **gültig** ist. Mit einem Klick auf "**Details...**" können Sie sich weitere Informationen zum Zertifikat ansehen. Beispielsweise Firmenname, E-Mail und Vor- und Nachname.



Um eine E-Mail zu verschlüsseln, öffnen Sie eine neue Nachricht und wählen den Menüpunkt "**Optionen**" aus und dort "**Verschlüsseln**". Wenn das Feld farbig hinterlegt ist, sehen Sie, ob die Mail nur signiert, oder auch verschlüsselt versendet wird.



# Bestellung / Installation / Backup von S/MIME

Wenn der Empfänger Outlook verwendet, können die folgenden beiden Symbole erscheinen:

 signiert

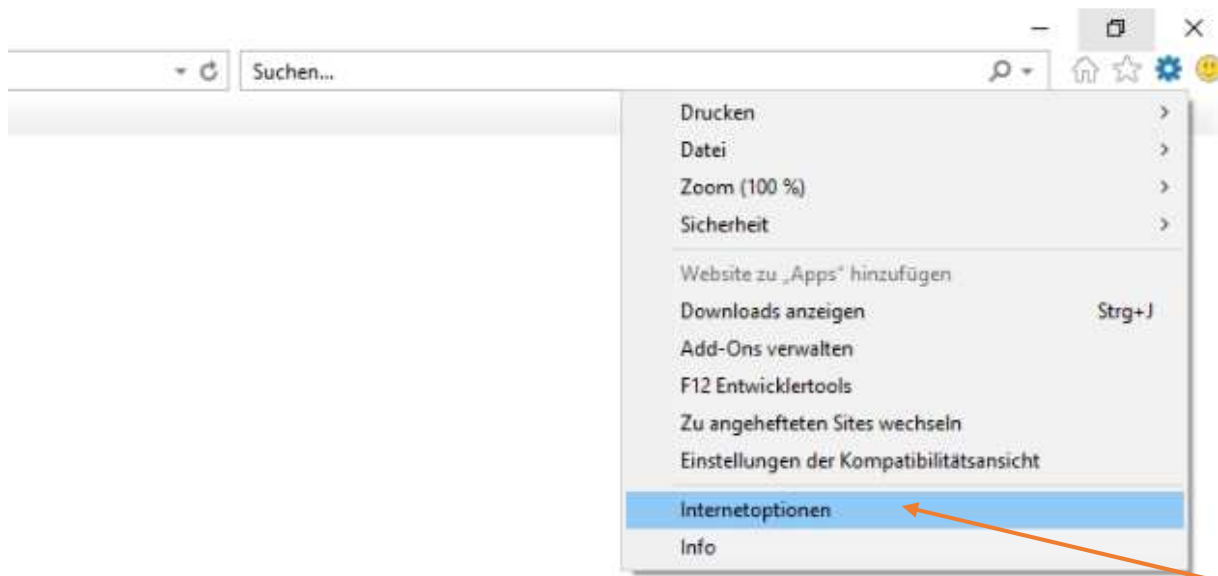
 verschlüsselt

Der Installationsprozess ist für den User abgeschlossen. Als Admin empfehlen wir Ihnen, nun ein Backup zu erstellen.

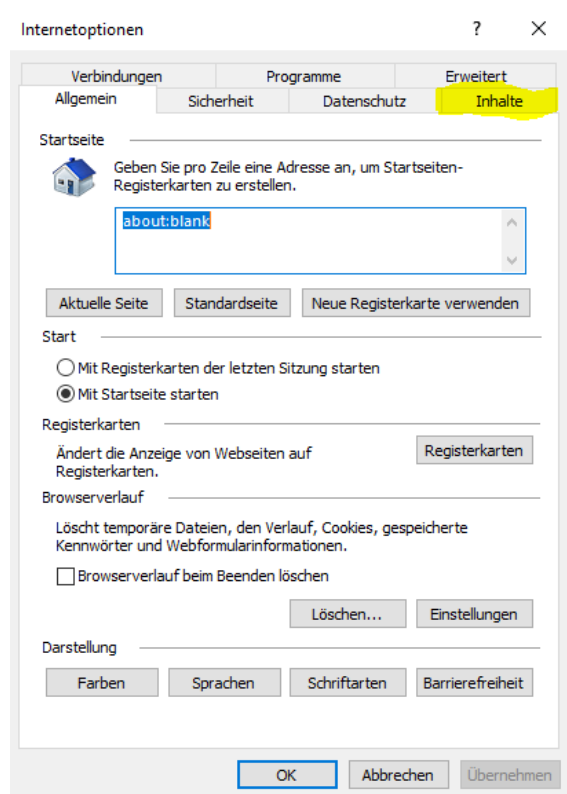
## Backup erstellen

Wir empfehlen Ihnen, nach der Installation des Zertifikates von diesem zusammen mit dem Privat Key ein Backup zu erstellen (pfx-File). Damit kommen Sie auch der Aufbewahrungspflicht für die E-Mail Kommunikation nach. Dieser Vorgang ist jeweils auf dem Rechner des Users auszuführen.

Öffnen Sie Internet Explorer bei Windows und Google Chrome bei Apple iOS. Öffnen Sie anschliessend unter Einstellungen das Menu „**Internetoptionen**“.



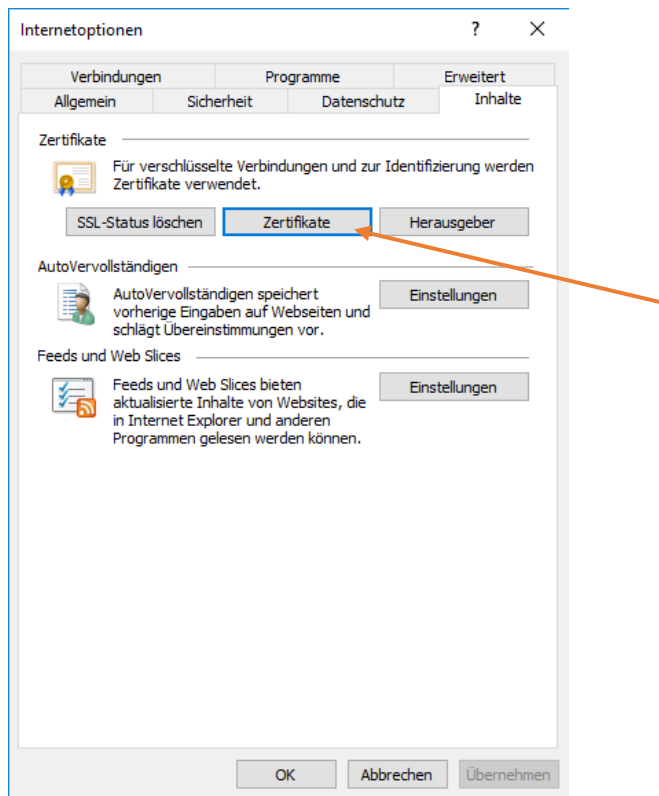
# Bestellung / Installation / Backup von S/MIME



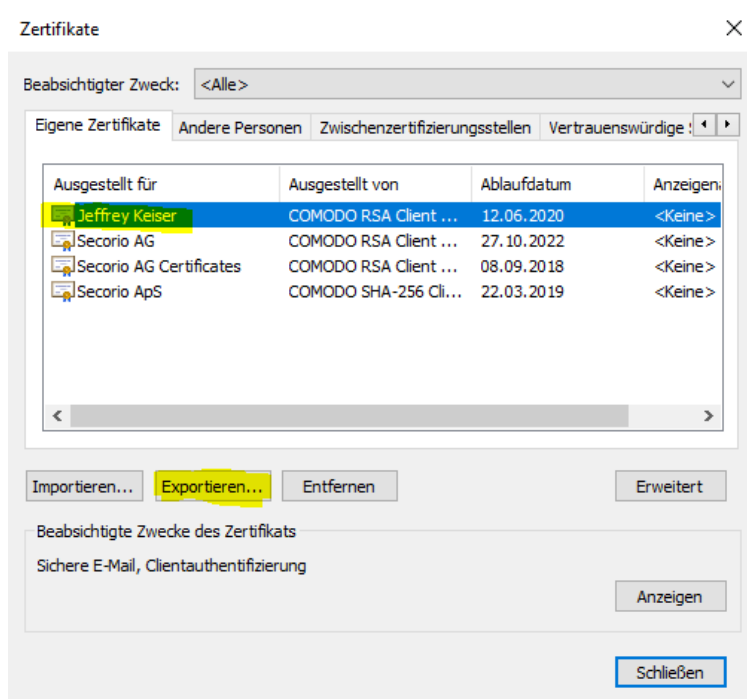
Wählen Sie das Registerfeld **„Inhalte“** an, um in den Bereich der Zertifikate zu kommen.



# Bestellung / Installation / Backup von S/MIME



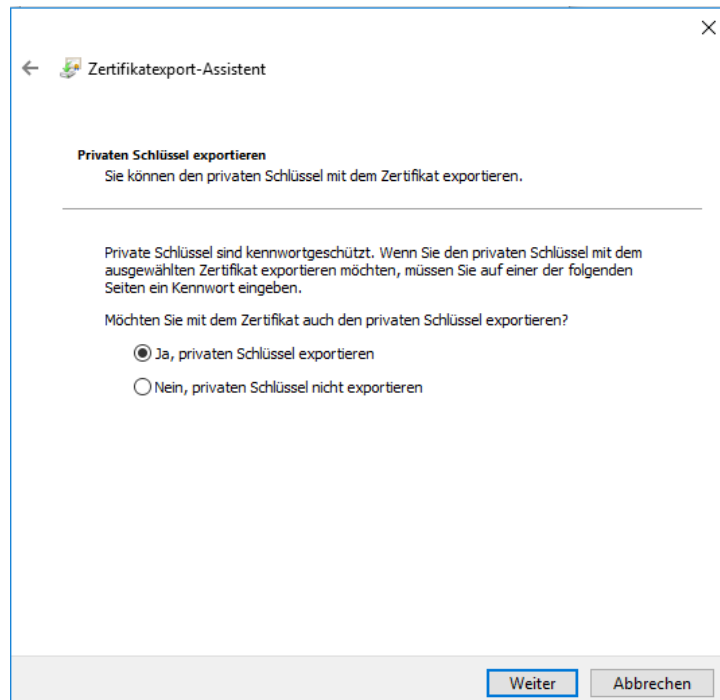
Öffnen Sie mit einem Klick auf des Feld „**Zertifikate**“ eine Übersicht sämtlicher Zertifikate, welche aktuell auf Ihrem Rechner installiert sind.





# Bestellung / Installation / Backup von S/MIME

Sie erhalten nun eine Übersicht sämtlicher Zertifikate, welche auf Ihrem Rechner installiert sind. Wählen Sie das Zertifikat an, welches Sie exportieren möchten. Anschliessend öffnet sich automatisch ein Zertifikatsexport-Assistent von Windows, welcher Sie beim Export Schritt für Schritt anleitet.



The screenshot shows a Windows dialog box titled "Zertifikatsexport-Assistent". The main heading is "Privaten Schlüssel exportieren" with the instruction "Sie können den privaten Schlüssel mit dem Zertifikat exportieren." Below this, a note states: "Private Schlüssel sind kennwortgeschützt. Wenn Sie den privaten Schlüssel mit dem ausgewählten Zertifikat exportieren möchten, müssen Sie auf einer der folgenden Seiten ein Kennwort eingeben." The question "Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?" is followed by two radio button options: "Ja, privaten Schlüssel exportieren" (which is selected) and "Nein, privaten Schlüssel nicht exportieren". At the bottom, there are two buttons: "Weiter" and "Abbrechen".

**WICHTIG: Privater Schlüssel anwählen für den Export**



# Bestellung / Installation / Backup von S/MIME

← Zertifikatexport-Assistent

**Format der zu exportierenden Datei**  
Zertifikate können in verschiedenen Dateiformaten exportiert werden.

Wählen Sie das gewünschte Format:

- DER-codiert-binär X.509 (.CER)
- Base-64-codiert X.509 (.CER)
- Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
  - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Privater Informationsaustausch - PKCS #12 (.PFX)
  - Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
  - Privaten Schlüssel nach erfolgreichem Export löschen
  - Alle erweiterten Eigenschaften exportieren
  - Zertifikatdatenschutz aktivieren
- Microsoft Serieller Zertifikatspeicher (.SST)

Weiter Abbrechen

In der Regel sollte dies als Standard hinterlegt sein. Allenfalls empfehlen wir Ihnen, die beiden markierten Kästchen einen Hacken zu setzen.

← Zertifikatexport-Assistent

**Sicherheit**  
Zur Gewährleistung der Sicherheit müssen Sie den privaten Schlüssel mit einem Sicherheitsprinzipal oder mithilfe eines Kennworts schützen.

Gruppen- oder Benutzernamen (empfohlen)

Hinzufügen  
Entfernen

Kennwort:

Kennwort bestätigen:

Weiter Abbrechen



# Bestellung / Installation / Backup von S/MIME

Zudem empfehlen wir Ihnen, ein Passwort für den Export des Zertifikates zu setzen. Notieren oder Speichern Sie das gesetzte Passwort an einem sicheren Ort ab, auf welchen Sie jederzeit wieder zurückgreifen können.

Sollte Ihnen etwas Unklar sein oder haben Sie Anregungen, so kommen Sie doch bitte auf uns zu. Gerne sind wir für Sie da und unterstützen Sie bei der Bestellung, der Installation oder beim Backup unserer S/MIME Zertifikate.

