



V2.1 / 11. Dezember 2023

Gruppenmailboxzertifikate

Arbeitsleitfaden

Inhaltsverzeichnis

Gruppenmailboxzertifikate	1
Arbeitsleitfaden	1
1 Einleitung	2
1.1 Zweck des Dokumentes	2
1.2 Ziel des Dokumentes	2
1.3 Aufbau des Dokumentes	2
2 Allgemeines zum Gruppenmailboxzertifikat	3
2.1 Beschreibung	3
2.2 Gültigkeit	3
2.3 Bestellung	3
2.4 Publikation	3
2.5 Revokation	3
2.6 Erneuerung	3
2.7 CP/CPS	3
3 Besitzer eines Gruppenmailboxzertifikates	4
3.1 Installation eines Gruppenmailboxzertifikates	4
3.2 „Public Key“ veröffentlichen falls nicht das Directory des Bundes genutzt wird	6
4 Benutzer eines Gruppenmailboxzertifikates	7
4.1 Kontakt hinzufügen und Zertifikat assoziieren	7
4.2 Verschlüsselte E-Mail an Kontakt senden	8

1 Einleitung

1.1 Zweck des Dokumentes

Der Einsatz von Gruppenmailboxzertifikaten ist nicht ganz trivial und erfordert von den Besitzern und den Benutzern einige Vorbereitungen. Dieses Dokument soll Besitzer von Gruppenmailboxzertifikaten und allen Mitbenutzern der Gruppenmailbox als „Benutzer“ davon als Handbuch dienen.

1.2 Ziel des Dokumentes

Das Dokument soll die Arbeit mit dem Gruppenmailboxzertifikat erleichtern und Tipps und Tricks auch für deren Benutzern liefern.

1.3 Aufbau des Dokumentes

Das Dokument ist in 2 Teile aufgeteilt sein, wobei der erste für die Besitzer der Gruppenmailboxen und des Zertifikats ist. Hier wird beschrieben, wie man das Zertifikat installiert und welchen Schlüssel man publizieren muss, damit das Zertifikat von Personen, die die Mailbox anschreiben zur Verschlüsselung der Mails benutzt werden kann.

Der zweite Teil dieses Handbuchs ist für die „Kunden“, also Dritte, die einem Amt eine verschlüsselte Nachricht übermitteln wollen. Dazu brauchen Sie den sog. „Public Key“ der Gruppenmailbox und müssen dieses Zertifikat der anzuschreibenden Mailadresse ihrem persönlichen Adressbuch zuordnen.

2 Allgemeines zum Gruppenmailboxzertifikat

2.1 Beschreibung

Gruppenmailboxes unterstützen Organisationseinheiten bei der Abwicklung ihrer Geschäftsprozesse (elektronischer Behördenverkehr). Gruppenmailboxzertifikate dienen primär dem verschlüsselten Austausch von Daten im Behördenverkehr zwischen Bürger und der Verwaltung. Mit Gruppenmailboxzertifikaten können mehrere Personen Zugriff auf die verschlüsselten E-Mails erhalten.

Technisch handelt es sich um ein Soft-Zertifikat, welches auf den Clients installiert werden kann. Dieses bietet die Funktionen Verschlüsselung und Signatur. Das Soft-Zertifikat wird von der Swiss Government PKI publiziert.

2.2 Gültigkeit

Gruppenmailboxzertifikate haben eine Gültigkeit von 3 Jahren und sind durch den Besitzer vor Ablauf neu zu bestellen.

2.3 Bestellung

Die Behörde stellt beim MAC-Manager (MAC-Manager@bit.admin.ch) eine Bestellung für Gruppenmailboxzertifikate aus, oder erfasst den MAC direkt über die Remedy Requester Console mittels Remedy-MAC. Die Swiss Government PKI erfasst das Zertifikat mittels CRW Tool und sendet jeweils eine Validierungsmail an die Gruppenmailbox. Sobald die Daten vom Besitzer validiert worden sind, wird das Gruppenmailboxzertifikat ausgestellt und an den Besitzer der Gruppenmailbox gesendet.

2.4 Publikation

Gruppenmailboxzertifikate werden von der Swiss Government PKI im Directory des Bundes publiziert. Benutzen die Behörden nicht das Directory des Bundes für die Publikation des Zertifikats, sind sie für deren Publikation und Installation selbst zuständig.

2.5 Revokation

Die berechtigten Personen der Verwaltungseinheit können die Revokation mittels Remedy-MAC beantragen.

2.6 Erneuerung

Für die Erneuerung der Gruppenmailboxzertifikate gilt der Prozess der Initialausstellung.

2.7 CP/CPS

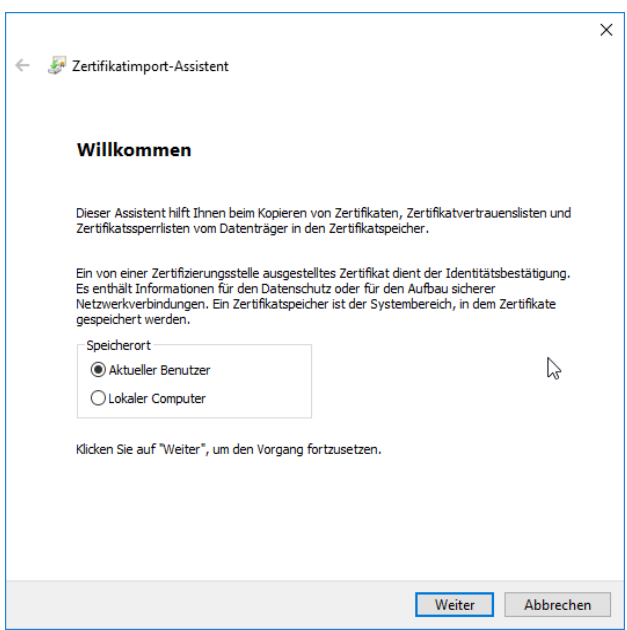
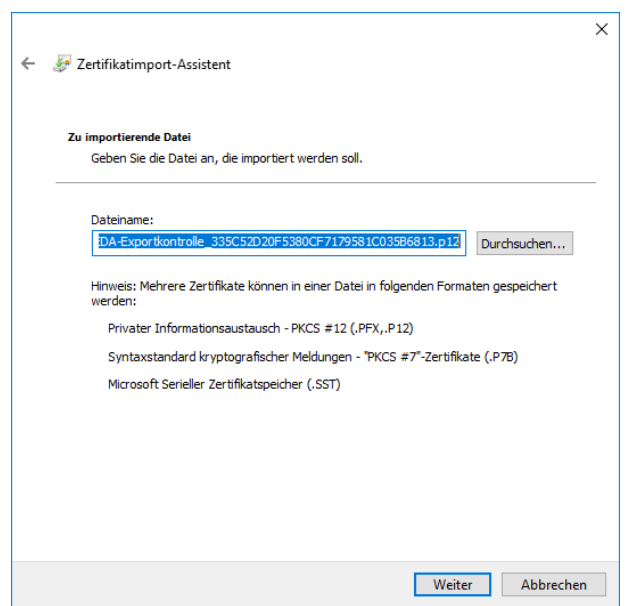
Die Rechte und Pflichten beim Bezug und Einsatz der Gruppenmailboxzertifikate sind in der CP/CPS beschrieben, sowie in den Nutzungsbedingungen und Guidelines der Klasse C Standardzertifikate.

Nähere Informationen, Formulare und die CP/CPS finden Sie auch unter: [Gruppenmailboxzertifikate auf unserer Homepage www.pki.admin.ch](http://www.pki.admin.ch).

3 Besitzer eines Gruppenmailboxzertifikates

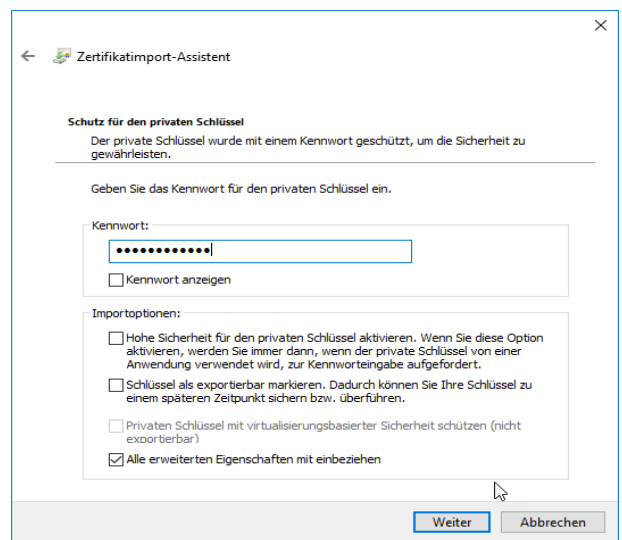
3.1 Installation eines Gruppenmailboxzertifikates

Die Installation eines Gruppenmailboxzertifikates muss auf jedem Rechner erfolgen, der mit dieser Gruppenmailbox arbeitet. Die erhaltene *.P12 Datei wird im Zertifikatsspeicher „importiert“. So funktioniert es:

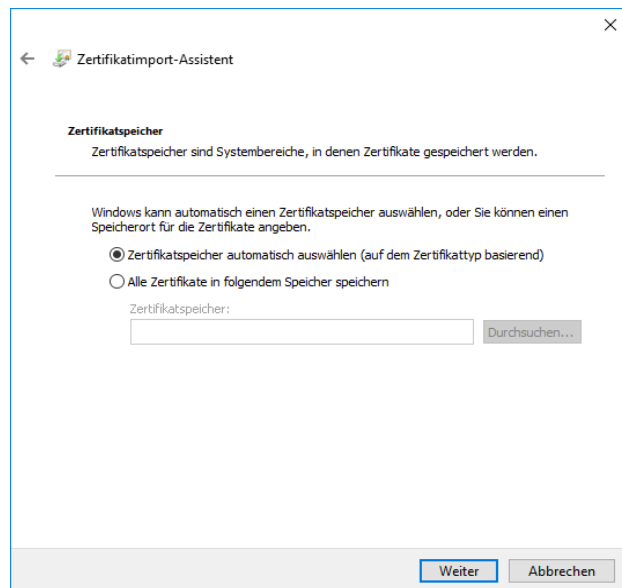
<p>Die *.p12 –Datei doppelklicken, und auf „Weiter“ klicken.</p>	
<p>Dateipfad mit „weiter“ bestätigen.</p>	

Das per Mail erhaltene Kennwort eingeben, und **KEINE** weiteren Elemente anklicken!

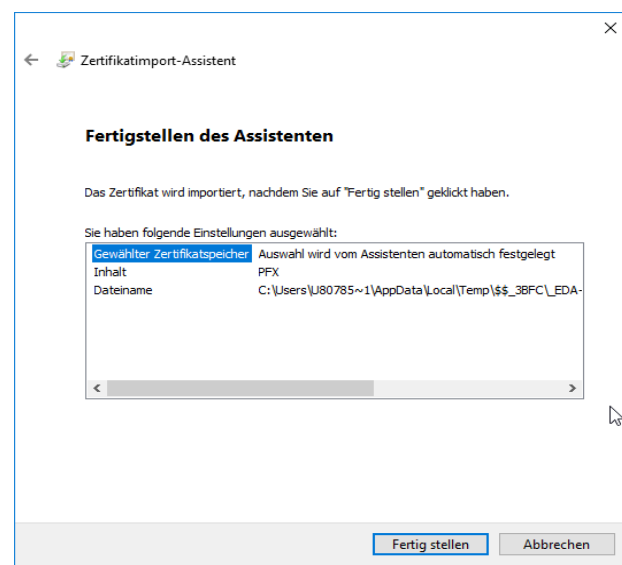
Mit „weiter“ zum nächsten Fenster.



„Zertifikatsspeicher automatisch auswählen“ auswählen und auf „weiter“ klicken.

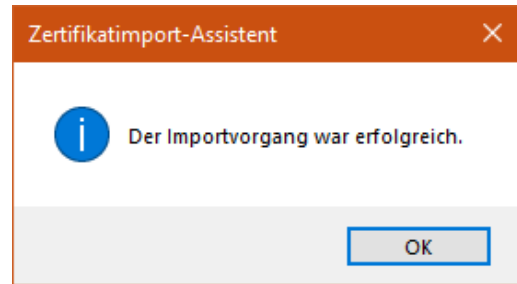


„Fertig stellen“.



„OK“.

Das Zertifikat ist nun im Speicher importiert.



3.2 „Public Key“ veröffentlichen falls nicht das Directory des Bundes genutzt wird

In der Regel wird das Gruppenmailboxzertifikat im Directory des Bundes publiziert. Benutzen die Behörden nicht dieses Directory für die Publikation des Zertifikats, sind sie für deren Publikation und Installation selbst zuständig. Damit Dritte Mails für Ihre Gruppenmailbox verschlüsseln können, müssen diese Zugang zum öffentlichen Schlüssel („Public Key“) des Gruppenmailboxzertifikates haben. Der öffentliche Schlüssel hat die Endung *.cer und nicht *.p12 wie Ihr eigenes importiertes Zertifikat! Der öffentliche Schlüssel ist in der erhaltenen ZIP Datei enthalten.

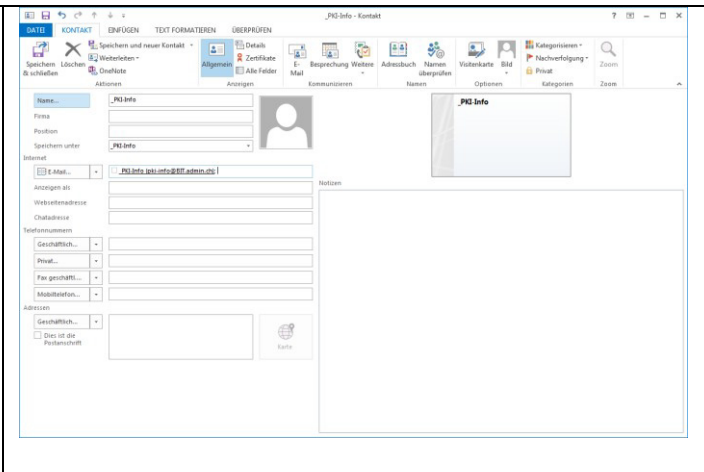
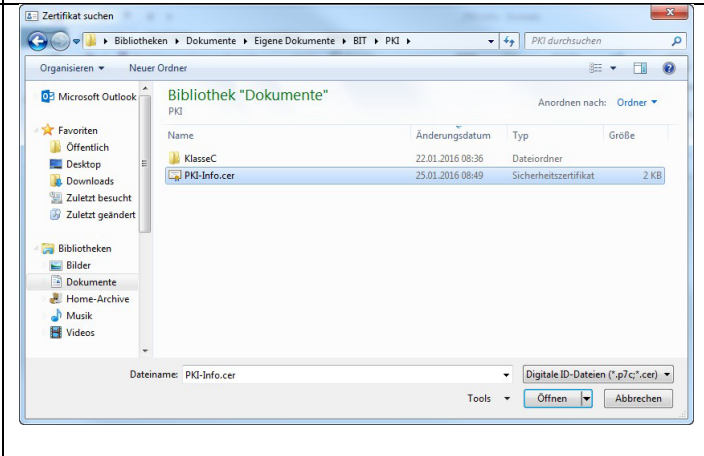
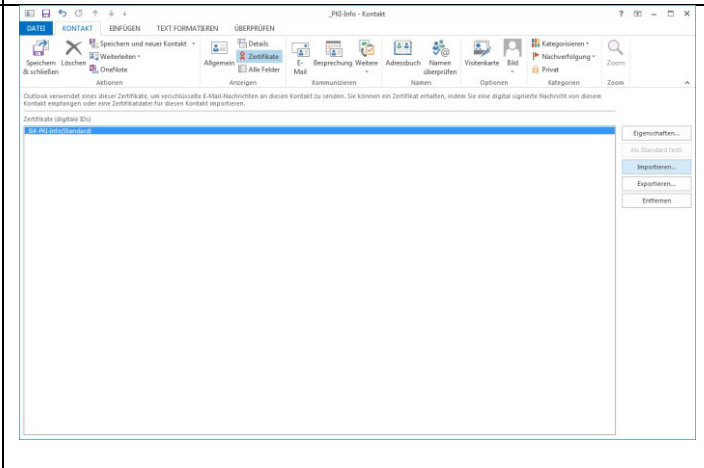
Diese *.CER –Datei müssen Sie Dritten zur Verfügung stellen, damit man Ihnen verschlüsselte Mails zusenden kann. Sollte dieser Vorgang unter Punkt 3.2 nicht möglich sein können Sie dies z.B. tun, indem Sie eine signierte Mail von dieser Mailbox senden

4 Benutzer eines Gruppenmailboxzertifikates

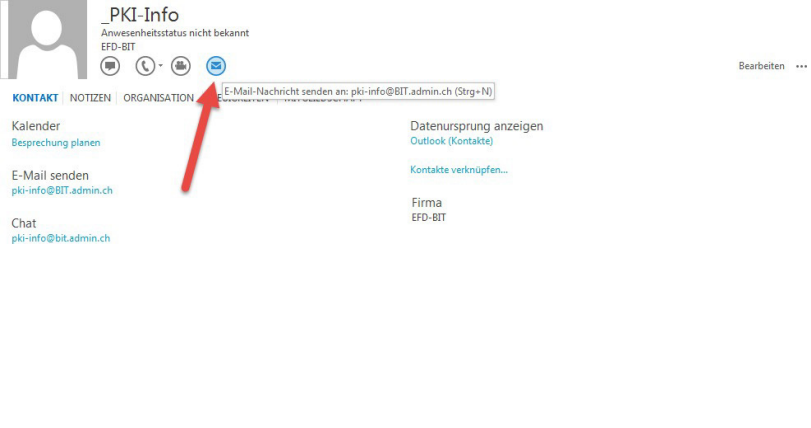
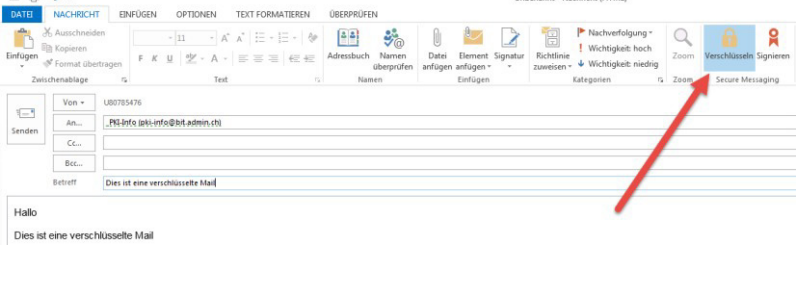

Grundsätzlich müssen Mails, die verschlüsselt versendet werden müssen, mit dem öffentlichen Schlüssel („Public Key“) des Empfängers codiert werden. Der öffentliche Schlüssel muss vom Empfänger zur Verfügung gestellt werden, sei es per Mail oder auf einer Homepage zum Download.

Im Anschluss zeigen wir einen Vorschlag, wie man im MS Outlook einer Gruppenmailbox eine verschlüsselte Mail zustellt. Wichtig ist, dass der „Kontakt“ aufgenommen wurde und das Zertifikat der Kontaktinfo schon zugeordnet wurde. So wird es im Outlook gemacht:

4.1 Kontakt hinzufügen und Zertifikat assoziieren

<p>Einen neuen „Kontakt“ erstellen, und die Mindestanforderungen eingeben:</p> <ul style="list-style-type: none">- Name- E-Mail <p>(Der Bezug zum Zertifikat wird mit der E-Mailadresse gemacht!)</p>	 The screenshot shows the 'Kontakt' (Contact) form in Microsoft Outlook. The contact name is '_PKI Info'. The email address is '_PKI-Info-Info@BIT.admin.tu-berlin.de'. The form includes fields for Name, Firma, Position, E-Mail, and various phone numbers. The 'Zertifikate' (Certificates) tab is active, showing a list of certificates associated with the contact.
<p>Zum Button „Zertifikate“ wechseln und auf „importieren“ klicken.</p> <p>Das Zertifikat im Ablageordner suchen, an-klicken und auf „öffnen“ klicken.</p>	 The screenshot shows a Windows Explorer window with the address bar set to 'Bibliotheken > Dokumente > Eigene Dokumente > BIT > PKI'. The main pane shows a file named 'PKI-Info.cer' with a size of 2 KB. The file type is 'Sicherheitszertifikat'. The 'Dateiname' field at the bottom shows 'PKI-Info.cer' and the file type is set to 'Digitale ID-Dateien (*.p7c;*.cer)'. The 'Tools' bar includes 'Offnen' and 'Abbrechen' buttons.
<p>Das Zertifikat ist jetzt mit dem Kontakt verknüpft. Klicken Sie auf „Speichern und schliessen“ um den Kontakt zu speichern.</p>	 The screenshot shows the 'Kontakt' form in Microsoft Outlook, similar to the first screenshot. The 'Speichern und schliessen' (Save and Close) button is highlighted in the top-left corner of the ribbon. The contact information remains the same.

4.2 Verschlüsselte E-Mail an Kontakt senden

<p>Senden Sie zu verschlüsselnden Mails für eine Gruppenmailbox direkt aus der Kontaktliste heraus:</p> <p>Öffnen Sie Ihr gespeicherter „Kontakt“ aus Kap. 4.1. und klicken Sie auf das Symbol:</p>	 <p>The screenshot shows the contact card for '_PKI-Info' in Outlook. The contact's name is '_PKI-Info' with the status 'Abwesenheitsstatus nicht bekannt' and 'EFD-BIT'. Below the name are icons for calendar, meeting planning, email, and chat. A red arrow points to the email icon, which has a tooltip that reads 'E-Mail-Nachricht senden an: pki-info@BIT.admin.ch (Strg+N)'. Other options like 'Kalender', 'Besprechung planen', 'E-Mail senden', 'Chat', 'Datenursprung anzeigen', 'Outlook (Kontakte)', 'Kontakte verknüpfen...', and 'Firma EFD-BIT' are also visible.</p>
<p>Schreiben Sie Ihr Mail und klicken Sie vor dem Absenden auf das Verschlüsselungs-Symbol:</p> <p>Senden Sie Ihr Mail.</p>	 <p>The screenshot shows the Outlook 'Compose' window. The ribbon includes 'DATEI', 'NACHRICHT', 'EINFÜGEN', 'OPTIONEN', 'TEXT FORMATIEREN', and 'ÜBERPRÜFEN'. The 'NACHRICHT' ribbon is active, showing options like 'Einfügen', 'Ausschneiden', 'Kopieren', 'Format übertragen', 'Zwischenablage', 'Text', 'Adressbuch überprüfen', 'Namen überprüfen', 'Datei anfügen', 'Element anfügen', 'Signatur', 'Richtlinie zuweisen', 'Kategorien', 'Zoom', 'Verschlüsseln', and 'Signieren'. A red arrow points to the 'Verschlüsseln' button, which has a lock icon. The email body contains the text 'Hallo Dies ist eine verschlüsselte Mail'.</p>
<p>Der Empfänger erhält die Mail mit dem gleichen Symbol!</p>	 <p>A small icon of a lock with a keyhole, indicating that the email is encrypted.</p>