Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

V2.1 / 11. Dezember 2023

Gruppenmailboxzertifikate

Arbeitsleitfaden

Inhaltsverzeichnis

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

Gruppenmailboxen 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

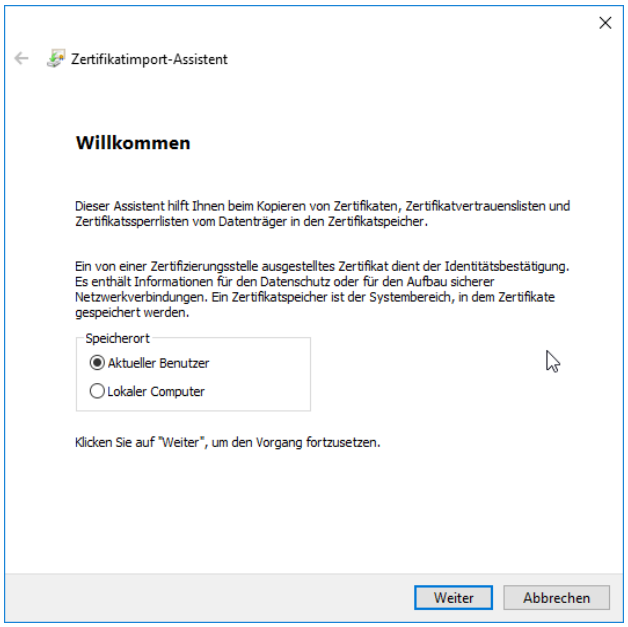
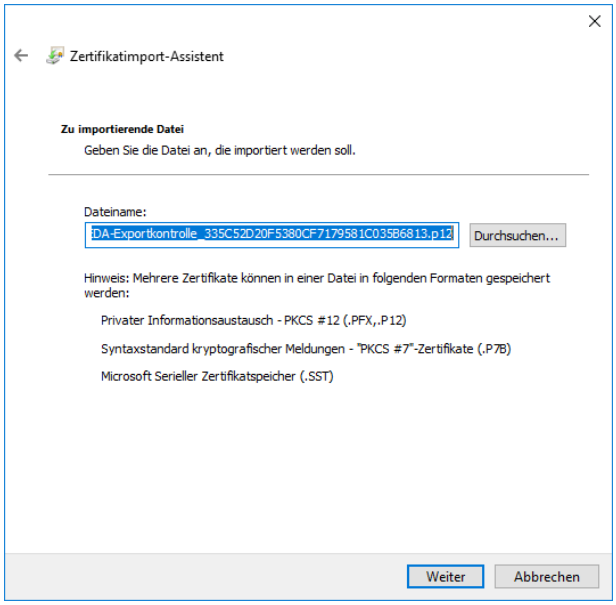
Die Rechte und Pflichten beim Bezug und Einsatz der Gruppenmailboxzertifikate sind in der CP/CPS beschrieben, sowie in den Nutzugsbedingungen und Guidelines der Klasse C Standardzertifikate.

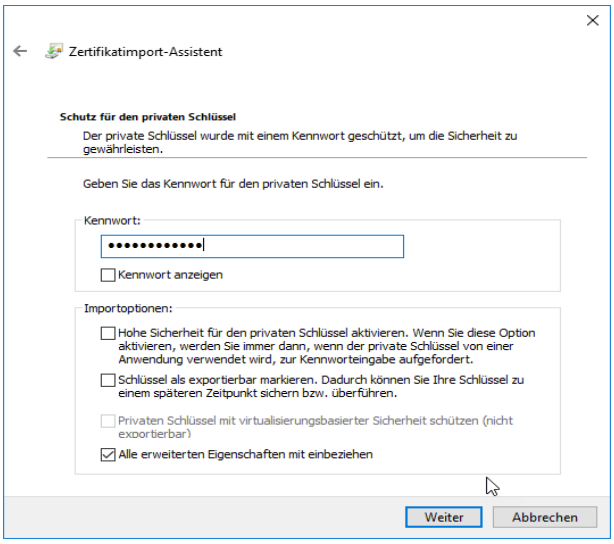
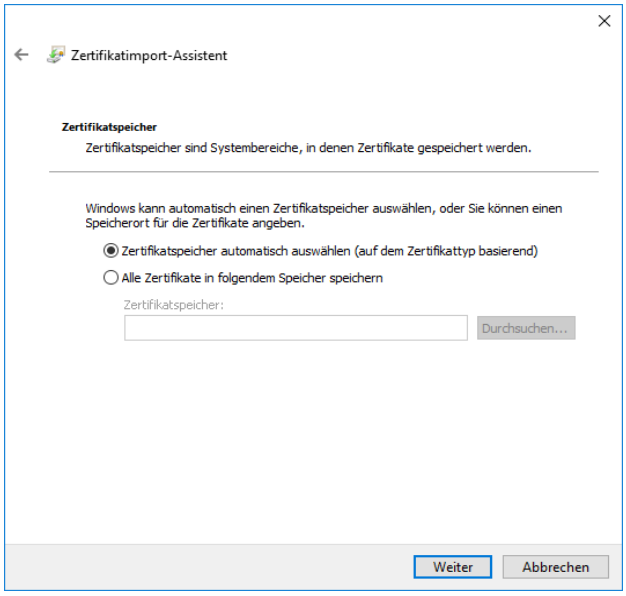
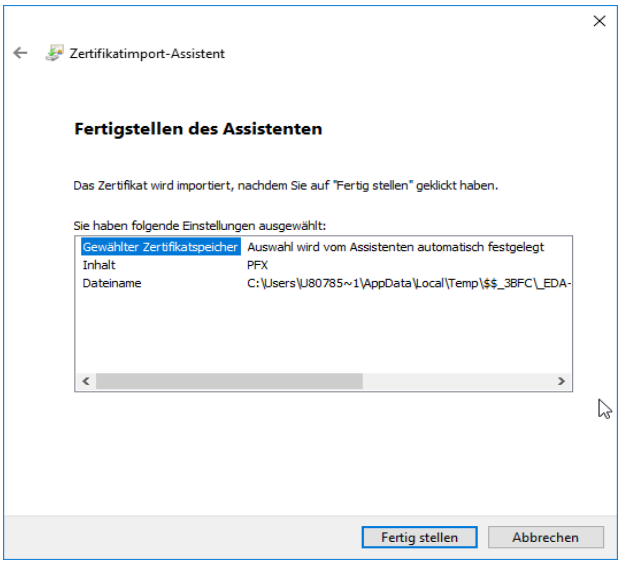
Nähere Informationen, Formulare und die CP/CPS finden Sie auch unter: Gruppenmailboxzertifikate **auf unserer Homepage** www.pki.admin.ch.

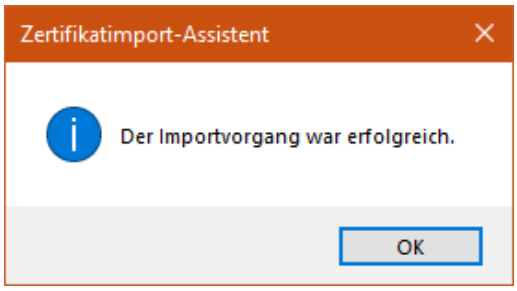
3 Besitzer eines Gruppenmailboxzertifikates

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:

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

Das per Mail erhaltene Kennwort eingeben, und **KEINE** weiteren Elemente anklicken! Mit „weiter“ zum nächsten Fenster.	
„Zertifikatsspeicher automatisch auswählen“ anwählen 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.

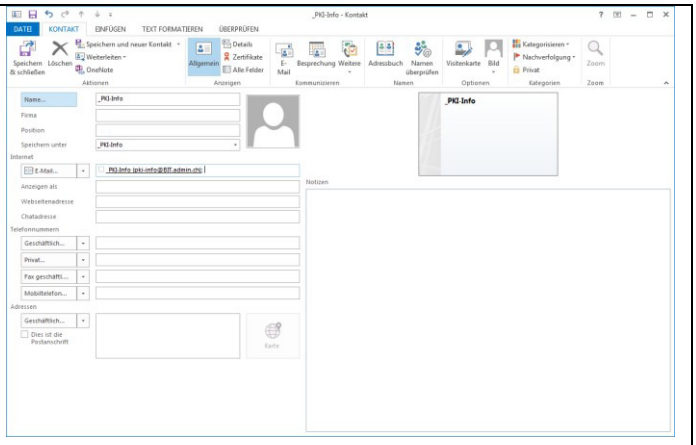
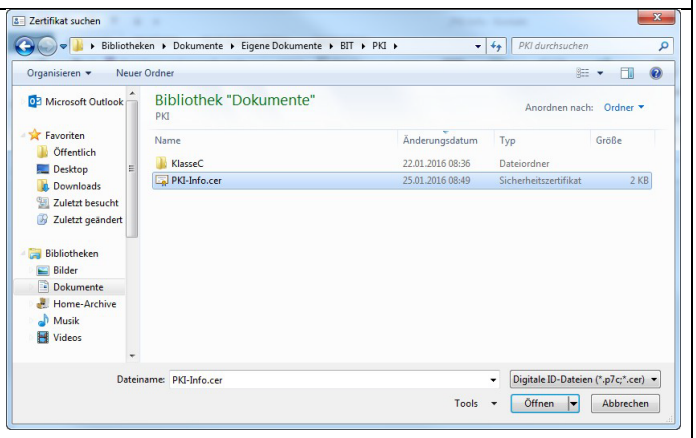
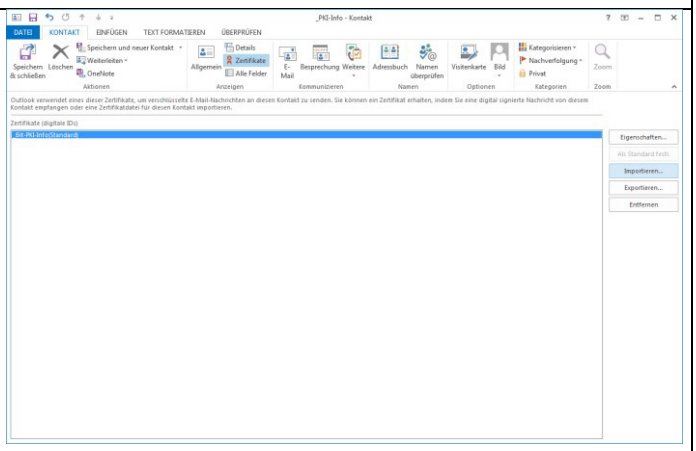
Diese *.CER –Datei müssen Sie Dritten zur Verfügung stellen, damit man Ihnen verschlüsselte Mails zusenden kann. Sollte dieser Vorgang unter Punkt 3.2 nicht möglich sein können Sie dies z.B. tun, indem Sie eine signierte Mail von dieser Mailbox senden

4 Benutzer eines Gruppenmailboxzertifikates

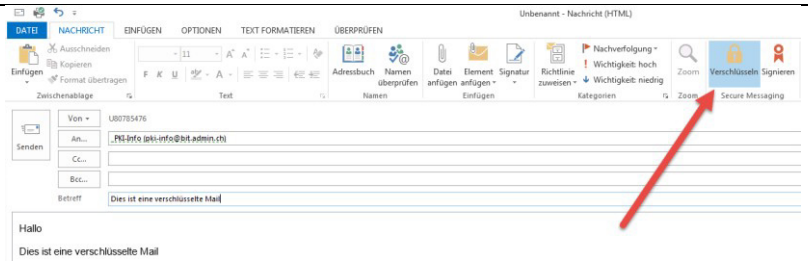
Grundsätzlich müssen Mails, die verschlüsselt versendet werden müssen, mit dem öffentlichen Schlüssel („Public Key“) des Empfängers codiert werden. Der öffentliche Schlüssel muss vom Empfänger zur Verfügung gestellt werden, sei es per Mail oder auf einer Homepage zum Download.

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

Einen neuen „Kontakt“ erstellen, und die Mindestanforderungen eingeben: - Name - E-Mail (Der Bezug zum Zertifikat wird mit der E-Mailadresse gemacht!)	
Zum Button „Zertifikate“ wechseln und auf „importieren“ klicken. Das Zertifikat im Ablageordner suchen, an- klicken und auf „öffnen“ klicken.	
Das Zertifikat ist jetzt mit dem Kontakt verknüpft. Klicken Sie auf „Speichern und schliessen“ um den Kontakt zu speichern.	

4.2 Verschlüsselte E-Mail an Kontakt senden

Senden Sie zu verschlüsselnden Mails für eine Gruppenmailbox direkt aus der Kontakteliste heraus: Öffnen Sie Ihr gespeicherter „Kontakt“ aus Kap. 4.1. und klicken Sie auf das Symbol:	
Schreiben Sie Ihr Mail und klicken Sie vor dem Absenden auf das Verschlüsselungs-Symbol: Senden Sie Ihr Mail.	
Der Empfänger erhält die Mail mit dem gleichen Symbol!