

Schlüsselaustausch

Version 1.1

 Copyright AGCS AG

 File:
 P:\Technisches Clearing\DATENFORMATE\Schlüsselaustausch.doc
 Status:
 Review

 Ablage:
 Datum:
 02.05.2002



Dokumentenverwaltung

Dokument-Historie

Version	Status	Datum	Verantwortlicher	Änderungsgrund
Version 1.0	Entwurf	19.04.2002	Cornelia Paril	Erstellung
Version 1.1	Review	13.09.2007	Cornelia Paril/	Überarbeitung
			DI Gerhard Schwarz	

Dokument wurde mit folgenden Tools erstellt:

MS WORD 2000



Inhaltsverzeichnis

 Einleitung Schüsselaustausch 		leitung	4	
		nüsselaustausch	. 5	
	2.1	Anforderung Schlüsselaustausch	. 5	
	2.2	Verspeicherung des Zertifikats	. 5	
	2.3	Überprüfen und Beenden des Schlüsselaustausches	. 9	



1 Einleitung

Auf Grund der AB-BKO ist es notwendig, clearingrelevante Daten mittels digital signierter und verschlüsselter Email an die Daten-Emailadresse des Bilanzgruppenkoordinators zu übermitteln.

Bevor verschlüsselte Emails ausgetauscht werden können, ist ein Schlüsselaustausch durchzuführen.

In diesem Dokument wird der Schlüsselaustausch auf Basis von Outlook 2000 erklärt.



2 Schüsselaustausch

2.1 Anforderung Schlüsselaustausch

Die Anforderung des Schlüsselaustausches erfolgt immer von demjenigen, der ein neues Zertifikat bekommen hat. Lässt sich ein Marktteilnehmer neu bei AGCS registrieren, hat er unter dem Betreff "Key Exchange 1" eine digital signierte Email, in deren Anhang sich sein Public Key als Attachement befindet, an die Daten-Emailadresse (<u>data@agcs.at</u>) zu senden. Dieselbe Vorgehensweise ist auch bei bereits registrierten Marktteilnehmer anzuwenden, wenn das bereits verwendete Zertifikat abgelaufen ist und ein Neues ausgestellt wurde.

2.2 Verspeicherung des Zertifikats

Wenn Sie ein Email mit den Betreff "Key Exchange 1" erhalten, gibt es zwei Möglichkeiten das Zertifikat mit dem Public Key zu importieren.

1. Abspeichern des als Attachement beigefügten Zertifikats und importieren in den Kontaktordner

Dafür öffnen Sie das Email und klicken mit der rechten Maustaste auf das Attachement und gehen auf "Speichern unter…". Sie können das Zertifikat nun in einem beliebigen Ordner auf Ihrer Festplatte oder Server verspeichern.

Nach dem Abspeichern des Zertifikats mit dem Public Key ist dieser dem Kontakt hinzuzufügen. Dafür wird im Outlook im Kontaktordner der entsprechende Eintrag geöffnet (oder ein Neuer angelegt, falls noch keiner existiert). Danach wird das Karteiblatt "Zertifikate" ausgewählt und auf "Importieren" geklickt. Nun können Sie den Ordner auswählen in welchem Sie das Zertifikat abgespeichert haben und das Zertifikat importieren. Nach erfolgreichem Import erscheint das Zertifikat beim Kontakt. Sie können die Gültigkeit des Zertifikates über die Eigenschaften überprüfen.



🖙 Clearing and Settlement(3. 03) - Kontakt			_ 8 ×
	2		
🔚 Speichem und Schließen 🔚 🎒 🕕 🔻 🄗 🐁 🔊	• 4 • • • •		
Allgemeines Details Aktivitäten zertinkate Alle F	Felder		
Name Clearing and Settlement (3.02) Position: Firma:	Geschäftlich		
Speichern unter: Clearing and Settlement(3.03			
Adresse	E-Mail		
Dies ist die Postanschrift	Webseite:		
Kontakte		Kategorien	Privat
📕 Start 🕜 🛞 🔕 💽 🖉 👩 👋 🧱 smart balance	- APCS\pa 🐻 Schlüsselaustausch.doc 🔞 Kontal	kte - Microsoft Outl	🚺 DE 🗐 🖾 💿 13:22

Abb. 1: Öffnen des Kontaktes /Zertifikate





Abb. 2: Importieren des Zertifikats

Gibt es zu einem Kontakt mehrere Zertifikate, ist es notwendig, ein Zertifikat als Standard festzulegen. Dies ist besonders wichtig, wenn ungültige bzw. abgelaufene Zertifikate darunter sind. Abgelaufene Zertifikate sollten nicht gelöscht werden, damit man auch alte Emails noch lesen kann.

Um ein Zertifikat als Standard festzulegen, markieren Sie das gewünschte Zertifikat und klicken Sie auf "als Standard fest.". Neben dem ausgewählten Zertifikat erscheint in Klammer gesetzt "Standard".



🖫 Clearing and Settlement(3. 03) - Kontakt	_ 8 ×
Datei Bearbeiten Ansicht Einfügen Format Extras Aktionen ?	
🖳 Speichem und Schließen 🔚 🎒 🕕 🔻 🏈 🐁 🦣 + 🔺 + 🔹	
Allgemeines Details Aktivitäten Zertifikate Alle Felder	
Outlook verwendet eines dieser Zertifikate, um verschlüsselte E-Mail-Nachrichten an diesen Kontakt zu senden. Sie können ein Zertifikat erhalten, indem Sie eine digital signierte Nachricht von diesem Kontakt empfangen oder eine Zertifikatsdatei für diesen Kontakt importieren.	
Zertifikate (Digitale IDs):	
Daten APC5 37920209+MAIL=data@apcs.at(Standard)	Eigenschaften
	Als Standard festl.
	Importieren
	Exportieren
	Entfernen

Abb. 3: Zertifikat als Standard festlegen

2. Hinzufügen des Zertifikats über den Absenderkontakt

Dafür klickt man mit der rechten Maustaste auf den Absender der geöffneten "Key Exchange 1" – Email und wählt "zu den Kontakten hinzufügen" aus. Bei dieser Variante kann es aber zu Problemen kommen (z. B. wird das Zertifikat nicht übernommen).



🔀 Key Exchange 1 - Nachricht (HTML)	_ 6 3				
Datei Bearbeiten Ansicht Einflügen Format Extras Aktionen ?					
🖉 Antworten 🕵 Allen antworten 😡 Weiterleite	n 🖴 🖻 🔻 🖹 🗙 + 🔸 - 🛠 🖉 -				
Von: <u>Cleaner end Cattlement</u> Eigenschaften An: Sendeoptionen Cc: Zu den Kontakten hinzufügen	Gesendet: Do 28.03.2002 14:13				
Bcc: Kontakt nachschlagen					
Ausschneiden Betreff: Key F	e e e e e e e e e e e e e e e e e e e				
Sicherheit: Signie Markierung löschen	۹				
Alles markieren Wegen des b arorgen Abradis unseres A-org i	- - Zertifikats ist es leider notwendig, einen neuerlichen Schlüsselaustausch durchzuführen.				
Wir ersuchen Sie daher das dieser Mail beig Verschlüsselungen zu verwenden. Späteste	lefügte Zertifikat mit unserem öffentlichen Schlüssel in Ihre Schlüsselverwaltung zu übernehmen und für alle zukünftigen ns nach Ablauf des alten Zertifikats werden auch alle unsere Mails mit dem neuen. Zertifikat signiert.				
Zum Test ersuchen wir Sie, diese Mail verso Betreff "Key Exchange 2"	hlüsselt und signiert zu beantworten. Sie erhalten dann bei erfolgreichem Schlüsselaustausch ebenfalls eine Antwort mit dem				
Mit freundlichen Grüßen					
APCS Datenmanagement mailto:data@apcs.at Tel: +43(1)3190701					
Since our A-Sign Certificate expires soon, it is necessary to make a new key exchange.					
For this reason we ask you to add our public old certificate has expired, all mails will be s	: key from the certificate we enclosed to this mail, to your key administration. Please use this new key in the future. When the igned with the new certificate.				
For testing we ask you to answer this mail o successful.	ligitally signed and encrypted. You will receive an answer with the subject "Key Exchange 2" when the key exchange was				
Kind regards					
🏽 🔀 Start 🛛 🛃 🍪 🖄 🔯 🖉 🔣 🔹	📢 📴 🗐 🕎 🖤 12:25				

Abb. 4: Zertifikat (Public Key) zu den Kontakten hinzufügen

2.3 Überprüfen und Beenden des Schlüsselaustausches

Wurde das neue Zertifikat verspeichert, ist ein digital signiertes und verschlüsseltes Antwort-Email an den Schlüsselaustauschanforderenden zu retournieren. Kann der Empfänger dieses Antwort-Email öffnen und wurde das gültige Zertifikat verwendet, hat dieser unter dem Betreff "Key Exchange 2" ebenfalls ein digital signiertes und verschlüsseltes Email an den Absender zu übermitteln.

Wenn auch dieses Email geöffnet werden konnte ist der Schlüsselsaustausch erfolgreich abgeschlossen.