APCS Power Clearing and Settlement AG

Schlüsselaustausch

Version 1.1

File:	P:\Technisches Clearing\DATENFORMATE\Schlüsselaustausch.doc	Status:	Freigabe
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	Freigabe	02.05.2002	Cornelia Paril/ DI Gerhard Schwarz	Überarbeitung

Dokument wurde mit folgenden Tools erstellt:

MS WORD 2000

Inhaltsverzeichnis

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 APCS 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 (data@apcs.at) zu senden. Dieselbe Vorgehensweise ist auch bei bereits registrierten Marktteilnehmer anzuwenden, wenn das bereits verwendete Zertifikat abgelaufen ist und ein Neues ausgestellt wurde.

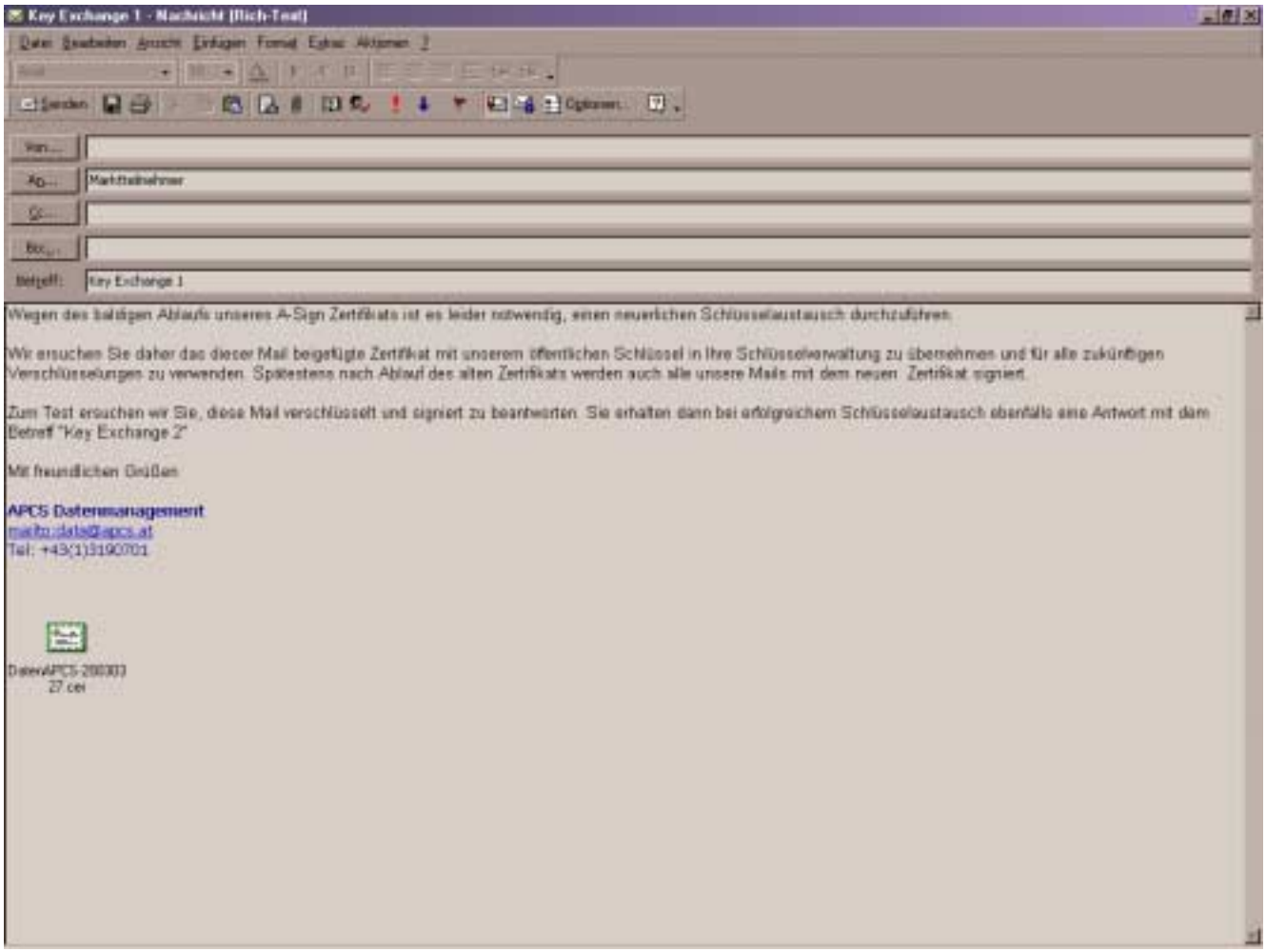

Abb. 1: Beispiel für Anforderung Schlüsselaustausch durch APCS

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.

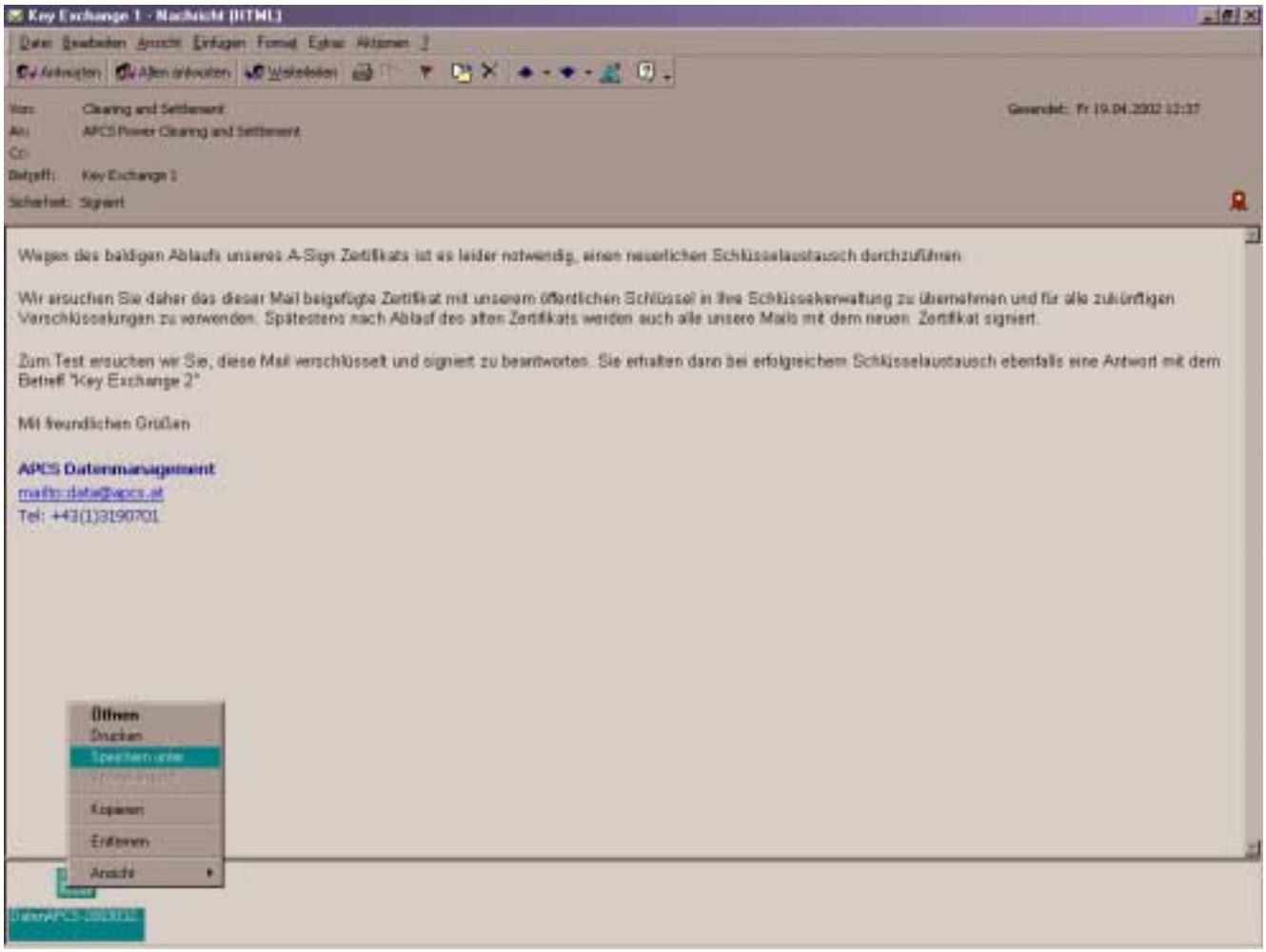

Abb. 2: Importieren des Zertifikats

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.

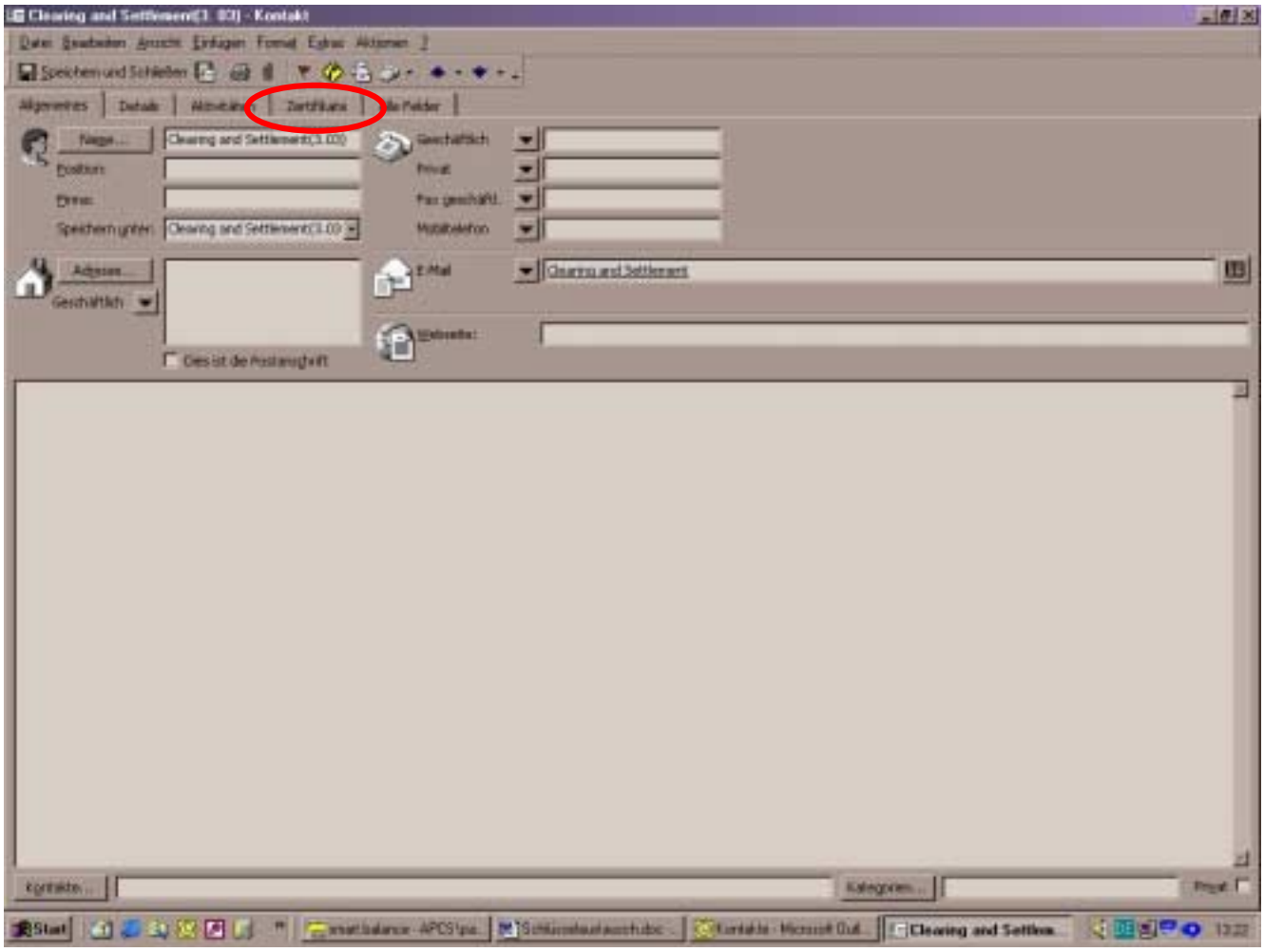

Abb. 3: Öffnen des Kontaktes /Zertifikate

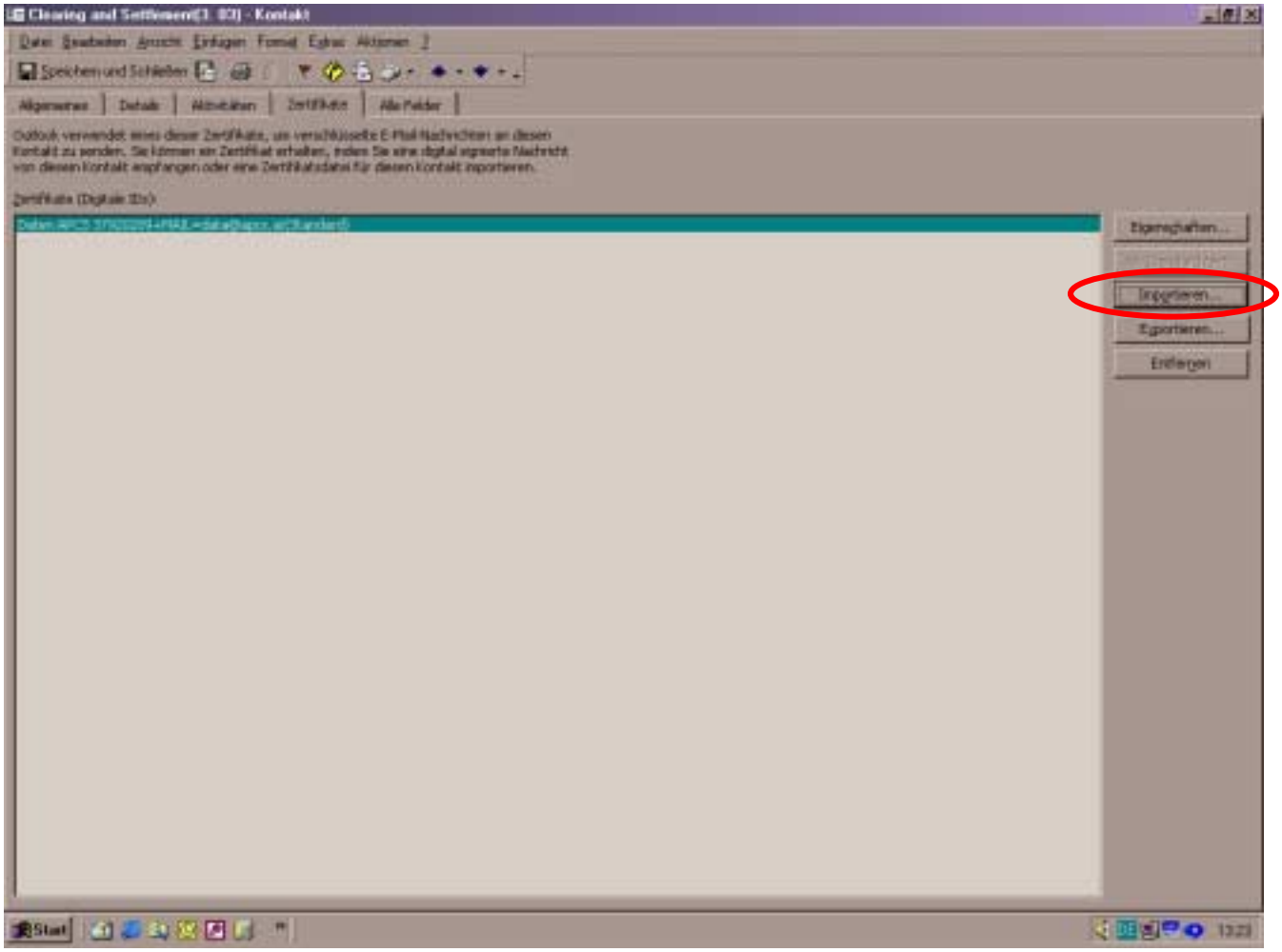

Abb. 4: Importieren des Zertifikats

Gibt es zu einem Kontakt mehrere Zertifikate, ist es notwendig, ein Zertifikat als Standard festzulegen. Dies ist besonders wichtig, wenn ungültige Zertifikate darunter sind.

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“.

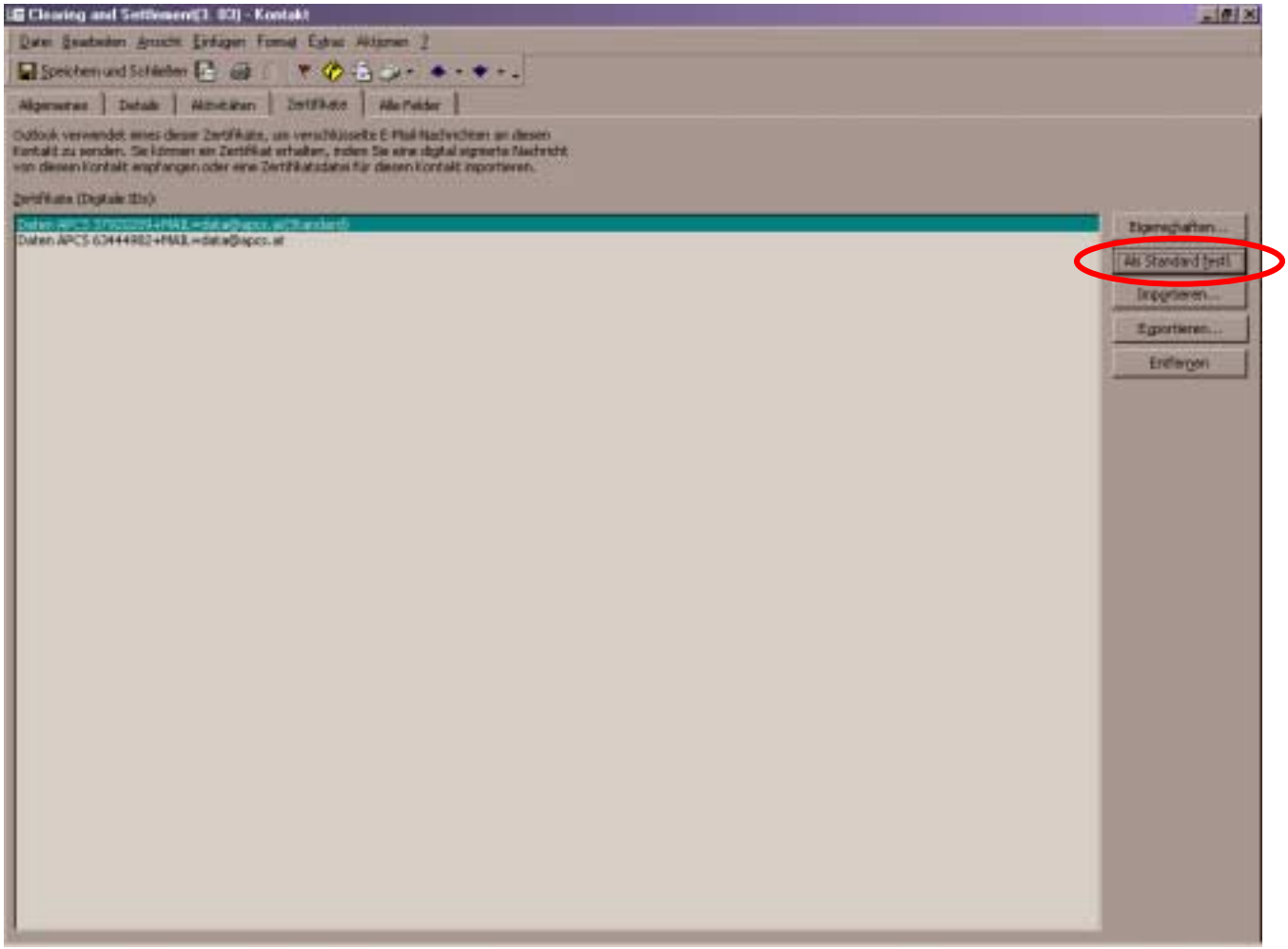

Abb. 5: Zertifikat als Standard festlegen

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).

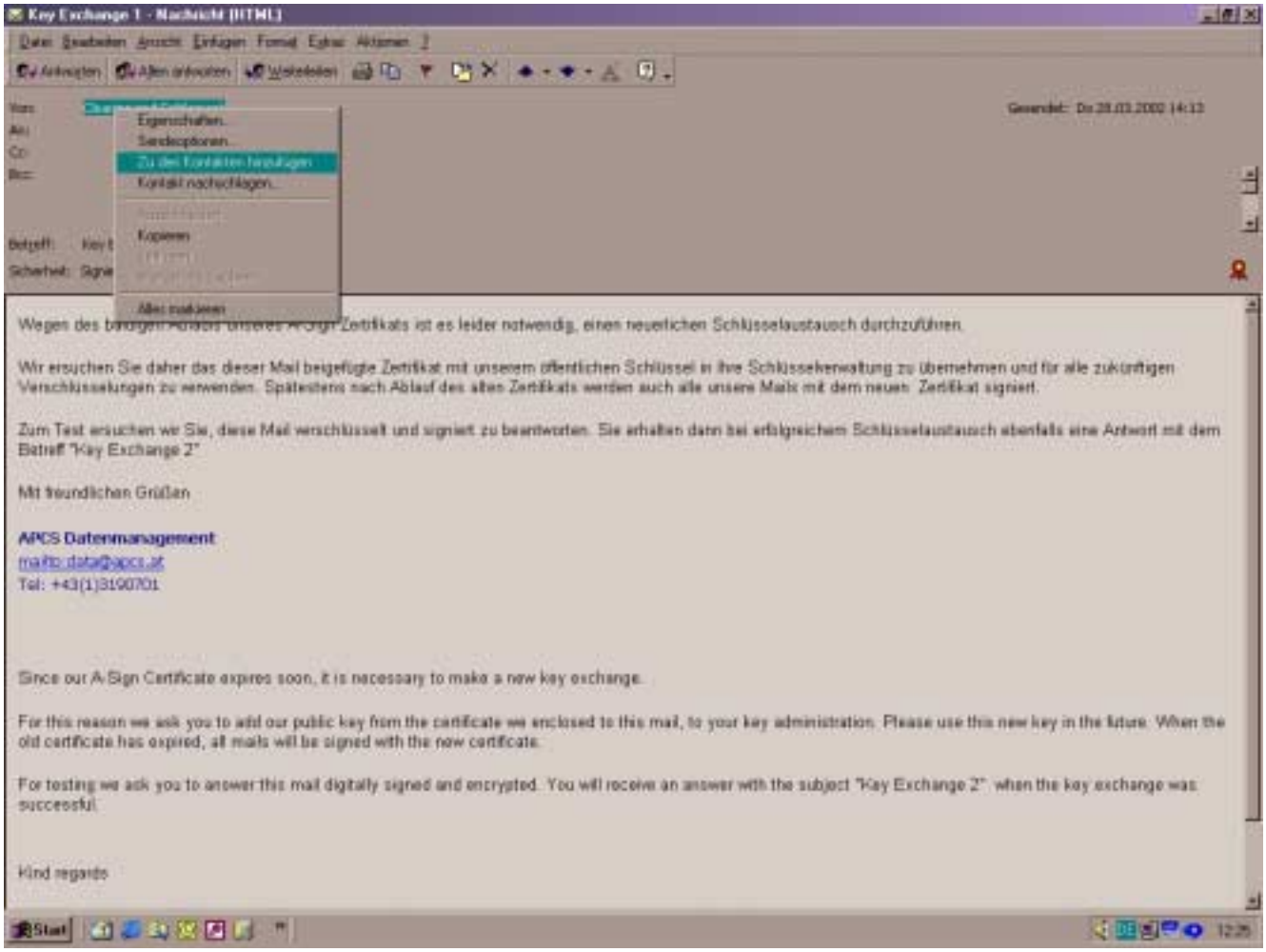

Abb. 6: Zertifikat (Public Key) zu den Kontakten hinzufügen

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.

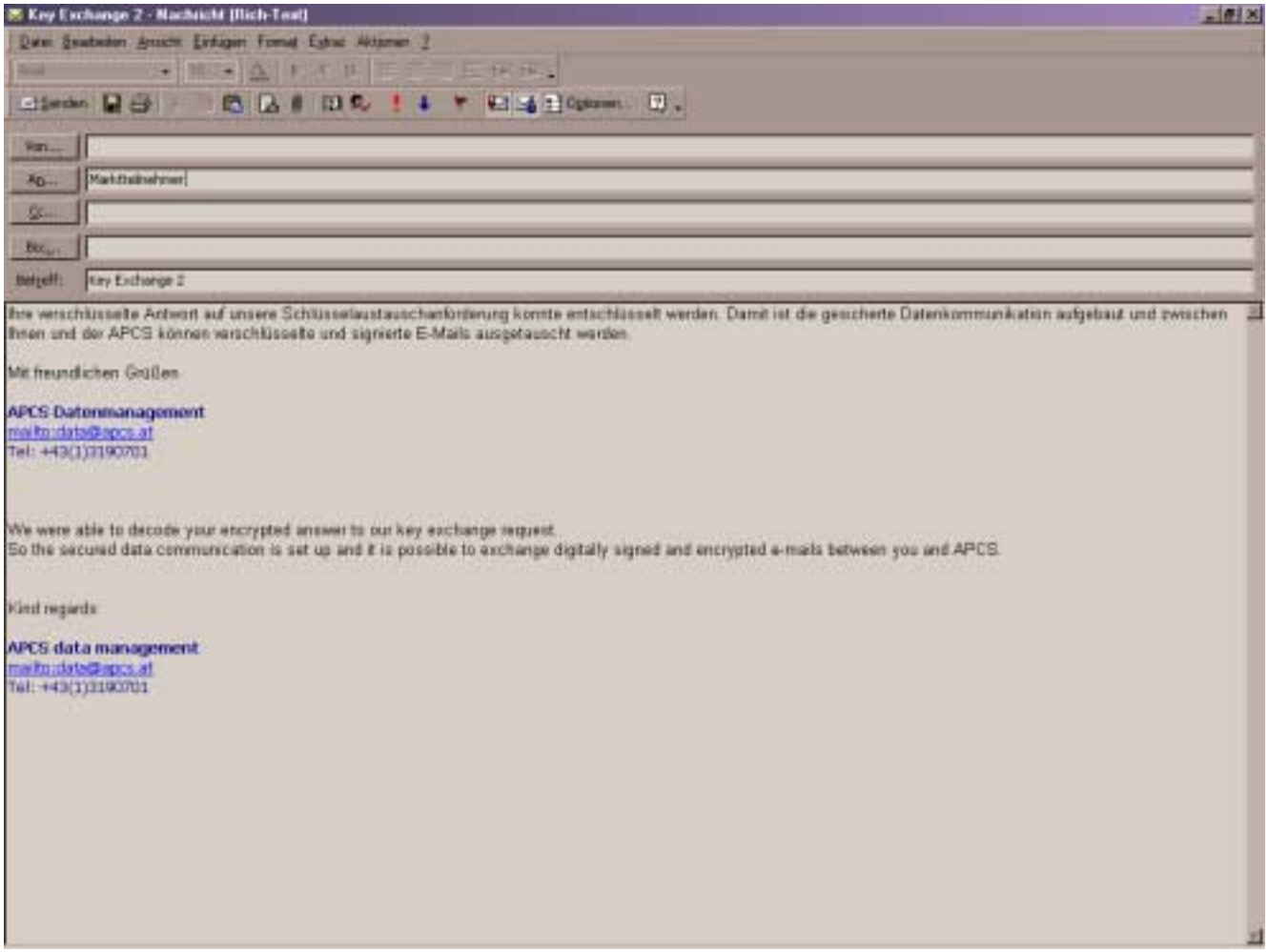

Abb. 7: Bestätigung über den erfolgreich abgeschlossenen Schlüsselaustausch