



# **Intercede MyID 7.1**

## **Konfiguration, Teil1**

### **Vorbereitung des Active Directory**

**CRYPTAS it-Security GmbH**

Modecenterstrasse 22/B2  
A-1030 Wien

[www.cryptoshop.com](http://www.cryptoshop.com)  
[www.cryptas.com](http://www.cryptas.com)

## Konfigurationsaufgaben in der Windows Active Directory Domäne

Vor der Nutzung von Intercede MyID müssen wir noch 3 Aufgaben in der Windows Active Directory Domäne erledigen:

- 1.) wir erstellen Templates für die auszustellenden Zertifikate und setzen alle notwendigen Berechtigungen
- 2.) wir rüsten die Certification Authority mit den erstellten Templates auf und setzen die nötigen Berechtigungen in der CA
- 3.) wir erstellen einen Key Recovery Agent und tragen ihn in der CA ein.

Tip: Alle diese Aufgaben sind eigentlich Aufgaben des Domain Admins, also rechtzeitig mit ihm in Verbindung setzen.

Es empfiehlt sich auch an dieser Stelle kurz halt zu machen und zu evaluieren, welche Arten von Zertifikaten überhaupt benötigt werden. Wir hinterfragen: zu welchem Zwecke werden die Smartcards eingesetzt, welche Aufgaben sollen erledigt werden, welche Applikationen wollen die Zertifikate auf den Smartcards verwenden, gibt es Vorgaben bezüglich der Schlüsselstärke (Authentisierung auf älteren Cisco Geräten!), Lebensdauer, wer soll aller zur Nutzung von Smartcards berechtigt sein, wie sollen sie verwaltet werden, welche verschiedenen Klassen von Smartcards werden im Einsatz sein, welche verschiedenen Benutzergruppen sind betroffen. Antworten auf diese Fragen erhalten wir vom IT Leiter, vom Domain Admin, vom Sicherheitsverantwortlichen und auch vom Helpdesk. Sie sollten die Grundlage für unser Smartcard Konzept bilden.

In unserer Beispielininstallation wollen wir Smartcards ausschließlich zum Anmelden an Windows Computern verwenden.

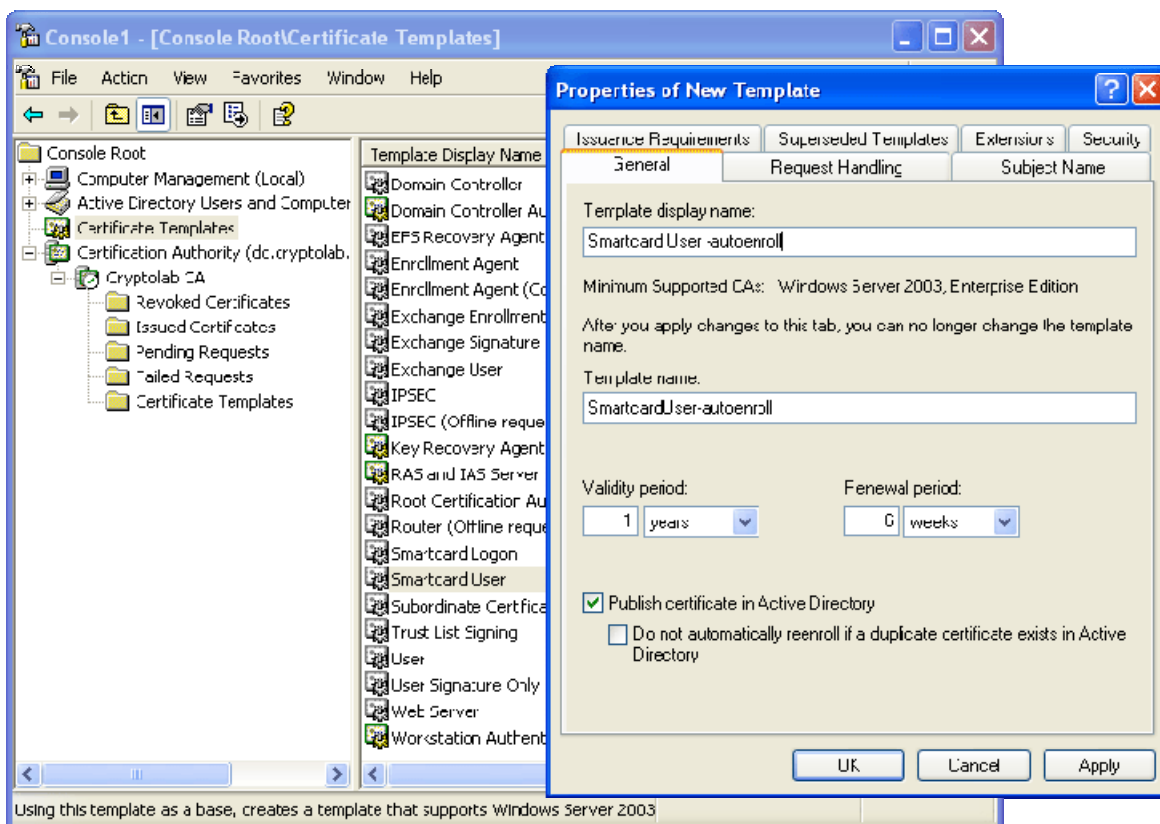
Unser Labor enthält:

- Eine Windows Active Directory Domäne (single domain model, function level Windows Server 2003)
- Eine Certification Authority (Windows 2003 enterprise edition, domain integrated, Root CA)

### Add 1.) Erstellen von Certificate Templates in Active Directory

Wir melden uns mit Domain Admin Rechten an einem Computer der Domäne an, auf dem „adminpak.msi“ installiert ist (an einem Domain Controller geht's natürlich auch) und öffnen eine MMC mit dem Snap in „Certificate Templates“

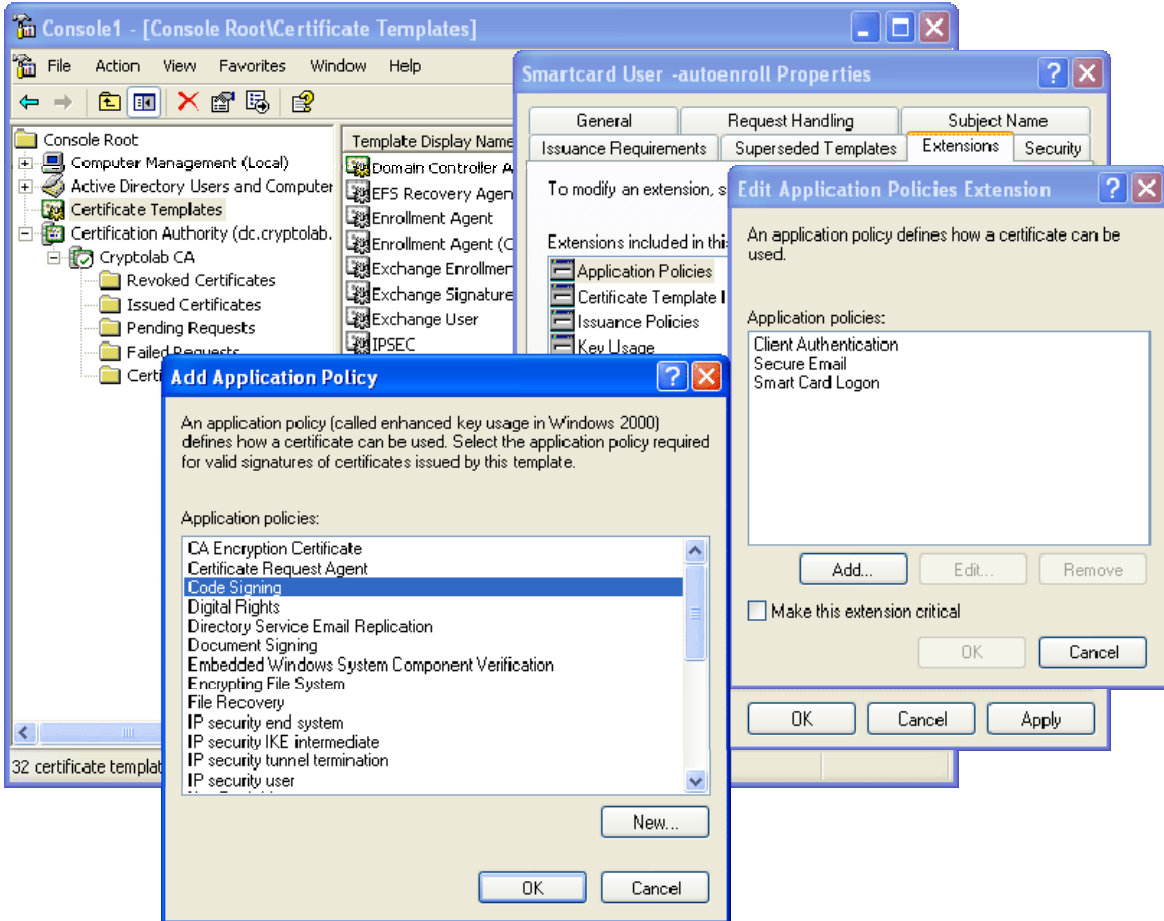
Wir klicken mit der rechten Maustaste auf das Template „Smartcard User“ und wählen „Duplicate Template“



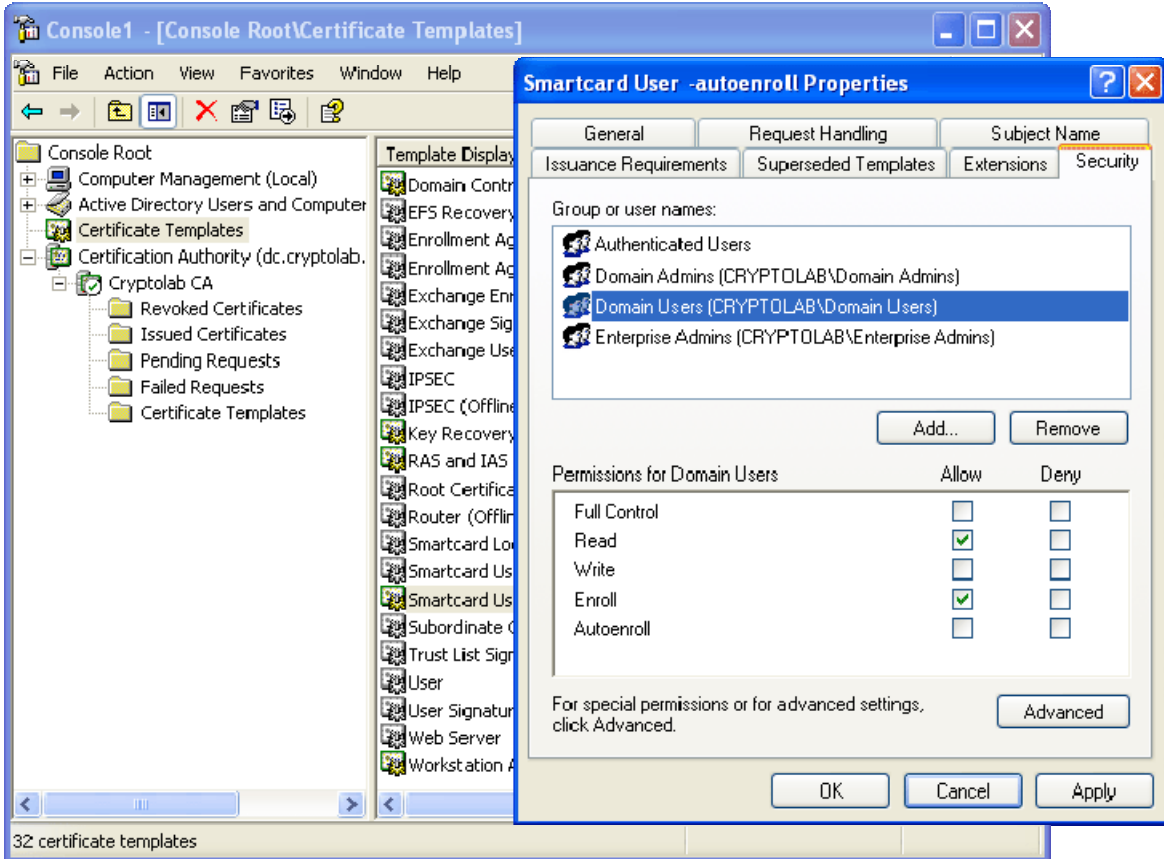
Wir geben dem neuen Template einen sprechenden Namen und speichern es ab, indem wir auf „Apply“ klicken.

Nun gehen wir die Registrierkarten eine nach der anderen durch und setzen die notwendigen Einstellungen. In unserer Beispielininstallation wollen wir besonders auf 2 Einstellungen hinweisen:

Zum Einen sehen wir uns kurz die Einstellung der Application Policies an, in denen dem Template Verwendungszwecke wie etwa „Document Signing“ oder „Encrypting File System“ hinzugefügt werden können (siehe oben genanntes Konzept).



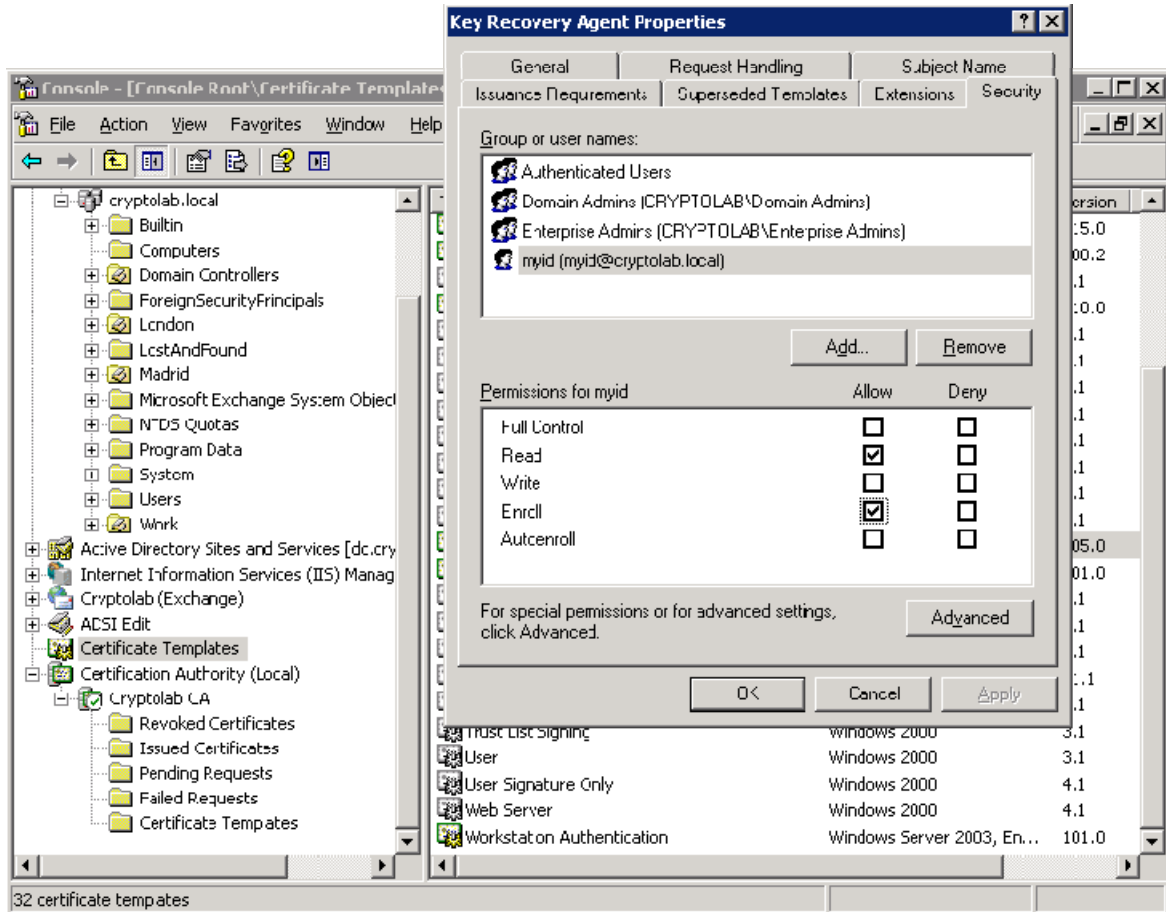
Zum Anderen werfen wir auch einen Blick auf die Zugriffsberechtigungen des Templates. Hier tragen wir ein, wer berechtigt ist, Zertifikate ausgestellt zu bekommen, die auf dieser Vorlage beruhen. In unserem Falle berechtigen wir undifferenziert die Gruppe der Domain Users.



Wir speichern unsere Änderungen mit „ok“ ab

Zusätzlich setzen wir noch Berechtigungen an folgenden Templates:

- Enrollement Agent
- Key Recovery Agent



An beiden Templates muss das Dienstkonto (in unserem Falle myid) mit „**Read**“ und „**Enroll**“ berechtigt sein

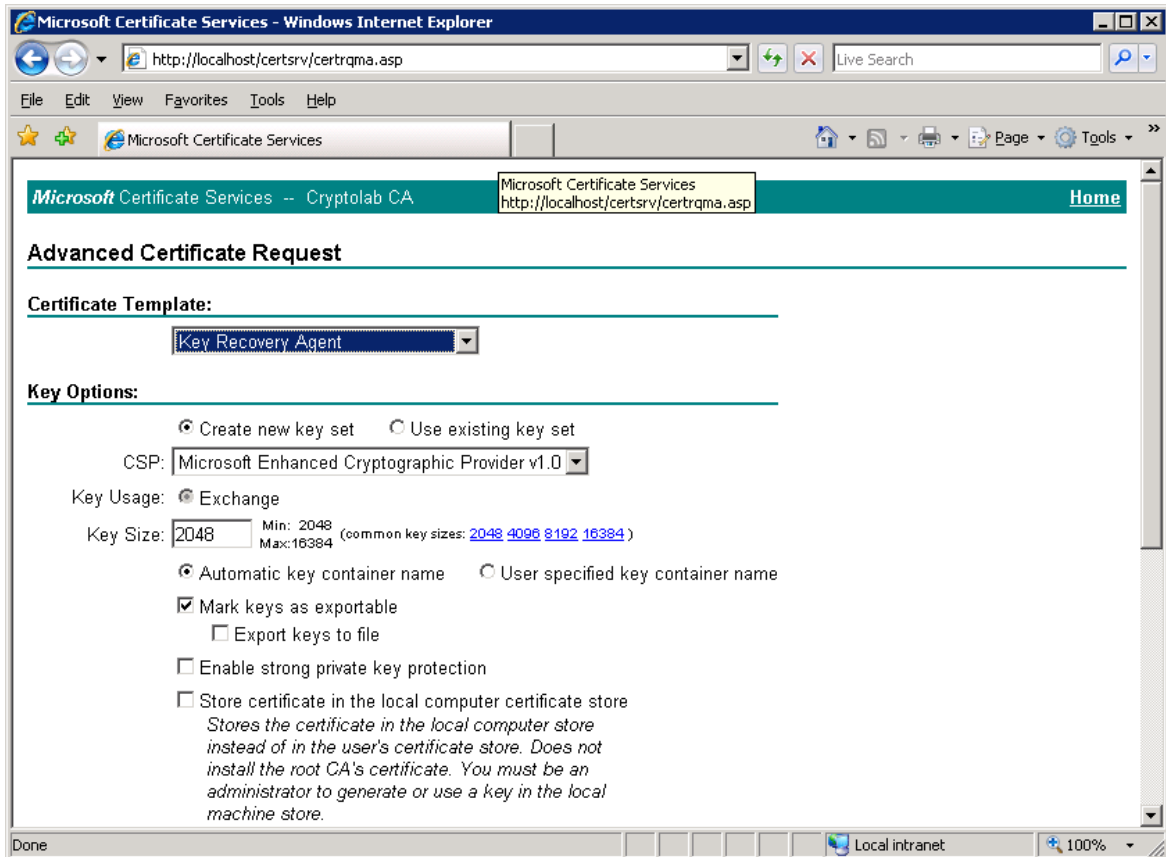
Add 2.) Aufrüsten unserer CA mit den neu erstellten Templates und Setzen der Berechtigungen.

## Hier fehlen 2 Screenshots und die dazugehörige Beschreibung

Wenn Sie an der vollständigen Version des Dokumentes interessiert sind, kontaktieren Sie uns bitte unter [sales@cryptas.com](mailto:sales@cryptas.com).

Add 3.) Erstellen eines Key Recovery Agent und Eintragen in der CA.

Nun melden wir uns am Application Server mit dem Dienstkonto von Intercede MyID an (in unserem Falle „cryptolab/myid“) und öffnen einen Webbrowser. Auf der Webseite unserer CA (<http://Servername/certsrv>) beantragen wir ein „Key Recovery Agent Certificate“

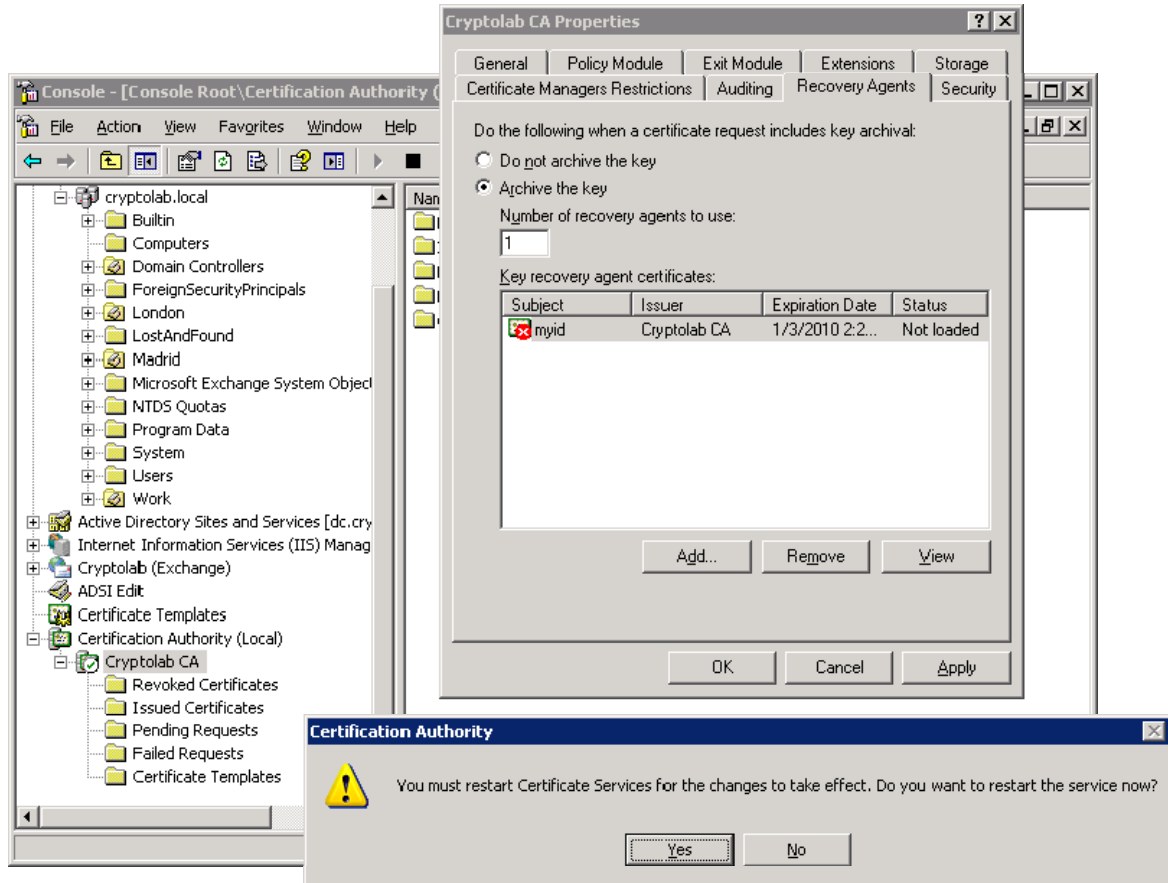


Tipp: „advanced certificate request“

Nun lassen wir das neue Zertifikat von einer dazu berechtigten Person in der CA ausstellen (Rechtsklick auf die Zertifikatsanfrage in „Pending Requests“ – „All Tasks“ – Issue“) und holen es dann auf der selben Webseite ab.

Tip: Es empfiehlt sich, Zertifikat und Schlüssel als Kopie in eine PKCS#12 Datei zu exportieren und an einem sicheren Ort aufzubewahren.

Anschließend melden wir uns wieder am DC (oder der Admin Workstation) als Domain Admin an und öffnen die MMC mit dem Snap in „Certification Authority“ und öffnen dort das Eigenschaftsfenster der CA.



Auf der Registrierkarte „Recovery Agents“ aktivieren wir die Schlüsselarchivierung und fügen unseren „Key Recovery Agent“ hinzu. Um das Zertifikat zu laden, müssen wir den Dienst neu starten.

Fertig

CRYPTAS it-Security  
Modecenterstrasse 22/B2  
A-1030 Wien, Austria  
T +43 (1) 798 96 96 – 0  
F +43 (1) 798 96 96 – 99  
info@cryptas.com

[www.cryptoshop.com](http://www.cryptoshop.com)  
[www.cryptas.com](http://www.cryptas.com)