



Intercede MyID 7.1

Installation, Teil1

Application Server und Datenbank

CRYPTAS it-Security GmbH

Modecenterstrasse 22/B2
A-1030 Wien

www.cryptoshop.com
www.cryptas.com

Installation von Intercede MyID 7.1 Application Server und der Datenbank, eine Beispielinstallation.

Wir haben uns zu einer „Tier2“ Installation entschlossen. Das bedeutet, wir wollen den Application Server und die dazugehörige Datenbank auf einem Server, und die Web Konsole auf einem anderen installieren. Wir gehen in unserem Beispiel davon aus, dass wir einen dedizierten Server in einem geschützten Netzwerksegment zur Verfügung haben, das Webinterface aber auf einem von allen Benutzern zugänglichen Server (gemeinsam mit anderen Webapplikationen) „hosten“ lassen.

Wir melden uns in unserem Labor also an einem Datenbank Server (Domain Member) mit lokalen administrativen Rechten an. Bevor wir mit der eigentlichen Installation beginnen, wollen wir eine Reihe von Vorbereitungen treffen:

1.) Wir installieren auf dem vorgesehenen Server:

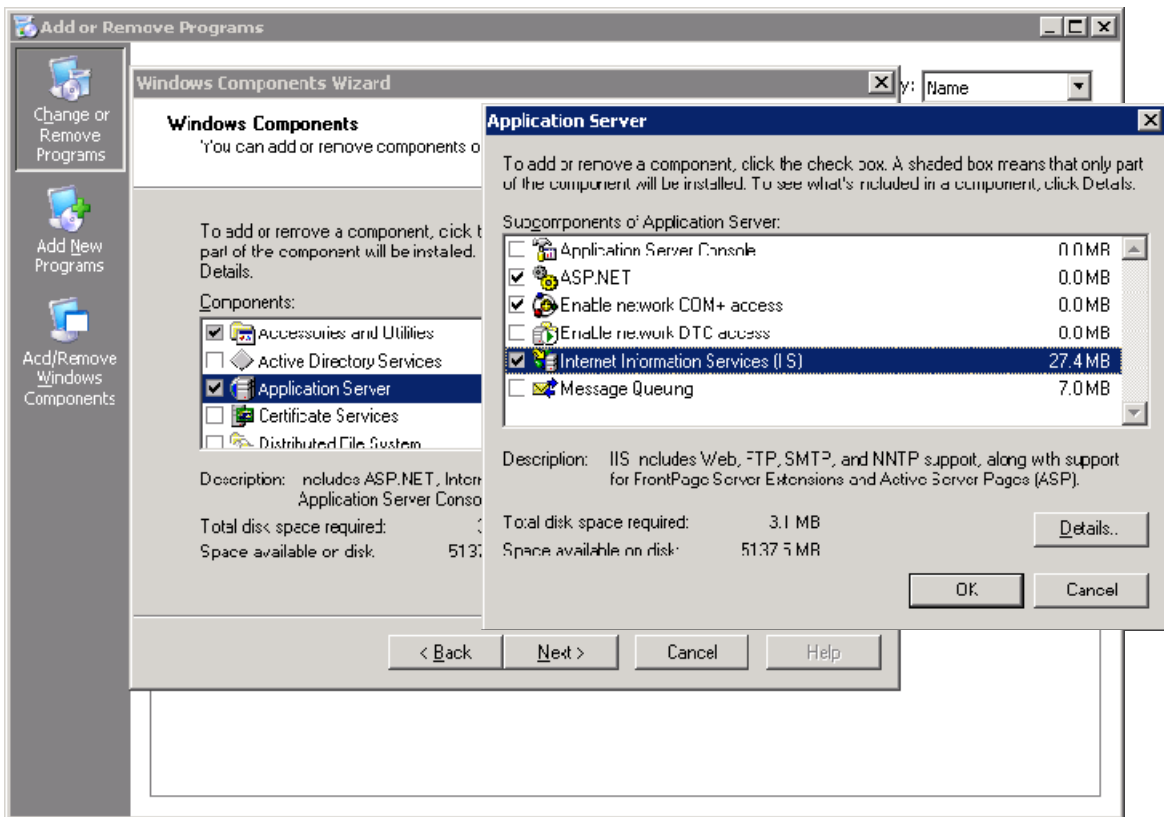
- MDAC
- XML4
- Microsoft .Net Framework 1.1 SP1+
- SQL 2000 SP3a + (MSDE2000 mit SP3 würde ebenfalls genügen)
- Einen Smartcard Reader
- Smartcard Middleware

2.) Wir erstellen 2 Benutzerkonten (Domain User)

- Dienstkonto für den Application Server (hier Cryptolab\myid)- für dieses Konto benötigen wir folgende Einstellungen:
 - Log on as Service im „Domain Controllers GPO“
 - Mitglied von der lokalen Admin Gruppe am Application Server (Computer Configuration\ Windows Settings\ Security Settings\ Local Policies)
- Dienstkonto für die Security Management Console (hier Cryptolab\myid-iis)

3.) wir extrahieren die Datei **xpsmtp80.dll** aus dem Verzeichnis **\MyID 7.1.0.18\PreReq\XPSMTP** Und kopieren sie in das Verzeichnis **C:\Program Files\Microsoft SQL Server\MSSQL\Binn**

4.) wir aktivieren den Zugriff auf Com+ Objekte und installieren ASP.Net: Start – Control Panel - Add or remove Programs

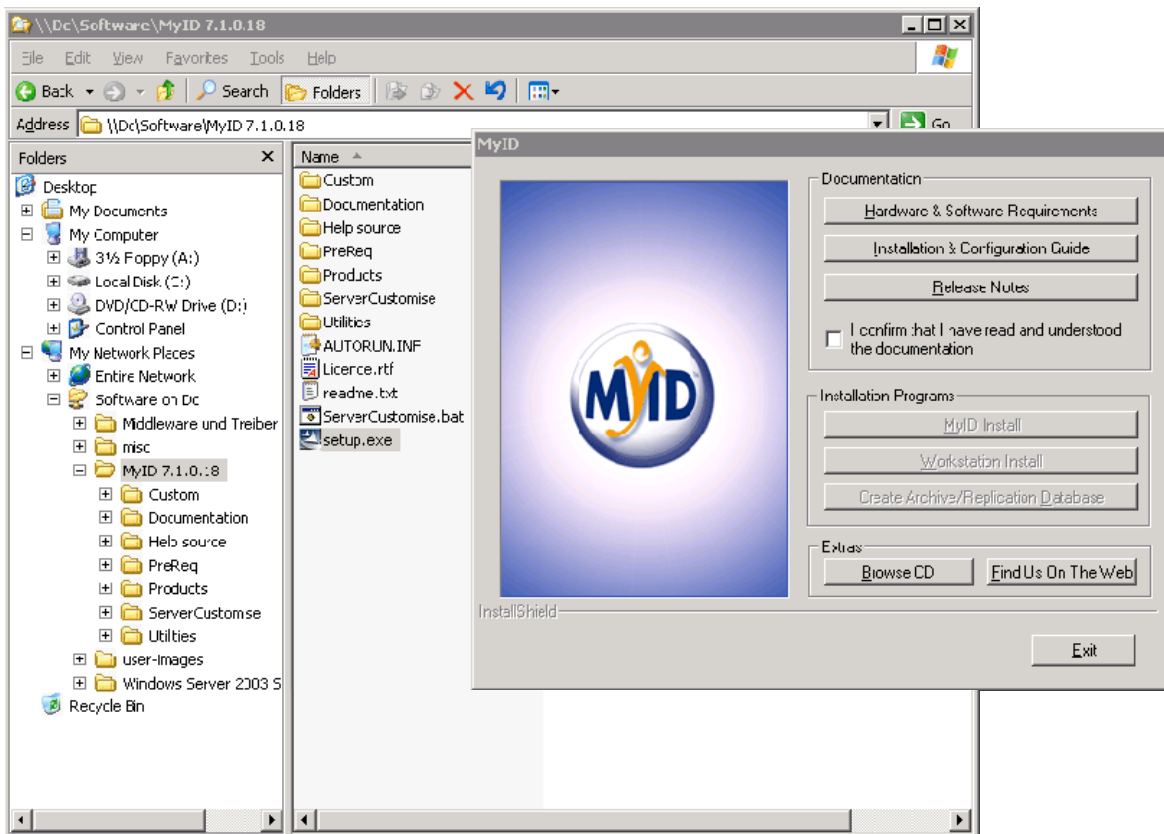


Hier installieren wir IIS, ASP.NET und aktivieren den COM+ Zugriff (nicht vergessen, in der MMC Internet Information Server: Active Server Pages, ASP.Net und WebDAV auf „allow“ setzen)

In unserer Beispielinstallation verwenden wir:

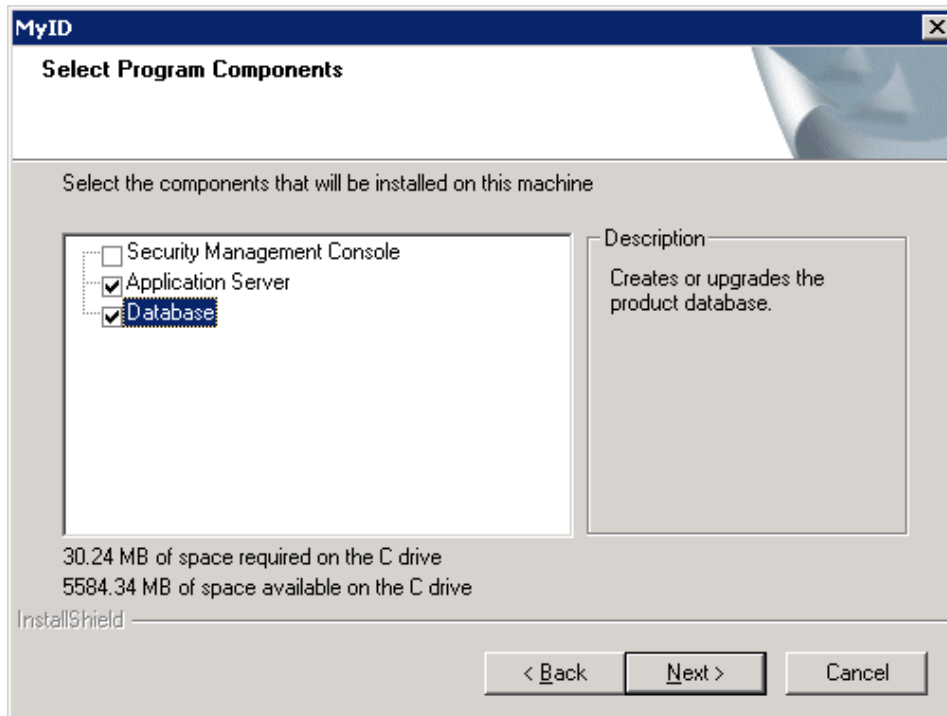
- Windows Server 2003 SR2 standard edition
- Microsoft SQL 2000 Server enterprise edition, SP4
- Microsoft .Net Framework 2.0
- Gemalto PC USB-SL Reader
- GemSafe Xpresso Smartcard und GemSafe Libraries 4.2.0 –SP4

Wenn wir bereit sind, führen wir setup.exe aus.

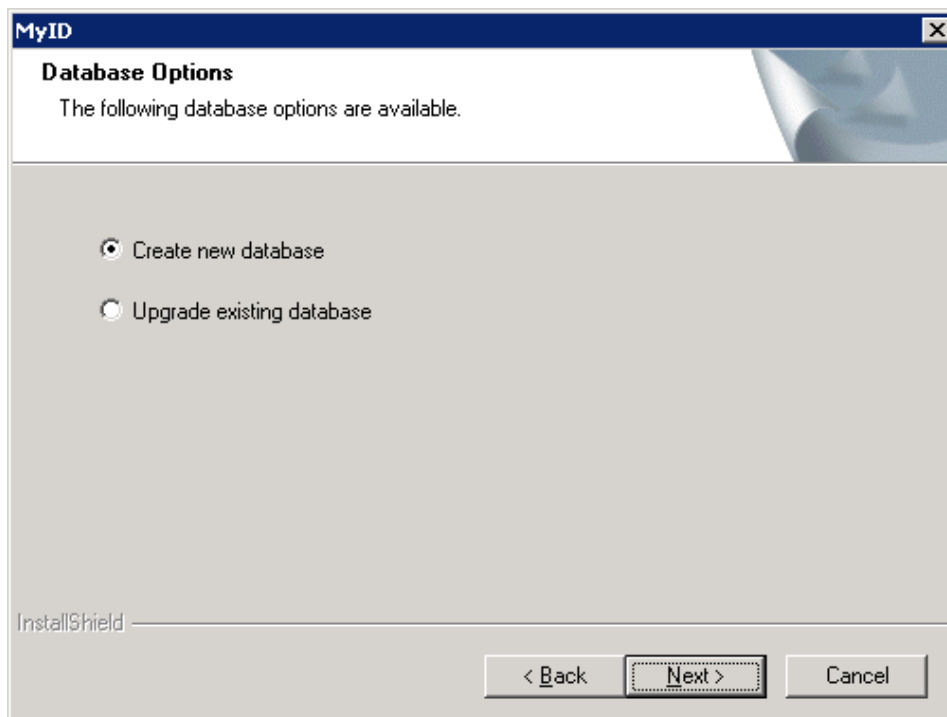


Wir bestätigen, dass wir die Dokumentationen gelesen UND verstanden haben ☺ ... und klicken auf **MyID Install**. (Hier können wir eventuell noch fehlende Voraussetzungen nachinstallieren, wenn es notwendig sein sollte)

Nach dem „Willkommen“ und unserem Einverständnis mit dem „License Agreement“ wählen wir einen Installationspfad und klicken auf **Next**.



Wir aktivieren also nur „Database“ und „Application Server“, da wir ja die Webkomponente auf einem anderen Server betreiben wollen, und klicken wieder auf **next**



Create new database – **next**

Wir benötigen für die Installation von MyID Application Server ein Dienstkonto zum Zugriff auf die Datenbank. In unserer Beispielinstallation haben wir ein Domain User Konto namens MyID erstellt. Tipp: rechtzeitig mit dem Domain Admin in Verbindung setzen – da die Installation eines an das AD angeschlossenen Smartcard-Verwaltungssystems ein tiefer Eingriff in die Verwaltung der Domäne darstellt, ist diese Installation und Inbetriebnahme eigentlich Sache des Domain Admin selbst. Er sollte daher wenigstens anwesend sein. Seine Vorstellungen der Delegation sollte in unserem Konzept umgesetzt werden.

Wir geben das Dienstkonto nun an, damit bei der Erstellung der Datenbank gleich die Berechtigungen gesetzt werden können:



MyID

Service Account Details

Some components and services run under a named account. This account will be given permission to access the database. Please provide details of an existing user account below. This account should be configured with a non-expiring password.

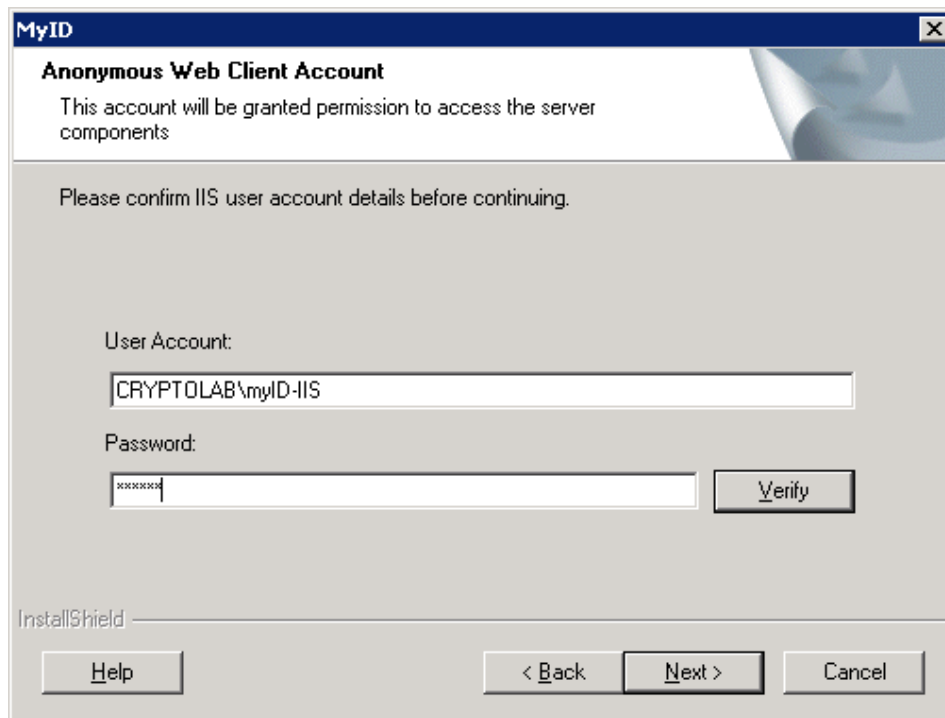
User Account:

Password:

InstallShield

->Next

Die Security Management Console benötigt ebenfalls ein Dienstkonto zum Zugriff auf die Datenbank. Da wir die Konsole auf einem anderen Server installieren wollen, erstellen wir dazu ein Domain User Konto und tragen es ein



-> Next

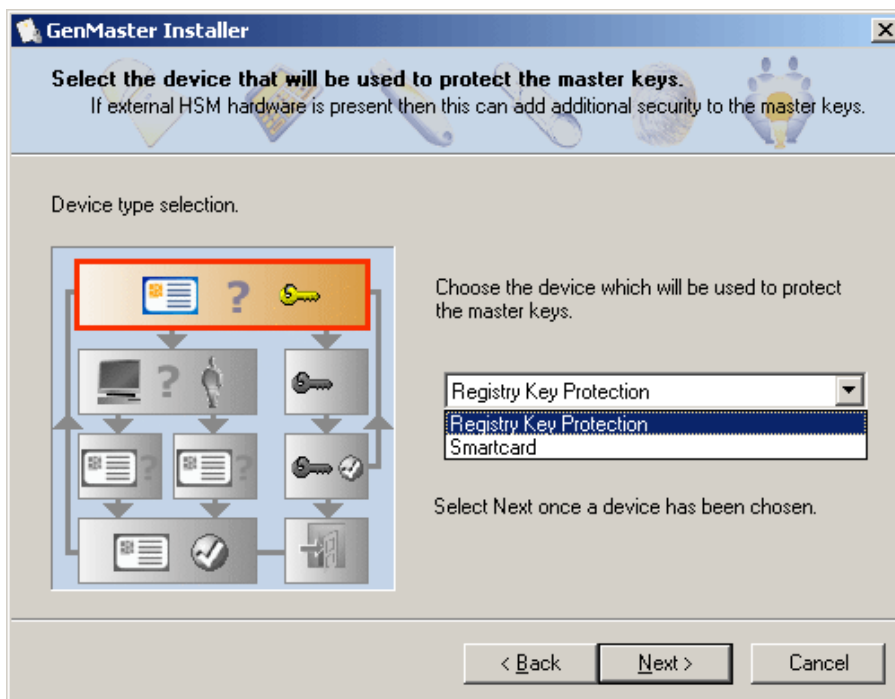
Hier fehlen 4 Screenshots und die dazugehörige Beschreibung

Wenn Sie an der vollständigen Version des Dokumentes interessiert sind, kontaktieren Sie uns bitte unter sales@cryptas.com.

Vor dem Abschluss der Installation startet das eben neu installierte Programm „Genmaster“. Es dient zum Erstellen eines „Masterkey“ (zum Zugriff auf die verschlüsselte Datenbank) und zum Erstellen von Administrator Zugriffskarten..



-> Next



Hier wählen wir aus Bequemlichkeit „Registry Protection“. In diesem Fall wird der Masterkey der Datenbank lokal in der Registry des Servers abgelegt und der Server kann ohne Aufsicht eines Administrators gestartet werden. Dies kann jedoch in einer operativen Umgebung ein Sicherheitsrisiko darstellen, da in vielen Organisationen die Verantwortung für die Betriebssysteme der Server bei anderen Personen liegt, als die Verantwortung für Applikationen oder für die Einrichtungen der Infrastruktur, wie etwa Microsoft Active Directory. Kurz gesagt: Server Administratoren sind keine Domain Admin und sollen auch nicht so weitreichende Berechtigungen haben (Outsourcing Partner, z.B.)

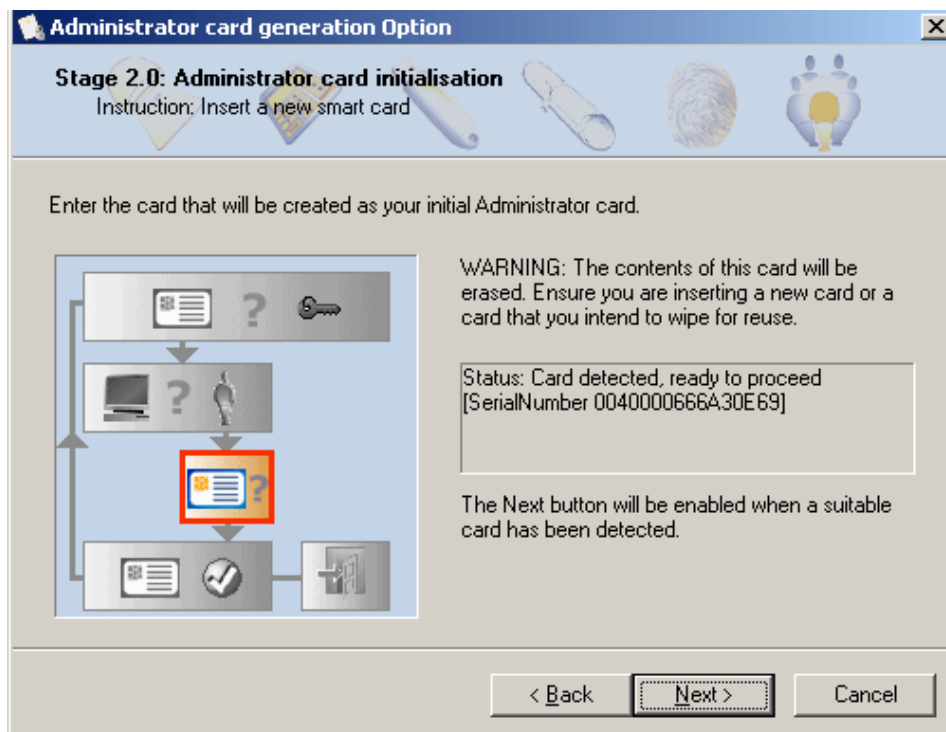
Daher empfiehlt es sich, den Masterkey der Datenbank auf einer Smartcard abzulegen und diese dann an einem sicheren Ort aufzubewahren. Nun benötigt man allerdings bei jedem Start des Server die persönliche Anwesenheit des verantwortlichen Administrators, der die Karte zum Start einlegt und anschließend wieder entfernt.

(Tip: wir erstellen eine 2. Masterkeycard und legen sie im Firmensafe ab.)

→ **Next**

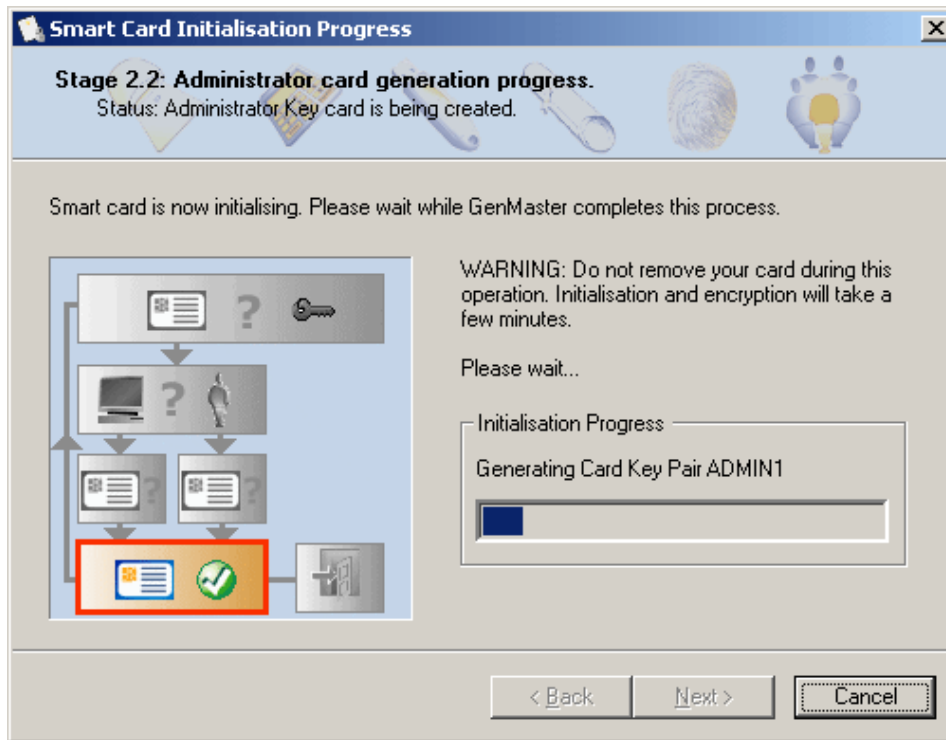
Im Falle einer „Registry Key Protection“ werden wir nun zum Erstellen einer Backupdiskette aufgefordert. Dem gehen wir besser nach ☺

Anschließend erstellen wir eine Smartcard für den MyID Administrator



-> **Next**

Wir geben die Standard PIN der neuen Gemalto Karten ein (1234) und klicken auf **Next**



Finish

Wir können „GenMaster“ jederzeit mit Start – All Programs – MyID – Genmaster erneut aufrufen, um weitere Administrator Token zu erstellen, etwa wenn die Admin Karte verloren geht oder nicht verfügbar ist.

Tipp: Wir bewahren diese Karte an einem sicheren Ort auf.

Da wir uns auf Windows 2003 Server SR2 befinden (Sicherheitseinstellungen!), müssen wir nun noch unser MyID Dienstkonto ermächtigen, Komponenten am Server zu starten.

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.

Fertig

CRYPTAS it-Security
Modcenterstrasse 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
www.cryptas.com