Step by Step Guide der Implementierung einer CA unter Windows 2000 mit einem Smart-Card-Reader

Hardware:

- USB Smart Card Reader und USB Token der Fa. Aladdin (E-Token Pro)

Software

- Aladdin Smart Card Runtime Environment (Version 2.65 – RTE.MSI)
- Windows 2000 Server Build 2195 SP2 als FRD konfiguriert
- AD integrierte Root CA

Voraussetzung:

- Installation der Smart Card Reader Umgebung (RTE.MSI)
- Installation der erforderlichen Aladdin USB Treiber

Ziel:

- Smartcard Anmeldung
- Smartcard – E-Mail Verschlüsselung / -Signierung
- Automatisches Abmelden bei Entfernen der Smartcard

Einzelne Schritte:

1. Installation der eToken Runtime Umgebung (RTE.MSI) von der Aladdin CD
2. Installation der Smart Card Treiber
3. Auswahl der entsprechenden Zertifikatsvorlage . . .
   Smartcard Anmeldung
   Smartcard Benutzer
   Registrierungs-Agent
   Registrierungs-Agent (Computer)
4. Anlegen eines Benutzer in AD Benutzer und Computer
5. Einen PC als Smartcard Enrollment Agent konfigurieren
   Auf diesem Computer muß auch die eToken Runtime Environment installiert werden (RTE)
6. Der Smartcard Enrollment Agent ist der einzige Benutzer welcher das Recht hat stellvertretend für andere Benutzer Zertifikate (in diesem Fall Smartcard-Zertifikate anzufordern
7. Benutzer muß das Attribut „Benutzer muß sich mit einer Smartcard anmelden“ zugeteilt bekommen
8. Gruppenrichtlinie – Computerkonfiguration – Windows Einstellungen – Sicherheitsoptionen – „Verhalten beim Entfernen von Smartcards“ – Richtlinie auf „Abmeldung erzwingen“ einstellen
9. Anwendung der Gruppenrichtlinie forcieren – SECEDIT /REFRESHPOLICY MACHINE_POLICY
10. Anforderung von Zertifikaten
11. Internet Explorer starten – URL: http:://SERVERNAME/CERTSRV

12. Ein Zertifikat anfordern – Weiter
13. Benutzerzertifikatsanforderung – Weiter
14. Weitere Optionen
15. Erweiterte Zertifikatsanforderung
16. Zertifikatsvorlage – Registrierungs-Agent
17. Einsenden
18. „Dieses Zertifikat installieren“ – auswählen
19. Ein Zertifikat anfordern – Weiter
20. Erweiterte Anforderung – Weiter
21. Fordern Sie ein Smartcard Zertifikat für . . . . auswählen – Weiter
22. Smartcard-Benutzer oder Smartcard-Anmeldung auswählen
23. Kryptografie-Dienstanbieter = eToken Base Cryptographic Provider
24. den entsprechenden Benutzer auswählen welcher ein Smartcard-Anmeldungszertifikat erhalten soll
25. Klicken Sie danach auf Einschreiben
26. Es öffnet sich das Fenster „eTCAPI – Select a Token“. Geben Sie hier das Kennwort (PIN) ein
27. Die Schlüssel werden erzeugt und auf die Smart-Card „gebrannt“
28. Wählen Sie danach „Zertifikat anzeigen“ um sich von der korrekten Erstellung zu überzeugen
29. Schließen Sie den Internet Explorer
30. Melden Sie sich mit dem aktuellen Benutzer ab und melden Sich mit dem neuen Smartcard-Benutzer an.
31. Ziehen Sie die Smartcard aus dem Smartcard-Reader und stecken die Smartcard danach sofort wieder in den Reader rein
32. Nach erfolgter Anmeldung ziehen Sie während des Betriebes von Windows 2000 die Smartcard aus dem Reader. Der Benutzer wird jetzt automatisch abgemeldet