Setup AD with etoken Smartcard Authentication

Thomas Glanzmann
<thomas@glanzmann.de>

May 2012

Thomas Glanzmann

- Strong Unix background including kernel and virtual machine programming
- Linux, VMware, Storage, HP Trainer and Consultant
- Diplom-Informatiker Univ. (bachelor and master degree in computer science)
- Self-employed

Agenda

- Prerequists
- DNS delegation
- Setup Active Directory
- Install Active Directory Certificate Services
- Install SafeNet Authentication Client
- Configure Certificate Services
- Sources

Prerequists

- Fully patched Windows 2008 R2
- Configure hostname and static ip address
- SafeNet Authentication Client

DNS delegation

```
directory       IN      NS ad.gmvl.de.
ad.gmvl.de.     IN      A 10.10.20.2
```

Setup Active Directory

- Call `dcpromo`
- Create a domain in a new forest
- Specify forest and domain functional level as Windows 2003
- Configure the DNS Server as part of the setup
- Specifiy a recovery password

Install Active Directory Certificate Services

- Add Role Active Directory Certificate Services
- Select Certificate Authority, Certificate Authority Web Enrollment, Online Responder
- Configure Enterprise Root CA
- Choose RSA#Microsoft Software Key Storage Provider and SHA 256 Hash

Install SafeNet Authentication Client

- Install SafeNet Authentication Client on every system in the domain
- Install SafeNet Authentication Client on every system accessing the domain

Configure Certificate Services: Configure Template

- Start → Administrative Tools → Certification Authority
- Right click Certificate Templates → Manage
- Right click Smart Card Login → Duplicate Template
  - [x] Windows Server 2003
  - Template Display Name: GMVL Smartcard Logon
  - [x] Publish Certificate in Active Directory
  - Request Handling
    - Purpose: Signature & Encryption
    - CSPs → Requests must use one of the following CSPs:
      [x] eToken Base Cyrptographic Provider
  - Issuance Provider
    - This number of authorized signatures: 1
    - Application Policy: Certificate Request Agent

Configure Certificate Services: Issue Certificate Templates

- Right click on Certificate Templates
  → New Certificate Template to Issue
  → Select Enrollment Agent
  → OK

- Right click on Certificate Templates
  → New Certificate Template to Issue
  → Select GMVL Smartcard Logon
  → OK

Configure Certificate Services: Enroll the Enrollment Agent Certificate

- Run mmc
  → Certificate
  → My user

- Right click on Personal
  → Certificates
  → Request New Certificate
  → Enrollment Agent

Configure Certificate Services: Enroll smartcard

- Run Adsi Edit
  → Set UserPrincipalName to administrator@DOMAIN

- Right click on Personal
  → Certificates
  → Advacned
  → Request New Certificate on behalf of new user

References

- Installing Windows 2008 R2 Certificate Services for SmartCard Authentication