Windows 2000 Smartcard Authentication

A road to OpenCA as TTP ...

Overview

- AD integration of TTPs
- Infrastructure requirements
- Special CA requirements
  - Domain controller
  - Clients
- Certs with OpenSSL
- Certs with OpenCA
- Common pitfalls

AD integration of TTPs - structure

- First you must be an enterprise administrator
- Second PKI Services must be enabled
- Configuration -> Services -> Public Key Services = 5 Containers
  - AIA
  - CDP
  - 3 others for MS CA
  - One object NTAuthCertificates must be created (adsi)

AD integration of TTPs - content

- Use dsstore
  - Add CA cert
  - Add CRL
  - Declare trusted root
- See Microsoft Knowledge Base Article 313197

Special CA requirements - DC

- Certificate Template (1.3.6.1.4.1.311.20.2) must be "DomainController" (bmpString)
- GUID in subject alternative name
- There must be a CDP
- See Microsoft Knowledgebase Article 830056
- WARNING: you cannot use TTPs with SMTP replication of ADS

Special CA requirements – user certs

- Certificate template (1.3.6.1.4.1.311.20.2) can be "SmartcardUser" (bmp string)
- Extended key usage must contain smartcardlogin (1.3.6.1.4.1.311.20.2.2)
- The UPN (1.3.6.1.4.1.311.20.2.3) must be placed in othername of subject alternative name (e.g. testuser@cms.hu-berlin.de)
- See Microsoft Knowledgebase article 281245

Certs with OpenSSL - DCs

- You need OpenSSL 0.9.8 – the actual snapshots
- Certificate Template: 1.3.6.1.4.1.311.20.2=DER:1e:20:00:44:00:6f:00:6d:00:61:00:69:00:6e:00:43:00:6f:00:6e:00:74:00:72:00:6f:00:6c:00:6c:00:65:00:72
- Extra section for subjectAltName with GUID: othername=1.3.6.1.4.1.311.25.1;FORMAT:HEX,OCT:00:11:22.....
- Add a CDP

Certs with OpenSSL – User certs

- Certificate Template (optional): 1.3.6.1.4.1.311.20.2=DER:1e:1a:00:53:00:6d:00:61:00:72:00:74:00:63:00:61:00:72:00:64:00:55:00:73:00:65:00:72
- Smartcard login in extended key uasge: extendedKeyUsage = clientAuth, emailProtection, 1.3.6.1.4.1.311.20.2.2
- Extra section for subjectAltName with UPN: othername=1.3.6.1.4.1.311.20.2.3;UTF8:testuser@cms.hu-berlin.de

Certs with OpenCA - Installation

- Perform normal installation of OpenCA 0.9.2.0 with OpenSSL 0.9.7 (do not use 0.9.7d!)
- Install OpenSSL 0.9.8
- Configure OpenSSL 0.9.8 in CA token
  token.xml:

```
<name>CA</name>
<option>
  <name>SHELL</name>
  <value>/usr/local/ssl-0.9.8/bin/openssl</value>
</option>
```

- Activate Certificate Template for role User (optional)

Certs with OpenCA - DCs

- Create a normal request with server side keygeneration
- Edit request on RA
  - Add GUID to subject alternative name (use hexformat of OpenSSL)
  - Select role „DomainController“ (required!)
- Download the key and the certificate in PKCS#12 format.
- Install PKCS#12 file on DC.

Certs with OpenCA – User certs

- Create a normal request
- Edit request in RA
  - Add UPN to subject alternative name (like an emailaddress)
  - Select role „User“
- Please ensure that the key and the certificate are on the smartcard.

Common Pitfalls

- Old and incompatible CSPs (e.g. Gemplus)
- Wrong ATRs in registry (e.g. Schlumberger eGate/Cryptoflex 32K)
- Confusion with OpenSSL versions 0.9.7, 0.9.8 and snapshot
- OpenSSL 0.9.7d
- Ignored Microsoft Knowledgebase articles