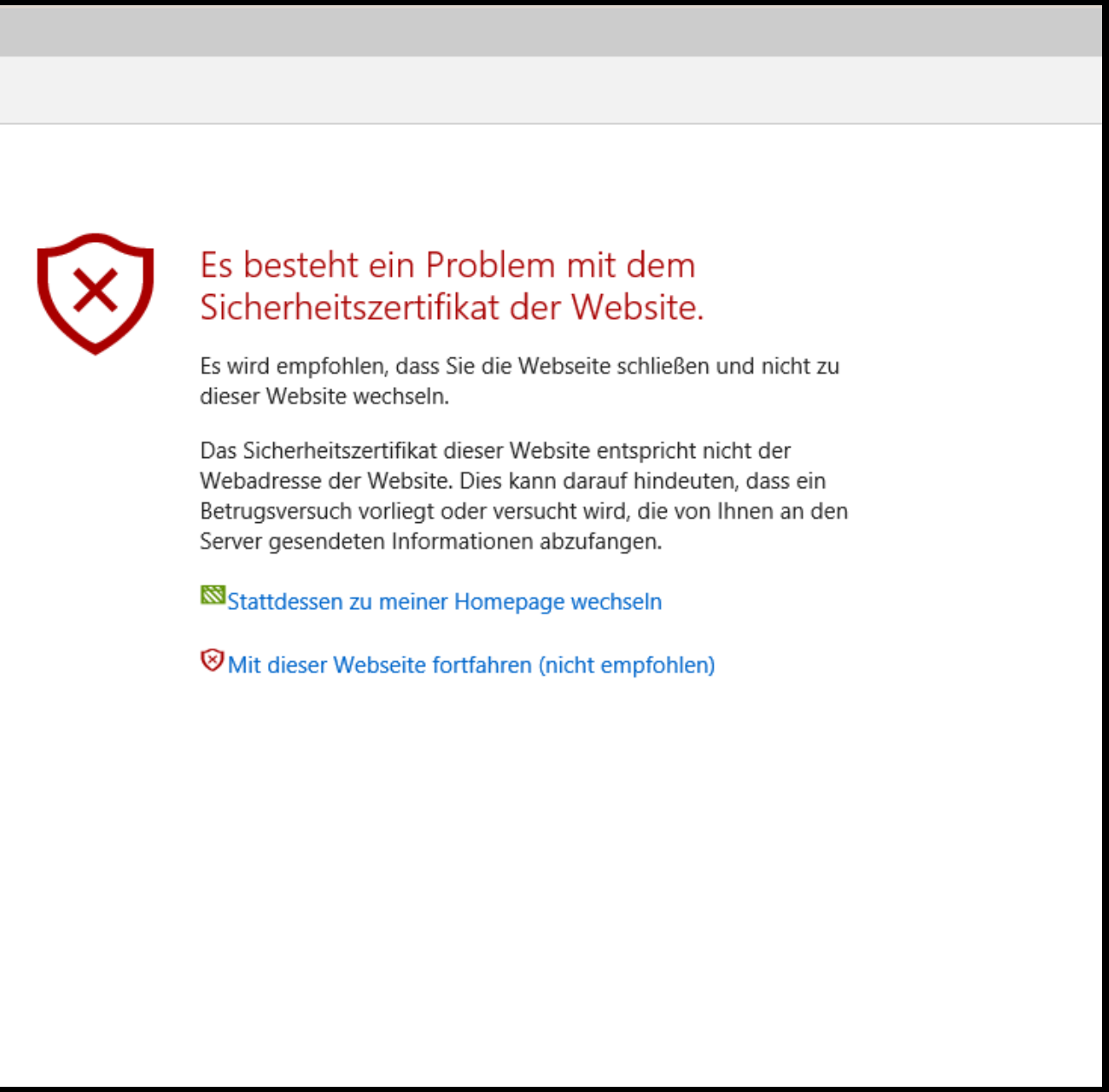


Sicher in einer heterogenen Welt - TLS-Zertifikate von einer Microsoft CA

CLT 2018

Cornelius Kölbel

@cornelinux

Vorstellungsrunde: Cornelius Kölbel

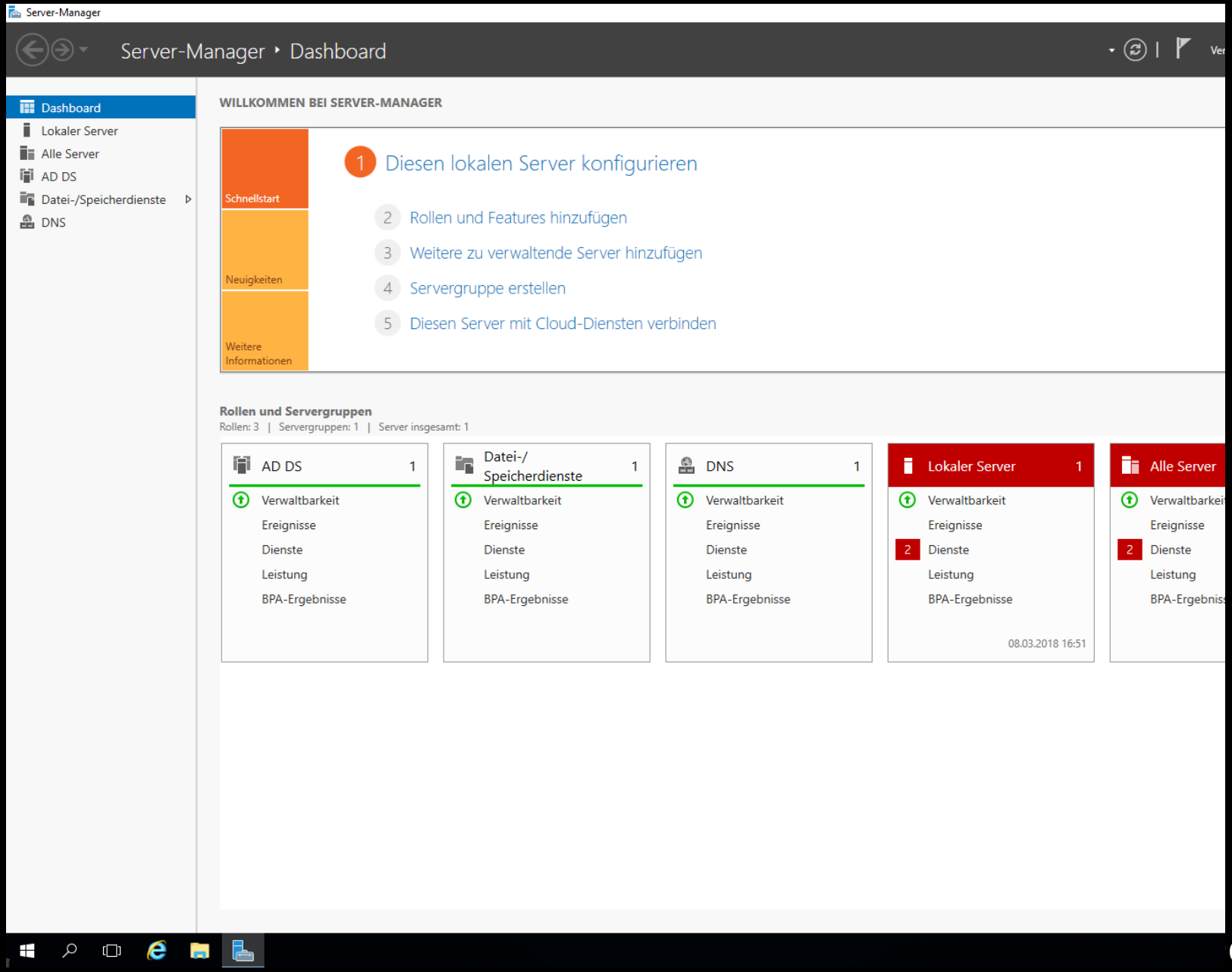
- Cornelius Kölbel
- 2FA seit 2005
  - Smartcards, Aladdin eToken (MS PKI)
  - privacyIDEA seit 2014
- Cornelius.koelbel@netknights.it
- @cornelinux

heterogenen Welt
TLS-Zertifikate von einer Microsoft CA

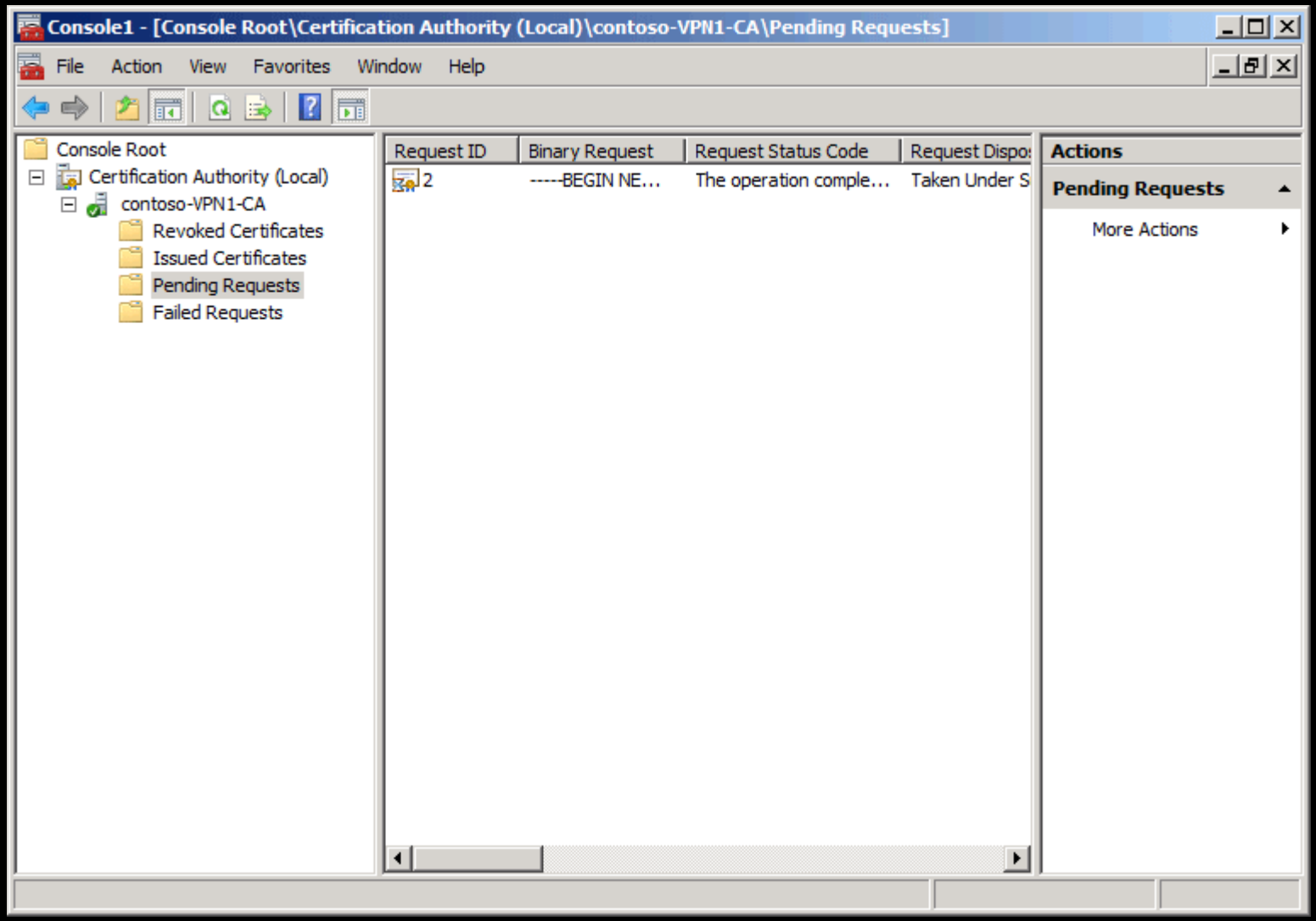
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1c:95:e1:59:ba:bc:15:a1:4c:01:26:ef:3b:1f:26:ca
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=intranet, DC=mimikatz, CN=mimikatz-MOON-CA
        Validity
            Not Before: Feb 15 07:05:34 2017 GMT
            Not After : Feb 15 07:15:34 2022 GMT
        Subject: DC=intranet, DC=mimikatz, CN=mimikatz-MOON-CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:22:cb:89:3c:19:4e:2f:4f:c4:78:db:1e:5f:
                    89:08:a7:1c:8d:ce:58:b1:41:c3:6e:a2:a3:7d:dc:
                    67:72:3c:5e:ac:ac:5f:d0:80:6f:c3:80:6e:86:07:
                    70:4e:41:32:17:a6:56:43:df:00:ab:76:23:0c:53:
                    68:05:96:4e:35:52:af:0c:2c:da:03:c1:56:06:da:
                    6c:a3:a3:4c:62:37:3a:58:99:0d:d2:b9:4e:ee:a6:
                    eb:66:1e:cf:0d:96:ef:70:f7:7a:47:34:0c:22:f2:
                    da:ad:40:a7:c7:74:57:54:2b:ae:00:0b:85:11:5a:
                    c5:4d:00:e5:98:48:04:41:68:53:0e:e5:57:fa:a3:
                    b2:de:25:00:e5:76:53:02:4f:5e:05:03:ef:b2:ce:
                    2e:d1:70:14:b6:b5:1b:8f:a0:0f:ae:d7:24:74:04:
                    42:6c:6a:c4:00:b4:c1:71:43:5e:ca:34:fd:f7:1e:
                    d1:7d:ae:71:ff:ed:48:85:5b:2a:f2:e9:c2:84:b7:
                    29:92:86:dd:88:2a:05:e2:87:64:bf:ab:53:f5:d9:
                    e9:46:25:52:25:1a:42:0a:83:4c:b6:f4:7d:25:ac:
                    ce:22:4d:7a:f0:14:27:f5:4f:ee:d7:87:8b:e3:f1:
                    08:d0:8b:e6:2c:55:4b:43:dc:e5:e8:09:1a:6c:b0:
                    31:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                4A:A2:20:07:4A:CC:78:97:84:46:81:EA:1C:82:4A:D0:29:22:6C:10
            1.3.6.1.4.1.311.21.1:
                ...
    Signature Algorithm: sha256WithRSAEncryption
         5f:b6:b5:68:45:3b:0a:e7:0d:df:ac:60:66:56:a2:4c:a7:1a:
         ab:0d:28:e6:ae:6a:60:bd:33:4e:5a:b9:a3:58:07:03:85:02:
```

Vorstellungsrunde: TLS Zertifikat

Vorstellungsrunde: Microsoft Server 2003-2016



Vorstellungsrunde: Microsoft CA



Vorstellungsrunde: Admin im heterogenen Netzwerk

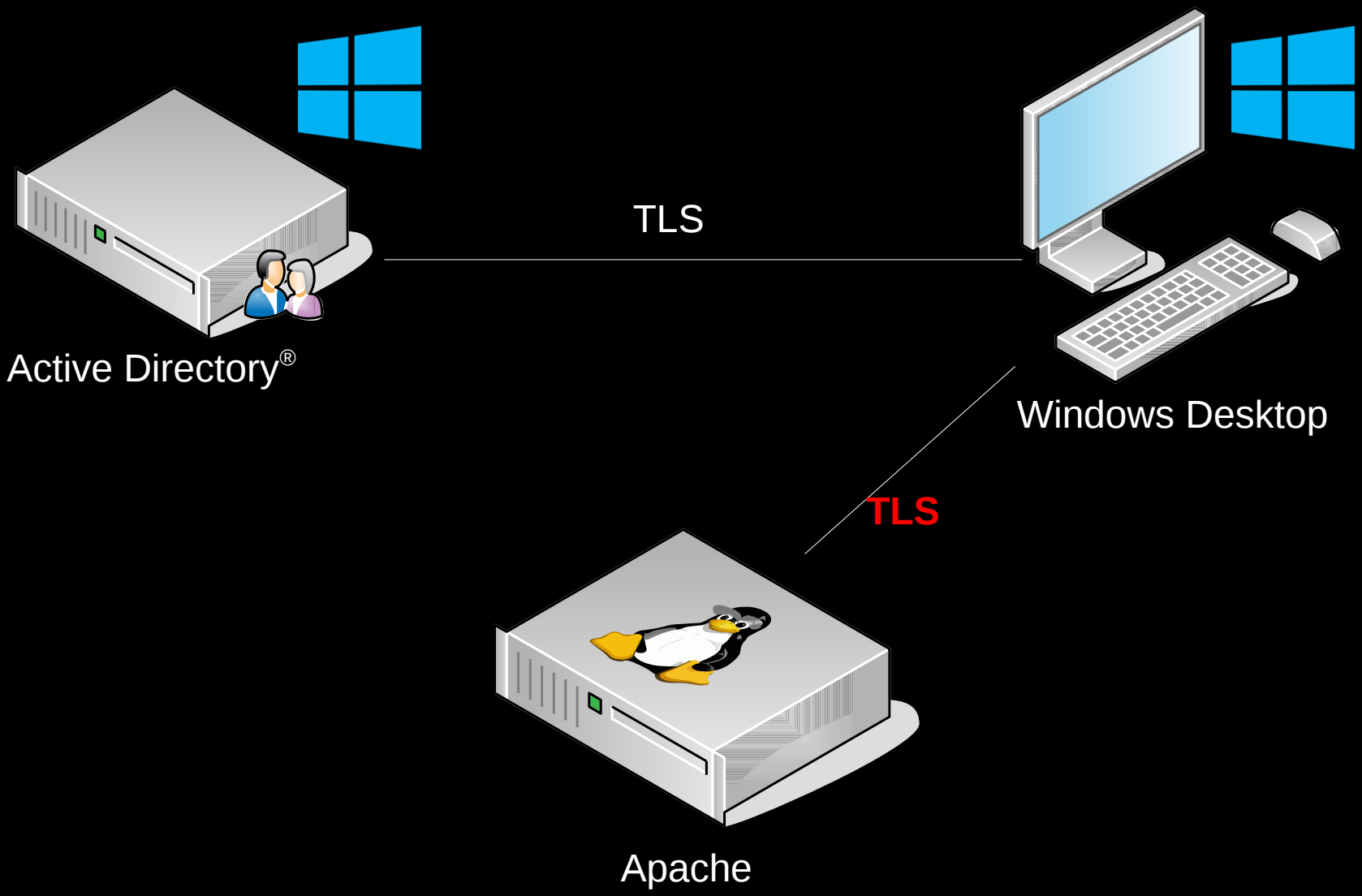
Vorstellungsrunde: so schön warm hier...

Schluss mit Lustig

Meine Motivation

- privacyIDEA ist Apache/Nginx Applikation.
- Benutzer per LDAPS aus AD lesen.
- Windows Clients greifen via https auf Apache zu.

Im Gepäck: Heterogenes Netzwerk



The Windows Logo and the term „Active Directory“ are Trademarks to Microsoft Corporation.

Agenda

- Micrsoft CA installieren
- Domain Controller-Zertifikat
- Apache Zertifikats-Reqeust
- Apache Zertifikat
- Browsen

Microsoft CA

- Server-Rolle
- Varianten:
  - Stand-Alone
  - Domänenintegriert (Zertifikatstemplates…)

Microsoft CA: Installation

- ...mittels Rollen-Wizard,
- aber: capolicy.inf
- CA ≠ PKI

Ohne capolicy.inf

- Beliebig viele Sub-CA!
- Domaincontroller-Zertifikate mit 1024 bit!
- Fehlende Infos (CPS) in Root-Zertifikat...

Microsoft CA: capolicy.inf

```
[Version]
Signature = "$Windows NT$"
[PolicyStatementExtension]
Policies=InternalPolicy
[InternalPolicy]
OID=1.3.6.1.4.1.{PEN}.1.1
Notice="Legal Policy Statement"
URL=http://pki.corp.contoso.com/pki/cps.txt
[Certsrv_Server]
RenewalKeyLength = 4096
RenewalValidityPeriod = Years
RenewalValidityPeriodUnits = 5
LoadDefaultTemplates = 0
[BasicConstraintsExtension]
PathLength = 2
Critical = Yes
[RequestAttributes]
# CertificateTemplate
# Gut für SubCAs
```

Siehe auch:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj125373(v=ws.11)
https://www.sysadmins.lv/blog-en/certificate-policies-extension-all-you-should-know-part-2.aspx

Microsoft CA installieren

Domain Controller Zertifikate

- LDAP → LDAPS
- `LoadDefaultTemplates=0` → Wir müssen uns selber drum kümmern

Zertifikats-Vorlagen / Templates

- Definieren
  - Wofür das Zertifikat ist
  - Was im Zertifikat steht
  - Wer was mit dem Zertifikat machen darf
- Stehen in der **Configuration** Partition in **Forest-Root**

Domain Controller Zertifikate

- Neue Templates:
  - Domain Controller Authentication
  - Directory Email Replication
  - Kerberos Authentication
- Eigene Templates vererben

Autoenrollment Domain Controller Zertifikate

- GPO Default Domain Controller Policy anpassen:
  - Computer Configuration → Policies → Windows Settings → Security Settings → Pub Key Policies → Automatic Request Settings (New ACR: Domaincontroller)
- Autoenrollment einschalten:
  - Computer Configuration → Policies → Windows Settings → Pub Key Policies: Certificate Service Client – Certificate Erollment Policiy
    - Certificate Services Client – Certificate Enrollment Policy
    - Certificate Services Client – Auto Enrollment

Zugriff mittels LDAPS

- Mit Domain Controller Zert bietet AD Zugriff mittels LDAPS an.

Apache Webserver

- Windows Client erhält Zertifikatswarnung
- Neues Webserver-Template
  - Laufzeit
  - Schlüssellänge

Apache: Zertifikats Request

- `openssl req -new -newkey rsa:2048 -subj /CN=privacyidea.cltlab.intranet -nodes -outform DER -out privacyidea.req -keyout privacyidea.key`

Microsoft CA: Zertifikate mit SubjectAltName

- Damit die Microsoft CA Zertifikate mit SAN ausstellen kann:

```
certutil -setreg policy\EditFlags
        +EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
```

Microsoft CA: Zertifikats-Request signieren

- Web-Interface
- Kommandozeile:
  - `certreq submit attrib „CertificateTemplate:TemplateName“ c:\privacyidea.req`
- `san:dns=<name1>&dns=<name2>&ip=<IP>`