Nutzung der Community PKI auf einem Session Border Controller

Kevin Scheffler | IT Center RWTH Aachen University

IT Center | RWTH AACHEN UNIVERSITY

Nutzung der Community PKI auf einem Session Border Controller

Topics

- Was ist die Community PKI
  - Vorteile / Nachteile
- Zertifikate
  - Antrag Erstellen
  - Signieren
  - PKCS-12 erzeugen
- Wechsel des Zertifikats
- Fazit

Was ist die Community PKI?

- Alternative für die Zertifikate des Trusted Certificate Service von GÉANT
- Community PKI Zertifikate sind nicht im Browser oder OS vorinstalliert
- Unterliegen nicht den Beschränkungen des Browser-CA-Forums
- Anwendungszwecke:
  - Shibboleth IdP/SP Metadaten (https://doku.tid.dfn.de/de:certificates#eigene_lokale_ca)
  - interne Systeme wie bspw. Datenbank bzw. wo die Risiken der öffentlichen PKI vermieden werden sollen
  - 802.1X für den Netzzugang
  - Active Directories
  - für **DFN SIP-Zugänge**

Vorteile / Nachteile

Vorteile	Nachteile

• längere Laufzeiten
  • 1170 Tage für Serverzertifikate
  • 1825 Tage für Nutzerzertifikate
- weniger Interaktion notwendig
	• Community PKI Zertifikate sind nicht im Browser oder OS vorinstalliert
	• Daher nicht „Trusted by Default“
	• CA muss auf jedem beteiligten System installiert werden
	• primär für interne Systeme nutzbar

Ausnahme:

Community PKI wurde von der Telekom in die entsprechenden Knoten für die DFN-Telefonie implementiert, sodass diese Zertifikate auch für die Nutzung von verschlüsselter Telefonie verwendet werden können.

Zertifikate

Antrag Erstellen

- Erstellen der Zertifikate via OpenSSL per Shell
- Nutzung einer Conf-Datei für die Parameter
- openssl req -nodes -new -newkey rsa:4096

  -keyout cert_name.key -sha256

  -out certname.csr

  -config ./csr.conf

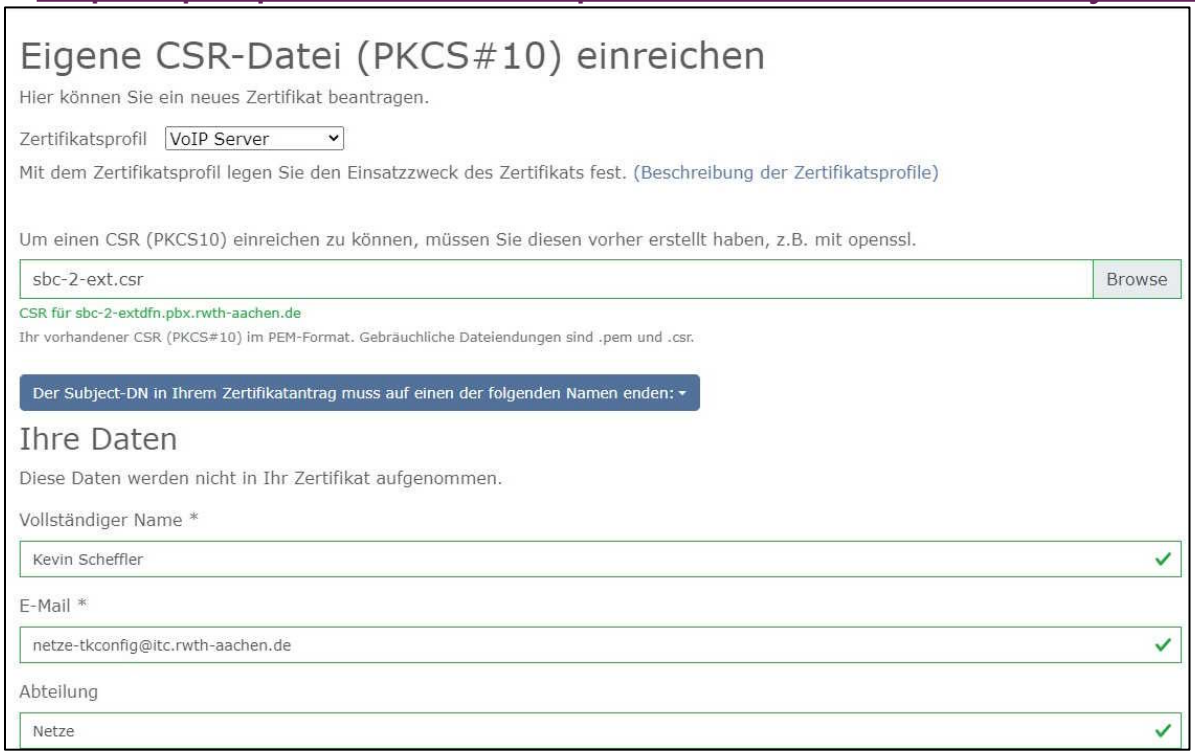
```
~/certs$ cat csr.conf
[ req ]
default_bits                = 4096
distinguished_name          = req_distinguished_name
req_extensions              = v3_req
prompt                      = no

[ req_distinguished_name ]
countryName                 = "DE"
stateOrProvinceName         = "Nordrhein-Westfalen"
localityName                = "Aachen"
organizationName            = "RWTH Aachen"
commonName                  = "cn.rwth-aachen.de"

[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
```

Zertifikate

Signieren

- Hochladen des CSRs auf:

  https://pki.pca.dfn.de/dfn-pki/dfn-verein-community-ca/3550/



Wurzelzertifikat herunterladen

- Herunterladen des Wurzelzertifikats:

  https://doku.tid.dfn.de/de:dfnpki:dfnpki_root_certs#dfn-verein_community_pki

DFN-Verein Community PKI

Das Wurzelzertifikat der DFN-Verein Community PKI ist **nicht** in Browsern oder Betriebssystemen vorinstalliert.

	CommonName	Gültigkeitsende	SHA256 Fingerprint	
Wurzelzertifikat				
	DFN-Verein Community Root CA 2022	Jan 21 14:08:41 2042 GMT	3C:DC:2C:9E:9E:5A:36:CB:58:88:FD:17:96:CB:91:2F :84:62:53:B6:82:C1:B3:20:57:53:20:33:51:0C:7B:B6	.cer .pem
Issuing CAs				
	DFN-Verein Community Issuing CA 2022	Jan 21 14:08:41 2042 GMT	BA:D0:41:D6:29:16:B6:A3:80:97:14:79:1F:86:F1:7D: 54:70:CB:3D:6F:8C:7A:87:CB:B6:FB:C5:60:B8:C7:A2	.cer .pem
	Fraunhofer Service CA 2022	Jan 21 14:08:41 2042 GMT	DC:C4:B2:DC:FC:13:CD:0A:CB:18:B4:79:82:D0:D2:65: C6:D1:D3:21:16:03:4B:E5:3E:ED:02:14:A6:E5:D8:98	.cer .pem
	Fraunhofer User CA 2022	Jan 21 14:08:41 2042 GMT	00:7E:15:47:AD:AA:FD:66:07:2D:71:17:F4:26:15:D2: F1:85:1D:7B:9D:E7:34:64:10:A3:E5:41:69:76:2E:A1	.cer .pem
	MPG Community CA	Jan 21 14:08:41 2042 GMT	BE:65:6C:B6:01:7D:77:7C:B8:A7:06:A9:21:DB:2F:85: 93:B7:D0:F2:0C:7A:C3:DA:2F:55:7B:53:EC:12:87:5A	.cer .pem

PKCS12-Datei erzeugen

- PKCS-12 Datei erzeugen für den Import in den SBC
- „openssl pkcs12 -export

  -in certificatefile.pem

  -inkey devicenam.private.pem

  -certfile chain.pem

  -out devicename.p12“

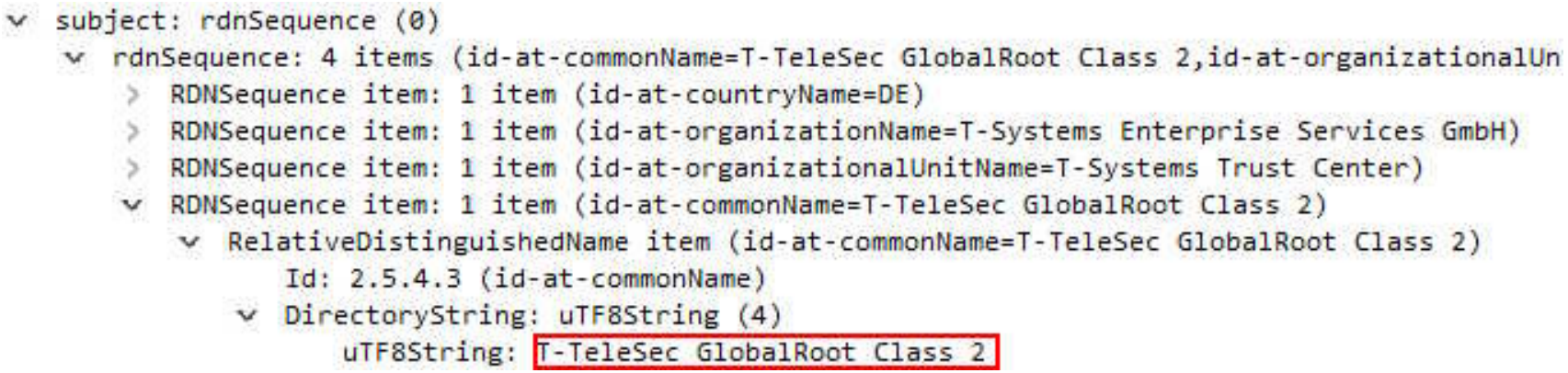
Wechsel des Zertifikats

- Session Border Controller (SBC) ist ein Cisco ISR-4431
- Geplanter Ablauf des Wechsels:
  - Zertifikat auf den SBC kopieren
  - Service stoppen
  - Altes Zertifikat entfernen und Trustpoints löschen
  - Neues Zertifikat importieren und Trustpoints anlegen
  - Service starten

- Leider doch nicht so einfach!

Wechsel des Zertifikats

- Was ist passiert?
  - Keine SIP TLS Verbindung mehr zur Telekom
  - SSL Error, da das Zertifikat der Telekom nicht validiert werden kann
  - Analyse via Wireshark



Wechsel des Zertifikats

- **Lösung:**
  - Root-CA der Telekom auf den SBC kopieren
  - Diese ist identisch mit dem Root-CA der alten DFN-PKI
  - Neustart der Dienste

- Wechsel erfolgreich abgeschlossen
- Gespräche sind verschlüsselt

```
Remote-Agent:141.39.219.53, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =========== ======= ========== =========== ============= ===========
         5061     830 Established           0 [redacted]        TLSv1.2
        33295     839 Established           0 [redacted]        TLSv1.2

Remote-Agent:141.39.219.21, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =========== ======= ========== =========== ============= ===========
         5061     790 Established           0 [redacted]        TLSv1.2
        49615     840 Established           0 [redacted]        TLSv1.2
```

Fazit

- Community PKI funktioniert
- ausgestellte Zertifikate werden von Telekom akzeptiert
- Lange Zertifikats-Laufzeiten => weniger Aufwand

- Offene Punkte:
  - Warum verwendet die Telekom nicht das DFN VoiP Zertifikat? (in Klärung)

Vielen Dank
für Ihre Aufmerksamkeit

Kontaktdaten:
Kevin Scheffler
Tel: +49 241 80 29223
E-Mail: scheffler@itc.rwth-aachen.de

Mailing-Liste: https://www.listserv.dfn.de/sympa/info/dfn-voip-forum