Opennet CA
Workshop Zertifikate

Opennet Initiative e.V.
http://www.opennet-initiative.de/

2011-09-19
Frieda23

Opennet CA

- Zertifizierungsstelle („Certification Authority“)
- Signieren von Zertifikatsanfragen
- Basis ist OpenSSL Software
- Hosting auf heartofgold
- Alternativ: Unter-/Sub-CA („Intermediate-CA“)

- Einsatz für Verwaltung von OpenVPN Zugängen

Opennet Initiative

Zertifikate

Schlüsselgenerierung (KEY)
- bleibt immer beim Nutzer!

Zertifikatsanfragen (CSR)
- Access Point
- Mobiler Knoten
- Usergateway

Signatur durch CA → Zertifikat (CRT)

Opennet Initiative

KEY u. CSR erzeugen

```
# openssl req -days 3650 -nodes -new -keyout
keys\1_aps_on.key -out keys\1_aps_on.csr
-config openssl.cnf
```

- Common Name (eg, your name or your server's hostname) []: 1.aps.on
- Email Address [mail@host.domain]: du@provider.tld

Opennet Initiative

Signieren / CRT erzeugen

Nutzerzertifikat (AP/Mobiler Knoten)

openssl ca -config openssl.cnf -days 3650 -in csrs\1_on_aps.csr -out certs\1_on_aps.crt

heartofgold:

/etc/openvpn/auth/opennet

sign.sh 1_aps.on

Opennet Initiative

Signieren / CRT erzeugen

Usergateway Zertifikat

openssl ca -config openssl.cnf -days 3650 -in csrs\1_on_ugw.csr -out certs\1_on_ugw.crt

heartofgold:

/etc/openvpn/auth/opennet_usergateways

sign.sh 1_on_ugw

Opennet Initiative

OpenVPN Zugang aktivieren

- Für ein Zertifikat einen VPN Zugang aktivieren, nur notwendig für Nutzerzertifikate.
- Mitgliedschaft notwendig / prüfen.

opennetca@heartofgold:~/opennet_users

touch 1.aps.on

Opennet Initiative

Weiter lesen....

Opennet

https://wiki.opennet-initiative.de/wiki/OpenVPN

https://wiki.opennet-initiative.de/wiki/Opennet_CA

Wikipedia

http://de.wikipedia.org/wiki/Digitales_Zertifikat

http://de.wikipedia.org/wiki/Certification_Authority

http://de.wikipedia.org/wiki/OpenSSL

Opennet Initiative

Über den Tellerrand...

- Schon einmal mit XCA gearbeitet?

- Versendest du signierte und/oder verschlüsselte E-Mails?
- Kennst du CAcert?

- Was ist X.509?
- Was sind PEM, DER, PKCS#7, PKCS#12?