SURFCERTIFICATEN 2020~2030

GÉANT Trusted Certificate Service 4

David, Fedor, Freddie, Nicole, Sigita...

Sectigo 1.5 Mega certs per day: not manually...
Own support staff in 4 timezones
You: Monday – Friday 04:00 – 20:00 EST
SURFcertificaten staff: Premium 365 x 24

https://cert-manager.com/customer/surfnet?login=username
No trackers; whitelist Javascript and cookies
Whitelist noreply_support@trust-provider.com in spamfilter
Read mail From surfnet To scs-ra@<your institute> !!!
Chains: https://crt.sh/?CAName=%25GEANT+Vereniging%25

Planning

- Critical Paths (unofficial)
  - Provisioning our 110+ Orgs & 6350+ Domains. And 30+ other NRENs
  - SSO, eduGAIN; SAML and WAYF discovery. IGTF eScience certs

- Jan 15th (13:00 – 15:00) 3 NREN MasterRAOs on-boarded in PoC setup
- First Signed mail 16:14. First TLS server 16:48
- ...
- End of March: commissioning complete and ready for large-scale roll-out
- End of April: all Subscribers on-boarded, trained, and ready to issue
- May 1st: production

Todo list

- Als je DNS CAA records hebt, verifieer dan of je sectigo.com al hebt toegevoegd (dig mijndomain.nl type257 | grep CAA)
- Zorg dat je huidige DigiCert certs die snel verlopen vervangt
  - Al is het maar door een vers OV exemplaar in voorraad te hebben
- Geen mailtje gehad met je Sectigo username? Dan staat er niets voor je klaar
- Mail aan scs-ra@surfnet.nl Subj: **Aanmelding**
  - SURFnet B.V.
  - KVK 30090777
  - Nee geen key escrow
  - Teun
  - Nijssen
  - teun.nijssen@surfnet.nl
  - +31 6 xxxx yyyy
  - Silly-passsWord

Na je zoom bijeenkomst

- Maak minimaal een extra ‘RAO admin’ collega aan
  - Daarna mail To: scs-ra@surfnet.nl
  - Subj: ‘**Extra RAO**; graag privileges voor Jan de Vries’
- Zet 1 onschuldig domain dat fout mag gaan in SCM
  - Twee vormen: mijndomain.nl en ook *.mijndomain.nl (geen subdomains!)
  - Wacht tot je een delegated/approved mail krijgt en stel de DCV in (cname/mail)
  - Bestel 1 OV certificaat in het ingevoerde domain e.g. www.mijndomain.nl
- Als dat goed gaat zet je je domains in SCM; altijd een met en een zonder ‘*.’
  - Niet meer dan 5 dubbele tegelijk; medische instellingen: voorrang: alles tegelijk!
- Ga los op OV TLS certificaten
- Laat in mei weten wanneer je een **stabiele** set domains hebt waarvoor je EV TLS wil
  - Daarna wordt EV makkelijk, daarvoor is EV heel lastig. Niet in april, te druk bezig

Sectigo TCS 4 versus DigiCert TCS 3

- **Native** Sectigo Certificate Manager (SCM), no ‘djangora’ like in the Comodo days
- No email for support: webinterface to Ticket system
- No ‘Divisions’; the NREN MasterRAO admin creates Organizations and their RAO
- Only admins; so far no DigiCert request-only ‘users’
- Your Organization RAO admin may create Departments with own DRAO admins
- Unlimitted rights at MRAO, not read-only
- Multiple Factor Authentication 1 username/password
  - 2 Client certificate in browser or even 3 Client cert in hardware like Yubikey
- Much better automatic ordering and renewal
  - ACME like letsencrypt with OV EV; Sectigo sponsors the letsencrypt CT-logs
  - Intune SCEP, Azure, Agents, Certificate Discovery scans...
- IdP login; configuring allows even admins to use SSO
- Tuning admin rights e.g. delegating domains to specific departments

What do we get?

- Forecasting 10 years: Crypto strength, embedded applications
  Chains RSA 4096 SHA384, Elliptic Curve NIST P-256, sadly no Curve25519
- Full chain RSA and ECC with OV and EV; Sectigo uses 2 roots for TCS
  - Roots in many Root Programs; five year or newer versions (e.g. not older Android)
  - At least MS Win, RedHat, Debian, Ubuntu, Mac OS, Android, iOS
  - All platforms use the same chains
- GÉANT branded intermediates (DigiCert 5+1, Sectigo 2*5+1=11)
- Softlimit 250 SubjAltNames (FQDN, wildcard, ipAddress)
- TLS OV and EV, Personal 3 versions, Code Signing, EV CS, Adobe AATL doc signing
- IGTF grid eScience Server OV Classic, Personal MICS and Robot
- ‘Qualified’ signatures EU Regulation No 910/2014 (eIDAS). 2020Q1? Countries?
- Unlimited numbers fixed price