LISTING UITLEG

```
> Start nieuwe regel
regel met spatie na afbreking
regel zonder spatie na afbreking
```

Je eigen certificaatautoriteit met step-ca

Met Let's Encrypt is het heel eenvoudig om tls-certificaten aan te vragen en automatisch te vernieuwen, maar dat is voornamelijk voor publiek toegankelijke websites. Wil je een gelijkaardige functionaliteit in je lokale netwerk, dan komt step-ca goed van pas: hiermee creëer je je eigen certificaatautoriteit, inclusief automatische vernieuwingen van certificaten. > **Koen Vervloesem**

> Let's Encrypt (**https://letsencrypt.org/)** heeft in enkele jaren tijd de industrie van certificaatautoriteiten (CA's) overhoop gegooid. Iedereen kan nu heel eenvoudig gratis een tls-certificaat voor een domein aanvragen en automatisch via het ACME-protocol (Automatic Certificate Management Environment) vernieuwen. Dat is overigens in 2019 als RFC 8555 (**https://tools.ietf.org/html/rfc8555**) aangenomen.

Met Let's Encrypt voorzie je dus heel eenvoudig je publiek toegankelijke webserver van een tls-certificaat, maar voor interne servers is het minder geschikt. Je lekt de domeinnamen waarvoor je een tls-certificaat aanvraagt immers naar internet: als onderdeel van het project Certificate Transparency (**https://www.certificate-transparency.org/**) worden alle uitgereikte tls-certificaten gelogd in een publiek toegankelijke database. Die kun je doorzoeken op websites van aggregators zoals **https://crt.sh/** en **https://censys.io/certificates**. Zo krijgt iedereen een vrij goed inzicht van wat je allemaal in je interne netwerk hebt draaien.

JE EIGEN CERTIFICAATAUTORITEIT

Voor interne servers draai je dus beter je eigen privé-certificaatautoriteit. Dat kan zelfs met enkele OpenSSL-opdrachten al: in feite is een certificaatautoriteit gewoon een instantie met een rootcertificaat dat andere certificaten ondertekent, en dat kun je perfect manueel. Maar voor een serieuze infrastructuur (en om fouten te vermijden) automatiseer je dat beter.

Het bedrijf smallstep (**https://smallstep.com/**) biedt één oplossing hiervoor aan: step-ca (**https://smallstep.com/certificates/).** Het programma is opensource (**https://github.com/smallstep/certificates**) en laat je toe om je eigen certificaatautoriteit te draaien, inclusief een server die het ACME-protocol spreekt en dus clients toelaat om net zoals bij Let's Encrypt automatisch certificaten aan te vragen en te vernieuwen. Het verschil met Let's Encrypt: je houdt dit alles in eigen beheer en zonder dat je informatie lekt over welke certificaten je hebt.

INSTALLATIE

Step-ca dien je op een computer te installeren die altijd toegankelijk is voor je clients. Een Linux-server die je als nas gebruikt of een Raspberry Pi is een ideale machine daarvoor. Op de GitHub-pagina van step-ca staan installatie-instructies voor Debian en Arch Linux. Voor dit artikel installeren we step-ca op Ubuntu Server 18.04 LTS en gaan we ervan uit dat je de certificaatautoriteit op Ubuntu Desktop 19.10 gebruikt.

Helaas zit step-ca nog niet in Debians repository's en voor Ubuntu bestaat er nog geen ppa. Ga dus naar **https://github.com/smallstep/certificates/releases** en **https://github.com/smallstep/cli/releases** en download van elk het deb-bestand (alleen voor amd64) van de nieuwste versie. Installeer beide programma's daarna. Op de server allebei:

```
> server:~$ sudo dpkg -i Downloads/step-certificates_0.13.3_amd64.deb
server:~$ sudo dpkg -i Downloads/step-cli_0.13.3_amd64.deb
```

En op de client alleen step-cli:

```
> client:~$ sudo dpkg -i Downloads/step-cli_0.13.3_amd64.deb
```

Even opletten, want de naamgeving is verwarrend: het pakket step-certificates installeert het programma step-ca en het pakket step-cli installeert het programma step (wat overigens een symbolische link is naar step-cli).