Install CFSSL and CFSSLJSON - CloudFlare's KPI toolkit

Written by Pim on Wednesday January 10, 2018 - 0 Comments (http://www.pimwiddershoven.nl/entry/install-cfssl-and-cfssljson-cloudflare-kpi-toolkit#disqus_thread) - Permalink (/entry/install-cfssl-and-cfssljson-cloudflare-kpi-toolkit)
Categories: devops (/categories/devops), howto (/categories/howto) - Tags: certificates (/tags/certificates), pki (/tags/pki)

The tools CFSSL and CFSSLJSON from CloudFlare make life a lot easier when you have to generate certificate signing requests (CSR), certificates, and keys on a regular basis, or you want to use it as a development tool to automate this for you.

The installation of the tool is pretty straightforward:

```
$ curl https://pkg.cfssl.org/R1 (https://pkg.cfssl.org/R1).2/cfssl_linux-amd64 -o /usr/local/bin/cfssl
$ curl https://pkg.cfssl.org/R1 (https://pkg.cfssl.org/R1).2/cfssljson_linux-amd64 -o /usr/local/bin/cfssljson
$ chmod +x /usr/local/bin/cfssl /usr/local/bin/cfssljson
```

The tools are now ready-to-use!

Generating a CSR is now super easy. First, create a JSON file and save it to disk:

```
{
    "hosts": [
        "www.my-awesome-company.com (http://www.my-awesome-company.com)"
    ],
    "CN": "www.my-awesome-company.com (http://www.my-awesome-company.com)",
    "key": {
        "algo": "rsa",
        "size": 2048
    },
    "names": [{
        "C": "NL",
        "L": "Amsterdam",
        "ST": "Noord-Holland",
        "O": "My Company",
        "OU": "Operations"
    }]
}
```

Then, use the CFSSL and CFSSLJSON tools to generate a CSR and key:

```
cfssl genkey csr.json | cfssljson -bare my_awesome_company_com
```

Send the CSR to the CA to receive a signed certificate or sign it yourself:

```
cfssl selfsign www.my-awesome-company.com (http://www.my-awesome-company.com) csr.json | cfssljson -bare my_awesome_company_com
```

It's also possible to create your own CA. You need a CA JSON configuration file to enable signing and a JSON file to generate the certificate and key.

ca-csr.json:

```
{
  "CN": "Dev CA",
  "key": {
    "algo": "rsa",
    "size": 2048
  },
  "names": [
    {
      "C": "NL",
      "L": "Amsterdam",
      "ST": "Noord-Holland"
    }
  ]
}
```

And initialize the CA:

```
cfssl gencert -initca ca-csr.json | cfssljson -bare ca –
```

Then create the ca-config.json to configure the signing and profiles:

```
{
  "signing": {
    "default": {
      "expiry": "168h"
    },
    "profiles": {
      "client": {
        "expiry": "43800h",
        "usages": [
          "signing",
          "key encipherment",
          "client auth"
        ]
      }
    }
  }
}
```

Generate new certificates using your own CA:

```
cfssl gencert -ca=ca.pem -ca-key=ca-key.pem -config=ca-config.json -profile=client my-cert.json | cfssljson -bare my_certificate
```

Done for now! Have fun generating CSR, certs, and keys using CFSSL and CFSSLJSON!

(https://twitter.com/Piwi_91) (https://github.com/piwi91/)

(https://www.linkedin.com/pub/pim-widdershoven/3a/b91/983)