



LEEC: Let's Encrypt Erlang with Ceylan

Organisation: Copyright (C) 2020-2021 Olivier Boudeville

Contact: about (dash) leec (at) esperide (dot) com

Creation date: Wednesday, November 11, 2020

Lastly updated: Saturday, January 2, 2021

Dedication: Users and maintainers of the LEEC library, version 0.6.

Abstract: The role of the LEEC library is to interact from Erlang/OTP with Let's Encrypt servers, mostly in order to generate X.509 certificates.

The latest version of this documentation is to be found at the [official LEEC website](http://leec.esperide.org) (<http://leec.esperide.org>).

The documentation is also mirrored [here](#).

Table of Contents

LEEC: Let's Encrypt Erlang with Ceylan	1
Overview	3
Design Notes	3
Multiple Domains Having Each Multiple Hostnames	3
Concurrent Certificate Operations	3
Getting Information about the Generated Certificates	3
Support	5
Please React!	5
Ending Word	5

Overview

The online documentation for LEEC is currently available [here](#).

Design Notes

Multiple Domains Having Each Multiple Hostnames

At least the ACME servers from Let's Encrypt enforce various fairly low [rate limits](#), which leads to preferring requesting certificates only on a per-domain basis (ex: for `foobar.org`) rather than on a per-hostname one (ex: for `baz.foobar.org`, `hurricane.foobar.org`, etc., these hosts being virtual ones or not), as such requests would become too numerous to respect these thresholds.

A per-domain certificate should then include directly its various hostnames as *Subject Alternative Names* (SAN entries).

With the `http-01` challenge type, no wildcard for such SAN hosts (ex: `*.foobar.org`) cannot be specified), so all the wanted ones have to be explicitly listed¹.

Concurrent Certificate Operations

LEEC implemented independent (`gen_statem`) FSMs to allow typically for concurrent certificate renewals to be triggered. A drawback of the aforementioned Let's Encrypt rate limits is that, while a given FSM is to remain below said thresholds, a set of parallel ones may not.

If a [task ring](#) may be used to avoid by design such FSMs to overlap, another option is to use a single FSM and to trigger certificate requests in turn.

Getting Information about the Generated Certificates

If using LEEC to generate a certificate for a `baz.foobar.org` host, the following three files shall be obtained from the Let's Encrypt ACME server:

- `baz.foobar.org.csr`: the PEM certificate request, sent to the ACME server (~980 bytes)
- `baz.foobar.org.key`: the TLS private key regular file, kept on the server (~1675 bytes)
- `baz.foobar.org.crt`: the PEM certificate itself of interest (~3450 bytes), to be used by the webserver

To get information about this certificate:

```
$ openssl x509 -text -noout -in baz.foobar.org.crt
```

```
Certificate:
```

```
  Data:
```

```
    Version: 3 (0x2)
```

```
    Serial Number:
```

```
      04:34:17:fd:ee:9b:bd:6b:c2:02:b1:c0:84:62:ed:a6:88:5c
```

¹As a result, the certificate may disclose virtual hosts that would be otherwise invisible from the Internet (as no even declared in the DNS).

```

Signature Algorithm: sha256WithRSAEncryption
Issuer: C = US, O = Let's Encrypt, CN = R3
Validity
    Not Before: Dec 27 08:21:38 2020 GMT
    Not After : Mar 27 08:21:38 2021 GMT
Subject: CN = baz.foobar.org
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)

        Modulus:
            [...]
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
    X509v3 Basic Constraints: critical
        CA:FALSE
    X509v3 Subject Key Identifier:
        [...]
    X509v3 Authority Key Identifier:
        keyid:C0:CC:03:46:B9:58:20:CC:5C:72:70:F3:E1:2E:CB:20:B6:F5:
Authority Information Access:
    OCSP - URI:http://ocsp.stg-int-x1.letsencrypt.org
    CA Issuers - URI:http://cert.stg-int-x1.letsencrypt.org/
X509v3 Subject Alternative Name:
    DNS:hello.baz.foobar.org.crt, DNS:world.foobar.org.crt, DNS:
X509v3 Certificate Policies:
    Policy: 2.23.140.1.2.1
    Policy: 1.3.6.1.4.1.44947.1.1.1
    CPS: http://cps.letsencrypt.org
CT Precertificate SCTs:
    Signed Certificate Timestamp:
        Version    : v1 (0x0)
        Log ID     : [...]
        Timestamp  : Jan  2 09:23:20.310 2021 GMT
        Extensions: none
        Signature  : ecdsa-with-SHA256
    Signed Certificate Timestamp:
        Version    : v1 (0x0)
        Log ID     : [...]
        Timestamp  : Jan  2 09:23:20.320 2021 GMT
        Extensions: none
        Signature  : ecdsa-with-SHA256
                    [...]

```

Signature Algorithm: sha256WithRSAEncryption
[...]

Support

Bugs, questions, remarks, patches, requests for enhancements, etc. are to be sent through the [project interface](#), or directly at the email address mentioned at the beginning of this document.

Please React!

If you have information more detailed or more recent than those presented in this document, if you noticed errors, neglects or points insufficiently discussed, drop us a line! (for that, follow the [Support](#) guidelines).

Ending Word

Have fun with LEEC!

LEEC