

# SSL certificates

[[ssl](#), [certificates](#), [letsencrypt](#)]

[letsencrypt certification authority](#) is free, automated and open.

## acme.sh integration for letsencrypt

On host that has apache/nginx install acme.sh

```
wget -O - https://get.acme.sh | sh
. ~/.bashrc
# now /root/.acme.sh/acme.sh.env is available with bash alias
```

## certificate generation

with nginx enable this server on port 80 for initial challenge

[site.conf](#)

```
server {
    listen 80;
    server_name "mail.csgalileo.org";

    # create this folder empty
    location /.well-known/acme-challenge {
        root /var/www;
    }
    allow all;
}

location / {
    return 301 https://$server_name$request_uri;
}
}
```

```
# /var/www is documentroot of mail.csgalileo.org
acme.sh --issue -w /var/www -d mail.csgalileo.org --keylength ec-256
```

results in **/root/.acme.sh/mail.csgalileo.org\_ecc/**

```
[Fri Oct 14 08:05:13 CEST 2016] Creating account key
[Fri Oct 14 08:05:15 CEST 2016] Registering account
[Fri Oct 14 08:05:18 CEST 2016] Registered
[Fri Oct 14 08:05:20 CEST 2016] Update success.
[Fri Oct 14 08:05:20 CEST 2016] Creating domain key
```

```
[Fri Oct 14 08:05:20 CEST 2016] Single domain='mail.csgalileo.org'
[Fri Oct 14 08:05:20 CEST 2016] Verify each domain
[Fri Oct 14 08:05:20 CEST 2016] Getting webroot for
domain='mail.csgalileo.org'
[Fri Oct 14 08:05:20 CEST 2016] _w='/var/www'
[Fri Oct 14 08:05:20 CEST 2016] Getting new-authz for
domain='mail.csgalileo.org'
[Fri Oct 14 08:05:23 CEST 2016] Verifying:mail.csgalileo.org
[Fri Oct 14 08:05:31 CEST 2016] Success
[Fri Oct 14 08:05:31 CEST 2016] Verify finished, start to sign.
[Fri Oct 14 08:05:34 CEST 2016] Cert success.
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
[Fri Oct 14 08:05:34 CEST 2016] Your cert is in
/root/.acme.sh/mail.csgalileo.org_ecc/mail.csgalileo.org.cer
[Fri Oct 14 08:05:34 CEST 2016] Your cert key is in
/root/.acme.sh/mail.csgalileo.org_ecc/mail.csgalileo.org.key
[Fri Oct 14 08:05:34 CEST 2016] The intermediate CA cert is in
/root/.acme.sh/mail.csgalileo.org_ecc/ca.cer
[Fri Oct 14 08:05:34 CEST 2016] And the full chain certs is there:
/root/.acme.sh/mail.csgalileo.org_ecc/fullchain.cer
```

## certificate integration for apache

```
HOST=mail.csgalileo.org
acme.sh --installcert -d $HOST \
--certpath /etc/ssl/certs/${HOST}.cer \
--keypath /etc/ssl/private/${HOST}.key \
--capath /etc/ssl/certs/ca.cer \
--fullchainpath /etc/apache2/fullchain.cer \
--ecc \
--reloadcmd "service apache2 reload"
```

### apache.conf

```
SSLengine on
SSLCertificateFile /etc/ssl/certs/mail.csgalileo.org.cer
SSLCertificateKeyFile /etc/ssl/private/mail.csgalileo.org.key
SSLCertificateChainFile /etc/apache2/fullchain.cer
SSLCACertificateFile /etc/ssl/certs/ca.cer
```

## certificate integration for nginx

### site.conf

```
server {
    listen 443 ssl;
    server_name "scipio.csgalileo.org";

    # ...

    ssl_certificate /etc/ssl/certs/scipio.csgalileo.org.cer;
    ssl_certificate_key /etc/ssl/private/scipio.csgalileo.org.key;
}
```

```
HOST=mail.csgalileo.org
acme.sh --installcert -d $HOST \
--certpath /etc/ssl/certs/${HOST}.cer \
--keypath /etc/ssl/private/${HOST}.key \
--capath /etc/ssl/certs/ca.cer \
--fullchainpath /etc/ssl/cert/fullchain.cer \
--ecc \
--reloadcmd "service nginx reload"
```

## renew automatic every 60 days

in cron there is already

```
04 0 * * * "/root/.acme.sh"/acme.sh --cron --home "/root/.acme.sh" >
/dev/null
```

## renew manual

```
acme.sh --renew -d mail.csgalileo.org --force --ecc
```

From:  
<https://wiki.csgalileo.org/> - Galileo Labs

Permanent link:  
<https://wiki.csgalileo.org/tips/ssl?rev=1478804497>

Last update: 2016/11/10 20:01

