



APACHECON
ASIA 2021

ACME and mod_md

TLS made easy

Giovanni Bechis

Apache Httpd PMC

SSL, TLS and HTTPS

- SSL is short for Secure Sockets Layer.
It was released in 1995, it has been deprecated in 2015 in favor of TLS.
- TLS is short for Transport Layer Security and can be seen as the successor of SSL.
- HTTPS is short for Hypertext Transfer Protocol Secure, It can also be called “HTTP over TLS” or “HTTP over SSL”.

HTTPS certificates

- DV - Domain Validated Certificates
- OV - Organization Validated Certificates
- EV - Extended Validated Certificates



HTTPS certificates

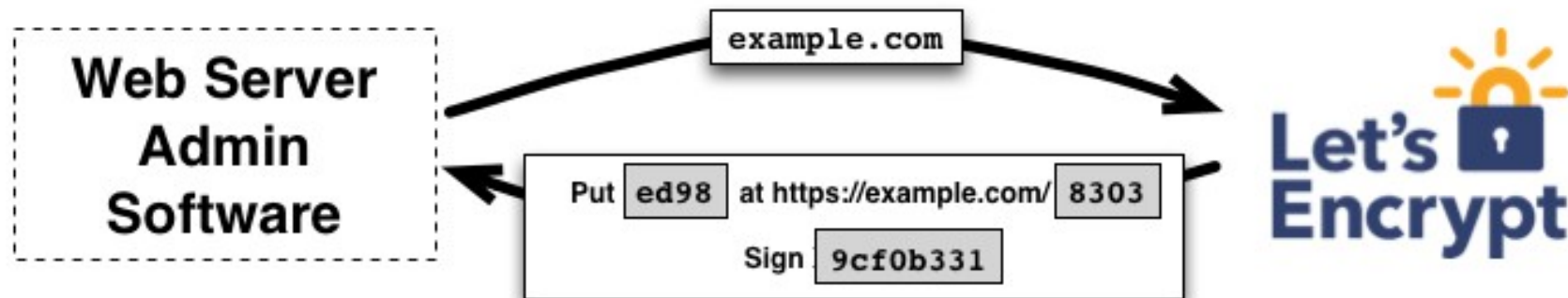
- Choose a Certificate Authority
- Select the certificate you need
- Purchase the certificate
- Generate and submit a CSR (Certificate Signing Request) to the CA
- Download the SSL certificate from the CA website and install it
- Remember to renew the cert

ACME Protocol



ACME is a communications protocol for automating interactions between certificate authorities and their users' web servers.

ACME Protocol



Let's Encrypt



Let's Encrypt is a non-profit certificate authority run by Internet Security Research Group that provides X.509 certificates for TLS encryption at no charge.

It uses ACME protocol to deploy certificates for free and it's used by more than 265 million web sites.

ACME clients

- Certbot
- acme.sh
- OpenBSD acme-client(1)
- win-acme
- Apache httpd(8) mod_md

mod_md features

- Certificate request using ACME protocol
- Automatic certificate renewal
- Wildcard certificate support
- Certificate status monitoring
- Notifications when certificate is next to expire
- OCSP stapling support

mod_md configuration

MDomain *domain.tld*

MDCertificateAgreement *accepted*

<VirtualHost *:443>

ServerName *domain.tld*

DocumentRoot */var/www/domain.tld*

SSLEngine *on*

</VirtualHost>

mod_md configuration

```
$ ls /var/www/md
```

accounts

challenges

httpd.json

ocsp

tmp

archive

domains

md_store.json

staging

mod_md wildcard certificates



APACHECON
ASIA 2021



`https://*.lets-encrypt`

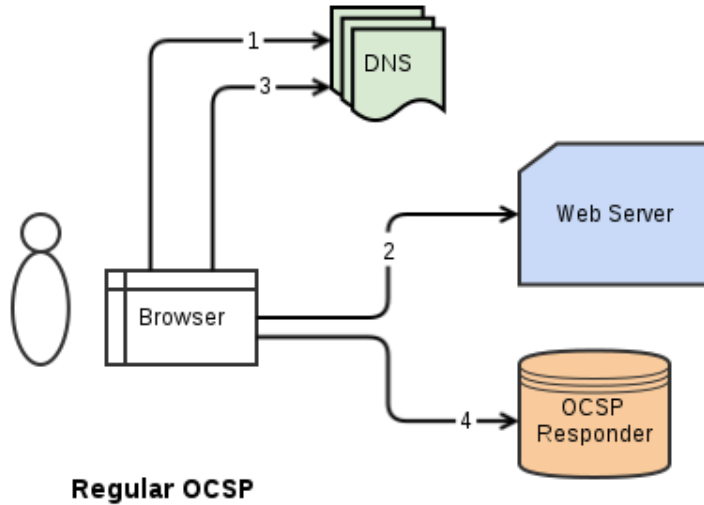
To deploy wildcard certificates, ACME protocol asks you to create a TXT record in dns.

`MDChallengeDns01 /usr/bin/acme-setup-dns`

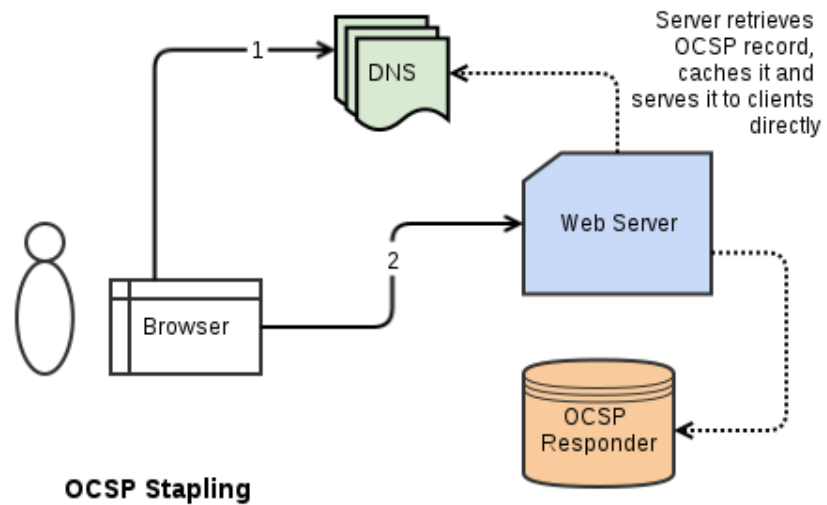
mod_md features

- MDRequireHttps *Off|Temporary|Permanent*
- MDRenewWindow *33%*
- MDWarnWindow *10%*
- MDPrivateKeys *RSA 2048*
- MDContactEmail *email@domain.tld*
- MDStapleOthers *On|Off*

OCSP Stapling



MDStapling *off*



MDStapling *on*

mod_md monitoring



```
$ curl https://dom.tld/.httpd/certificate-status
{
  "valid": {
    "from": "Sun, 16 May 2021 14:47:06 GMT",
    "until": "Sat, 14 Aug 2021 14:47:06 GMT"
  },
  ...
```

mod_md monitoring

```
{  
  "when": "Wed, 19 Jun 2019 14:45:58 GMT",  
  "type": "progress", "detail": "Retrieving certificate chain for test-901-  
003-1560955549.org"  
}, {  
  "when": "Wed, 19 Jun 2019 14:45:58 GMT",  
  "type": "progress", "detail": "Waiting for finalized order to become  
valid"  
}
```

mod_md monitoring



MDNotifyCmd */usr/local/bin/md-notify*

MDMessageCmd */usr/local/bin/md-message*

THANK YOU

QUESTIONS?



gbechis@apache.org



[giovannibechis](#)



[@_gbechis](#)