Servidor web/dades

Actualització d'HTTP a HTTPS amb certificats RedIris - Setembre de 2022

Let's Encrypt no és una opció possible per aconseguir un certificat per `sermn.uab.cat` perquè requereix poder demostrar que el sol·licitant controla el domini del servidor, en aquest cas “uab.cat”, i aquest domini no està sota el meu control.

Per altra banda, tampoc puc sol·licitar un certificat per “sermnserver.sermn.net” perquè el domini “sermn.net” és local i no es pot verificar la seva existència a través d'un servidor de noms.

Així doncs,

la única solució sembla ser tramitar una sol·licitud de certificat a través del formulari de sol·licitud de certificats SSL de servidor del servei SCS de RedIris disponible a Tiquets UAB / DTIC - Suport / Certificat de Servidor (DigiCert)

En aquesta pàgina se'ns proposa fer servir l'eina OpenSSL CSR Wizard de Digicert

> Our OpenSSL CSR Wizard is the fastest way to create your CSR for Apache (or any platform) using OpenSSL. Fill in the details, click Generate, then paste your customized OpenSSL CSR command in to your terminal.

per generar una sol·licitud per signatura de certificat (CSR) per “sermn.uab.cat”. El problema és que només permet generar el CSR per “sermn.uab.cat” quan aquest servidor té altres alies com “sermn.uab.es”, “rmn3.uab.cat” i “rmn3.uab.es”.

Així doncs, hauré de generar el fitxer CSR a mà amb el programa `openssl` o amb una eina alternativa, per exemple, amb CertificateTools.com CSR Generator. Aquesta eina permet:

> - Includes support for multiple domain names (comma separated)
> - First domain name listed is used as the Common Name
> - All domain names entered are added as Subject Alternative Names
> - Choose from a 2048 bit RSA Key or 256 bit ECC Key
> - SHA-256 is used as the signature hash
> - Copy/Paste or download CSR and private key
> - CSR and key are generated using best practices and industry standards to avoid browser errors
> - The OpenSSL commands are shown and can be executed securely on a local system
> - Additional customizations and more powerful features are available using the Advanced x509 Generator

> *https://certificatetools.com/csr-generator*

Generar un fitxer CSR i clau amb OpenSSL

- The Most Common OpenSSL Commands - SSLShoper.
- Frequently used OpenSSL Commands - Xolphin.com
- Verifying the validity of an SSL certificate - Acquia.
- OpenSSL - useful commands - KINAMO.

Generar un fitxer CSR i clau amb CSR Generator de CertificateTools.com

Provo a generar un CSR amb la següent informació:

- **Domain name:** sermn.uab.cat, sermn.uab.es, rmn3.uab.cat, rmn3.uab.es
- **Country:** ES
- **State:** Catalunya
- **Locality:** Bellaterra, Cerdanyola del Valles
- **Organization:** Universitat Autonoma de Barcelona

que equival a aquesta configuració:

```
[ req ]
default_md = sha256
prompt = no
req_extensions = req_ext
distinguished_name = req_distinguished_name
[ req_distinguished_name ]
commonName = sermn.uab.cat
countryName = ES
stateOrProvinceName = Catalunya
localityName = Bellaterra, Cerdanyola del Valles
organizationName = Universitat Autonoma de Barcelona
[ req_ext ]
keyUsage=critical,digitalSignature,keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName = @alt_names
[ alt_names ]
DNS.0 = sermn.uab.cat
DNS.1 = sermn.uab.es
DNS.2 = rmn3.uab.cat
DNS.3 = rmn3.uab.es
```

Un cop generats els fitxers `cert.csr` amb el CSR i `priv.key` amb la clau, els comprovo amb `openssl`.

Fitxer CSR generat

```
$ openssl req -text -noout -verify -in cert.csr
verify OK
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = sermn.uab.cat, C = ES, ST = Catalunya, L =
"Bellaterra, Cerdanyola del Valles", O = Universitat Autonoma de Barcelona
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:e5:11:2a:94:ca:dd:ec:57:6d:c3:cb:39:f3:83:
                    7d:7b:3a:d8:f4:2b:b9:d2:48:43:61:58:2d:8c:72:
                    7f:aa:f0:90:8f:88:6d:ef:d4:d3:44:79:42:d8:9f:
                    a2:91:ff:75:25:27:68:c3:a5:09:c0:eb:cc:ce:7f:
                    cf:42:a0:73:16:f0:26:f0:53:f3:2c:92:8b:d1:12:
                    6c:9d:42:a4:e2:69:6d:66:c9:9c:96:26:fc:c1:e4:
                    f0:29:6f:7c:f0:ac:9e:8c:24:bb:66:a7:f4:0a:12:
                    db:69:51:db:49:38:52:9b:de:88:14:f7:80:b9:91:
                    3f:cd:0e:69:d3:b3:21:95:7b:46:51:9f:a1:74:49:
                    18:b0:70:e7:91:e0:05:ec:a8:c0:56:59:d2:58:1d:
                    05:55:d8:76:2a:6f:ca:02:23:3e:04:ea:54:77:a9:
                    e3:1e:26:af:53:66:40:f2:ff:e4:c4:fa:da:79:12:
                    bf:00:e0:0f:6f:bd:e8:88:83:db:84:a3:6e:16:fc:
                    3f:e1:be:6a:76:07:e5:fe:9c:b5:d6:6c:aa:85:b3:
                    3d:4d:14:a2:1e:9e:ea:88:b5:33:4a:75:5f:3f:8c:
                    a6:35:24:f9:60:d6:b8:d0:1a:2b:e0:02:5a:63:66:
                    59:49:a5:13:31:f2:3b:36:f3:43:65:a4:4a:ce:98:
                    09:07
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                DNS:sermn.uab.cat, DNS:sermn.uab.es, DNS:rmn3.uab.cat,
DNS:rmn3.uab.es
    Signature Algorithm: sha256WithRSAEncryption
         4d:ee:0d:d2:50:b5:cc:91:f4:fa:90:d7:e4:6d:01:6b:93:12:
         09:c8:ce:e8:e5:f4:ab:69:d0:c7:cc:a1:b2:ea:2c:c4:39:fa:
         d2:7f:49:1a:cf:2b:c3:47:c8:d1:4c:40:65:83:d1:1a:6b:e7:
         d5:5b:9a:83:24:01:e6:c8:c8:00:9f:4f:6e:16:c5:e3:bc:99:
         b2:b2:5d:84:53:30:1d:e2:35:95:1b:db:b1:8e:5a:81:ac:98:
         81:74:e2:b1:89:88:0a:cf:bf:1b:ba:f0:4e:1c:5e:f1:67:ae:
         ee:b2:2e:50:f1:98:7c:d7:e0:4d:95:65:ed:43:39:4f:6f:16:
         b7:2d:a1:e3:58:1c:98:eb:8f:ee:bd:1d:42:fb:42:90:88:32:
```

```
        5c:e8:f0:f1:b9:72:7c:ed:e8:80:55:6f:5f:81:f4:1a:9a:85:
        80:2d:2c:59:77:b7:28:19:a3:ce:04:82:3d:2a:04:f8:d5:51:
        11:33:19:67:10:e7:23:c4:cc:3a:3d:b1:de:51:bc:78:69:37:
        8a:80:06:b4:25:ca:20:16:d0:e2:76:3d:c8:b7:7c:3d:2d:b9:
        b8:89:ae:85:dc:07:90:86:d8:ea:28:35:c3:df:fb:ba:3c:e1:
        1c:43:f9:e6:6a:2e:8b:32:c3:95:04:22:0b:de:b3:94:a4:14:
        1e:4d:85:63
```

Fitxer clau generat

```
$ openssl rsa -in priv.key -check
RSA key ok
writing RSA key
-----BEGIN RSA PRIVATE KEY-----

[removed]

-----END RSA PRIVATE KEY-----
```

Sol·licitar un certificat a través del SI de la UAB

Faig servir el servei “Certificats servidors UAB” de la DTIC-UAB

> Sol·licitud de certificats per a servidors del domini UAB (nom_servidor.uab.cat i nom_servidor.uab.es). Aquests certificats els gestiona la xarxa acadèmica de l'estat RedIRIS.
>
> El Servei d'Informàtica fa d'intermediari en les sol·licituds.
>
> Actualment el servei el proporciona l'empresa Sectigo.
>
> *https://www.uab.cat/web/serveis-dtic/certificats-servidors-uab-1345826750494.html?detid=1345838627704*

per sol·licitar un certificat a partir del CSR generat anteriorment amb les següents opcions:

- **Responsable diferent del sol·licitant:** No
- **Durada del certificat (en anys):** 2
- **Tipus de Servidor:** Apache/ModSSL

i envio la sol·licitud.

Referències

- openssl csr multiple common names - Cercar amb Google.

- How To Generate A CSR For A Multi-Domain SSL Certificate Using OpenSSL? - The Sec Master.
- Multi-Domain SSL Setup with "Subject Alternative Names".
- CertificateTools.com - Online X509 Certificate Generator.
- Should include server alias as alternative name in certificate signature request - Cercar amb Google.
- SAN Certificates: Subject Alternative Name – Multi-Domain (SAN).
- HOW TO: Create server certificate and include DNS alias | vStrong.info