H6 salataampa

Hommat aloitettu 29.9 klo 21:52 kotikoneella.

x) Lue ja tiivistä

- Lets Encrypt tekee HTTPS:n helpoksi ja automaattiseksi, ilman että tarvitsisi hakea itse manuaalisesti sertifikaatteja
- ACME client todistaa, että weppipalvelin hallitsee domainia
- Kun domain on validoitu, asiakas voi pyytää, uusia tai peruuttaa sertifikaatteja
- Sertifikaatti haetaan PKCS#10 CSR -pyynnöllä, allekirjoitetaan valtuutetulla avaimella, ja CA palauttaa sertifikaatin.
- Sertifikaatit voidaan myös peruuttaa, jolloin selain tai muut palvelut tietää, ettei serttiä pidä hyväksyä.
- SSL konfiguraatio vaatii minimissä LoadModule ssl_module, Listen 443, <VirtualHost*:443> jossa on SSLEngine on, serverillä on nimi, löytyy certifikaattitiedosto ja avaintiedosto
- OCSP Stapling kertoo selaimelle nopeasti, onko sertti peruutettu, ilman ylimääräistä CA-kyselyä

a) Hanki ja asenna palvelimelle ilmainen TLS-sertifikaatti

Asennettaan certbotti

```
rauli@debian-rauli:~$ sudo apt install certbot python3-certbot-apache
Installing:
  certbot  python3-certbot-apache

Installing dependencies:
  augeas-lenses  python3-acme     python3-configargparse  python3-openssl        python3-rfc3339
  libaugeas0     python3-augeas   python3-icu             python3-parsedatetime
  libicu76       python3-certbot  python3-josepy          python3-pytz

Suggested packages:
  augeas-doc          python3-certbot-nginx  python-acme-doc           python-openssl-doc
  python-certbot-doc  augeas-tools           python-certbot-apache-doc
```

```
rauli@debian-rauli:~$ sudo certbot --apache -d saresoja.page -d www.saresoja.page
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address or hit Enter to skip.
 (Enter 'c' to cancel):

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at:
https://letsencrypt.org/documents/LE-SA-v1.5-February-24-2025.pdf
You must agree in order to register with the ACME server. Do you agree?
```

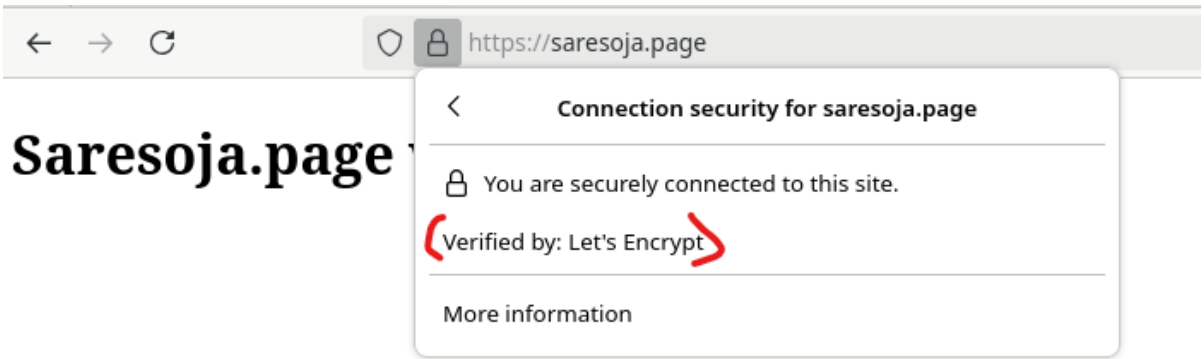
Ai niin, voisi laittaa sertifikaatit myös alidomaineille.

```
rauli@debian-rauli:~$ sudo certbot --apache -d saresoja.page -d www.saresoja.page -d testi.saresoja.page -d linuxkurssi.sa
resoja.page
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
You have an existing certificate that contains a portion of the domains you
requested (ref: /etc/letsencrypt/renewal/saresoja.page.conf)

It contains these names: saresoja.page, www.saresoja.page

You requested these names for the new certificate: saresoja.page,
www.saresoja.page, testi.saresoja.page, linuxkurssi.saresoja.page.

Do you want to expand and replace this existing certificate with the new
certificate?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(E)xpand/(C)ancel: e
```

Katsotaan sitten että löytyykö sieltä sitä sertifikaattia nyt

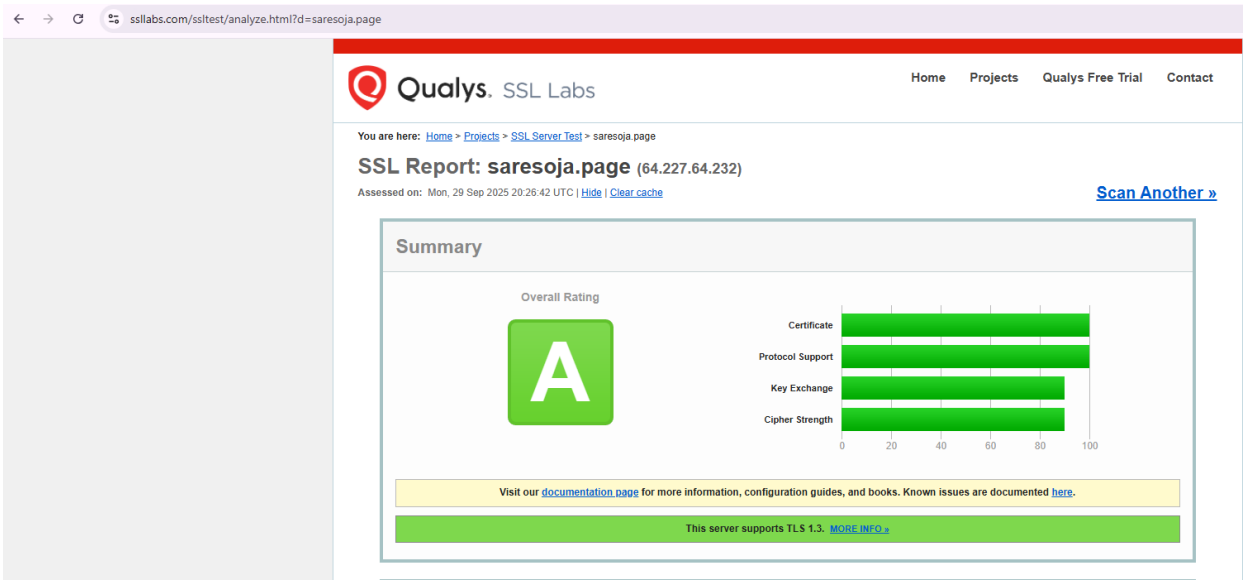
```
rauli@debian-rauli:~$ curl -v https://saresoja.page
* Host saresoja.page:443 was resolved.
* IPv6: (none)
* IPv4: 64.227.64.232
*   Trying 64.227.64.232:443...
* ALPN: curl offers h2,http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
*  CAfile: /etc/ssl/certs/ca-certificates.crt
*  CApath: /etc/ssl/certs
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384 / X25519MLKEM768 / id-ecPublicKey
* ALPN: server accepted http/1.1
* Server certificate:
*  subject: CN=saresoja.page
*  start date: Sep 29 19:32:15 2025 GMT
*  expire date: Dec 28 19:32:14 2025 GMT
*  subjectAltName: host "saresoja.page" matched cert's "saresoja.page"
*  issuer: C=US; O=Let's Encrypt; CN=E7
*  SSL certificate verify ok.
*   Certificate level 0: Public key type EC/prime256v1 (256/128 Bits/secBits), signed using ecdsa-with-SHA384
*   Certificate level 1: Public key type EC/secp384r1 (384/192 Bits/secBits), signed using sha256WithRSAEncryption
*   Certificate level 2: Public key type RSA (4096/152 Bits/secBits), signed using sha256WithRSAEncryption
* Connected to saresoja.page (64.227.64.232) port 443
* using HTTP/1.x
> GET / HTTP/1.1
> Host: saresoja.page
> User-Agent: curl/8.14.1
```

Hyvältä näyttää! Katsotaan vielä selaimen kautta.Testasin myös alidomainit ja nekin ovat kunnossa.



b) Testaa oma sivusi TLS jollain yleisellä laadunvarmistustyökalulla, esim. SSLLabs

Menen testaamaan sivuani SSLLabsissa.



Certificate #1: EC 256 bits (SHA384withECDSA)

Server Key and Certificate #1

Subject	saresoja.page Fingerprint SHA256: 6f8295fd0996d18577a1b78e17eb46a12c07f7bf3c2019e63321202d642287f9 Pin SHA256: xl8zkPaeCImE+PrMYjzV90C2GtMZbe+BNdke5sFXGaQ=
Common names	saresoja.page
Alternative names	saresoja.page www.saresoja.page
Serial Number	056f87333224a8333e2d416bb1461f2e24a5
Valid from	Mon, 29 Sep 2025 19:20:48 UTC
Valid until	Sun, 28 Dec 2025 19:20:47 UTC (expires in 2 months and 28 days)
Key	EC 256 bits
Weak key (Debian)	No
Issuer	E7 AIA: http://e7.i.lencr.org/
Signature algorithm	SHA384withECDSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL CRL: http://e7.c.lencr.org/38.crl
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Ajoin vielä testin alidomaineilla varmuuden vuoksi ja samaa tulosta näytti.

Valmista tuli klo 23:20

Lähteet

Let’s Encrypt. 2.8.2025. How it works. Luettavissa: https://letsencrypt.org/how-it-works/ Luettu 29.9.2025

Apache Software Foundation. SSL/TLS Strong Encryption: How-To. Luettavissa: https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html#configexample Luettu 29.9.2025.