Kurvid

Elliptilistel kurvidel põhineva krüpto kasutamise lubamine nõuab rakenduskihis teatavaid modifikatsioone.

Alljärgnevalt näited enamlevinud rakenduskihtidel

Riistvaralised koormusjaoturid

F5

https://f5.com/Portals/1/Premium/Architectures/RA-SSL-Everywhere-deployment-guide.pdf

```
ECDHE:DEFAULT:!SSLv3:!DHE:RSA+HIGH:!3DES
```

Tulemusena

- ssllab testis peaks saavutama A
- Chrome brauser peaks ütlema 'The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with P-256 (a strong key exchange), and AES_128_GCM (a strong cipher).'

Apache

https://www.digicert.com/ssl-support/ssl-enabling-perfect-forward-secrecy.htm

```
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite "EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384
EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH
EDH+aRSA RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS"
SSLHonorCipherOrder on
```

Võib ka siin lasta "modern" või "intermediate" profiiliga apache confi lasta koostada: https://mozilla.github.io/server-side-tls/ssl-config-generator/

Nginx

Kasutatud on https://mozilla.github.io/server-side-tls/ssl-config-generator/ valides

- NginX v. 1.10.3
- OpenSSL v. 1.0.2g
- Intermediate

Esmalt genereerida dhparam.pem, nt

```
openssl dhparam -out dhparam.pem 4096
```

ja kasutada seadistusfailis muu hulgas nt

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_ciphers
'ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES
128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:E
CDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SH
A384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-
SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384
:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA
-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-
SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-G
CM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!
DSS';

ssl_prefer_server_ciphers on;
ssl_dhparam /etc/ssl/localcerts/dhparam.pem;
```

Tulemusena

- ssllab testis peaks saavutama A
- Chrome brauser peaks ütlema 'The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with P-256 (a strong key exchange), and AES_128_GCM (a strong cipher).'