

No need to use `-engine cryptodev` in config as OpenSSL version 1.0.0 and up will use it automatically when available.

```
openssl speed aes-128-cbc
openssl speed -evp aes-128-cbc

openssl speed -evp aes-256-cbc
# With NI disabled
OPENSSL_ia32cap=0 openssl speed -evp aes-256-cbc

ls -l /usr/lib/engines-1.1/
total 68
-rwxr-xr-x  1 root    root      22768 Dec 26 13:56 afalg.so
-rwxr-xr-x  1 root    root      13856 Dec 26 13:56 capi.so
-rwxr-xr-x  1 root    root      26512 Dec 26 13:56 padlock.so
```

AF_ALG plugin for OpenSSL 7 takes advantage of the new AF_ALG interface present in kernels since 2.6.38.

```
openssl speed -evp aes-128-cbc -engine afalg
openssl speed -evp aes-128-cbc
```

From:

<https://niziak.spox.org/wiki/> - niziak.spox.org

Permanent link:

<https://niziak.spox.org/wiki/ssl:openssl:performance>

Last update: **2022/02/17 15:30**

