pcsc

```
dpavlin@x1:~$ sudo apt install pcscd pcsc-tools

dpavlin@x1:~$ wget https://www.eid.hr/sites/default/files/eidmiddleware_v3.2.0_amd64.deb

dpavlin@x1:~$ sudo dpkg -i eidmiddleware_v3.2.0_amd64.deb

dpavlin@x1:~$ /usr/lib/akd/eidmiddleware/Client
```

eid

Ove upute su bazirane na emardovom postu.

Evo za potpisivanje sa osobnim preko linuxa.
Skoro sve sam dobio osim tog secure pin readeara
trebao bi biti enablean je sa opcijom
"provider-eidosobna-allow-protected-auth"
ali meni to ne radi.

Probajte ako neko moÅ¾e to joÅ¡ dobit onda bismo
postali idealni eGradjanininini

aktiviraj karticu pomoÄ u pina na sigurnoj omotnici
instaliraj middleware 3.2.0
https://www.eid.hr/hr/eoi/clanak/programski-paket-eid-middleware

```
$ /usr/lib/akd/eidmiddleware/Client

postavi konfiguraciju za gpgsm i externi pkcs11 driver

$ mkdir .gnupg

$ cat ~/.gnupg/gpg-agent.conf
scdaemon-program /usr/bin/gnupg-pkcs11-scd

$ cat ~/.gnupg/gnupg-pkcs11-scd.conf
# pin cache period in seconds
pin-cache 5
providers eidosobna
provider-eidosobna-library /usr/lib/akd/eidmiddleware/pkcs11/libEidPkcs11.so
provider-eidosobna-allow-protected-auth

check:
$ gpg --card-status
should list something about card
$ echo "SCD LEARN" | gpg-agent --server gpg-connect-agent
should show some key info

$ gpgsm --import < /usr/lib/akd/eidmiddleware/certificates/AKDCARoot.pem
gpgsm: total number processed: 1
gpgsm:               imported: 1
$ gpgsm --import < /usr/lib/akd/eidmiddleware/certificates/HRIDCA.pem
gpgsm: total number processed: 1
gpgsm:               imported: 1
$ gpgsm --learn-card
```

```
# check: this should list keys learned from the card:
$ gpgsm --list-keys

Put the fingerprint of your root CA to "~/.gnupg/trustlist.txt".
After fingerprint append " S" (space S without quotes)
$ cat ~/.gnupg/trustlist.txt
# /CN=AKDCA Root/O=AKD d.o.o./C=HR/2.5.4.97=VATHR-99993087891
99:99:A6:C0:7A:1B:20:89:9E:89:6C:A1:A3:AD:D9:65:34:39:94:58 S

# use default key ID for signing
$ cat ~/.gnupg/gpgsm.conf
# use specific key ID for signing (choose key ID from gpgsm --list-keys)
default-key 0x1234ABCD

# use default key ID for signing
$ gpgsm --detach-sign file.txt > file.txt.sgn

# use specific key ID for signing (choose key ID from gpgsm --list-keys)
$ gpgsm --detach-sign -u 0x1234ABCD file.txt > file.txt.sgn
... dialog to enter card PIN for the chosen key will appear ...

# verify the signature
$ gpgsm --verify file.txt.sgn file.txt

# kill agent after use (eventual pins cached)
$ gpgconf --kill gpg-agent
```

firefox

preferences > privacy & security > certificates > security devices > load

/usr/lib/akd/eidmiddleware/pkcs11/libEidPkcs11.so