GDigiDoc

Kasutajajuhend

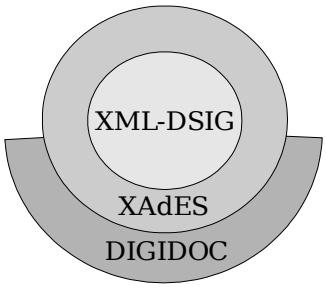
Veiko Sinivee

Sisukord

Ülevaade

GDigiDoc on graafiline kasutajaliides digitaalselt allkirjastatud dokumentide loomiseks, lugemiseks, allkirjade kontrolliks ja allkirjastamiseks. GDigiDoc tuleneb sõnadest “**G**NU **Digi**tally signed **Doc**uments”. GDigiDoc kasutab CDigiDoc teeki, mis on tuntud ka OpenXAdES teegi nime all. Nimetatud teegi algkoodi ja dokumentatsiooni leiab OpenXAdES veebilehelt. DigiDoc dokumendid on allkirjastatud XML failid, mis kasutavad XML-DSIG ja XAdES (ETSI – TS 101 903) digiallkirja standardeid. Digiallkirjastatud dokument võib sisaldada ka suvalisi binaarseid andmeid base64 kujul. Digidoc dokumendid on XML failid mis sisaldavad ühte või enamat andmefaili ja digiallkirja. Kõik allkirjad kinnitavad kõiki andmefaile. Seega ei saa enam lisada või eemaldada andmefaile dokumenti millel on vähemalt üks allkiri. Allkirjastatud andmed saab lisada digidoc faili algkujul juhul kui andmed olid puhasteksti või XML formaadis või siis Base64 kujul suvalisi muid andmeid. Võimalik on ka lisada viide andmetele mis ise jäävad eraldi faili.

CDigiDoc kasutab OpenXAdES faili formaati. OpenXAdES formaat on loodud rahvusvahelise standardi XAdES profileerimise teel, määrates ära Eestis kasutatavad elemendid ja lisades üldise XML konteineri mitme andmekogumi ja mitme allkirja salvestamiseks.



CDigiDoc teek kasutab ainult RSA-SHA1 allkirju. Teegi põhiosa sisaldab funktsioone ka kiipkaardi kasutamiseks PKCS#11 ohjurprogrammi abil. Selle teegi laiendatud versioon on loodud Microsoft Windows COM komponendina - DigiDocLibCOM. Viimane kasutab kiipkaartidega suhtlemiseks Microsoft CSP API-t. Teegist on olemas ka programeerimiskeeles Java loodud versioon - JDigiDoc.

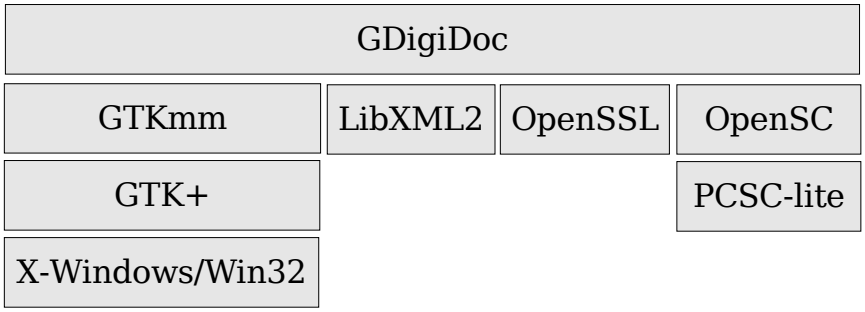
Rakenduse kasutamiseks on vajalik Eesti ID kaart (või mõni muu smartcard RSA võtmetega) ning kaardilugeja seade. Vajalikud on ka ohjurprogrammid kaardilugeja ja PKCS#11 ohjurprogramm kaardi jaoks. Ohjurprogrammide instaleerimisest on allpool juttu.

Eesti Digitaalallkirja seaduse kohaselt loetakse digitaalset allkirja võrdseks käsikirjalise allkirjaga. Pikaajalist tõestusväärtust omavada aga vaid

kehtivuskinnituseg allkirjad. Kehtivuskinnitus on allkirjastatud OCSP formaadis objekt mis kinnitab et allkirjastaja sertifikaat oli kehtiv allkirjastamise hetkel. Sertifitseerimiskeskuse kehtivuskinnituste server annab kehtivuse infot kõigi Eesti ID kaartidel olevate sertifikaatide kohta. Kui teil ei ole Eesti ID kaarti, siis saate siiski kasutada programmi digiallkirjastamiseks registreerides oma sertifikaadi siin: http://www.openxades.org/tryitout.html. Sellised kehtivuskinnitused väljastatakse demo-serveri poolt ja neil ei ole juriidilist jõudu aga sel kombel on võimalik tarkvara testida ilma ID kaardita. Muidugi saab tarkvara kasutada ka digidoc dokumentide lugemiseks ja allkirjade kontrolliks. Siis pole ka kaardilugejat vaja.

Installeerimine

GDigiDoc kasutab levinud GTK+/GNOME graafilist kasutajaliidest ja GTKmm teeki. Ta töötab ka KDE keskkonnas, aga selleks tuleb siiski installeerida GTK+ ja GTKmm teegid. GDigiDoc kasutab libdigidoc (CDigDoc Linuxi projekt) teeki digiallkirjastatud dokumentide käsitlemiseks. CDigiDoc teek aga kasutab omakorda OpenSSL krüptoteeki, LibXML2 XML parserit and OpenSC teeki kiipkaartide jaoks. OpenSC teek aga vajab kiipkaartidega suhtlemiseks PCSC-lite serverit.



GDigiDoc algkoodi leiab projekti lehelt SourceForge.net saidist: http://sourceforge.net/projects/gdigidoc.

GTKmm installeerimine

GTKmm installeerimisjuhendi leiab siit: http://www.gtkmm.org/download.shtml. On olemas ka valmis pakid Debiani ja RPM formaati kasutavate Linuxi versioonide nagu RedHat ja Mandrake jaoks. Mitteametlikke Fedora Core2 RPM-e leiab siit: http://www.poolshark.org/fc2.html. Installeerimispakette Win32 keskkonna jaoks saab siit: http://www.pcpm.ucl.ac.be/~gustin/win32_ports. Muidugi on võimalik ka tõmmata terve GTKmm algkood ja ise transleerida ja instaleerimida aga see võtab palju rohkem aega.

PCSC-lite installeerimine

Lihtsaim moodus pcsc-lite installeerimiseks on tõmmata pcsc-lite-1.2.0-1.i386.rpm

siit: http://www.sourceforge.net/projects/gdigidoc ja installida ta käsuga:

```
# rpm -i pcsc-lite-1.2.0-1.i386.rpm
```

See toimib vaid juhul kui teil on RPM paketiformaati kasutav Linuxi distributsioon nagu näiteks RedHat, Fedora Core, Mandrake või Suse. Testitud ja kompileeritud on antud RPM pakettt Fedora Core 2 keskkonnas.

Algkoodist installeerimiseks tõmmake PCSC-lite versiooni 1.2 algkood siit: https://alioth.debian.org/project/showfiles.php?group_id=1225.

Installeerimine käib järgnevalt:

```
# ./configure
# make
# make install
```

Nii instaleeriti **pcscd** server kataloogi /usr/local/sbin ja tema teegid kataloogi /usr/local/lib. Teekide kataloog /usr/local/lib tuleb lisada konfiguratsioonifaili /etc/ld.so.conf ja käivitada siis programm **ldconfig**. Võimalik oleks installeerida ka standardsesse süsteemikataloogi kui kasutada käsku:

```
# ./configure –prefix=usr --sysconfdir=/etc
```

Selleks et PCSC-lite server alati automaatselt koos arvutiga startida tuleb luua vajalikud start-skriptid ja registreerida server /etc/rc.d/init.d -s. PCSC-lite server pakub kõigile kiipkaardilugejatele sarnast ühendust aga vajab ise iga lugeja jaoks sobivat ohjurprogrammi, mille ehk leiate siit: http://www.linuxnet.com/sourcedrivers.html. Sellest saidist leiab ka PCSC-lite pisut vanemad RPM paketid RedHat ja Mandrake jaoks. Siin on ka paljude kaardilugejate ohjurprogrammide algkood ja mõningal juhul ka valmis moodulid. Ohjurprogrammi moodul tuleb registreerida konfiguratsioonifailis /etc/reader.conf. Osad kaardilugejate tootjad on valmistanud ise ka vajaliku ohjurprogrammi Linux keskkonna jaoks ning seda saab tõmmata vasta afirma veebilehelt. Järgmistest saitidest leiab veel ohjurprogramme ja infot nende installeerimise kohta:

- http://www.konsultant.ee/mod.php?mod=userpage&menu=110101&page_id=17
- http://www.id.ee/pages.php/030211?foorum=3
- http://martin.paljak.pri.ee./esteid/

OpenSC installeerimine

Lihtsaim moodus opensc instaleerimiseks on tõmmata opensc-0.8.1-mp1-1.i386.rpm siit: http://www.sourceforge.net/projects/gdigidoc ja installida ta käsuga:

```
# rpm -i opensc-0.8.1.mp1-1.i386.rpm
```

PCSC-lite ja kaardilugeja ohjurprogramm võimaldavad suhelda kaardilugejaga ja saata andmeid kaardile ning saada vastuseid, kuid see on kõik. Igal kaardil on oma protsessor ja operatsioonisüsteem ning ta pakub programmidele erinevaid

teenuseid. Kiipkaarti ei saa lugeda nagu floppit vaid talle tuleb saata käsklusi sellise süntaksiga nagu tema operatsioonisüsteem nõuab. Selleks et saaks kirjutada programme mis ei ole sõltuvad ühest kindlast kaardist vaid töötaksid paljude eri kaartidega kasutatakse PKCS#11 standardit. Iga kaardi jaoks tehakse oma PKCS#11 ohjurprogramm mis selle standardi poolt ettenähtud käsud vastava kaardi operatsioonisüsteemi poolt ettenähtud süntaksisse tõlgib. Eesti ja Soome ID kaartide jaoks saab kasutada OpenSC (http://www.opensc.org) projektis loodud teeki. Martin Paljak ja Marie tegid antud teegile hulga täustusi Eesti ID kaardi toetamiseks ja selle versiooni saab siit: http://martin.paljak.pri.ee./esteid/. Samas kohas on ka pikemalt juttu OpenSC konfigureerimisest ja instaleerimisest. Lühidalt öeldes tõmmake opensc-0.8.1.mp1.tar.gz ja installige nii:

```
# ./configure --prefix=/usr --sysconfdir=/etc --with-pcsclite=/usr
# make
# make install
```

Selliselt instaleeritud teegi puhul salvestatkse teegi põhiosa /usr/lib kataloogi aga PKCS#11 ohjurprogramm /usr/lib/pkcs11 kataloogi. Nimetatud kataloog tuleks lisada konfiguratsioonifaili /etc/ld.so.conf ja käivitada ldconfig. Nüüd registreerime ohjurprogrammi – opensc-pkcs11.so - Netscape/Mozilla brauseris ja katsetame seda mingil veebilehel mis nõuab ID kaardiga autentimist. Näiteks https://sk.ee/cgi-bin/tervitus. ID kaardiga autentimist kasutavate veebisaitid loetelu leiab siit: http://www.id.ee/pages.php/030207,157. Martin Paljaku veebilehel on ka paar nuppu antud PKCS#11 ohjurprogrammi brauseris registreerimiseks ja uuesti eemaldamiseks. Nende abil ohjurprogrammi registreerimine on parem kui otse Mozilla menüüs registreerimine sest nii omistatakse ohjurprogrammile lipp mis määrab et Mozilla ei küsiks autentimisel korraga kõiki PIN koode vaid ainult seda mida vaja – PIN1 -e.

Libdigidoc installeerimine

Lihtsaim moodus libdigidoc instaleerimiseks on tõmmata libdigidoc-1.90.0-1.i386.rpm siit: http://www.sourceforge.net/projects/gdigidoc ja installida ta käsuga:

```
# rpm -i libdigidoc-1.90.0-1.i386.rpm
```

GDigiDoc kasutab libdigidoc teeki. Tõmmake uusim teegi versioon samast kust gdigidoc programm (e.g. http://www.sourceforge.net/projects/gdigidoc) ja installeerige ta järgnevate käskudega:

```
# ./configure --sysconfdir=/etc
# make
# make install
```

Teegiga kaasneb väike kommandorea programm – digidoc. Selle abil saab kah allkirjastada aga ta on rohkem mõeldud testimiseks ja kontrolliks kas teek on õieti installeeritud. Sellest on allpool rohkem kirjutatud.

GDigiDoc installeerimine

Lihtsaim moodus libdigidoc instaleerimiseks on tõmmata gdigidoc-0.0.7-

1.i386.rpm siit: http://www.sourceforge.net/projects/gdigidoc ja installida ta käsuga:

```
# rpm -i gdigidoc-0.0.7-1.i386.rpm
```

Algkoodist installeerimiseks tõmmake gdigidoc viimane versioon projekti lehelt SourceForge.net saidis (http://www.sourceforge.net/projects/gdigidoc) ja installeerige ta järgnevate käskudega:

```
# ./configure --sysconfdir=/etc
# make
# make install
```

Nüüd võiks programmi jaoks vajalku käivitaja GNOME paneelile teha. Ikoonina saaks kasutada näiteks programmiga kaasenavat id-logo.png pilti. GdigiDoc-i saaks ka GNOME-s .ddoc failide vaatlejana registreerida sest kui käivitada gdigidoc programm käsurealt ja kasutada ainsa parameetrina faili nime siis üritab ta sellenimelist dokumenti avada, allkirju kontrollida ja tulemusi kuvada. Selleks lisame GNOME keskkonnas näiteks application/digidoc nimelise maimi tüübi, määrame ta laiendiks .ddoc ja registreerime gdigidoc selle jaoks sobivaks vaatlejaks.

Libdigidoc konfigureerimine

Libdigdoc kasutab üldist/süsteemset konfiguratsioonifaili - /etc/digidoc.conf ja iga kasutaja isiklikku konfiguratsioonifaili ~/.digidoc.conf. Üldises konfiguratsioonifailis on järgmised kirjed:

```
# CA sertifikaadid Eesti ID kaardi jaoks - siin pole midagi vaja muuta.
CA_CERTS=4
CA_CERT_1=/usr/local/share/certs/JUUR-SK.PEM.cer
CA_CERT_1_CN=Juur-SK
CA_CERT_2=/usr/local/share/certs/ESTEID-SK.PEM.cer
CA_CERT_2_CN=ESTEID-SK
CA_CERT_3=/usr/local/share/certs/TEST-SK.PEM.cer
CA_CERT_3_CN=TEST-SK
CA_CERT_4=/usr/local/share/certs/KLASS3-SK.PEM.cer
CA_CERT_4_CN=KLASS3-SK
CA_CERT_PATH=/usr/local/share/certs

# Vaikimisi kasutatav uue dokumendi formaadi versioon
DIGIDOC_FORMAT=DIGIDOC-XML
DIGIDOC_VERSION=1.3

# Kasutatavad PKCS#11 ohjurprogrammid
DIGIDOC_DEFAULT_DRIVER=2
```

```
DIGIDOC_DRIVERS=2
DIGIDOC_DRIVER_1_NAME=EYP driver
DIGIDOC_DRIVER_1_DESC=Eesti Yhispanga loodud ID kaardi PKCS#11 ohjurprogramm
DIGIDOC_DRIVER_1_FILE=/usr/local/lib/esteid-pkcs11.so
DIGIDOC_DRIVER_2_NAME=OpenSC
DIGIDOC_DRIVER_2_DESC=OpenSC baasil loodud PKCS#11 ohjurprogramm
DIGIDOC_DRIVER_2_FILE=/usr/local/lib/pkcs11/opensc-pkcs11.so
# Vaikimisi kasutatav allkirja võtme slot - sobivalt seatud Eesti ID kaartide
jaoks!
DIGIDOC_SIGNATURE_SLOT=1


# Kehtivuskinnituste serveri sertifikaadid - sobivalt konfigureeritud Eesti ID ja
AID kaartide jaoks
DIGIDOC_OCSP_RESPONDER_CERTS=3
DIGIDOC_OCSP_RESPONDER_CERT_1=/usr/local/share/certs/ESTEID-SK OCSP
RESPONDER.PEM.cer
DIGIDOC_OCSP_RESPONDER_CERT_1_CN=ESTEID-SK OCSP RESPONDER
DIGIDOC_OCSP_RESPONDER_CERT_1_CA=ESTEID-SK
DIGIDOC_OCSP_RESPONDER_CERT_2=/usr/local/share/certs/TEST-SK OCSP RESPONDER.pem.cer
DIGIDOC_OCSP_RESPONDER_CERT_2_CN=TEST-SK OCSP RESPONDER
DIGIDOC_OCSP_RESPONDER_CERT_2_CA=TEST-SK
DIGIDOC_OCSP_RESPONDER_CERT_3=/usr/local/share/certs/KLASS3-SK OSCP
RESPONDER.pem.cer
DIGIDOC_OCSP_RESPONDER_CERT_3_CN=KLASS3-SK OCSP RESPONDER
DIGIDOC_OCSP_RESPONDER_CERT_3_CA=KLASS3-SK
# OCSP responder URL
DIGIDOC_OCSP_URL=http://ocsp.sk.ee


# HTTP vahendaja URL - muuda seda kuidas vaja !
DIGIDOC_PROXY_HOST=proxy.yourhost.com
DIGIDOC_PROXY_PORT=8080
```

Üldises konfiguratsioonifailis on kirjed mis on enamasti samad kõigi antud arvuti kasutajate jaoks. Kasutaja isiklikus konfiguratsioonifailis on antud kasutaja isiklikud muutuajte väärtused. Kui muutuja on väärtustatud mõlemas konfiguratsioonifailis, siis kasutatakse isiklikus konfiguratsioonifailis määratud väärtust.

```
# Kehtivuskinnituste serveri juurdepääsutõendi faili täielik nimi ja salasõna.
# Juurdepääsutõendi saab tellida siit: http://www.sk.ee/pages.php/02020504
# Muuda seda!!!
```

```
DIGIDOC_PKCS_FILE=<pkcs12-token-filename-and-full-path>

DIGIDOC_PKCS_PASSWD=<pksc12-tokens-password>

DIGIDOC_OCSP_URL=http://ocsp.sk.ee

# Allkirjastaja aadresss ja manifesti kasutamise reshiim: 0=küsi, 1=ei kasuta,
2=kasuta neid väärtusi ilma täiendavalt küsimata.

MANIFEST_MODE=0

# Vaikeväärtused allkirjastaja aadressi ja manifesti jaoks. Muuda kuidas vaja.

DIGIDOC_ROLE_MANIFEST=Nõus

DIGIDOC_ADR_COUNTRY=Eesti

DIGIDOC_ADR_STATE=Harjumaa

DIGIDOC_ADR_CITY=Tallinn

DIGIDOC_ADR_ZIP=12918

# Lipp - kasuta HTTP vahendajat või mitte

USE_PROXY=TRUE

# Lipp - allkirjasta OCSP päringud või mitte. Eraisikud peavad alati oma OCSP
päringud allkirjastama.

SIGN_OCSP=TRUE
```

Digidoc kasutamine

Libdigdoc teegiga kaasneb väike käsureaprogramm – digidoc – mille abil saab kasutada enamust teegi funktsioonidest. Selle abil saate lugeda faile OpenXAdES formaadis, neid allkirjastada ja allkirju kontrollida.

1. **Abiinfo kuvamine** – “digidoc -help” või “digidoc -?”
2. **Uue dokumendi loomine** – “digidoc -new [format] [version]”. Vaikeväärtused võetakse konfiguratsioonifailist. See käsk ei ole nõutud. Kui kasutate näiteks **-add** käsku andmekogumi lisamiseks ja digidoc dokumenti sessioonis ei ole siis luuakse see automaatselt.
3. **Andmefaili lisamine** – “digidoc -add <faili nimi> <maimi-tüüp> [<sisu-tüüp>] [<tähestik>]”. Vaikeväärtused võetakse konfiguratsioonifailist.
4. **Allkirjade kontrollimine** – “digidoc -verify”
5. **digidoc dokumendi lugemine** – “digidoc -in <faili nimi>”
6. **digidoc dokumendi kirjutamine** - “digidoc -out <faili nimi>”
7. **Allkirjastamine –** “digidoc -sign <pin> [<manifest>] [<linn> <maakond> <postiindeks> <riik>]”. Vaikeväärtused võetakse konfiguratsioonifailist.
8. **Andmefaili eraldi faili salvestamine** – “digidoc -extract <doc-id> <faili nimi> [<tähestik >] [<faili-nime-tähestik >]”.

Kirjeldatud käsklusi saab keerukamateks käskudeks kombineerida. Näiteks:

- Loeme digidoc dokumendi failist ja kontrollime allkirju:

```
# digidoc -in <filename> -verify
```

- Loome uue digidoc dokumendi 1.1 formaadis, lisame PDF faili, allkirjastame, kontrollime tulemust ja salvestame uude faili.

```
# digidoc -new DIGIDOC-XML 1.1 -add mydoc.pdf application/pdf -sign <pin> “Olen nõus” -out mydoc.ddoc -verify
```

- Loeme olemasoleva digidoc dokumendi failist, lisame oma allkirja, kontrollime tulemust ja salvestame uude faili.

```
# digidoc -in mydoc.ddoc -sign <pin> “I reject this proposal!” -out mydoc2.ddoc -verify
```

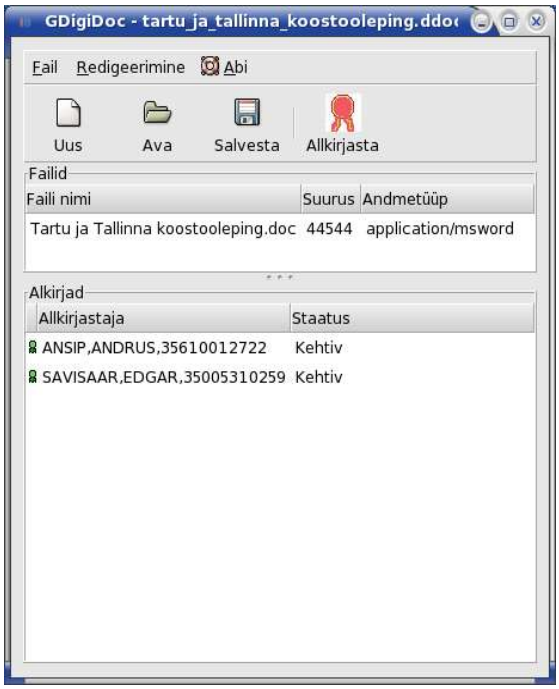
- Loeme olemasoleva digidoc dokumendi failist ja salvestame ühe andmefaili eraldi faili.

```
# digidoc -in mydoc.ddoc -extract D0 mydoc2.pdf
```

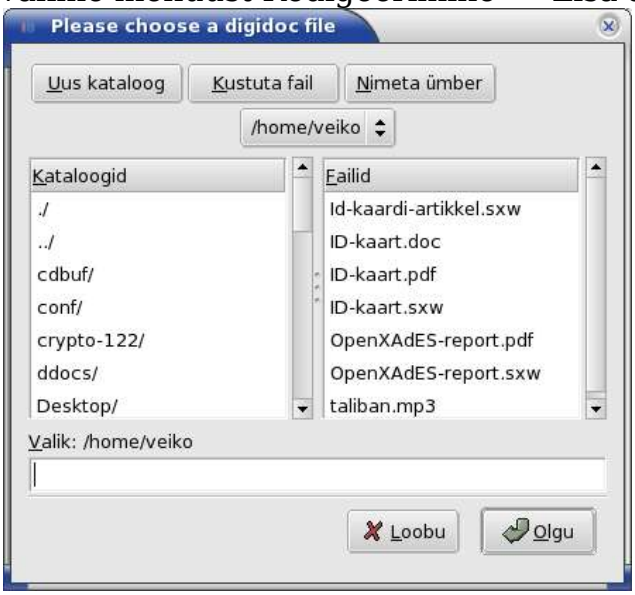
GDigiDoc kasutamine

Stardime GDigiDoc programmi tema käivitajale GNOME paneelis klõpsates. Programmi põhiaknal on kaks osa.

Ülemises loetelus kuvatakse digidoc dokumendi andmefaile ja alumises allkirju. Digidoc dokumendi lugemiseks valime menüüst Fail -> Ava ja avame sobiva dokumendi. Nüüd ilmub tiitlireale avatud dokumendi faili nimi ja loetelud täituvad andmefailide ning allkirjade infoga. Kehtivad allkirjad on märgitud rohelise ja kehtetud punase ikooniga.



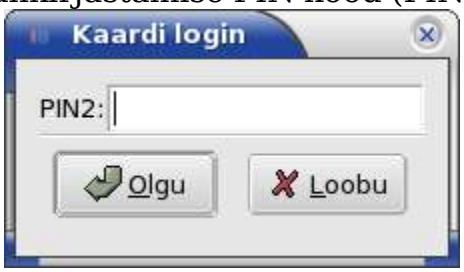
Uue dokumendi loomiseks valime menüüst Fail -> Uus. See käsk puhastab loetelud ja me saame asuda uuele dokumendile andmefaile ja allkirju lisama. Andmefail lisamiseks valime menüüst Redigeerimine -> Lisa andmefail.



Uue andmefaili info lisatakse ülemisse loetelusse. Andmefaili eemaldamiseks selekteerime vajaliku faili ülemises loetelus ja valime menüüst Redigeerimine -> Eemalda andmefail. Allkirjastatud dokumendile ei saa andmefaile lisada ega neid eemaldada. Enne tuleb kõik allkirjad eemaldada ja alles siis saab hakata andmefaile lisama või eemaldama. Andmefaili eraldi faili salvestamiseks selekteerime vajaliku faili ülemises loetelus ja valime menüüst Redigeerimine -> Kopeeri faili. Ilmuvas dialoogis valime andmefaili salvestamiseks sobiva kausta ja failinime. Nüüd saab seda faili mingi muu programmiga vaadelda.

Dokumendi allkirjastamiseks valime menüüst Redigeerimine -> Allkirjasta või klõpsame ikoonile kirjaga “Allkirjasta”. Vastavalt aadressi ja manifesti kasutamise resziimile võib ilmuda dialoog milles kuvatakse allkirjastaja aadressi ja manifesti vaikeväärtusi ja võimaldatakse neid uue allkirja jaoks kasutada ja muuta.

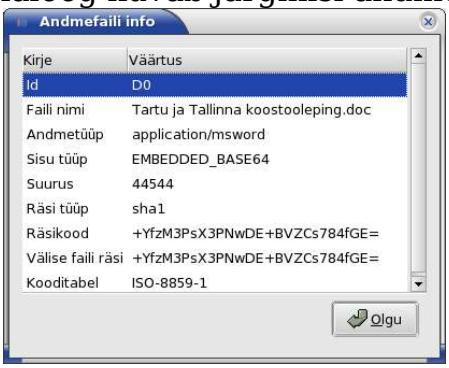
Järgnevalt tuleb sisestada allkirjastamise PIN kood (PIN2).



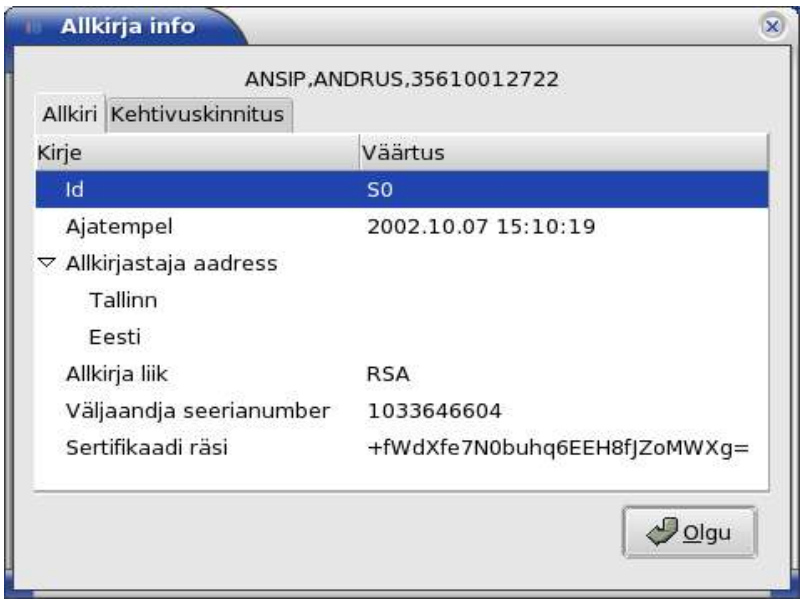
GDigiDoc allkirjastab nüüd dokumendi, hangib allkirjale kehtivuskinnituse ja lisab uue allkirja info alumisse loetelusse. Allkirja eemaldamiseks selekteerime vastava allkirja alumises loetelus ja valime menüüst Redgieerimine -> Eemalda allkiri.

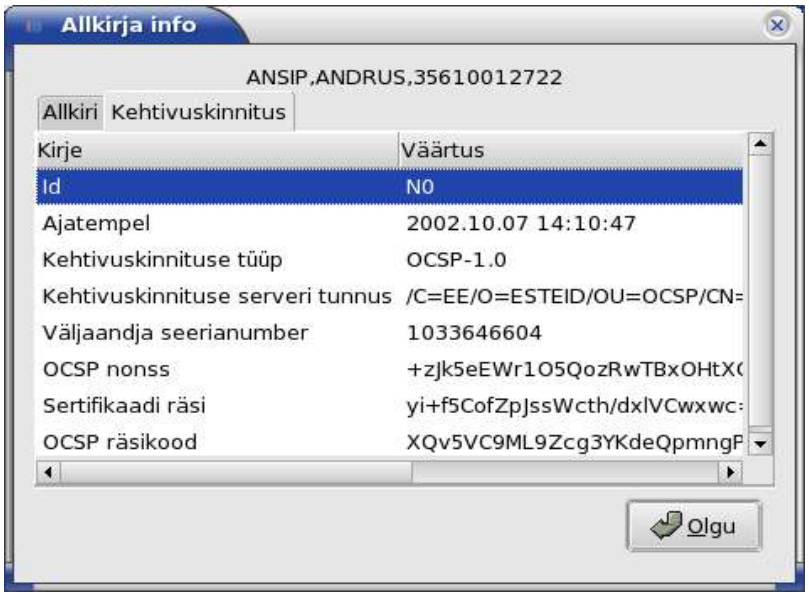
Mõlemas loetelus saab kasutada kontekstist sõltuvaid menüüsid mis avanevad hiire paremale nupule vajutades ja pakuvad menüükäskude kiirvalikuid. Sellisest menüüst saab näiteks avada antud andmefaili või allkirja detailandmeid kuvava dialoogi.

Andmefaili detailandmete dialoog kuvab järgmisi andmeid:

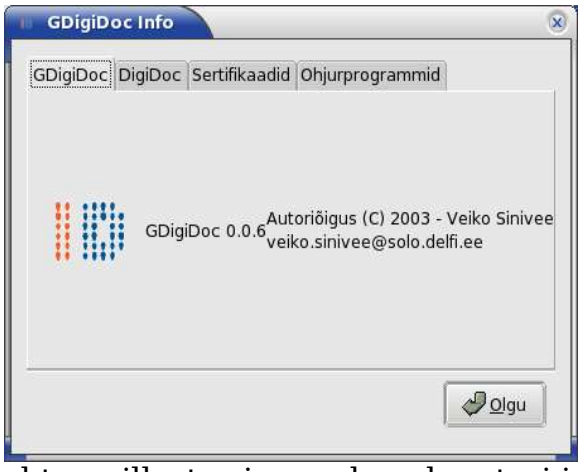


Allkirja detailandmete dialoogis on aga kaks lehte millest esimene kuvab allkirja andmeid ja teine kehtivuskinnituse andmeid.

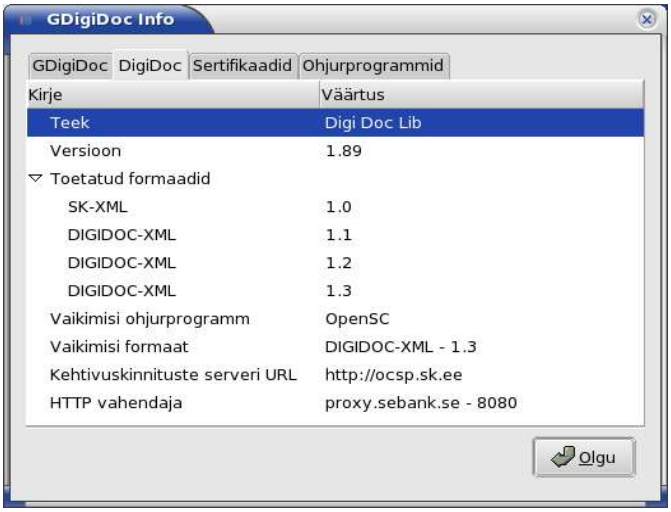




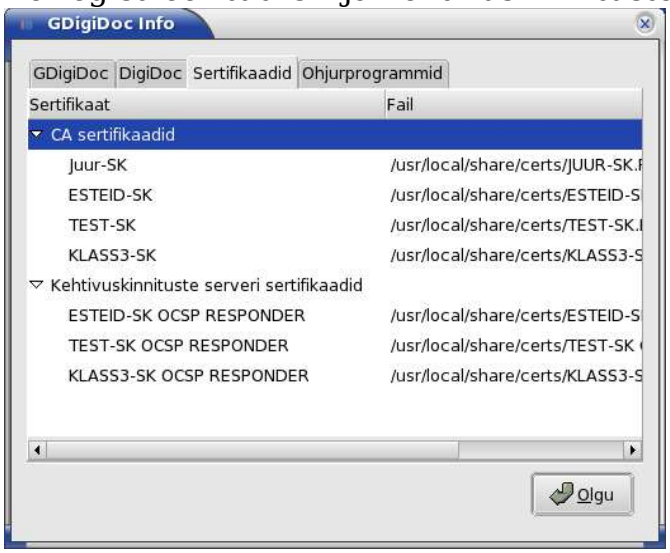
Menüüvalik Abi -> Info avab tegijaõigusi ja muid andmeid kuvava dialoogi.



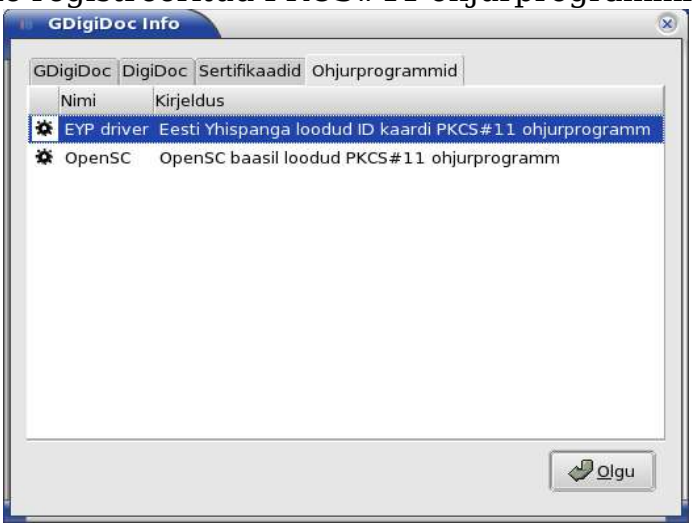
Sellel dialoogil on neli lehte, millest esimene kuvab autori infot. Teine leht kuvab Libdigdoc seadeid.



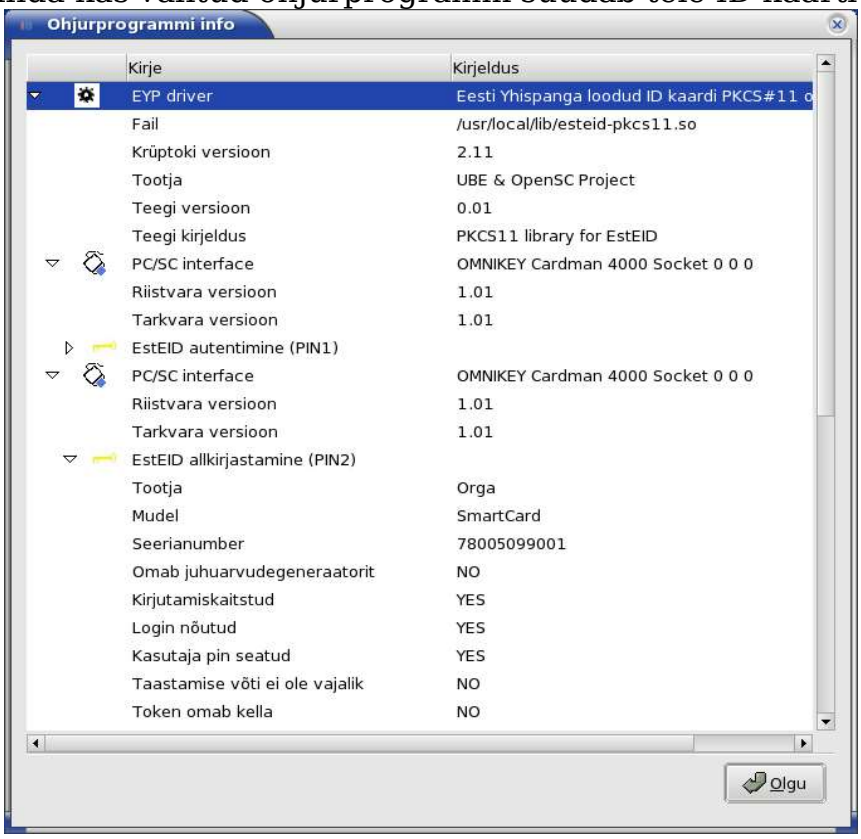
Kolmandal lehel näeme registreeritud CA ja kehtivuskinnituste serveri sertifikaate.



Viimasel lehel näeme registreeritud PKCS#11 ohjurprogrammide andmeid.



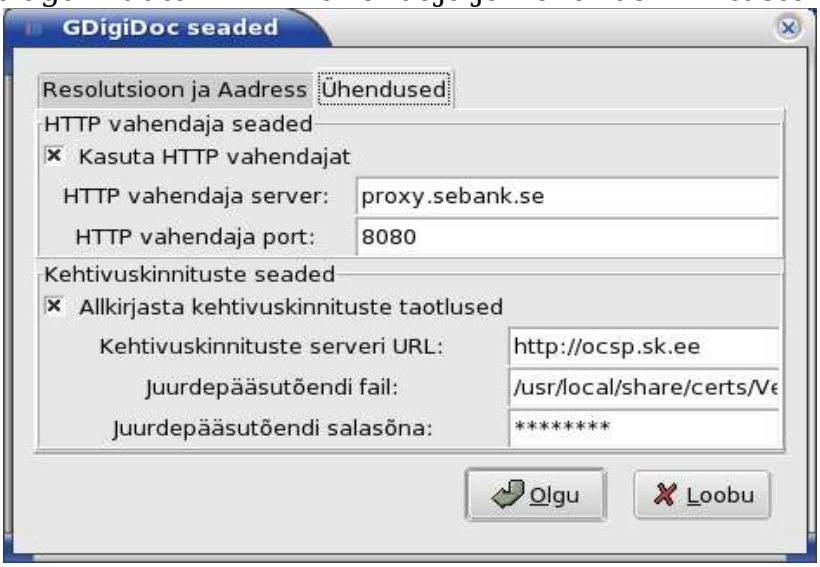
Siin on näha hetkel OpenSC teegi baasil valmistatud ohjurprogrammi ja Eesti Ühispanga tehtud ohjurprogrammi andmeid. Kui mõni ohjurprogramm välja valida ja hiire parema nupuga avanevast kontekstimenüüst “Driver Info” valida, avaneb dialoog, milles kuvatakse leitud kaardilugejate ja slottide andmeid. Nii saab näiteks kontrollida kas valitud ohjurprogramm suudab teie ID kaarti lugeda.



Siin kuvatud seadeid (sisuliselt kasutaja isiklikus konfiguratsioonifailis

salvestatavaid seadeid) saab muuta ka menüüst Redigeerimine -> Häälestus valides. Avaneval dialoogil on kaks lehte. Esimesel lehel saab valida allkirjastaja aadressi ja manifesti vaikeväärtusi ja kasutamise reziimi.

Teisel lehel saab aga muuta HTTP vahendaja ja kehtivuskinnituste serveri seadeid.



Seda tuleks alati teha kui gdigidoc on alles installeeritud sest vaja on registreerida tellitud kehtivuskinnituste serveri juurdepääsutõend.

Viited

- XML-DSIG – http://www.w3.org/Signature
- XAdES – http://www.w3.org/TR/XAdES
- OpenXAdES – http://www.openxades.org