TalTech IT Kolledž

Keybase

Koostanud: Edmund Laugasson
TalTech IT Kolledži lektor

2020

Sisukord

Keybase

Keybase'i[1] puhul on tegemist suhtlusrakendusega, mis toimib sarnaselt Slack'iga[2], Discord'iga[3] kuid mitmed võimalused on juures. Keybase on oluliselt kõrgema turvalisuse- ja privaatsusega tänu võtmepõhisele arhitektuurile[4] - kõik andmed on vaikimisi krüpteeritud. Kogu rakendus toimib nii graafiliselt kui ka käsureal ehk siis sisuliselt võimalik seda ka IRC[5] asemel kasutada.

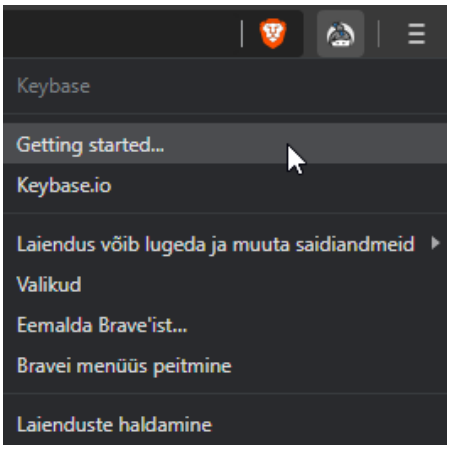
Lisaks tegemist sisuliselt pilvelahendusega: suur võrguketas (kasutatav nii arvutist kui nutiseadmest) + krüpteeritud versioonihaldus Git. Kirjeldav artikkel Keybase'ist on loodud ka IT Kolledži vikis[6].

Paigaldamine

Erinevate operatsioonisüsteemide jaoks on juhised Keybase'i kodulehel olemas[7]. Siiski on käesolevas dokumendis mõned paigaldused läbi tehtud ja täiendavad selgitused lisatud, mida Keybase'i kodulehelt ei leia. Allpool on eri operatsioonisüsteemide jaoks loodud näidiskasutajad – igaüks asendab siis praktikas enda kasutajaga.

Veebilehitseja laiendusena

Peale arvutisse paigaldamist võimalus Keybase'i kasutada ka veebilehitseja Chrome, Firefox laienduse[8] kaudu. Toetatud on ka kõik nende põhjal tehtud veebilehitsejad, nt Vivaldi[9], Chromium[10], Brave[11], jne[12]. Suhtlemiseks tuleb kasutada oma profiilile lisatud veebikeskkondades vastavat nuppu. Näiteks kui teil on kasutaja Hacker News veebikeskkonnas ja olete selle kaudu oma identiteeti tõestanud ka Keybase'is siis peale arvutis Keybase'i ja veebilehitsejas Keybase'i laienduse paigaldamist on näha nupp *Keybase chat*, mille kaudu saab siis käivitada suhtluse juba arvutipõhises rakenduses. Võimaldab Keybase'i abil vestluse krüpteerida ja mugavalt veebikeskkonnast otse krüpteeritud suhtlust avada. Vähe levinud viis Keybase'i kasutamiseks ent siiski võimalik.



1 https://keybase.io/
2 https://en.wikipedia.org/wiki/Slack_(software)
3 https://en.wikipedia.org/wiki/Discord_(software)
4 https://keybase.io/docs/crypto/overview
5 https://et.wikipedia.org/wiki/IRC
6 https://wiki.itcollege.ee/index.php/Keybase
7 https://keybase.io/download
8 https://keybase.io/docs/extension
9 https://en.wikipedia.org/wiki/Vivaldi_(web_browser)
10 https://en.wikipedia.org/wiki/Chromium_(web_browser)
11 https://en.wikipedia.org/wiki/Brave_(web_browser)
12 https://en.wikipedia.org/wiki/List_of_web_browsers

MS Windows

Siin näites on kasutatud *MS Windows 10 EDU build 1909*. Keybase'i allalaadimine ja paigaldusjuhis MS Windowsile - https://keybase.io/docs/the_app/install_windows – paigaldamisel üldiselt midagi valida ei ole – see tehakse automaatselt ära ja rakendus käivitatakse.

Tavaliselt paigaldatakse tarkvara kausta

- **`%programfiles%`** (64-bit rakendused)
- **`%programfiles(x86)%`** (32-bit rakendused)

Tehes seda tavakasutaja õigustes, paigaldatakse Keybase vaid konkreetsele kasutajale kausta **`%localappdata%\Keybase\`** ja lisasätted leiab **`%appdata%\Keybase\`**

GNU/Linux

Juhised leiab https://keybase.io/docs/the_app/install_linux – paigaldamine toimub terminalis (käsureal).

Ubuntu Linux

Paketi paigaldamine lisab omakorda ka vastava varamu ning edaspidi uuendatakse Keybase kogu süsteemiga. Kui siiski soovitakse seda varamu lisamist vältida siis käivitada

```
sudo touch /etc/default/keybase
```

... enne paketi paigaldamist.

64-bit

```
curl --remote-name https://prerelease.keybase.io/keybase_amd64.deb
sudo apt install ./keybase_amd64.deb
run_keybase  #rakenduse käivitamine käsurealt
```

32-bit

```
curl --remote-name https://prerelease.keybase.io/keybase_i386.deb
sudo apt install ./keybase_i386.deb
run_keybase -g # käivitamine graafilise liideseta ei ole 32-bit Linuxi puhul toetatud
```

Kui APT[13] on vanem kui v1.1 siis paigaldamine:

```
sudo dpkg -i keybase_amd64.deb
sudo apt-get install -f
```

macOS

Paigaldusjuhised leiab https://keybase.io/docs/the_app/install_macos

- laadida alla *keybase.dmg* ja avada see
- lohistada Keybase kausta *Applications* ja käivitada sealt

13 https://en.wikipedia.org/wiki/APT_(software)

Android, iOS

Androidi puhul:

https://keybase.io/_/download/keybase-for-android

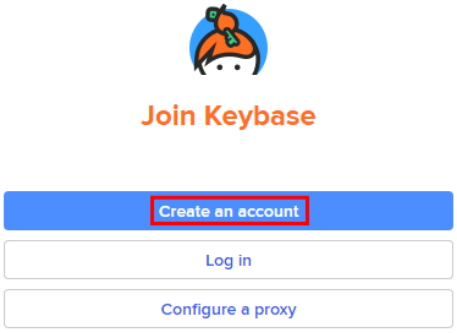
iOSi puhul

https://keybase.io/_/download/keybase-for-ios

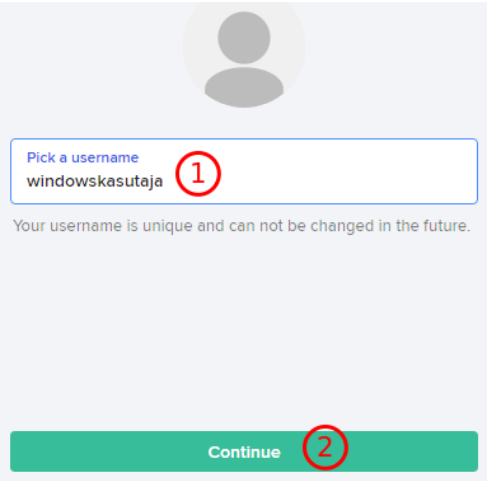
Viited võivad ka muutuda. Allalaadimise viited leiab https://keybase.io/download

Kasutajakonto loomine

Peale paigaldamist tuleb luua kasutajakonto: *Create an account*

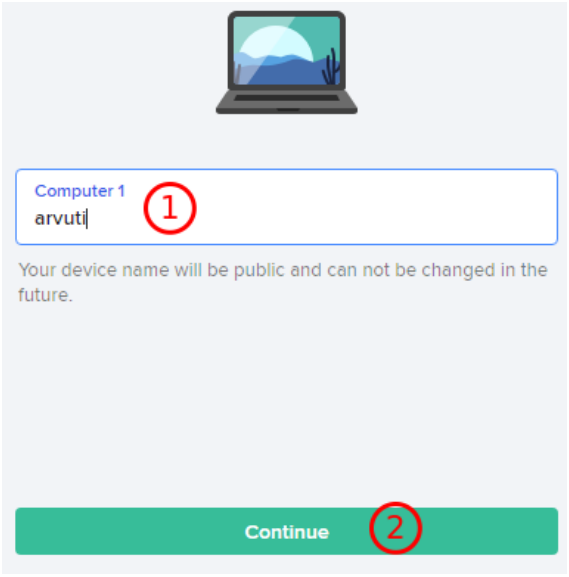


Seejärel tuleb valida kasutajanimi (1) (*Pick a username*) ning jätkata (2) (*Continue*)



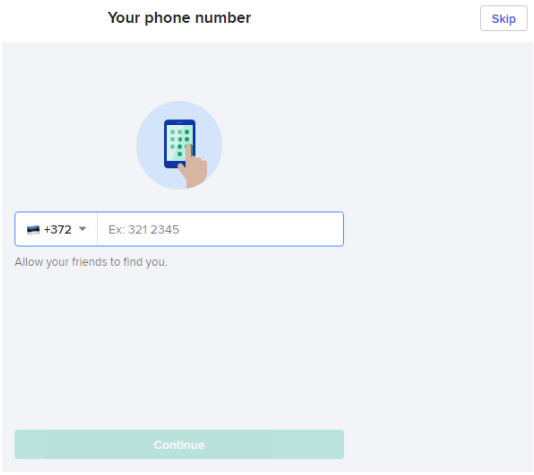
NB! Valitud kasutajanimi on unikaalne:
* seda ei saa hiljem muuta
* peale kasutaja kustutamist ei saa seda nime enam uuesti valida

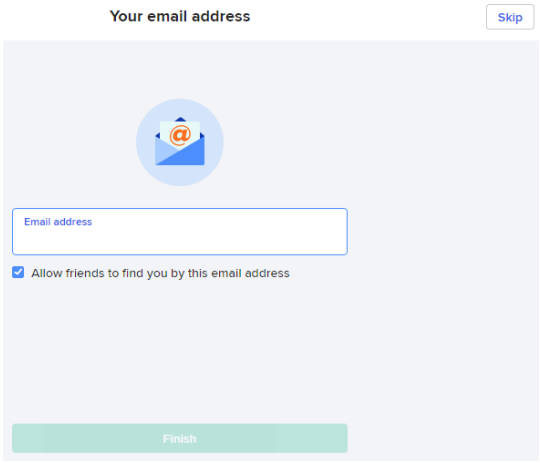
Seadme registreerimine



Seejärel registreeritakse iga seade kus Keybase töötab. Sellele seadmele tuleb anda nimi (1) ja see nimi saab olema avalik ning lihtsalt muuta ei saa – siis tuleb kustutada ja uuesti õige nimega lisada. Seega palun hästi läbi mõelda, mis nime panete. Kui see tehtud siis saab jätkata (2) (*Continue*). Sisuliselt tegemist sessiooniga, mida paljudes suhtlusrakendustes registreeritakse. Selles mõtes ei ole siin midagi erakorralist.

Peale seda võimalus lisada veel telefoninumber, e-postiaadress, et sõbrad paremini leiaksid (*Allow friends to find you by this email address*) või ka vahele jätta (*Skip*)





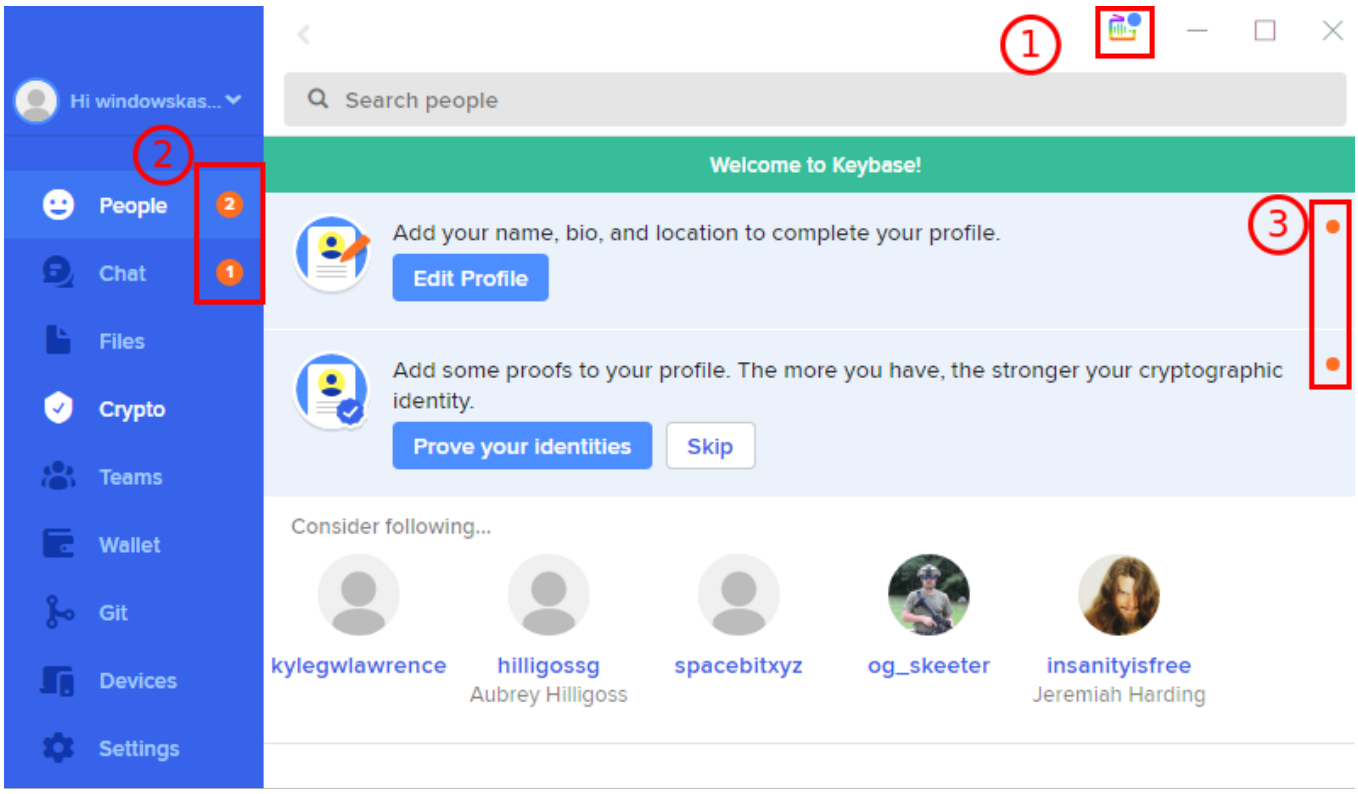
Peale sisselogimist

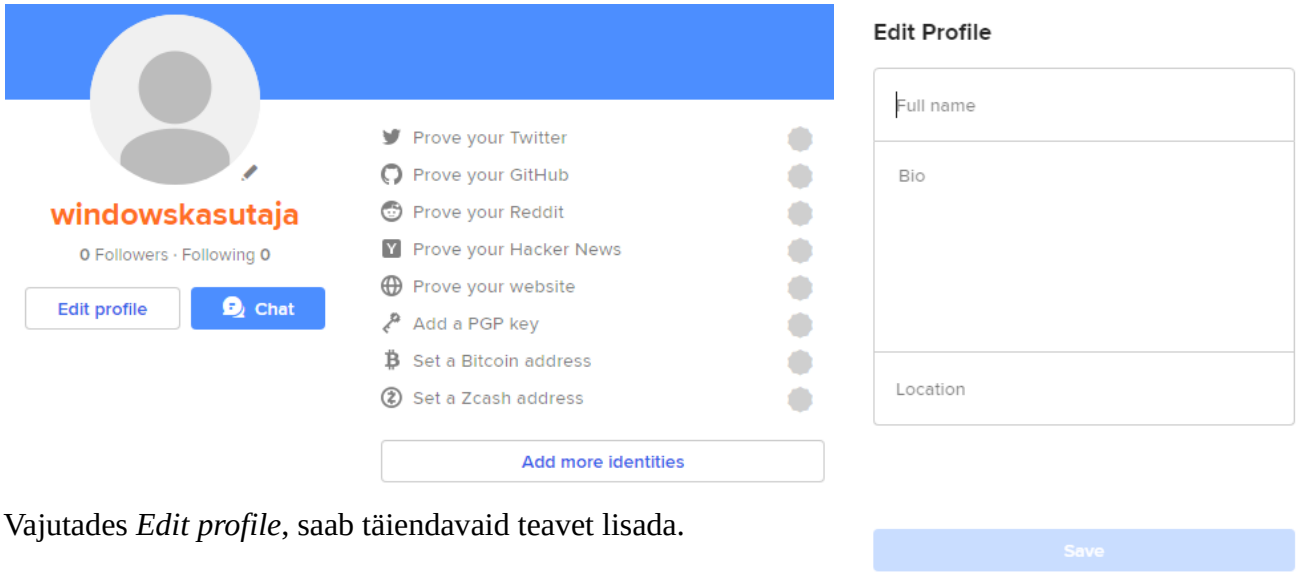
Peale sisselogimist saab lugeda Keybase'i teateid (1) ning lugemata teateid nii rakenduse kui vestluste osas (2). Kui vastav valik avada siis lugemata sõnumid on vastavalt tähistatud (3).

Siin palutakse täiendada oma kasutajaprofiili (*Edit profile*): lisada nimi (*name*), lühitutvustus (*bio*), asukoht (*location*).

Isiku tõestamine

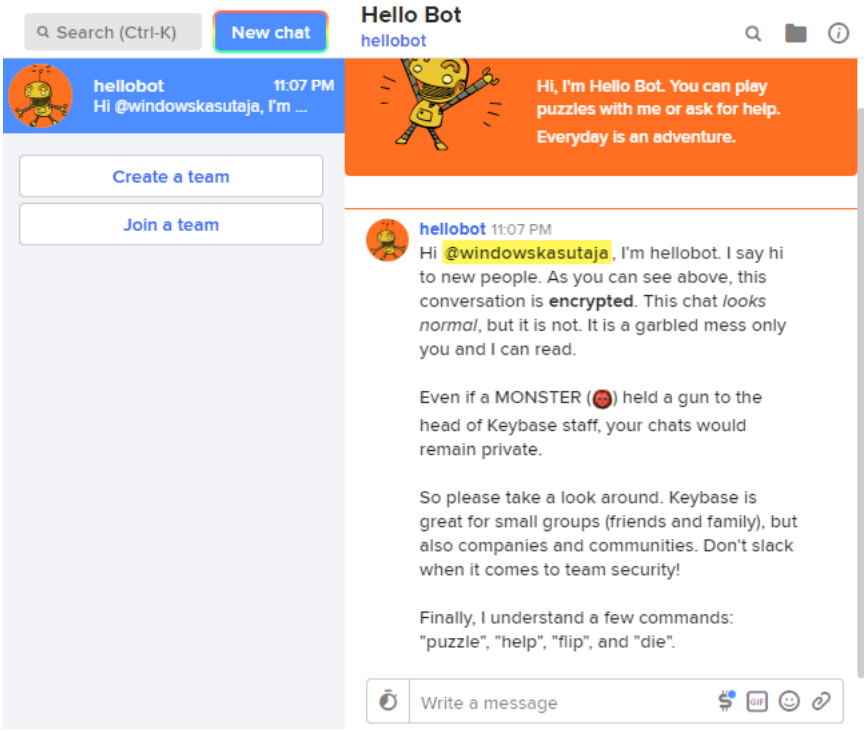
Teine oluline asi on tõestada oma isikut ehk siis läbi erinevate olemasolevate kontode lisada oma kontole usaldusväärsust (*Prove your identities*). See eristab Keybase'i kontot teistest kus võimalik teha kasutaja kus ei ole võimalik veenduda selle ehtsuses. Mida rohkem on tõestavaid võimalusi lisatud – seda usaldusväärsem on konto teiste jaoks.





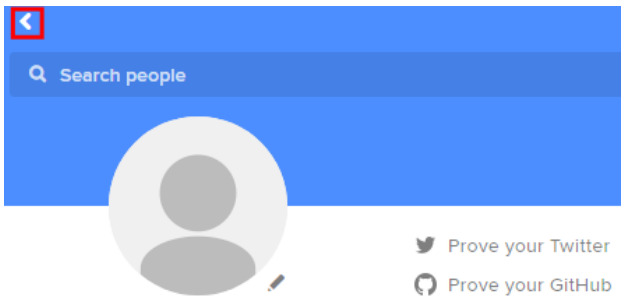
Vajutades *Edit profile*, saab täiendavaid teavet lisada.

Esimene tervitus vestlusroboti poolt:



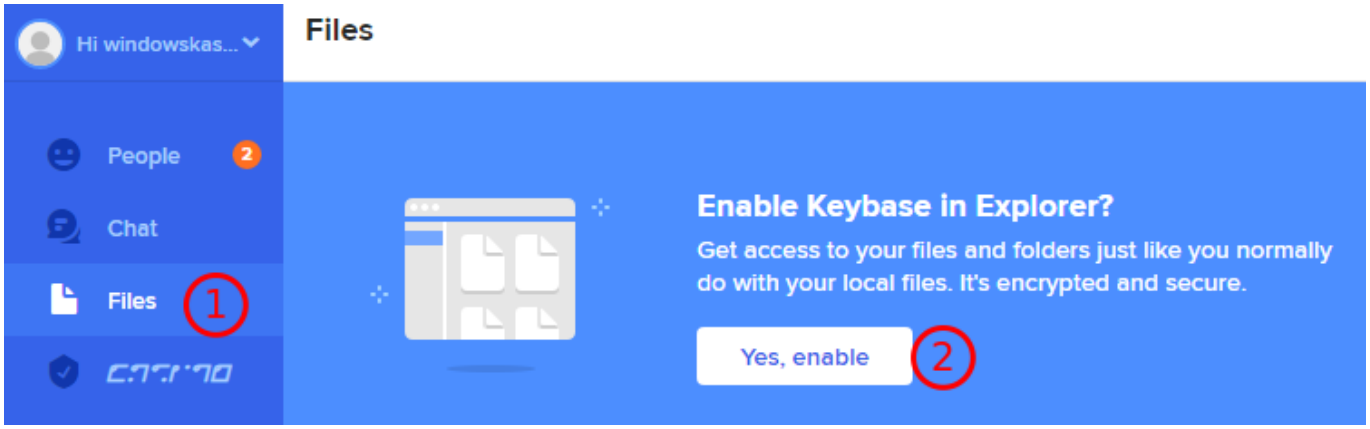
Võimalus ka luua rühm (*Create a team*) või ühineda olemasoleva rühmaga (*Join a team*).

Olles avanud vastavas vaates (*People*, *Chat*, *Files*, jne) mõne valiku, jäetakse see meelde ja tagasi saab liikuda vastavate noolte abil

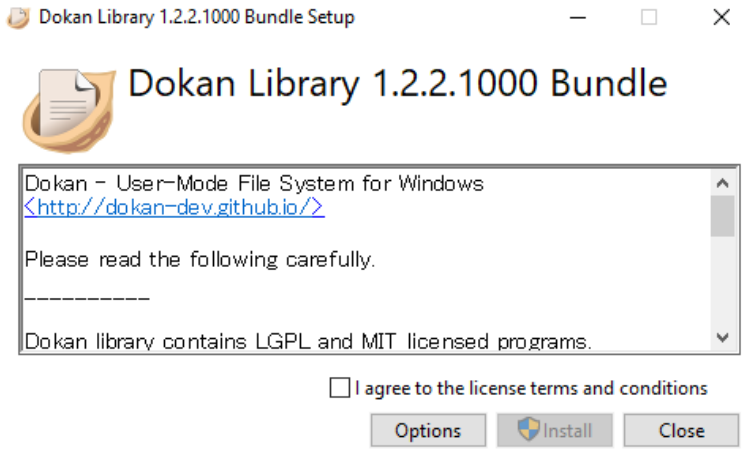


Võrguketas

Järgmine samm Keybase'i kasutamisel on lubada failihalduris Keybase'i võrguketas (*Enable Keybase in Explorer*). Selleks avada vaade *Files* (1) ning vajutada vastavat nuppu (2) *Yes, enable*

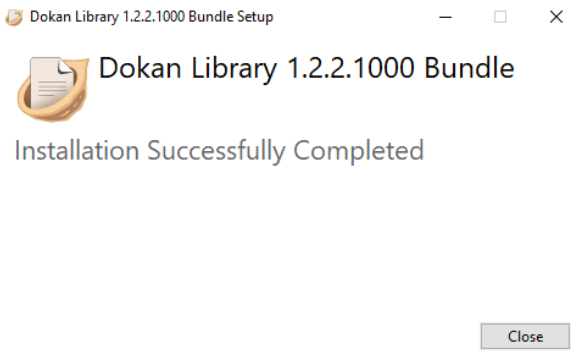


Seepeale käivitatakse Dokany teegi (*library*) paigaldus, jätkamiseks nõustuda litsentsi tingimustega (*I agree to the licence terms and conditions*)

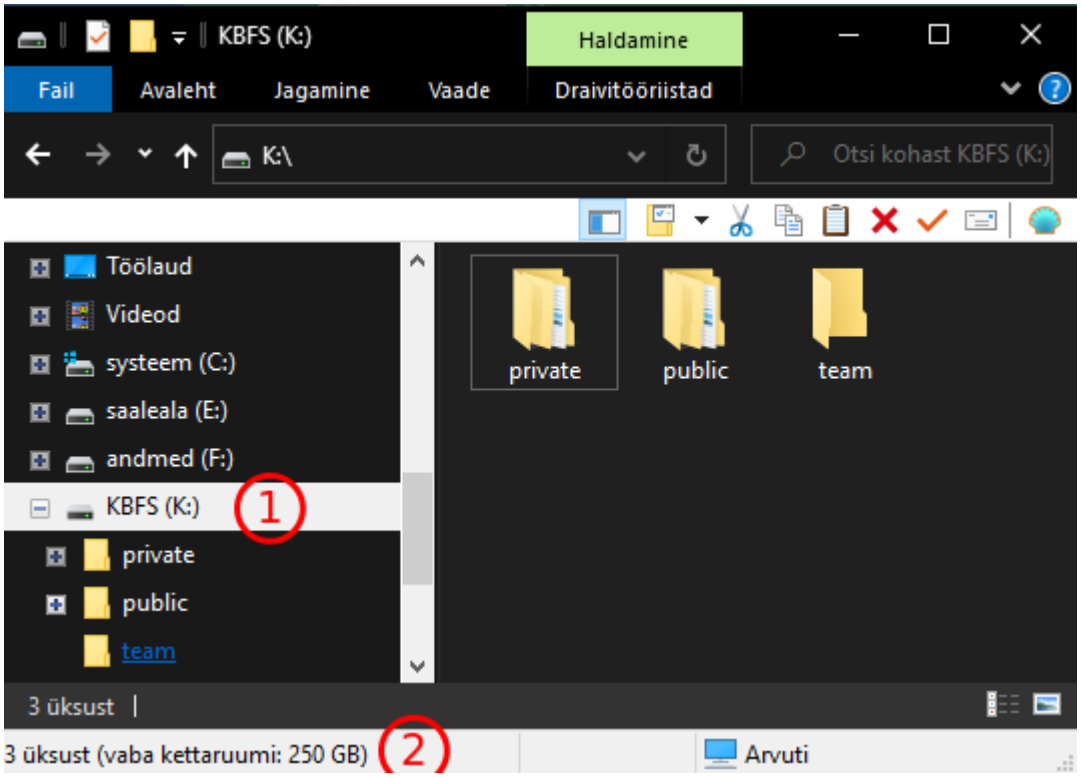


Vanemate MS Windowsi versioonidega võidakse ka arvuti taaskäivitust nõuda.

Kui paigaldamine edukalt lõppenud:



... siis võimalus Keybase'i võrguketast lehitseda:



Tavaliselt ühendatakse see K: kettana (1) ja 250 GB on vaba kettaruumi (2).
KBFS – *Keybase File System*[14].

Private nagu nimi ütleb, on isiklik kaust ja sinna alla ilmuvad isiklikud vestlused. Kataloogid nimetatakse kasutajate järgi, kes vastavas vestluses osalevad. Lisaks on seal alamkataloog, millel vaid teie kasutajanimi ja see on isiklik ning sinna keegi teine ligi ei saa.

Public seevastu on avalik kaust ja sinna pandud andmed on avalikult ligipääsetavad[15]. Selliselt võimalik lihtsalt faile avalikult jagada või lausa koduleht luua.

- *https://keybase.pub/kasutajanimi* - näitab faile kohe ilma avaleheta
- *https://kasutajanimi.keybase.pub/* - nõuab */keybase/public/kasutajanimi* kaustas faili *index.html* või *index.md*

Muidugi tuleks kasutajanimi asendada siin tegeliku Keybase'i kasutajanimega.

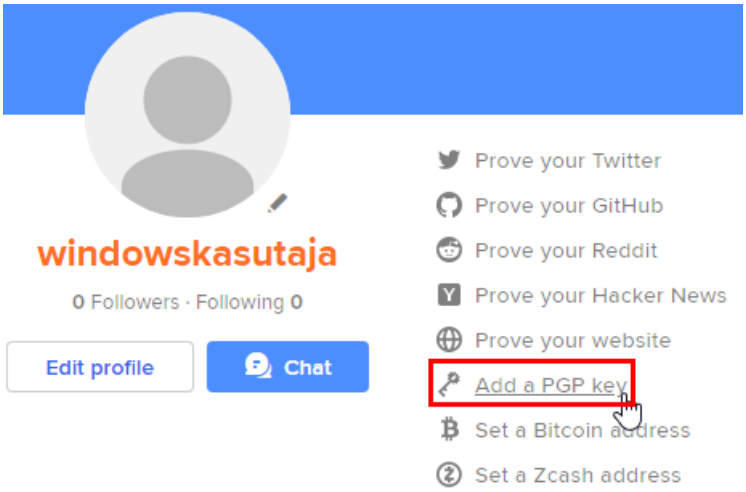
Team on rühmade poolt kasutatavad ühised kataloogid. Kui liitutakse mõne rühmaga siis sinna ka vastava rühma ühine kataloog ilmub.

Võrguketas annab mugavuse kasutada lisakettaruumi ning jagada faile vestluse teiste osapooltega. Näiteks e-postiga failide saatmise asemel on lihtsam jagada neid ühises vestluses võrguketta vahendusel. Selleks ei ole vaja teha muud kui vastavasse kataloogi fail(id) panna, muidugi võimalus omakorda alamkatalooge luua vastavalt vajadusele.

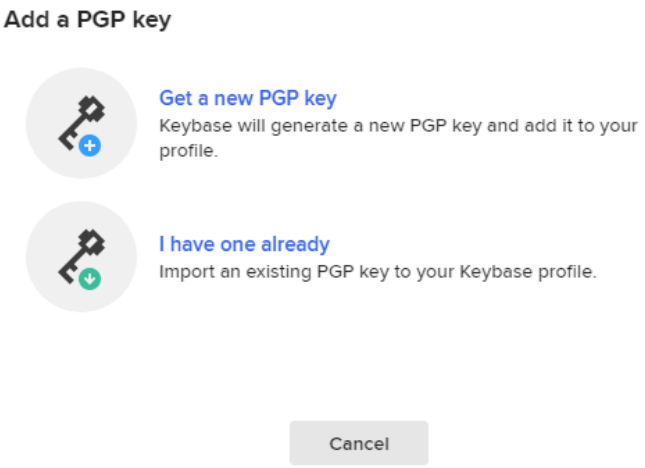
Võtmehaldus

Üks võimalus oma usaldusväärsust tõsta on võtmepaari lisamine – *Add a PGP key*.

14 https://keybase.io/docs/kbfs
15 https://keybase.io/docs/kbfs/keybase.pub

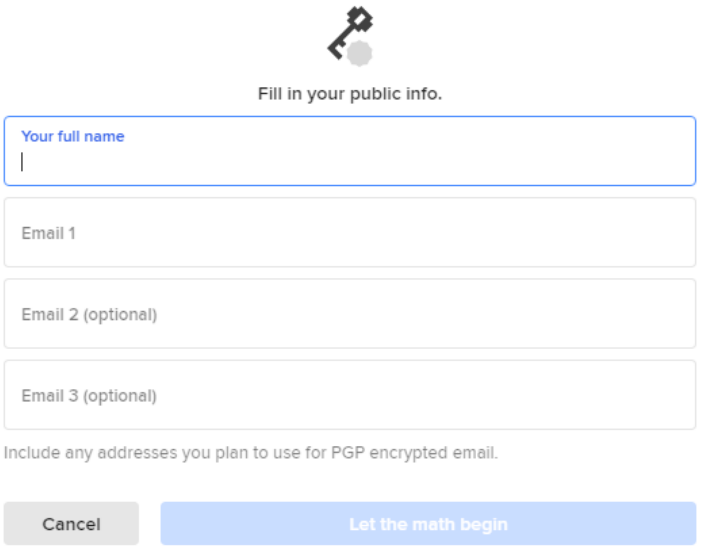


Siin võimalus luua uus võtmepaar (*Get a new PGP key*) või importida olemasolev (*I have one already*):

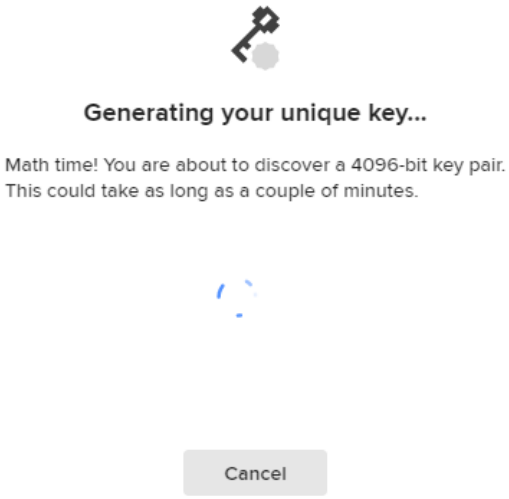


Soovitav on luua võtmepaar GPG abil ja see siis siia importida.

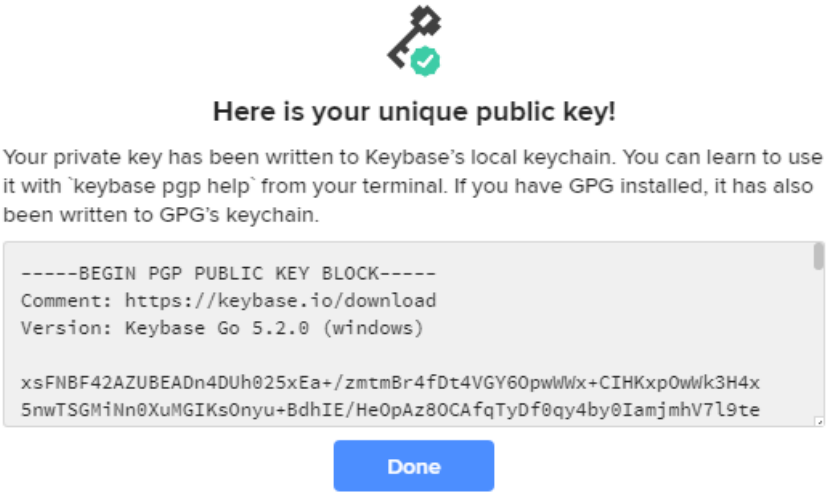
Uue võtmepaari loomisel küsitakse nime ja e-postiaadressi ja seejärel saab võtmepaari ära teha:



Luuakse 4096-bit RSA võti – seda ei ole soovitav kasutada, pigem elliptilise krüptoga võti – soovitav on jätkata peatükist *Elliptilise krüptoga võtmepaar*.

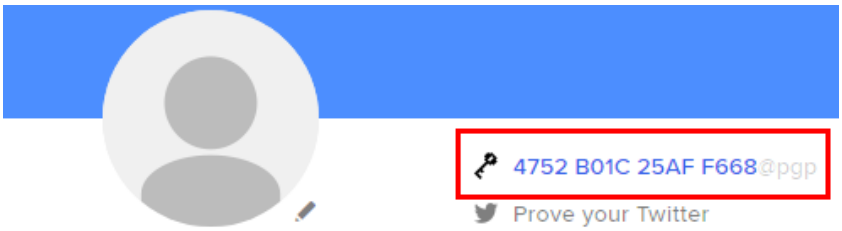


Kui see valmis siis vastav teade:

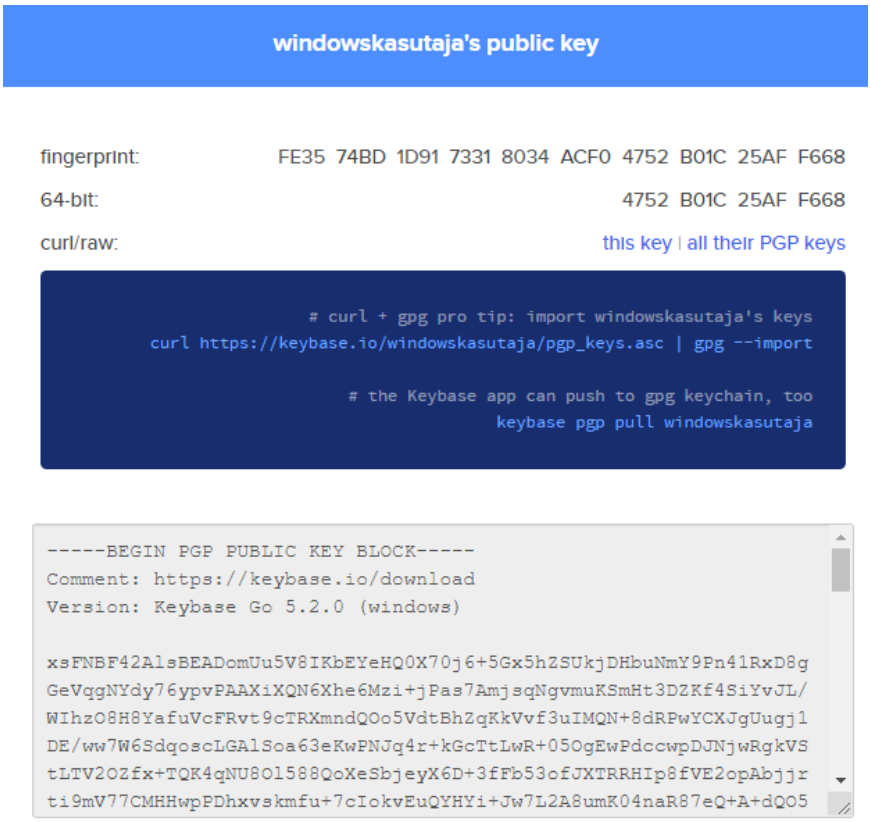


Paneme aga tähele, et graafiliselt võtmepaari loomisel ei saanud valida krüptoalgoritmi ega määrata ka võtmele salasõna. Käsureal on siiski täiendavad võimalused, abiteavet leiab **`keybase pgp h`**

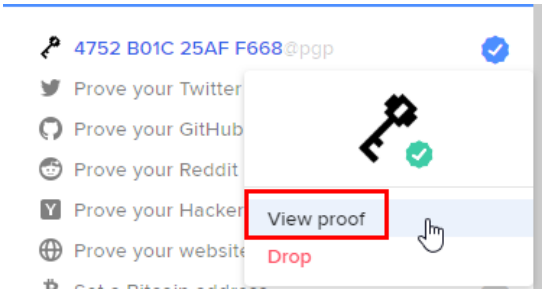
Loodud GPG-võti on ka profiilis näha:



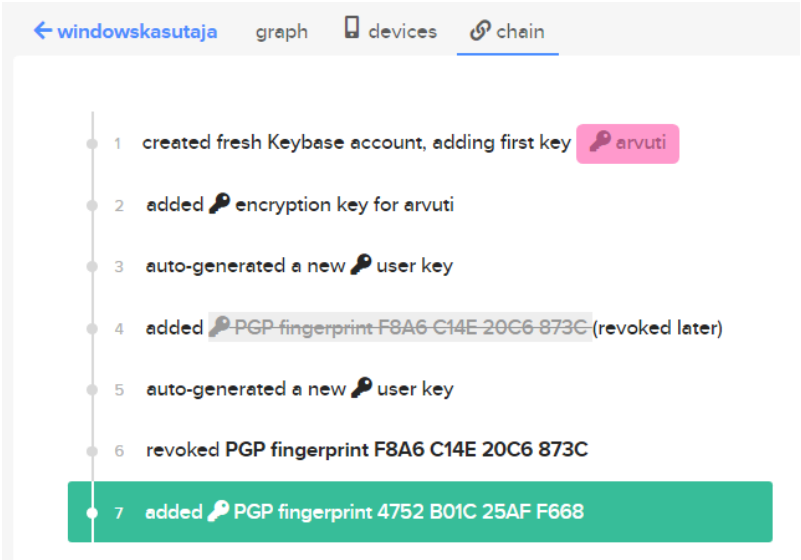
See võti toimib hüperlingina ja avatakse veebilehitsejas kasutaja avalik profiil kus saab täpsemalt võtme kohta teavet ja juhised kuidas avalikku võtit alla laadida, teistega jagada:



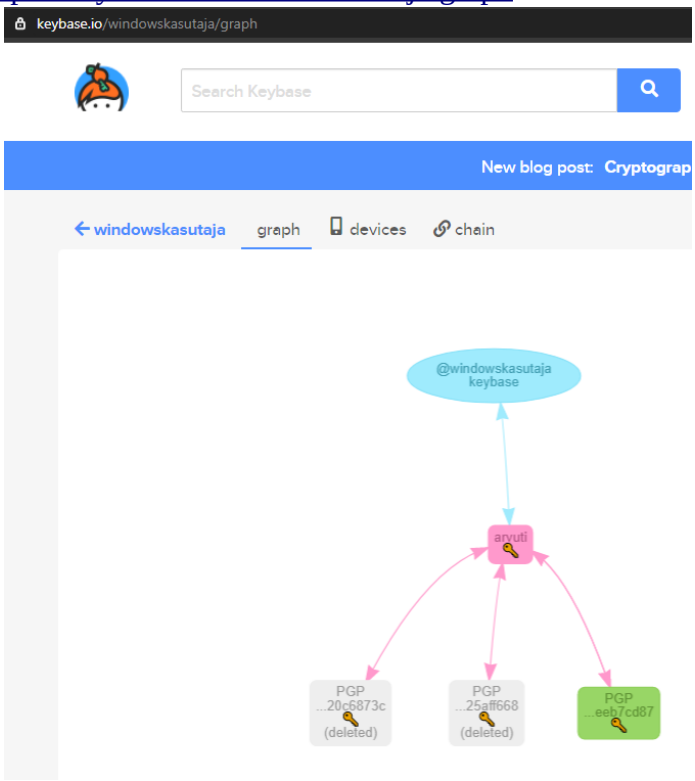
Hiljem oma profiili all võtme juures võimalus ka vaadata veebipõhist ajalugu. Esmalt avada konkreetse sammu tõestuse vaatamine (*View proof*):



... siis avatakse vastav koht veebis https://keybase.io/windowskasutaja/sigchain kus kõik sammud näha:



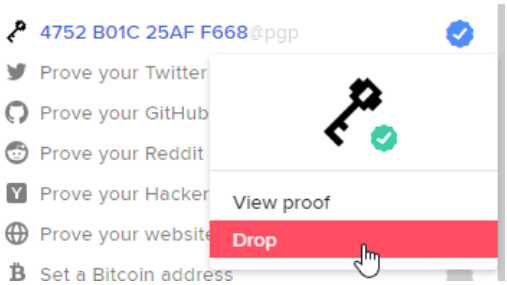
See on kõik ka graafiliselt https://keybase.io/windowskasutaja/graph aadressil näha



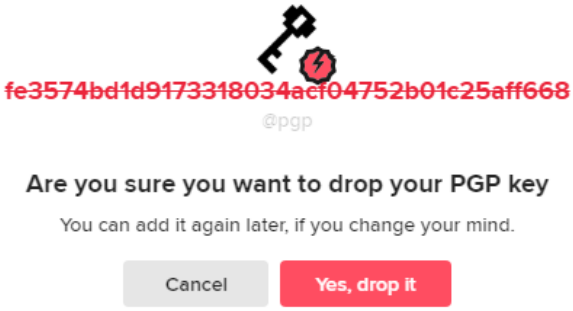
Elliptilise krüptoga võtmepaar

Siiski ei ole soovitav RSA võtit enam kasutada – pigem luua elliptilise krüpto abil endale võtmepaar. RIA pakub oma uuringute lehel[16] alapealkirja *Krüptograafiliste algoritmide elutsükli uuringud* all rida uuringuid, mis sellest räägivad.

Seega kui eespool sai tehtud RSA võtmepaar siis kustutame selle (*Drop*):



Kustutamisel küsitakse veelkord kinnitust ja kinnitame kustutamise (*Yes, drop it*):



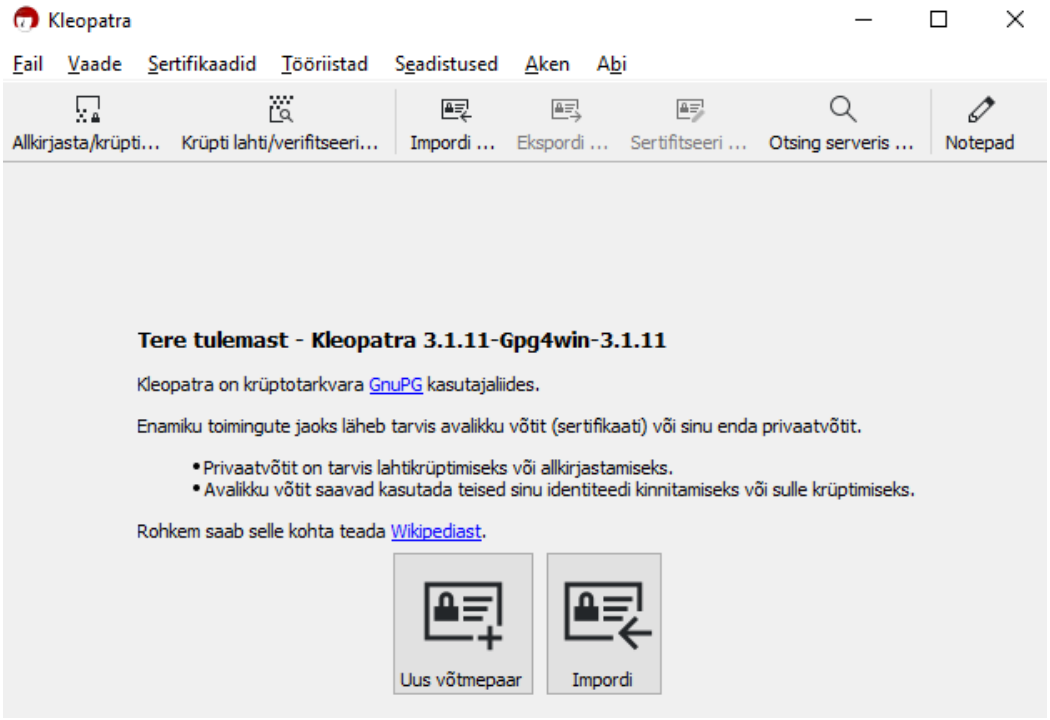
Kui aga paigaldada MS Windowsi vastav võtmete haldamise rakendus Gpg4win[17] siis tuleb sellega kaasa ka rakendus Kleopatra, millega saab juba ka elliptilise krüptoga uue võtmepaari luua.

16 https://www.ria.ee/et/ametist/uuringud-analuusid-ulevaated.html
17 https://www.gpg4win.org/

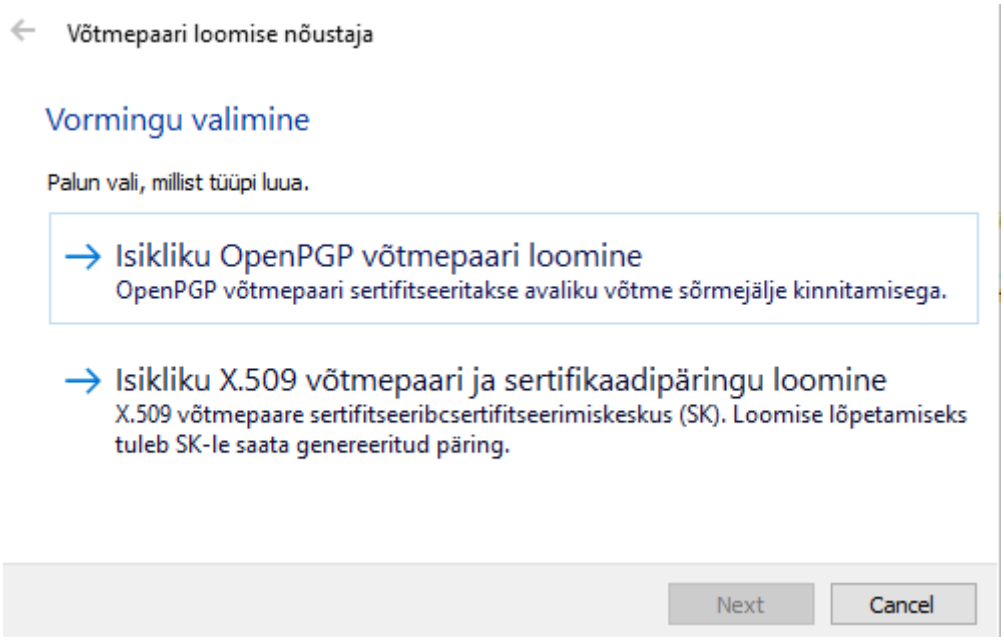
Kleopatra (MS Windows)

Kinnitamata andmeil on turvakaalutlustel soovitatav võtmepaar luua käsureal rakendusega GPG[18]. Näidisena on rakenduse kasutamine siin siiski ära näidatud.

Vajutame *Uus võtmepaar* nupule või rippmenüüst *Fail->Uus võtmepaar* (CTRL+N):

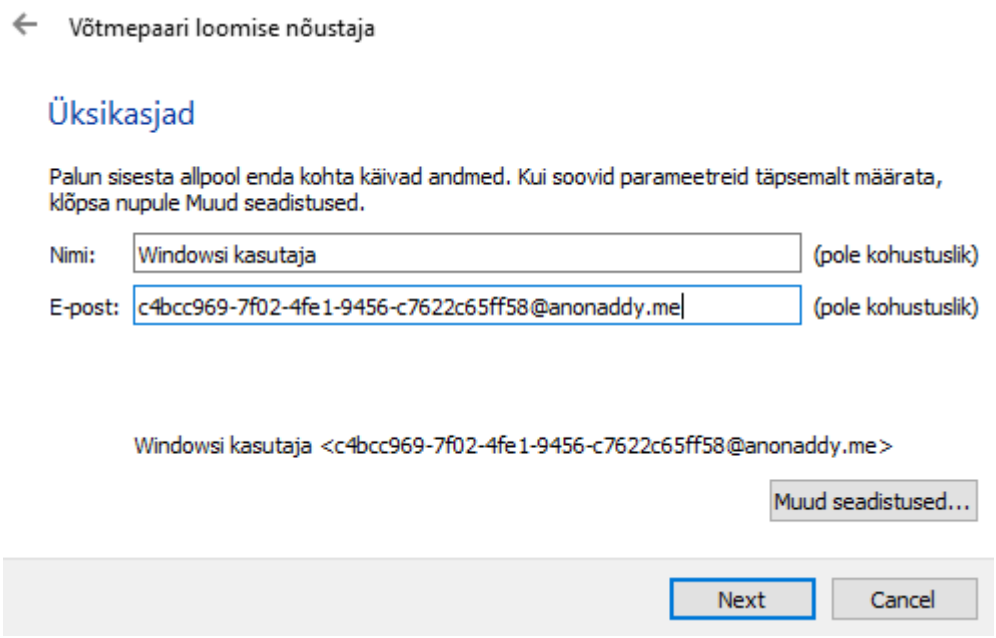


Vormingu valimisel valime OpenPGP

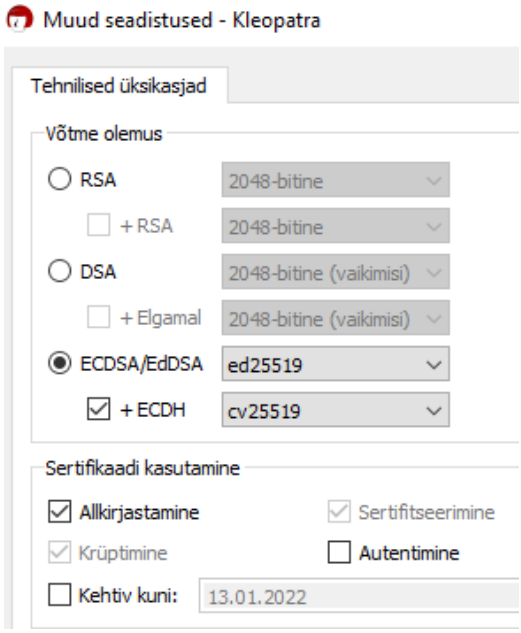


Seejärel sisestame andmed. Soovitav on lisada ka e-postiaadress – saame hiljem sama võtmepaari (salajane, avalik võti) ka e-posti puhul kasutada. Sama Kleopatra rakenduse abil saab ka mitu e-postiaadressi ühe võtmepaariga siduda:

18 https://wiki.itcollege.ee/index.php/GPG

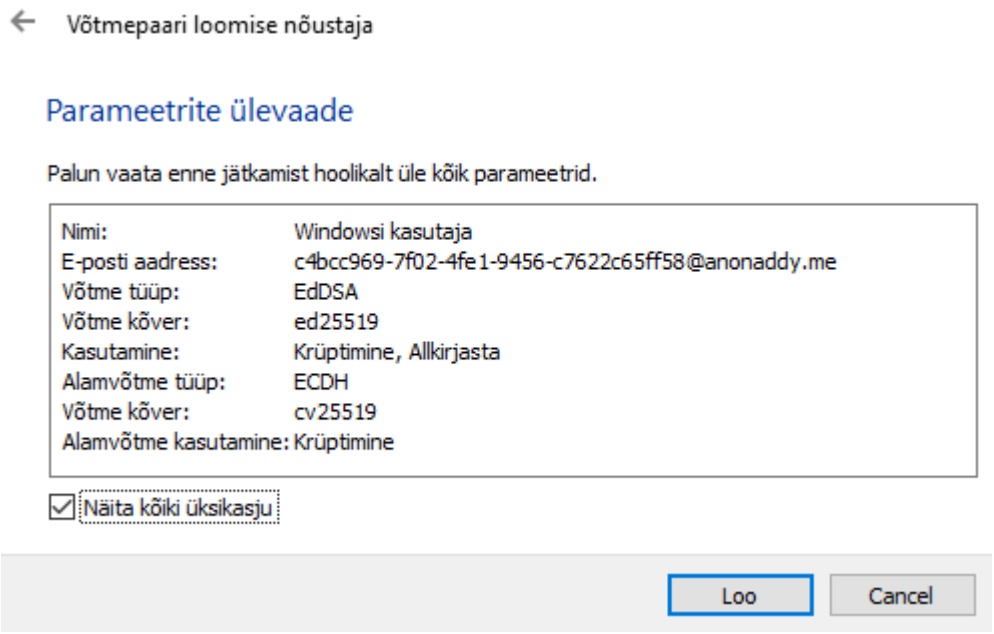


Nupu *Muud seadistused*... alt avaneb võimalus määrata Ed25519, mis esindab siis elliptilist krüptot:

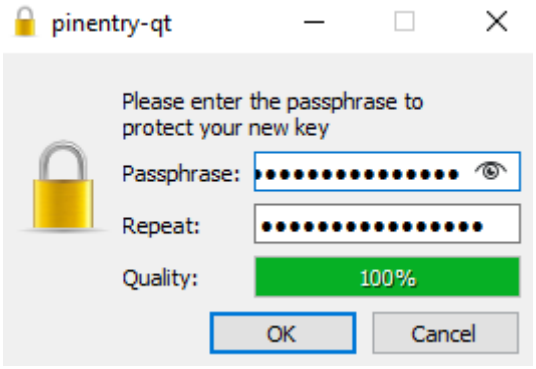


Selliselt loodud võtmepaari saab hiljem ka e-posti krüpteerimisel kasutada – lisatud on ka allkirjastamine. Kui valida ka *Autentimine* siis saab ka SSH võtmena kasutada, mis võib siiski tülikaks osutuda ja sageli on lihtsam eraldi SSH võtmepaari kasutada, mida ka elliptilise krüpto põhjal saab luua. Kehtivusaega ei pea määrama – siis saab võtit piiramatu aja jooksul kasutada.

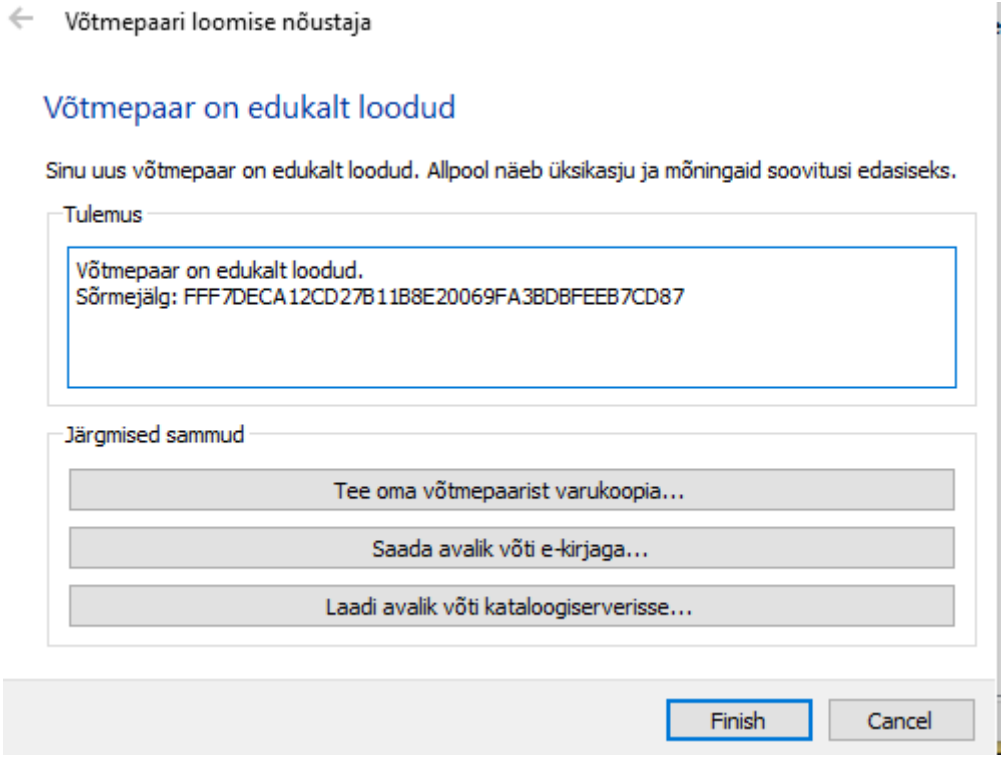
Enne lõplikku võtmepaari loomist vaadata üle valitud sätted:



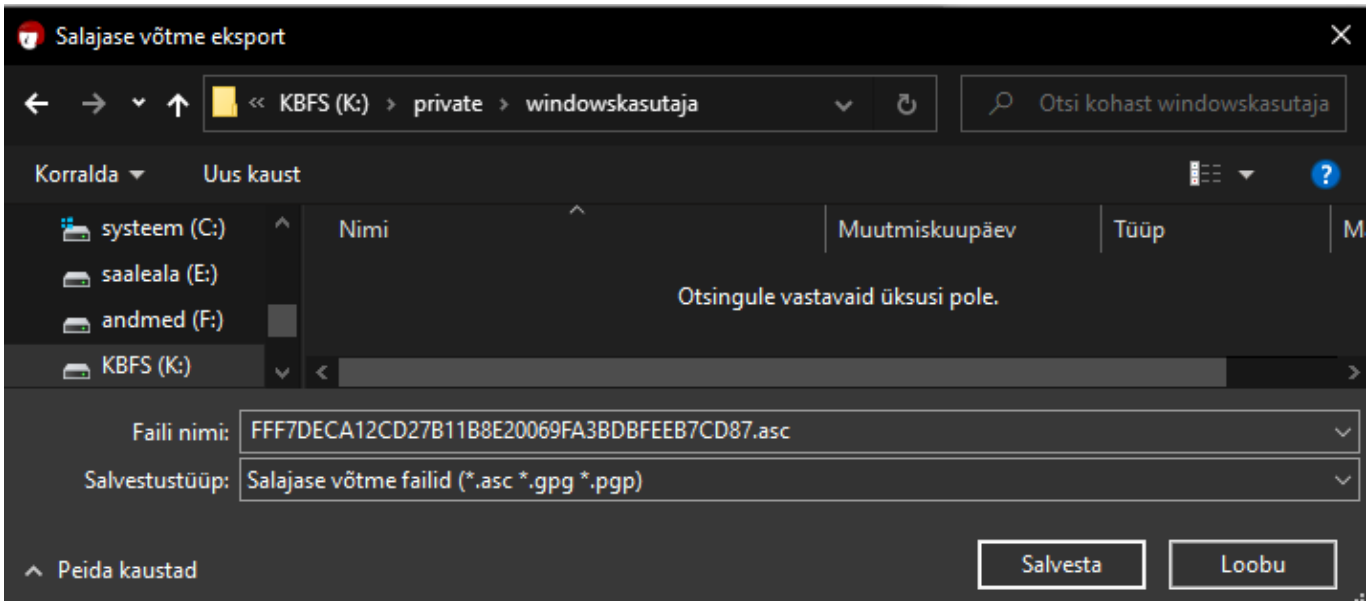
Küsitakse veel salasõna:



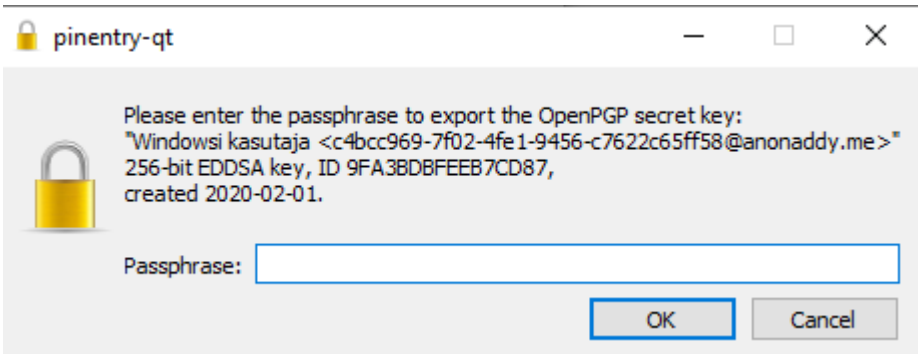
Seejärel eduka võtmepaari loomise järel ka vastav teade:



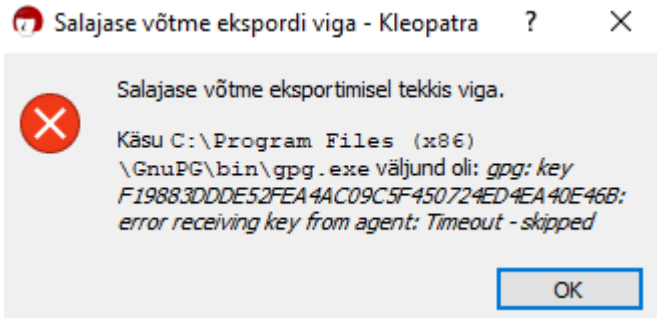
Enne *Finish* nupule vajutamist on soovitav vajutada ka nupule *Tee oma võtmepaarist varukoopia...* ja näiteks oma isiklikku kataloogi Keybase'i võrgukettal turvaliselt salvestada:



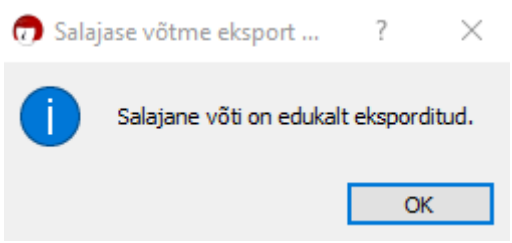
Salajase võtme eksportimisel küsitakse ka salasõna (mis loodetavasti oli määratud):



Kui liiga kauaks mõtlema jäädakse siis tuleb ka vastav teade (*timeout* - *aegumine*):



Edukal eksportimisel ka vastav teade:



Kui hiljem seda tekstifaili vaadata siis salajane (privaatne) võti jääb vastavate märgendite vahele:

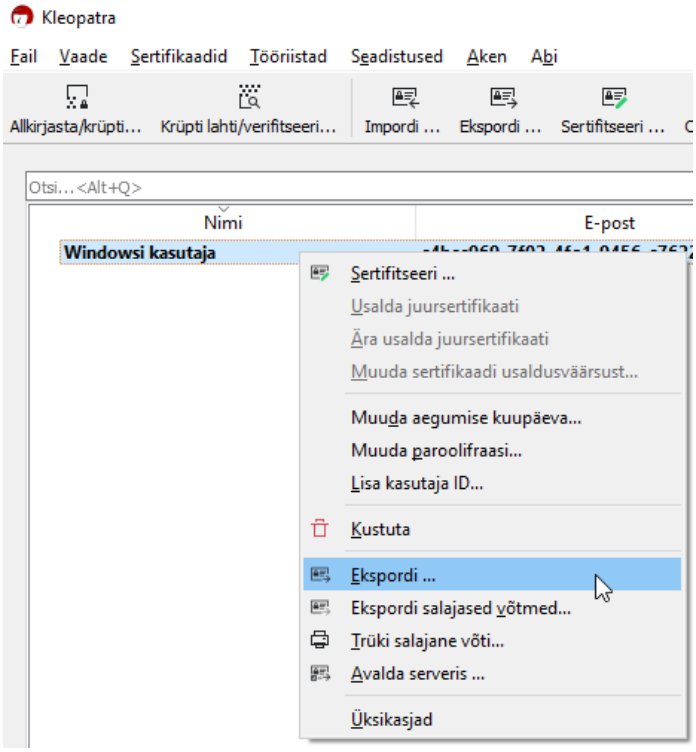
```
-----BEGIN PGP PRIVATE KEY BLOCK-----

üks tühi rida

<räsi>

-----END PGP PRIVATE KEY BLOCK-----
```

Vastavalt siis avalik võti:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

üks tühi rida

<räsi>

-----END PGP PUBLIC KEY BLOCK-----
```

Antud juhul eksporditi vaid privaatne võti, milles saab veenduda kui eksporditud tekstifail avada.

Rakenduses Kleopatra eksportimise funktsiooni kasutades eksporditakse vaid avalik võti.



Kui soovitakse ühte faili kus kogu võtmepaar koos siis:

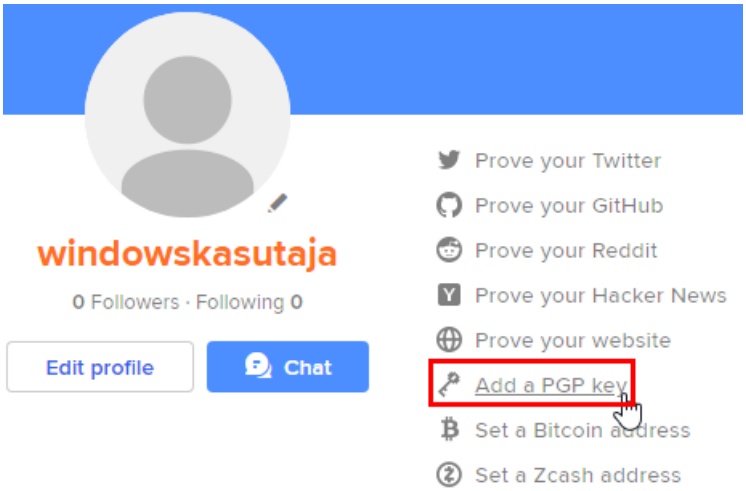
- luua uus tekstifail (Notepad vms palja teksti[19] redaktori abil), mille tüübiks määrata faili salvestamisel *.asc*
- esmalt avalik võti
- üks tühi rida vahet
- salajane võti
- lõpus üks tühi rida

19 https://en.wikipedia.org/wiki/Plain_text

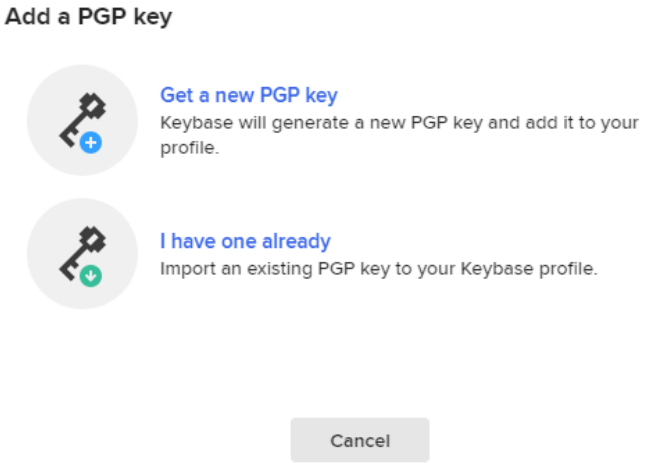
Kuna krüpteerimine toimub avaliku võtmega, lahti krüpteerimine aga salajasega (asümmeetriline krüpto) siis vajalik kogu võtmepaar importida Keybase'i.

Elliptilise võtmepaari importimine Keybase'i

Võtmepaari importimiseks Keybase'i valime uuesti PGP-võtme lisamise:

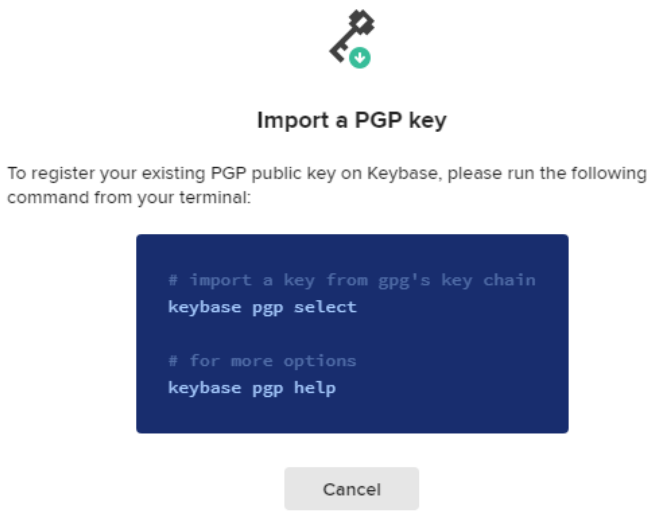


Taas võimalus luua uus võtmepaar (*Get a new PGP key*) või importida olemasolev (*I have one already*):



Valime seekord teise valiku (*I have one already*): kuna meil võtmepaar olemas.

Seda aga saab importida vaid käsurea kaudu, mis on tegelikult üsna lihtne:



Keybase'i ei pea sel ajal sulgema ja see võib avatuks jääda.

Avame cmd ja sisestame soovitud käsu, valime õige võtme (hetkel vaid üks ongi) ning peale salasõna sisestamist see imporditakse:

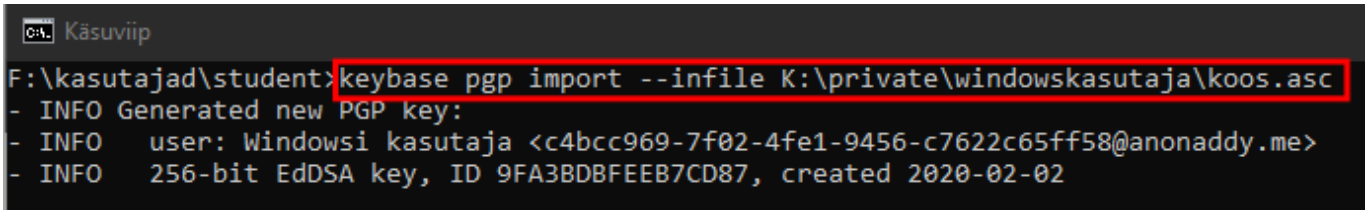
`keybase pgp select`

```
Käsuviip
Microsoft Windows [Version 10.0.18363.592]
(c) 2019, Microsoft Corporation. Kõik õigused on reserveeritud.
Clink v0.4.9 [git:2fd2c2] Copyright (c) 2012-2016 Martin Ridgers
http://mridgers.github.io/clink

F:\kasutajad\student>keybase pgp select
You are selecting a PGP key from your local GnuPG keychain, and
will publish a statement signed with this key to make it part of
your Keybase.io identity.

Note that GnuPG will prompt you to perform this signature.

You can also import the secret key to *local*, *encrypted* Keybase
keyring, enabling decryption and signing with the Keybase client.
To do that, use "--import" flag.

Learn more: keybase pgp help select

#    Algo   Key Id             Created   UserId
=    ====   ======             =======   ======
1    256?   9FA3BDBFEEB7CD87             Windowsi kasutaja <c4bcc969-7f02-4fe1-9456-c7622c65ff58@anonaddy.me>
Choose a key: 1
- INFO Generated new PGP key:
- INFO   user: Windowsi kasutaja <c4bcc969-7f02-4fe1-9456-c7622c65ff58@anonaddy.me>
- INFO   256-bit EdDSA key, ID 9FA3BDBFEEB7CD87, created 2020-02-02
```

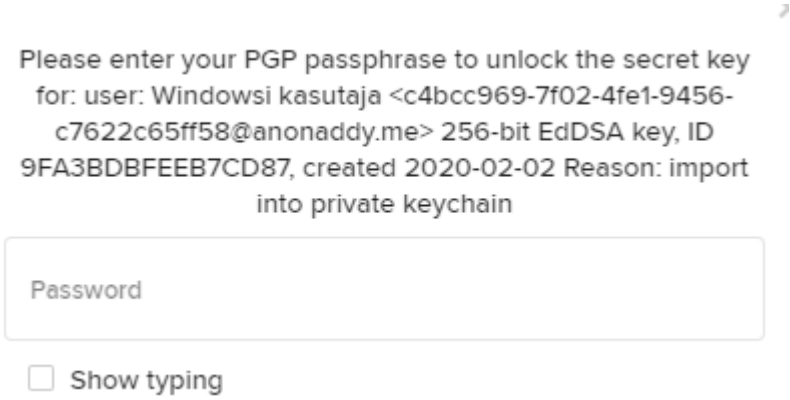
... ning näidatakse koheselt ka kasutaja profiilis:

Teine võimalus on otse failist importida kus avalik ja salajane võti koos sees:

`keybase pgp import --infile K:\private\windowskasutaja\koos.asc`



Importimisel küsitakse ka salasõna kuna salajane võti koos avalikuga imporditakse:



... ning näidatakse koheselt ka kasutaja profiilis:

Kuid võib muidugi GPG-võtmepaari mistahes süsteemis (nt GNU/Linuxis) luua ja siis MS Windowsis importida. Oluline, et oleks uusima krüptoga ja soovitud sätetega, andmetega.

Võtmete turvaline hoidmine

Üks võimalus turvaliselt hoida on Keybase'i võrgukettal isiklikus kaustas nagu ka eespool näidatud. Või mõni teine rakendus, näiteks pilves – siinkohal peab veenduma, et valitud pilves andmed turvaliselt hoitud on. Soovitav on tundlikud andmed enne pilve panemist krüpteerida[20]. Kasulik on mitmes kohas hoida – kui ühte kohta ligi ei saa siis teise ikka saab. Näiteks krüpteeritult saab hoida ka välisel andmekandjal (mälupulk, väline ketas vms). Krüpteerimiseks võib kasutada näiteks VeraCrypt[21] rakendust (nõuab superkasutaja õigusi) vms analoogi[22].

Loodetavasti on salajane võti ka salasõnaga kaitstud – seega ei ole seda riski, et kui ka keegi saab salajase võtme failina kätte siis salasõna tal ikka ei ole ja kasutada ei saa.

Teine võimalus on kasutada mõnda turvalist ligipääsuandmete hoidmise rakendust: Bitwarden[23] (vt alternatiivid[24]), Lastpass[25] (vt alternatiivid[26]), jne. Tasub otsida ka alternatiive. Nimetatud rakendustes saab luua uue turvalise märkuse ja sinna siis võtme sisu kopeerida. Kuna võtmefailide puhul tegemist sisuliselt tekstiga siis saab seda edukalt ka eespool nimetatud rakendustes hoida.

20 https://alternativeto.net/software/cryptomator/
21 https://www.veracrypt.fr/en/Home.html
22 https://alternativeto.net/software/veracrypt/
23 https://bitwarden.com/
24 https://alternativeto.net/software/bitwarden--free-password-manager/
25 https://www.lastpass.com/
26 https://alternativeto.net/software/lastpass/

Pabervõti

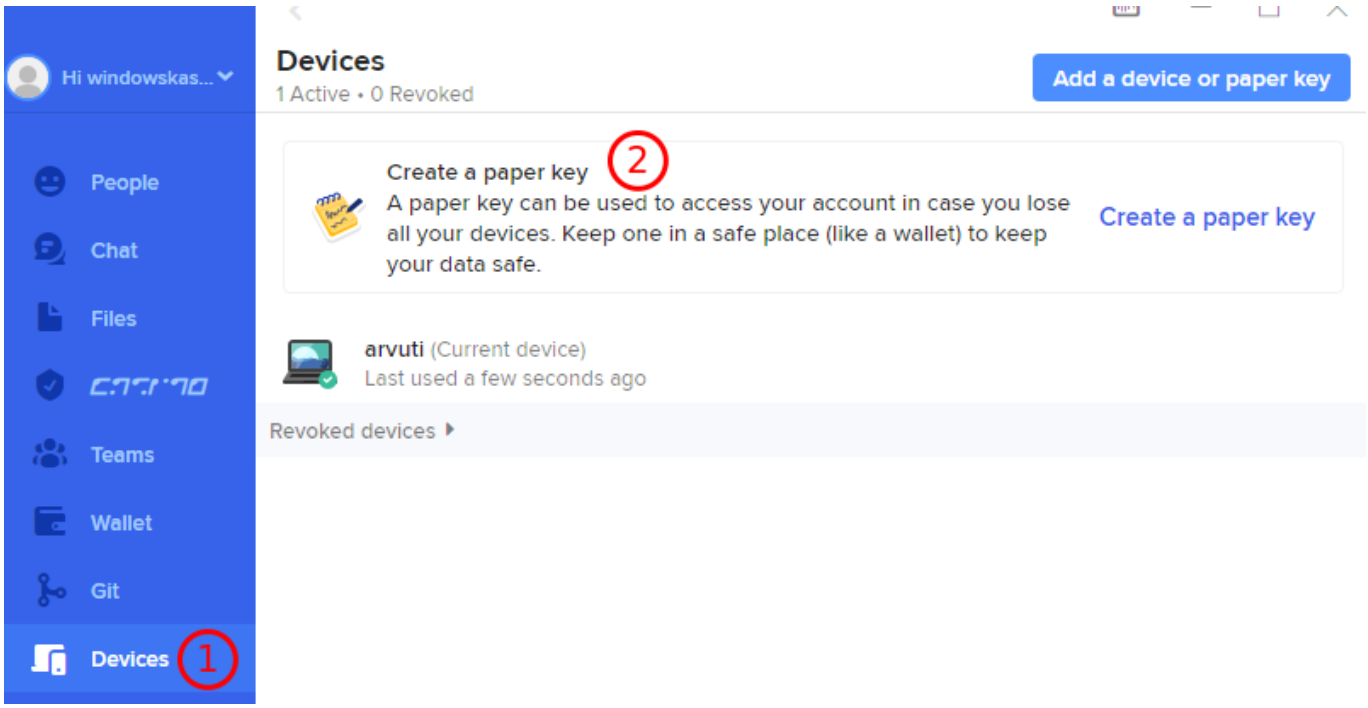
Üks oluline osa Keybase'ist on pabervõti[27]. See võimaldab hiljem oma kontole ligi saada kui Keybase on kõikidest varasematest seadmetest kustutatud või kui soovitakse teises seadmes lihtsamalt sisse logida. Lisaks muidugi teises seadmes sisse logida. Muidugi tuleks seda loodud pabervõtit identiteedivarguse vältimiseks väga turvaliselt hoida - sisuliselt on see konto taastamise võti (*recovery key*), mis võimaldab teie kontole täielikku ligipääsu. Kui pabervõtit ei ole siis vajalik Keybase'i poolt kasutatav PGP privaatne võti kõigepealt eksportida ja siis see eksporditud võti teise seadmesse kopeerida ja seal teise seadme käsureal importida Keybase'i, mida ei ole väga mugav teha (eriti nutiseadmetes).

Näiteks üks pabervõti:

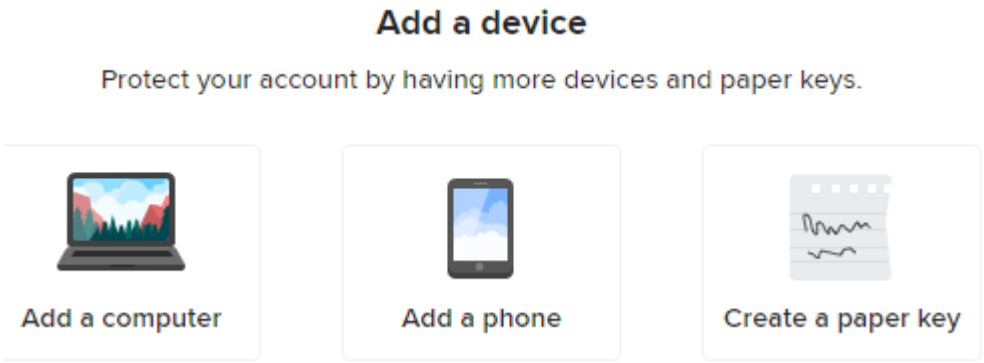
death punch correct staple battery horse clearly cherry picked words yeah moo car lisp

... ehk siis tegemist on pikema lausega sisuliselt. Üldiselt piisab ühe pabervõtme loomisest kuid võib ka mitu teha. Seda tuleb siis turvaliselt hoida, millest oli eelmises peatükis juttu.

Pabervõtme loomiseks avada *Devices -> Create a paper key*

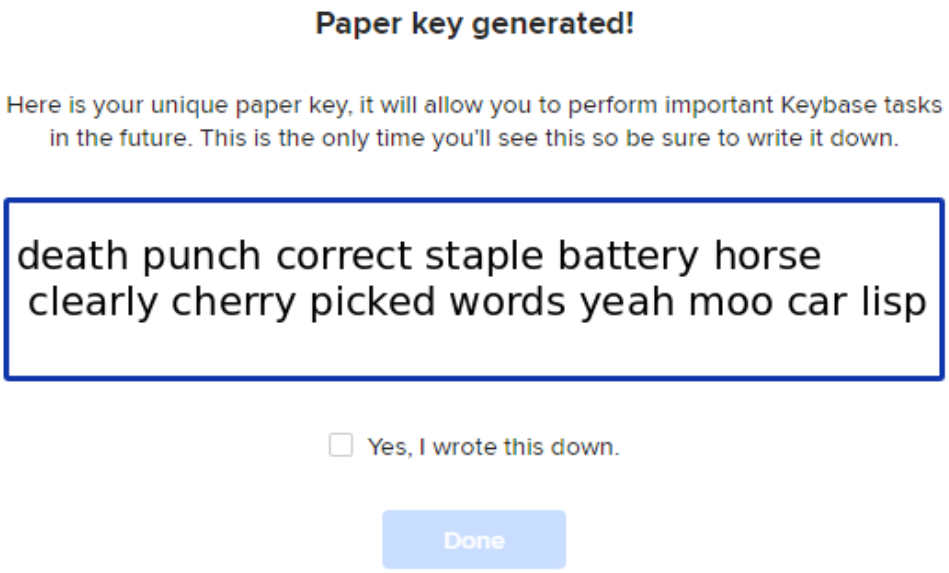


Seejärel saab omakorda kinnitada, mida soovitakse lisada. Pabervõtme lisamiseks valime *Create a paper key*:

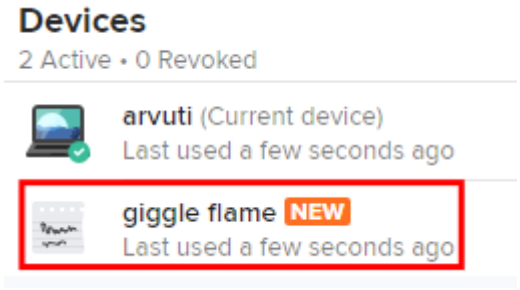


27 https://keybase.io/blog/keybase-new-key-model

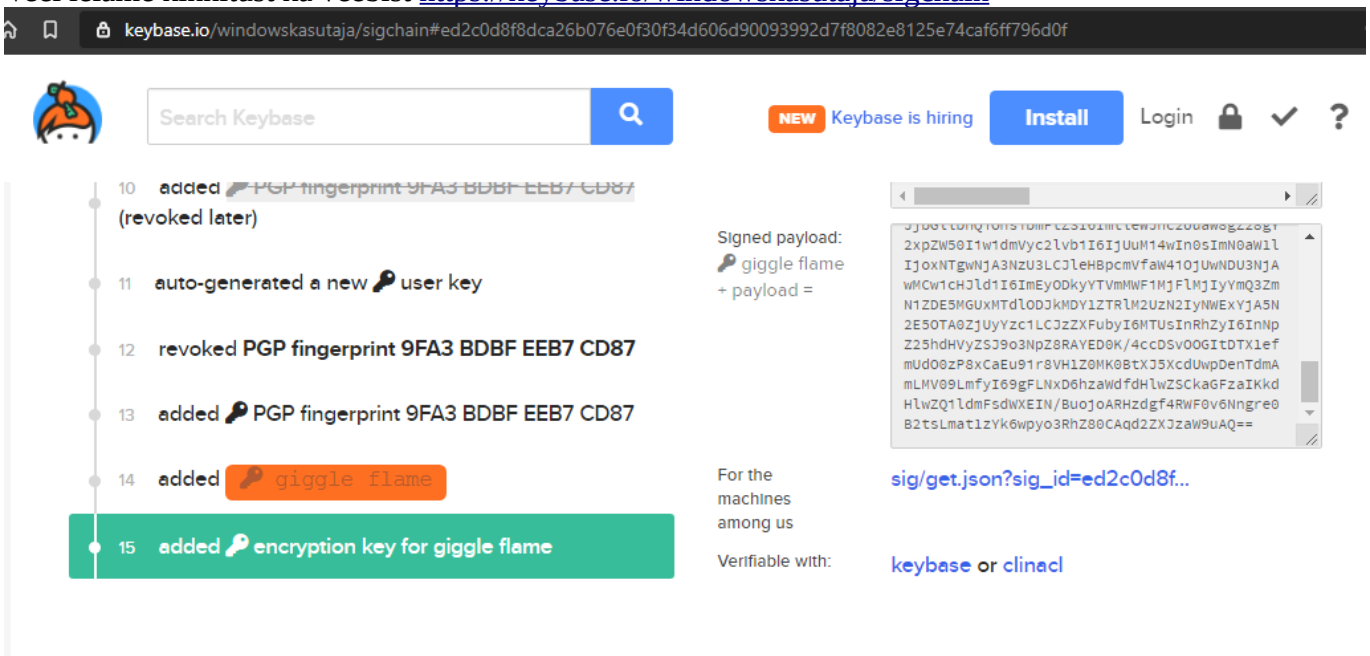
Seejärel näidatakse meile loodud pabervõtit:



Enne ei maksa kinnitada, et on reaalselt endale salvestatud (*Yes, I wrote this down*) kui seda reaalselt tehtud pole. Loodud pabervõtit saab sealt aknast ka kopeerida.
Seejärel leiame kinnituseks pabervõtme ka seadmete alt:



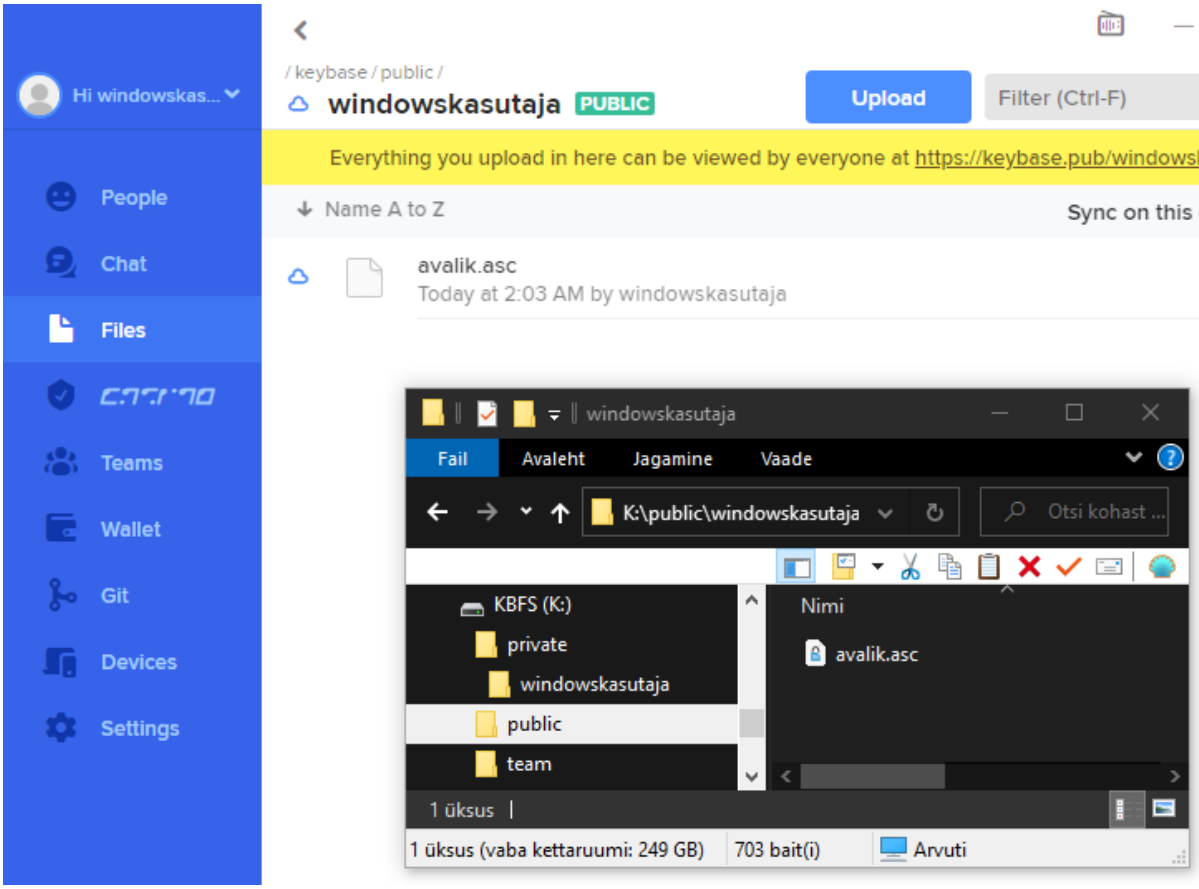
Veel leiame kinnitust ka veebist https://keybase.io/windowskasutaja/sigchain



Avaliku võtme levitamine

Kuna kasutasime ka allkirjastamise võimalust siis soovime seda ilmselt ka e-posti krüpteerimisel kasutada. Avalikesse võtmeserveritesse ei soovita oma avalikku võtit üles laadida – seda ei saa sealt pärast

ära kustutada, saab vaid tühistada ja see võib omakorda osutuda võimatuks kui tühistamise sertifikaati pole. Seetõttu on kõige lihtsam levitada seda ise, näiteks veebipõhiselt.



Siis avalik võti kättesaadav ka üle veebi https://keybase.pub/windowskasutaja/