

# Keybase

Koostanud: Edmund Laugasson  
TalTech IT Kollidži lektor



Käesolevat õppematerjali on lubatud jagada Creative Commons litsentsi CC BY-SA alusel:



Te peate viitama teose autorile samal kujul, nagu seda on teinud autor või litsentsiandja (kajastades kasutatud teose autori nime, kui see on teosel näidatud, teose nimetust, avaldamisallikat jms). Te ei tohi viidata teose autorile viisil, mis võib tekitada väärarusaama, et autor või litsentsiandja tõstavad teid või teie poolt teose kasutamist esile.



Kui te muudate või töötlete kõnesolevat teost või loote selle teose alusel tuletatud teose, siis te võite levitada tuletatud teost üksnes sama, samalaadse või ühilduva litsentsi alusel.

Lisateavet leiab Creative Commons'i veebilehtedelt:

- <http://www.creativecommons.ee/> - eesti keeles
- <http://creativecommons.org/> - inglise keeles

# Sisukord

Keybase.....	4
Paigaldamine.....	4
Veebilehitseja laiendusena.....	4
MS Windows.....	5
GNU/Linux.....	5
Ubuntu Linux.....	5
macOS.....	5
Android, iOS.....	6
Kasutajakonto loomine.....	6
Seadme registreerimine.....	6
Peale sisselogimist.....	7
Isiku tõestamine.....	7
Võrguketask.....	9
Võtmehaldus.....	10
Elliptilise krüptoga võtmepaar.....	14
Kleopatra (MS Windows).....	15
Elliptilise võtmepaari importimine Keybase'i.....	20
Võtmete turvaline hoidmine.....	22
Pabervõti.....	23
Avaliku võtme levitamine.....	24

# Keybase

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

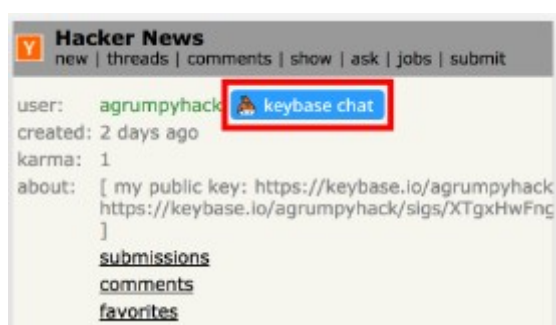
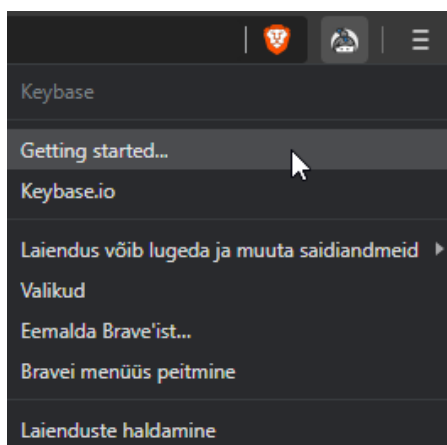
Lisaks tegemist sisuliselt pilvelahendusega: suur võrguketask (kasutatav nii arvutist kui nutiseadmest) + krüpteeritud versioonihaldus Git. Kirjeldav artikkel Keybase'ist on loodud ka IT Kolledži vikis<sup>6</sup>.

## Paigaldamine

Erinevate operatsioonisüsteemide jaoks on juhised Keybase'i kodulehel olemas<sup>7</sup>. 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<sup>8</sup> kaudu. Toetatud on ka kõik nende põhjal tehtud veebilehitsejad, nt Vivaldi<sup>9</sup>, Chromium<sup>10</sup>, Brave<sup>11</sup>, jne<sup>12</sup>. Suhtlemiseks tuleb kasutada oma profiilile lisatud veebikeskkonnades 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\\_\(software\)](https://en.wikipedia.org/wiki/Slack_(software))
- 3 [https://en.wikipedia.org/wiki/Discord\\_\(software\)](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\\_\(web\\_browser\)](https://en.wikipedia.org/wiki/Vivaldi_(web_browser))
- 10 [https://en.wikipedia.org/wiki/Chromium\\_\(web\\_browser\)](https://en.wikipedia.org/wiki/Chromium_(web_browser))
- 11 [https://en.wikipedia.org/wiki/Brave\\_\(web\\_browser\)](https://en.wikipedia.org/wiki/Brave_(web_browser))
- 12 [https://en.wikipedia.org/wiki/List\\_of\\_web\\_browsers](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 paigaldusjuhised MS Windowsile - [https://keybase.io/docs/the\\_app/install\\_windows](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 lisasätteid leiab `%appdata%\Keybase\`

## GNU/Linux

Juhised leiab [https://keybase.io/docs/the\\_app/install\\_linux](https://keybase.io/docs/the_app/install_linux) – paigaldamine toimub terminalis (käsuraal).

### 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 käsuraalt
```

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 Linux'i puhul toetatud
```

Kui APT<sup>13</sup> 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](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\\_\(software\)](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*



Join Keybase

[Create an account](#)

[Log in](#)

[Configure a proxy](#)

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 mõttes 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*)

Your phone number Skip




+372 Ex: 321 2345

Allow your friends to find you.

Continue

Your email address Skip



Email address

Allow friends to find you by this email address

Finish

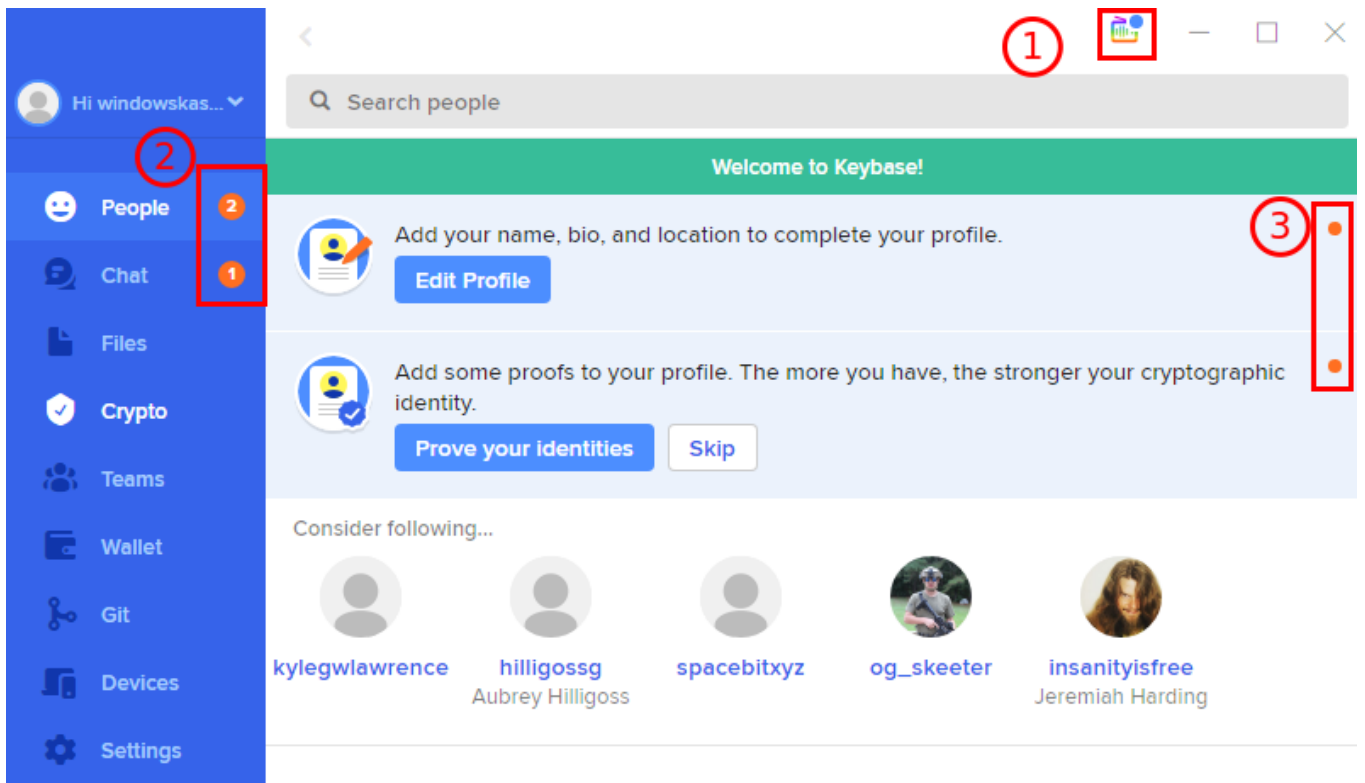
## Peale sisselogimist

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 usaldusväärsus (*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.



Hi windowskas... 1

Search people

Welcome to Keybase!

2 2 Add your name, bio, and location to complete your profile. 3

[Edit Profile](#)

1 1 Add some proofs to your profile. The more you have, the stronger your cryptographic identity.

[Prove your Identities](#) [Skip](#)

Consider following...

kyleglawrence hilligoss spacebityz og\_skeeter insanityisfree  
Aubrey Hilligoss Jeremiah Harding

The image shows a user profile for 'windowskasutaja' with 0 followers and 0 following. The profile includes a name, a bio, and a location field. To the right, the 'Edit Profile' sidebar contains fields for 'Full name', 'Bio', and 'Location'. Below the profile, there are buttons for 'Edit profile' and 'Chat'. A list of social media links is visible, including 'Prove your Twitter', 'Prove your GitHub', 'Prove your Reddit', 'Prove your Hacker News', 'Prove your website', 'Add a PGP key', 'Set a Bitcoin address', and 'Set a Zcash address'. A 'Save' button is located at the bottom right of the profile area.

Vajutades *Edit profile*, saab täiendavaid teavet lisada.

Esimene tervitus vestlusroboti poolt:

The image shows a chat window with 'Hello Bot'. The bot's message reads: "Hi, I'm Hello Bot. You can play puzzles with me or ask for help. Everyday is an adventure." Below this, the bot says: "Hi @windowskasutaja, I'm hellobot. I say hi to new people. As you can see above, this conversation is **encrypted**. This chat *looks normal*, but it is not. It is a garbled mess only you and I can read. Even if a MONSTER (👹) held a gun to the head of Keybase staff, your chats would remain private. So please take a look around. Keybase is great for small groups (friends and family), but also companies and communities. Don't slack when it comes to team security! Finally, I understand a few commands: "puzzle", "help", "flip", and "die"."

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

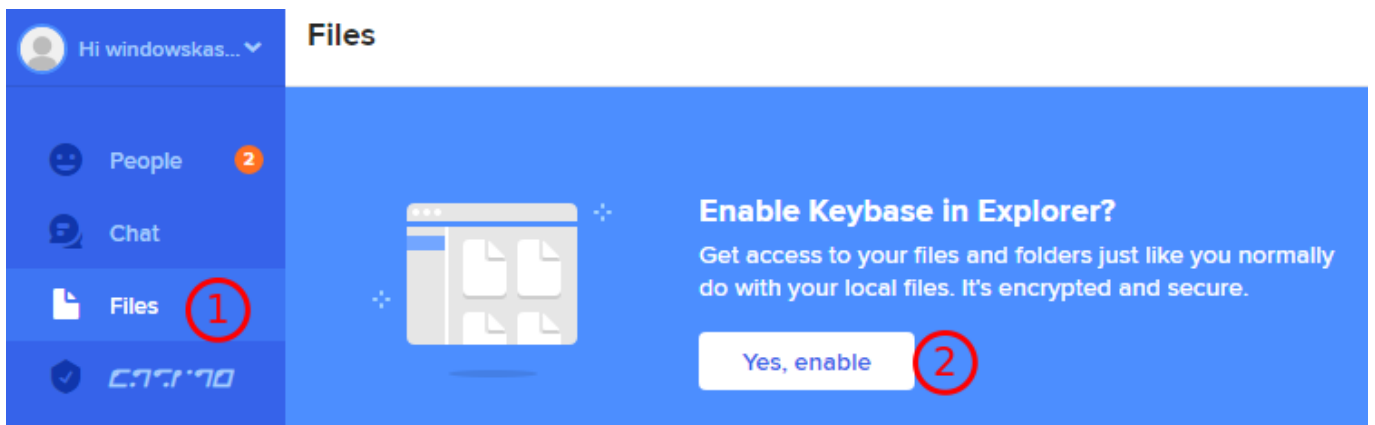
Olles avanud vastavas vaates (*People, Chat, Files, jne*) mõne valiku, jäetakse see meelde ja tagasi saab liikuda vastavate noolte abil

The image shows a close-up of a navigation bar. It features a search field with the text 'Search people' and a back arrow icon in the top left corner. Below the search field is a large circular profile picture placeholder.

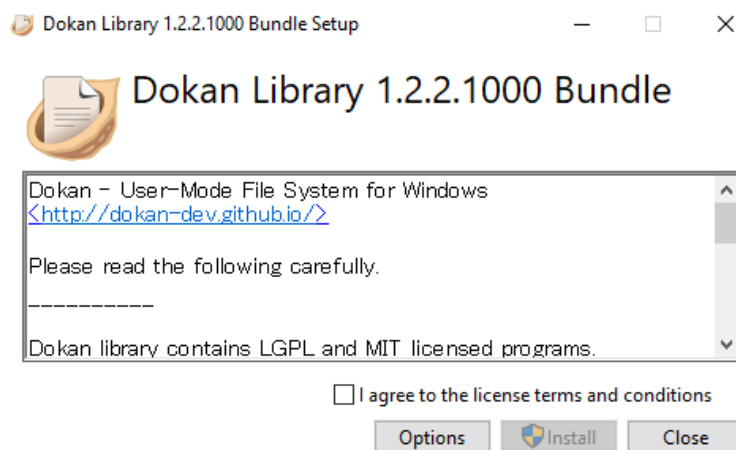


# Võrguketas

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*

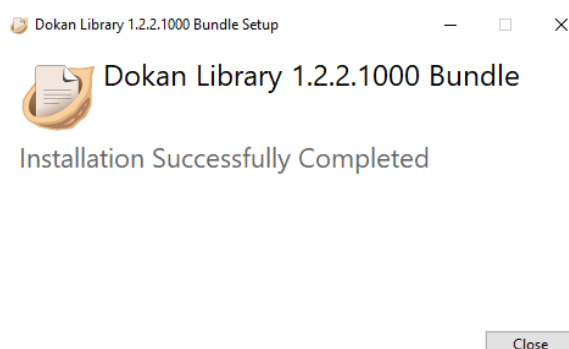


Seepeale käivitatakse Dokany teegi (*library*) paigaldus, jätkamiseks nõustuda litsentsi tingimustega (*I agree to the licence terms and conditions*)

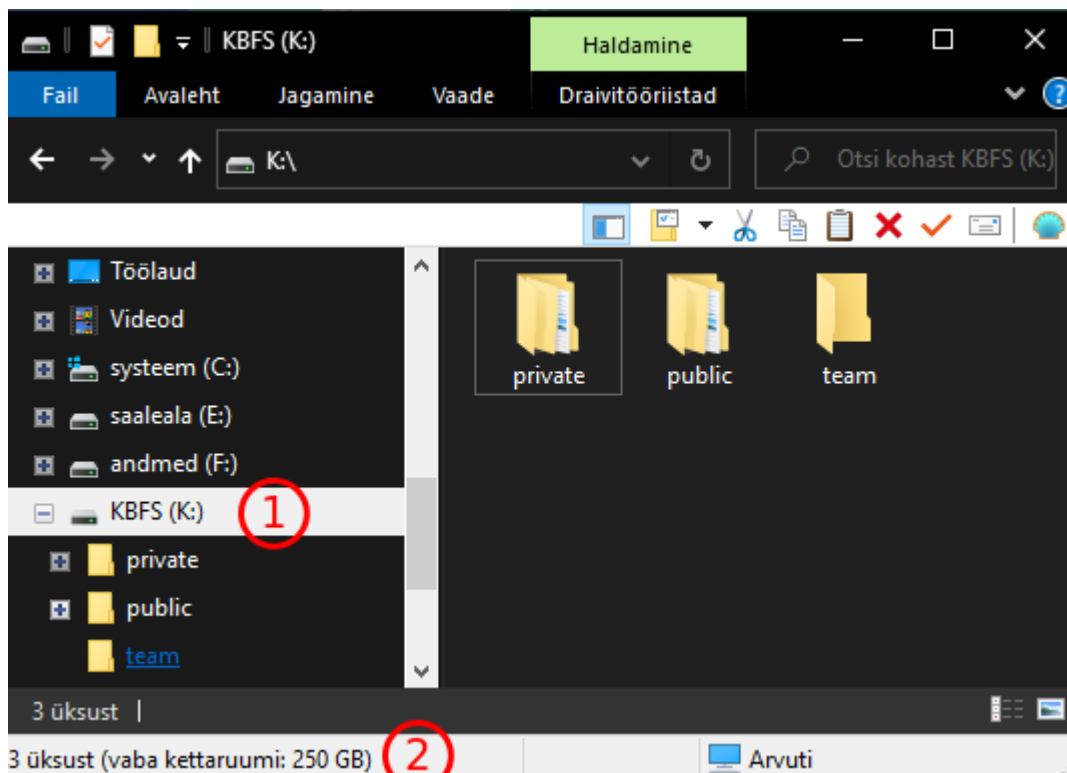


Vanemate MS Windowsi versioonidega võidakse ka arvuti taaskäivitust nõuda.

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*<sup>14</sup>.

*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<sup>15</sup>. 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 kasutajanimiga.

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

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

## Võtmehaldus

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

<sup>14</sup> <https://keybase.io/docs/kbfs>

<sup>15</sup> <https://keybase.io/docs/kbfs/keybase.pub>

Prove your Twitter  
Prove your GitHub  
Prove your Reddit  
Prove your Hacker News  
Prove your website  
Add a PGP key  
Set a Bitcoin address  
Set a Zcash address

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

#### Add a PGP key

**Get a new PGP key**  
Keybase will generate a new PGP key and add it to your profile.

**I have one already**  
Import an existing PGP key to your Keybase profile.

Cancel

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:

Fill in your public info.

Your full name  
|

Email 1

Email 2 (optional)

Email 3 (optional)

Include any addresses you plan to use for PGP encrypted email.

Cancel Let the math begin

**Luuakse 4096-bit RSA võti – seda ei ole soovitatav kasutada, pigem elliptilise krüptoga võti – soovitatav on jätkata peatükist [Elliptilise krüptoga võtmepaar](#).**



### Generating your unique key...

Math time! You are about to discover a 4096-bit key pair. This could take as long as a couple of minutes.



Cancel

Kui see valmis siis vastav teade:



### Here is your unique public key!

Your private key has been written to Keybase's local keychain. You can learn to use it with `keybase pgp help` from your terminal. If you have GPG installed, it has also been written to GPG's keychain.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
Comment: https://keybase.io/download  
Version: Keybase Go 5.2.0 (windows)  
  
xsFNBF42AZUBEADn4DUh025xEa+/zmtmBr4fDt4VGY60pwWlx+CIHKxp0wWk3H4x  
5nwTSGMiNn0XuMGIKs0nyu+BdhIE/HeOpAz80CAfQTyDf0qy4by0IamjmhV7l9te
```

Done

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:

4752 B01C 25AF F668@pgp

Prove your Twitter

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:

**windowskasutaja's public key**

fingerprint: FE35 74BD 1D91 7331 8034 ACF0 4752 B01C 25AF F668  
64-bit: 4752 B01C 25AF F668  
curl/raw: [this key](#) | [all their PGP keys](#)

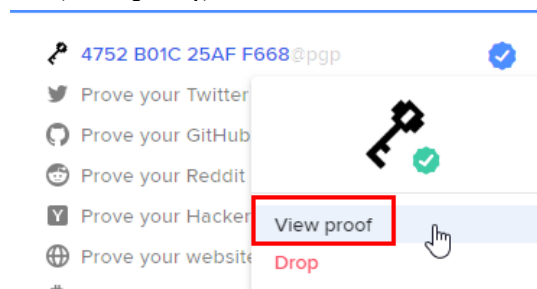
```
# curl + gpg pro tip: import windowskasutaja's keys
curl https://keybase.io/windowskasutaja/pgp_keys.asc | gpg --import

# the Keybase app can push to gpg keychain, too
keybase pgp pull windowskasutaja
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: https://keybase.io/download
Version: Keybase Go 5.2.0 (windows)

xsFNBf42AlsBEADomUu5V8IKbEYeHQ0X70j6+5Gx5hZSUkjDHbuNmY9Pn41RxD8g
GeVqgNYdy76ypvPAAxiXQN6Xhe6Mzi+jPas7AmjsqNgvmuKSmHt3DZKf4SiYvJL/
WIhz08H8YafuVeFRvt9cTRXmndQOo5VdtBhZqKkVvF3uIMQN+8dRPwYCXJgUugj1
DE/ww7W6SdqoscLGALSoa63eKwPNJq4r+kGcTtLwR+05OgEwPdcwppDJNjwRgkVS
tLTV2OZfx+TQK4qNU801588QoXeSbjeyX6D+3fFb53ofJXTRRHIp8fVE2opAbjrr
ti9mV77CMHHwpPDhvxskmfu+7cIokvEuQYHYi+Jw7L2A8umK04naR87eQ+A+dQO5
```

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

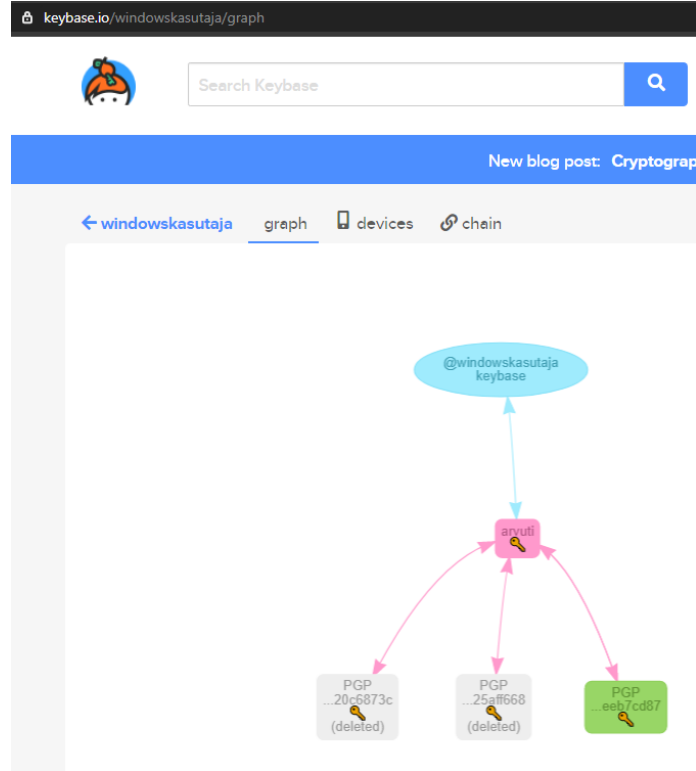


... siis avatakse vastav koht veebis <https://keybase.io/windowskasutaja/sigchain> kus kõik sammud näha:

[← windowskasutaja](#)   graph   devices   chain

- 1 created fresh Keybase account, adding first key arvuti
- 2 added encryption key for arvuti
- 3 auto-generated a new user key
- 4 added PGP fingerprint F8A6 C14E 20C6 873C (revoked later)
- 5 auto-generated a new user key
- 6 revoked PGP fingerprint F8A6 C14E 20C6 873C
- 7 added PGP fingerprint 4752 B01C 25AF F668**

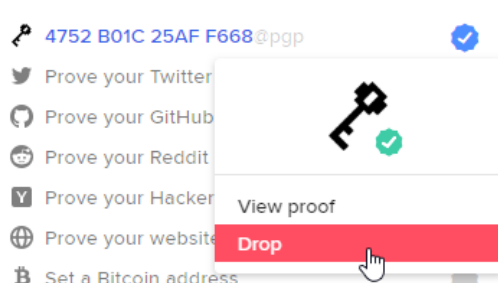
See on kõik ka graafiliselt <https://keybase.io/windowskasutaja/graph> aadressil näha



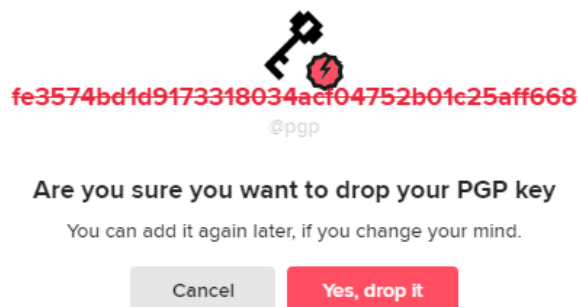
## Elliptilise krüptoga võtmepaar

Siiski ei ole soovitatav RSA võtit enam kasutada – pigem luua elliptilise krüpto abil endale võtmepaar. RIA pakub oma uuringute lehel<sup>16</sup> 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<sup>17</sup> siis tuleb sellega kaasa ka rakendus Kleopatra, millega saab juba ka elliptilise krüptoga uue võtmepaari luua.

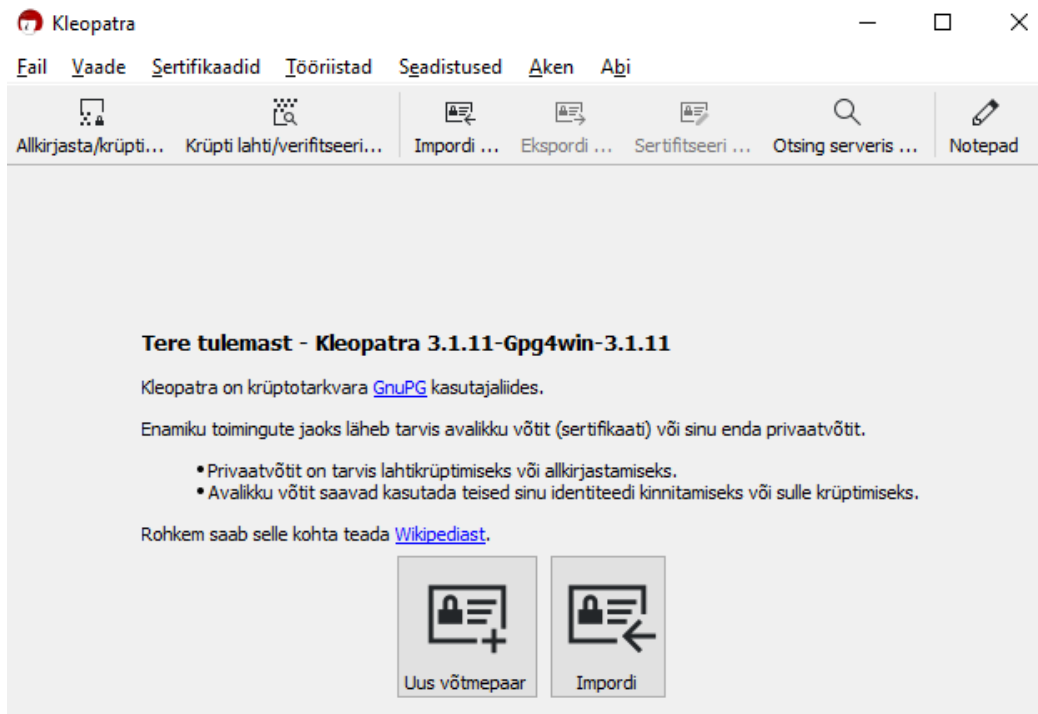
<sup>16</sup> <https://www.ria.ee/et/ametist/uuringud-analuusid-ulevaated.html>

<sup>17</sup> <https://www.gpg4win.org/>

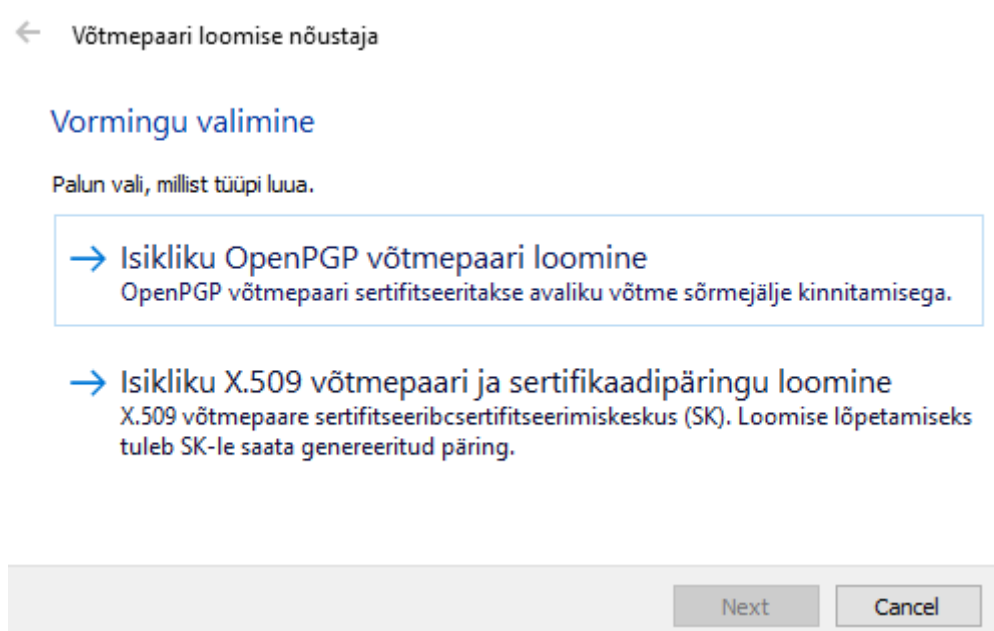
## Kleopatra (MS Windows)

Kinnitamata andmeil on turvakaalutlustel soovitatav võtmepaar luua käsureal rakendusega GPG<sup>18</sup>. Näidiseks 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:

<sup>18</sup> <https://wiki.itcollege.ee/index.php/GPG>

← Võtmepaari loomise nõustaja

## Üksikasjad

Palun sisesta allpool enda kohta käivad andmed. Kui soovid parameetreid täpsemalt määrata, klõpsa nupule Muud seadistused.

Nimi:  (pole kohustuslik)  
E-post:  (pole kohustuslik)

Windowsi kasutaja <c4bcc969-7f02-4fe1-9456-c7622c65ff58@anonaddy.me>

[Muud seadistused...](#)

[Next](#)

[Cancel](#)

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

**Muud seadistused - Kleopatra**

Tehnilised üksikasjad

Võtme olemus

RSA

+ RSA

DSA

+ Elgamal

ECDSA/EdDSA

+ ECDH

Sertifikaadi kasutamine

Allkirjastamine  Sertifitseerimine

Krüptimine  Autentimine

Kehtiv kuni:

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 tülilikaks osutada ja sageli on lihtsam eraldi SSH võtmepaari kasutada, mida ka elliptilise krüpto põhjal saab luua. Kehtivusaega ei pea määrama – siis saab võtit piiramatult aega kasutada.

Enne lõplikku võtmepaari loomist vaadata üle valitud sätteid:



## Parameetrite ülevaade

Palun vaata enne jätkamist hoolikalt üle kõik parameetrid.

Nimi:	Windowsi kasutaja
E-posti aadress:	c4bcc969-7f02-4fe1-9456-c7622c65ff58@anonaddy.me
Võtme tüüp:	EdDSA
Võtme kõver:	ed25519
Kasutamine:	Krüptimine, Allkirjasta
Alamvõtme tüüp:	ECDH
Võtme kõver:	cv25519
Alamvõtme kasutamine:	Krüptimine

Näita kõiki üksikasju

Loo

Cancel

Küsitakse veel salasõna:

The screenshot shows a window titled "pinentry-qt" with a lock icon. The text inside says "Please enter the passphrase to protect your new key". There are two input fields: "Passphrase:" and "Repeat:", both containing masked characters. A "Quality:" indicator shows a green bar at "100%". There are "OK" and "Cancel" buttons at the bottom.

Seejärel eduka võtmepaari loomise järel ka vastav teade:

## Võtmepaar on edukalt loodud

Sinu uus võtmepaar on edukalt loodud. Allpool näeb üksikasju ja mõningaid soovitusi edasiseks.

### Tulemus

Võtmepaar on edukalt loodud.  
Sõrmejalg: FFF7DECA12CD27B11B8E20069FA3BDBFEEB7CD87

### Järgmised sammud

Tee oma võtmepaarist varukoopia...

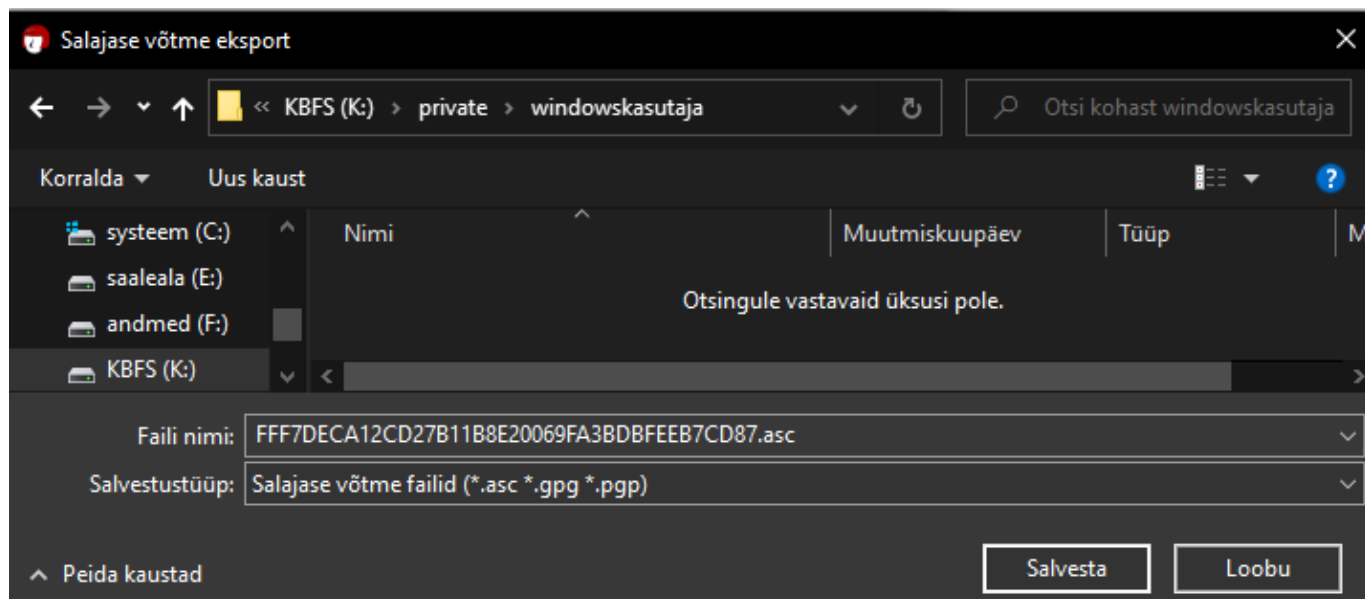
Saada avalik võti e-kirjaga...

Laadi avalik võti kataloogiserverisse...

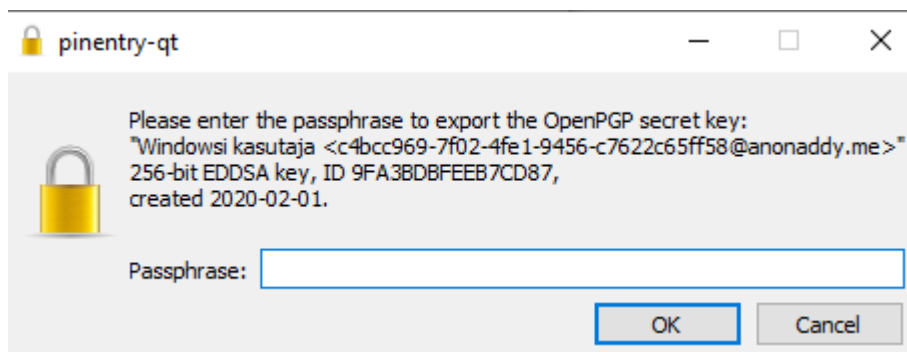
Finish

Cancel

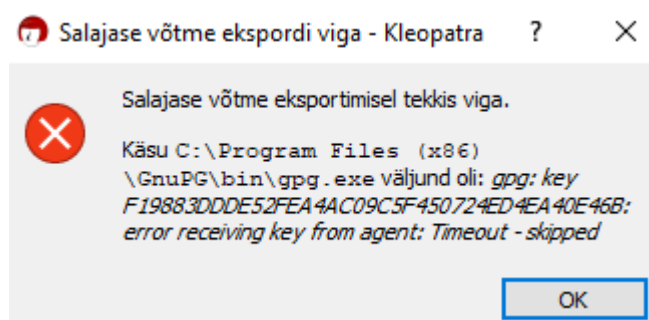
Enne *Finish* nupule vajutamist on soovitatav vajutada ka nupule *Tee oma võtmepaarist varukoopia...* ja näiteks oma isiklikku kataloogi Keybase'i võrgukettal turvaliselt salvestada:



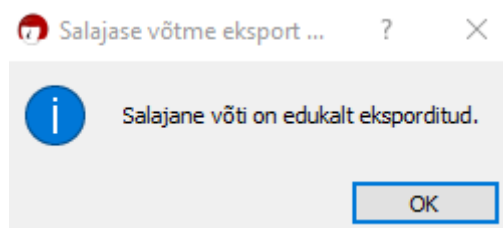
Salajase võtme eksportimisel küsitakse ka salasõna (mis loodetavasti oli määratud):



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



Edukalt 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-----
```

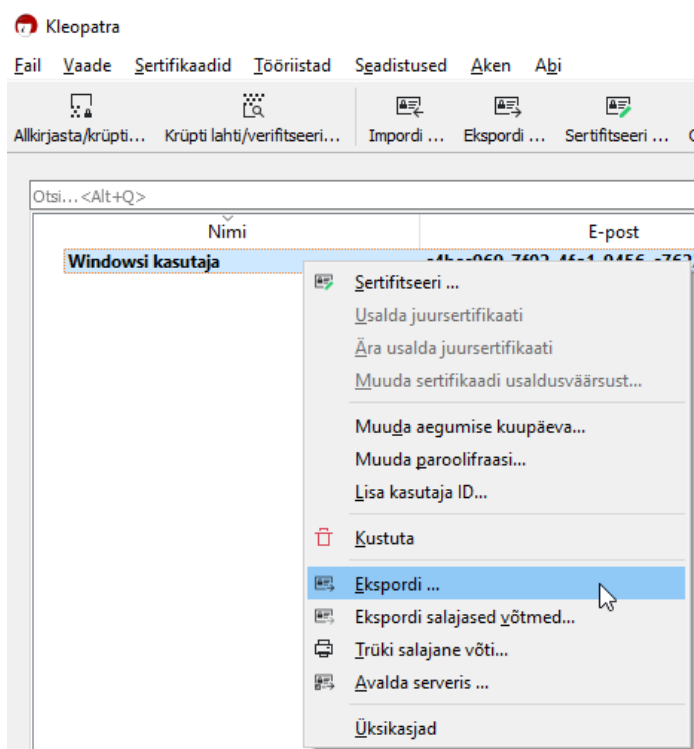
üks tühi rida

<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:

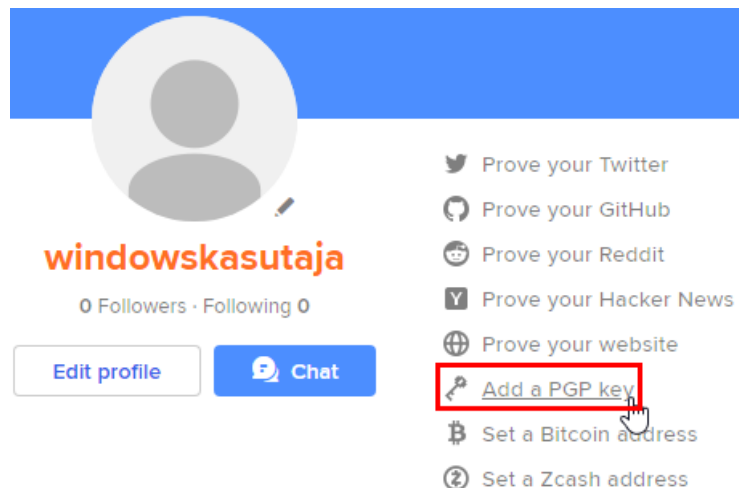
- luua uus tekstifail (Notepad vms palja teksti<sup>19</sup> redaktori abil), mille tüübiks määrata faili salvestamisel .asc
- esmalt avalik võti
- üks tühi rida vahet
- salajane võti
- lõpus üks tühi rida

19 [https://en.wikipedia.org/wiki/Plain\\_text](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:



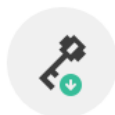
Taas võimalus luua uus võtmepaar (*Get a new PGP key*) või importida olemasolev (*I have one already*):

### Add a PGP key



#### Get a new PGP key

Keybase will generate a new PGP key and add it to your profile.



#### I have one already

Import an existing PGP key to your Keybase profile.

Cancel

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

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



## Import a PGP key

To register your existing PGP public key on Keybase, please run the following command from your terminal:

```
# import a key from gpg's key chain
keybase pgp select

# for more options
keybase pgp help
```

Cancel

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**

```
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:

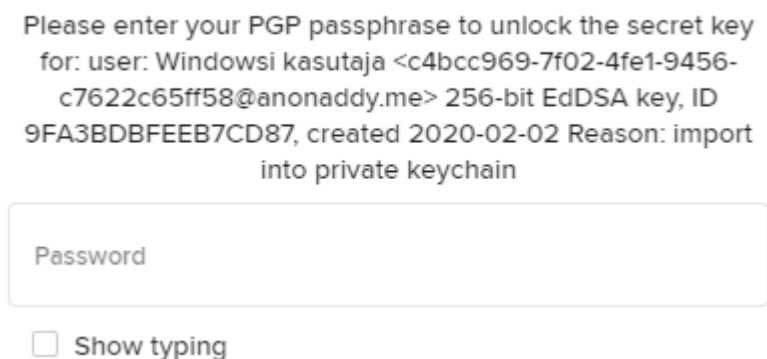
 9FA3 BDBF EEB7 CD87@pgp

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

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

```
C:\ Käsuviipl  
F:\kasutajad\student>keybase pgp import --infile K:\private\windowskasutaja\koos.asc  
- 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
```

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<sup>20</sup>. Kasulik on mitmes kohas hoida – kui ühte kohta ligi ei saa siis teise ikka saab. Näiteks krüpteeritult saab hoida ka välisel andmekandjal (mäluvulk, väline ketas vms). Krüpteerimiseks võib kasutada näiteks VeraCrypt<sup>21</sup> rakendust (nõuab superkasutaja õigusi) vms analoogi<sup>22</sup>.

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<sup>23</sup> (vt alternatiivid<sup>24</sup>), Lastpass<sup>25</sup> (vt alternatiivid<sup>26</sup>), 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

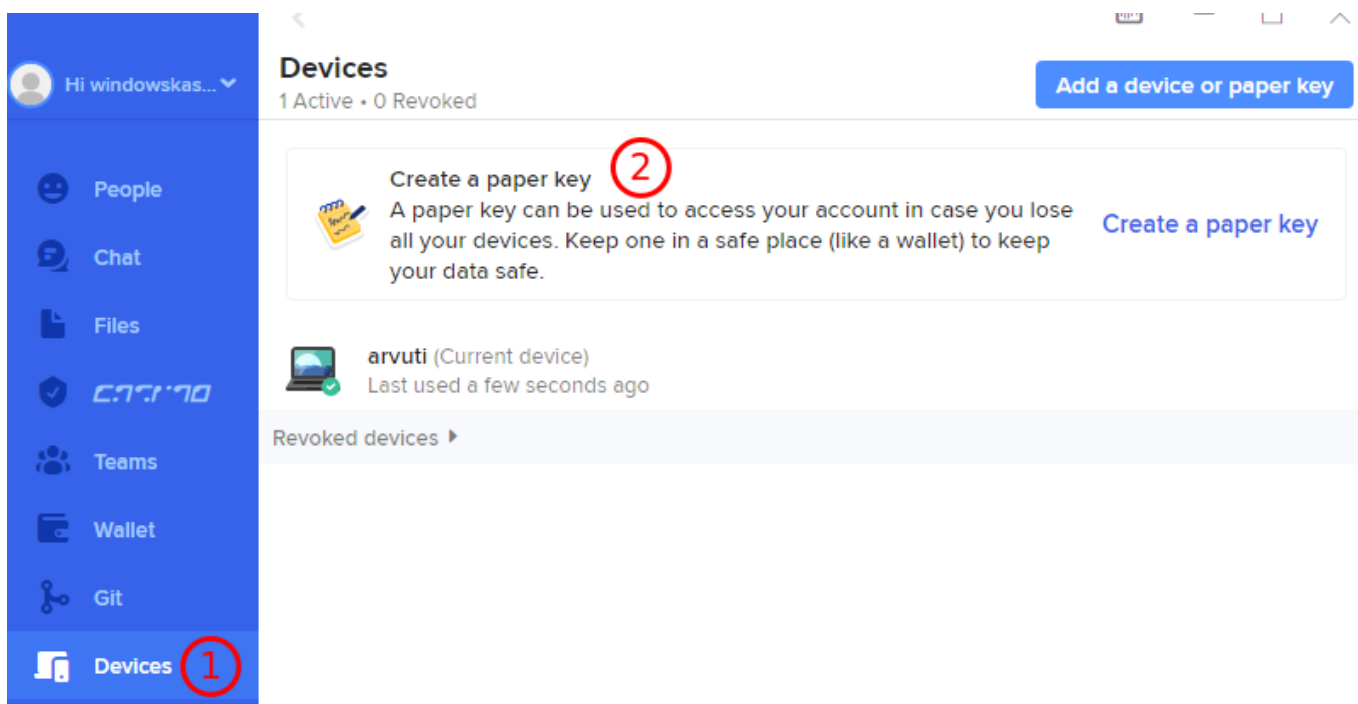
Üks oluline osa Keybase'ist on pabervõti<sup>27</sup>. See võimaldab hiljem oma kontole ligi saada kui Keybase on kõikidest varasematest seadmetest kustutatud või kui soovitakse teises seadmes lihtsamalt sisse logida. Lisaks muidugi teises seadmes sisse logida. Muidugi tuleks seda loodud pabervõtit identiteedivarguse 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 ekspordida ja siis see eksporditud võti teise seadmesse kopeerida ja seal teise seadme käsuraal importida Keybase'i, mida ei ole väga mugav teha (eriti nutiseadmetes).

Näiteks üks pabervõti:

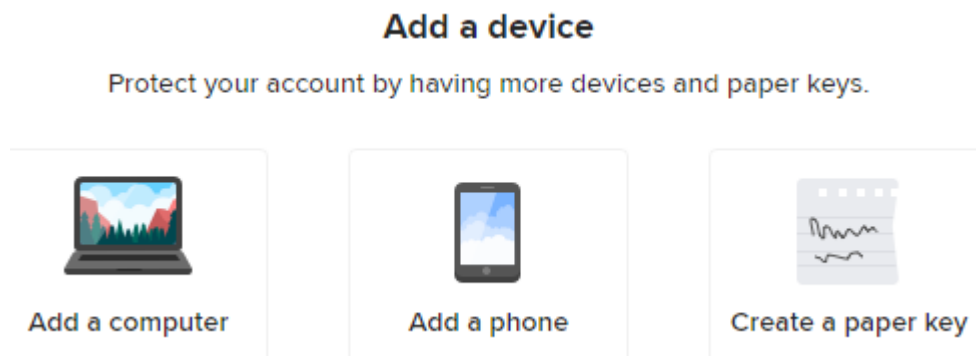
***death punch correct staple battery horse clearly cherry picked words yeah moo car lisp***

... 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*:



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

Seejärel näidatakse meile loodud pabervõtit:

## Paper key generated!

Here is your unique paper key, it will allow you to perform important Keybase tasks in the future. This is the only time you'll see this so be sure to write it down.

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

Yes, I wrote this down.

Done

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:

### Devices

2 Active • 0 Revoked



arvuti (Current device)

Last used a few seconds ago



giggle flame **NEW**

Last used a few seconds ago

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

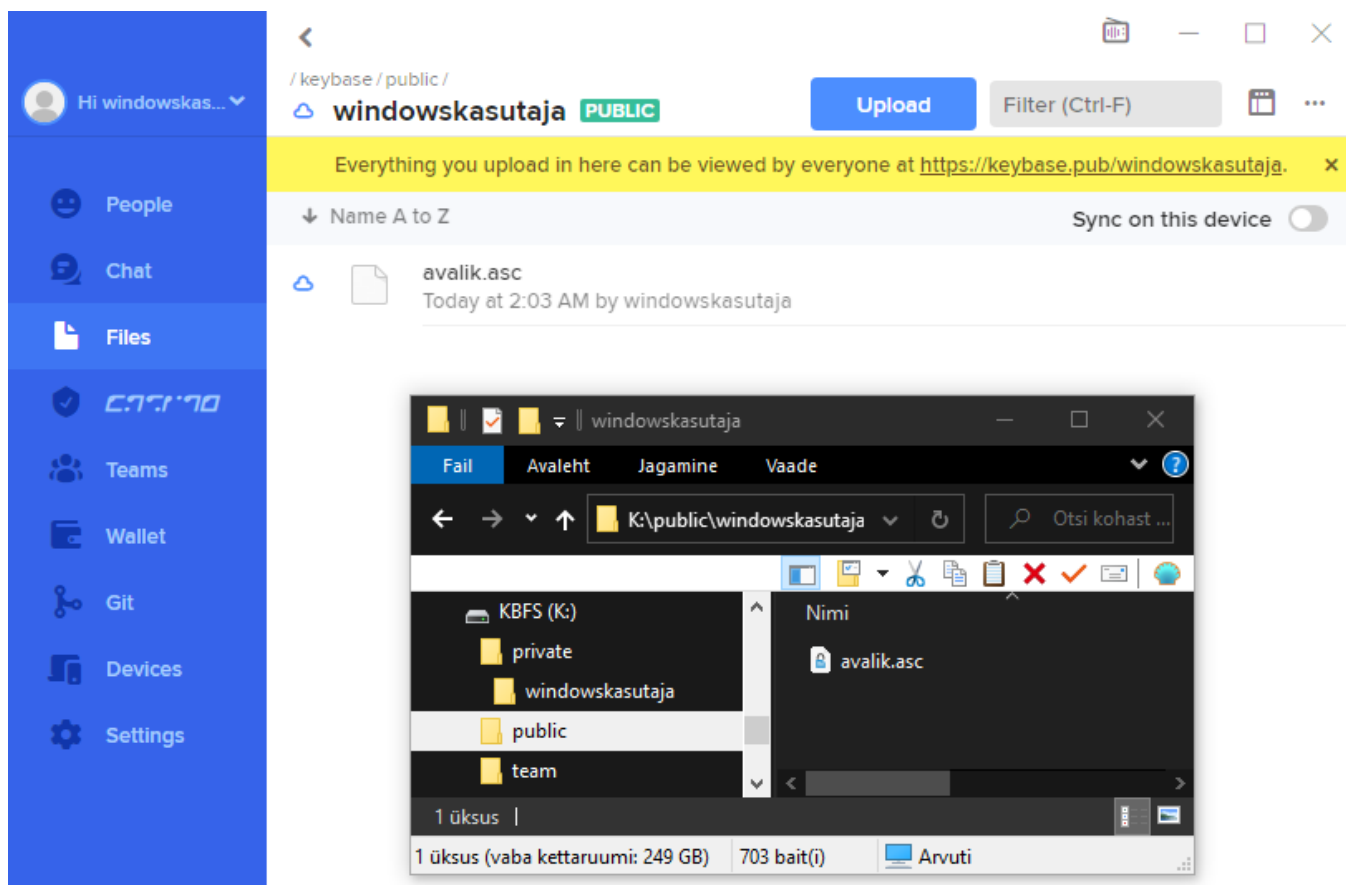
The screenshot shows the Keybase website interface. At the top, there is a search bar and navigation links for 'Keybase is hiring', 'Install', 'Login', and a lock icon. The main content area displays a 'sigchain' for the user 'giggle flame'. The chain consists of 15 items, with the most recent one (item 15) highlighted in green: 'added encryption key for giggle flame'. To the right of the chain, there is a section for 'Signed payload:' showing the key 'giggle flame' and a long alphanumeric string. Below this, it says 'For the machines among us' and 'Verifiable with: keybase or clinac!'. There is also a link 'sig/get.json?sig\_id=ed2c0d8f...'.

## 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 osutada 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/>

