

# Linux käyttöjärjestelmiä ja niiden asennus- ja käyttöönotto-ohjeita

*Windows 10 tietokoneiden tekninen tuki päättyi 14.10.2025. Jos sinun Windows 10 koneesi täytää Windows 11 teknisiä vaatimuksia, se ei päivity automaattisesti Windows 11:een. Näistä tärkeimmät vaatimukset ovat: 64 bittinen, uefi -tuki, TPM 2.0 turvapiiri ja vähintään 7. sukupolven prosessori, kts. tarkemmin: <https://www.microsoft.com/fi-fi/windows/windows-11-specifications> Microsoft saattaa ilmoittaa myös Suomen markkinoille Win10:n koneiden teknisen tuen maksullisesta jatkamisesta ja sen ehdoista.*

*Vaihtoehtoina on jatkaa Windows 10:n käyttöä ilman teknistä tukea ja suojausta, heivata kone kaatopaikalle tai asentaa siihen Windowsin paikalle Linux käyttöjärjestelmä.*

*Jos haluat jatkaa koneen käyttöä turvallisesti, asenna siihen maksuton Linux käyttöjärjestelmä. Jos jostain muusta syystä Linux kiinnostaa, niin asenna koneellesi Linux ja koet eron. Lue nämä ohjeet, niin voit itse asentaa koneelle Linux käyttöjärjestelmän ja osaat hakea apua Linuxin asentamiseen ja käyttöön.*

*Jos herää kysymys mistä tahansa tähän liittyvästä asiasta, ota siitä selvää **ennen**, kuin ryhdyt varsinaiseen ohjelmistojen lataukseen ja/tai asennukseen.*

## Sisältö:

### 0.1 Yleistietoa Linux käyttöjärjestelmistä

### 0.2 Tiedot omasta koneestasi

1. Linkkejä 64 bittisten Linux käyttöjärjestelmien suomen- tai englanninkielisiin esittelyihin sekä 32 bittisten Linux käyttöjärjestelmien englanninkielisiin esittelyihin

2.0 Linkkejä Ubuntu ja Linux Mint käyttöjärjestelmien / -jakeluiden suomenkielisiin asennusohjeisiin

2.1 Ubuntu

2.2 Linux Mint

2.3 Asennustikut

2.4 Käyttöjärjestelmän perusasennus

2.5 Perusasennuksen jälkeen tehtävät lisäasennukset ja -asetukset

3. Tehtäviä kaikkien asennusten ja asetusten jälkeen - tietoturvan ylläpitämiseksi

4. Lopuksi

5. Windows 11 + Linux kaksoiskäyttö- ja monikäyttöjärjestelmät (dual boot ja multi boot)

6. Linux + Linux kaksoiskäyttö- ja monikäyttöjärjestelmät (dual boot ja multi boot)

7. Lisäoppaat – pyydä s-postitse

\* Liitteet: LUKS -salausavainten muuttaminen Liite 1; lisääminen Liite 2 sekä poistaminen Liite 3

## 0.1 Yleistietoa Linux käyttöjärjestelmistä:

Suomeksi:

**Yle Digitreenit:** <https://yle.fi/aihe/a/20-299831>

<https://ubuntu-fi.org/esittely/miksi-kayttaisin-linuxia/>

<https://fi.wikipedia.org/wiki/Linux> ja [https://fi.wikibooks.org/wiki/Ubuntu\\_tutuksi/Linux](https://fi.wikibooks.org/wiki/Ubuntu_tutuksi/Linux)

<https://www.mikrobitti.fi/uutiset/linux-jakelut-2024-mika-on-paras-linux/3d2a3363-0804-44d5-8805-8387de67e70c>

Englanniksi:

\* Linux järjestelmien (distribution, jakeluiden) 'kehityspuu' ja linkit kunkin 'oksan' omalle Wikipedia- sivuille:

[https://en.wikipedia.org/wiki/Template:Linux\\_distributions](https://en.wikipedia.org/wiki/Template:Linux_distributions)

\* Eri Linux – jakeluiden lyhyt kuvaus ja linkit jakeluiden virallisille kotisivuille:

<https://distrowatch.com/>

## 0.2 Tiedot omasta koneestasi

Kaikki perustiedot:

<https://tecnobits.com/fi/Kuinka-tiet%C3%A4%C3%A4%C2%80C-onko-tietokoneeni-32--vai-64-bittinen/>

### 0.2.1 Onko koneeni 32 vai 64 bittinen ?

<https://support.microsoft.com/fi-fi/windows/32-ja-64-bittinen-windows-usein-kysytyt-kysymykset-c6ca9541-8dce-4d48-0415-94a3faa2e13d>

<https://mundobytes.com/fi/Kuinka-tiet%C3%A4%C3%A4%C2%80C-onko-tietokoneessasi-Windows-11-32--vai-64-bittinen-yksinkertaisia-%E2%80%8B%E2%80%8B%E2%80%8B%E2%80%8Bmenetelmi%C3%A4/>

### 0.2.2 Tukeeko koneeni BIOS moodi **legacy** vai **EFI** käynnistystä ?

Windows 10 koneen BIOS mode (eli onko se legacy vai efi tuettu kone) voidaan tarkistaa tällä ohjeella, jos asiakkaan Windows 10 toimii:

<https://www.tenforums.com/tutorials/85195-check-if-windows-10-using-uefi-legacy-bios.html>

Katso ao. kuva:

#### To Check if Windows 10 is using UEFI or Legacy BIOS in System Information

- 1 Press the **Win** + **R** keys to open Run, type **msinfo32** into Run, and click/tap on **OK** to open System Information.
- 2 In the right pane of **System Summary** in System Information, see if the **BIOS Mode** item has a value of **Legacy** or **UEFI**.

### 0.2.3 Muut perustiedot: löytyvät Windows → Asetukset → Järjestelmä -polun kautta.

0.2.4 Windows 11 + Linux kaksoiskäyttö- ja monikäyttöjärjestelmät (dual boot ja multi boot) → kts kohta 5. sekä Linux + Linux kaksoiskäyttö- ja monikäyttöjärjestelmät (dual boot ja multi boot) → kts kohta 6.

## **1.0 Linkkejä 64 Linux käyttöjärjestelmien /-jakeluiden (distributions) suomen – tai englannin kielisiin esittelyihin sekä 32 bittisten Linux käyttöjärjestelmien /-jakeluiden (distributions) englanninkielisiin esittelyihin**

Tässä yksi listaus (arvaus) suosituimmista Linuxeista 2025 <https://itsfoss.com/best-linux-distributions/?ref=news.itsfoss.com>.

Kuten näet sivustolta <https://distrowatch.com/> , eri Linux järjestelmiä on monenlaisia moneen eri tarpeeseen. Tässä tämän kirjoittajan testaamia yleiskäyttöön sopivia ja suosittuja Linux käyttöjärjestelmiä, joilla kaikilla on perusasennusta helpottava graafinen asennustyökalu:

### **1.1 Suosituimmat ja helposti asennettavat Debian pohjaiset 64 bittiset yleiskäyttöön hyvin sopivat käyttöjärjestelmät ovat Ubuntu ja Linux Mint (sivut suomeksi).**

1.1.1 **Ubuntu:** <https://ubuntu-fi.org/> ja [https://fi.wikibooks.org/wiki/Ubuntu\\_tutuksi](https://fi.wikibooks.org/wiki/Ubuntu_tutuksi)

1.1.2 **Linux Mint:** <https://www.linuxmint.com/> ja <https://fi.101-help.com/linux-mint-aloittelijan-opas-ja-ammattilaisvinkkejä-a7532ee48c/> sekä 'Linux-sauna' -ryhmän, Tampere, opas: <https://linux.blogaaja.fi/linux/> ja neuvova ryhmä <https://t.me/linuxsauna>

### **1.2 Suositut ja helpohkosti asennettavat openSUSE Enterprise Linux pohjaiset 64 bittiset yleiskäyttöön hyvin sopivat käyttöjärjestelmät (sivut suomeksi ja englanniksi):**

1.2.1 **openSuse Leap:** <https://www.opensuse.org/> ja <https://www.opensuse.org/#Leap>

1.2.2 **openSUSE Tumbleweed:** <https://www.opensuse.org/> ja <https://www.opensuse.org/#Tumbleweed>

ja suomenkielinen foorumi: <https://opensuse.fi/keskustelu/index.php>

### **1.3 Suosituimmat ja helpohkosti asennettavat Red Hat Enterprise Linux /Fedora pohjaiset 64 bittiset yleiskäyttöön hyvin sopivat käyttöjärjestelmät (sivut vain englanniksi):**

1.3.1 **Fedora:** <https://fedoraproject.org/>

1.3.2 **Alma Linux:** <https://almalinux.org/>

### **1.4 Suosituimmat ja helpohkosti asennettavat Arch Linux pohjaiset 64 bittiset yleiskäyttöön hyvin sopivat käyttöjärjestelmät (sivut vain englanniksi):**

1.4.1 **Manjaro:** <https://manjaro.org/>

1.4.2 **Endeavour OS:** <https://endeavouros.com/>

### **1.5 Tässä 2 helpohkosti asennettavaa Debian pohjaista 32 bittistä yleiskäyttöön hyvin sopivaa järjestelmää (sivut vain englanniksi):**

1.5 **Linux Mint Debian Edition**

<https://itsfoss.com/32-bit-linux-distributions/> ja [https://www.linuxmint.com/download\\_lmde.php?ref=its-foss](https://www.linuxmint.com/download_lmde.php?ref=its-foss)

### 1.5.2 AntiX-Linux

<https://itsfoss.com/32-bit-linux-distributions/> ja <https://antixlinux.com/?ref=its-foss> ja <https://antixlinux.com/download/>

## 2.0 Linkkejä Ubuntu ja Linux Mint käyttöjärjestelmien / -jakeluiden suomenkielisiin asennusohjeisiin:

**2.1 Ubuntu:** <https://ubuntu-fi.org/ohjeet-ja-tuki/asentaminen/>

Huom. Ubuntulle on tarjolla **3 erilaista työpöytää**: **Gnome** (Ubuntu; <https://ubuntu-fi.org/lataa-ubuntu/>) **KDE Plasma** (Kubuntu; <https://kubuntu.org/>) ja **Xfce** (Xubuntu; <https://xubuntu.org/>). Näistä **Xfce** on lähinnä Windows 10:n työpöytää.

**2.2 Linux Mint:** <https://fi.101-help.com/linux-mint-aloittelijan-opas-ja-ammattilaisvinkkejä-a7532ee48c> → kts. kohta → 'Linux Mintin asentaminen'

Huom. Linux Mintille on tarjolla **3 erilaista työpöytää**: **Cinnamon**, **Xfce** ja **Mate** ( kaikki nämä: <https://www.linuxmint.com/download.php> ). Näistä **Cinnamon** tai **Xfce** ovat eniten Windows 10:n työpöydän kaltainen.

## 2.3 Asennustikut:

**2.3.1 Lataa** halutun Linux käyttöjärjestelmän ja sen halutun työpöydän **levykuva** (kts 2.0) eli **.iso tiedosto**, koneen omalle kovalevyille tai -mieluiten - ulkoiselle kovalevyille/tikulle. **Älä lataa iso -tiedostoa mistään muualta kuin ko. järjestelmän kotisivuilta**. Kunkin Linux -jakelun kotisivut löytyvät osoitteesta <https://distrowatch.com/> . Latauksen virheettömyyden voit tarkistaa sha256sum -testillä, jonka ohjeet saat kunkin iso -tiedoston latauslähteestä tai minun laatimastani lisäoppaasta '**Ohje .iso -tiedoston aitouden tarkistamiseen\_ver1.0.pdf**', jossa on ohjeet ladatun .iso -tiedoston aitouden tarkistamiseen Windows 10 ja Linux -järjestelmillä.

Linux -jakeluiden käyttöjärjestelmillä on useita eri **työpöytäympäristöjä** (GNOME, KDE Plasma, Xfce jne.) ja niille kullekin on yleensä ko. jakelun erillinen .iso tiedostoversio. Joillakin Linux -jakeluissa työpöydän tyyppi voi valita vasta järjestelmän asennusvaiheessa (esim. open SUSE, EndeavourOS), jos koneella on samalla nettiyhteys.

Tämän .iso -tiedoston latauksen koko on järjestelmästä riippuen 1 – 6 Gt (gigatavua). Kts. kunkin Linux -jakelun kohdalta esim. <https://distrowatch.com/>

**2.3.2 Jos teet asennustikun Windows 10:llä**, lataa ensin Windowsiin Microsoft Storesta **Rufus tai Etcher** –sovellus, jolla **levykuva palautetaan** koneen kovalevyltä tai ulkoiselta kovalevyltä/tikulta asennustikulle. Tarkemmat tiedot näistä löytyy linkeistä: <https://rufus.ie/en/> ja <https://kotimikro.fi/ohjelmat/apuohjelmat/rufus> sekä <https://etcher.balena.io/>

- Kytke tyhjä USB -tikku Windows -koneeseen ja avaa Rufus tai Etcher. Alusta tyhjä USB -tikku Etcherillä tai Rufuksella joko **MBR/Dos** tai **GPT** –muotoon, kts. <https://kotimikro.fi/oheislaitteet/kiintolevy/mbr-vs-gpt-mitka-ovat-erot>

**2.3.3 Jos teet asennustikun Linuxilla**, kytke USB -tikku Linux koneeseen ja avaa Linuxin **Levyt** ('Disks') -sovellus, tai muu sovellus. Alusta USB -tikku Levyt -sovelluksella joko **MBR/DOS** tai **GPT** -muotoon, kts. <https://kotimikro.fi/oheislaitteet/kiintolevy/mbr-vs-gpt-mitka-ovat-erot>

Kytke ulkoinen kovalevy tietokoneeseen ja **palauta levykuva** ulkoiselta kovalevyltä USB – tikulle: [https://fi.wikibooks.org/wiki/Ubuntu\\_tutuksi/Asennusmedian\\_luominen](https://fi.wikibooks.org/wiki/Ubuntu_tutuksi/Asennusmedian_luominen)

- Nyt sinulla on valmis valittuun Linux järjestelmään käynnistävä asennustikku. Huom. älä lataa tälle asennustikulle mitään muuta dataa tai muita Linux järjestelmien asennusohjelmia.

## **2.4 Järjestelmän perusasennus – yksi Linux järjestelmä yhdelle kovalevylle:**

Nämä ohjeet on Ubuntu ja Linux Mint järjestelmien perusasennukseen ja viritykseen, mutta myös muiden kohdassa 1.0 lueteltujen Linux järjestelmien tapahtuu aika lailla samaan tapaan. Mutta etsi kunkin järjestelmän ajantasaiset asennusohjeet erikseen ja noudata niitä, koska yksityiskohdissa voi olla eroja. Tietotekniikassa tapahtuu jatkuvaa laite- ja ohjelmistokehitystä, joten myös tänään voimassa olevat ohjeet versiolle xxx eivät välttämättä päden uudelle versiolle yyy. Tarkista aina ko. ohjeet.

**2.4.1 Tee ensin varmuuskopio** kaikista tietokoneella olevista omista asiakirjoista, töistä, kuvista, videoista, musiikista, s-postiosoitteista, nettiselaimien kirjanmerkeistä, salasanoista jne. joko pilvipalveluihin tai ulkoiselle kovalevylle / tikuille tai molemmille. Vasta tämän jälkeen siirry seuraavaan vaiheeseen. Tämä on erittäin tärkeää, koska kun samalle kovalevylle asennetaan uusi Linux järjestelmä, kovalevy alustetaan ja kaikki sen tiedot häviävät (ylikirjoitetaan) ja niitä voi sen jälkeen palauttaa vain tekemistäsi varmuuskopioista. S-postien osalta katso 2.5.8

**2.4.2. Muutokset BIOS -järjestelmään:** Sammuta kone ja kytke USB-asennustikku koneeseen. Tarkista koneesi **Käyttöohjeesta**, miten käyttäjä pääsee **BIOS -järjestelmään** ('Basic Input/Output System', kts. Esim. <https://kotimikro.fi/tietokone/bios-nain-avaat-tietokoneen-perusasetukset> ). Tavallisesti se käy painamalla heti virtapainikkeen painamisen jälkeen vain **Esc, F1, F2, F10 tai F12** tai jotain muuta näppäintä tai niiden yhdistelmää. Kunkin koneen käyttäjän ohjeet BIOS -järjestelmään pääsemiseksi löytyvät internetistä haulla **User Manual** ja koneen merkki ja tyyppi, esim. 'User manual HP EliteBook 8570p'. Vanhempien koneiden suomenkielistä käyttäjän ohjetta voi olla vaikeaa löytää netistä.

**Kun tiedät varmasti, miten pääset BIOS -järjestelmään, tarkista / muuta BIOS -järjestelmässä seuraavat 4 asetusta, eli ao. kohdat a.), b.) sekä c.):**

**a.) Käynnistä kone** niin, että se ei avaudu koneen nykyiseen käyttöjärjestelmään (Windowsiin), vaan **avautuu koneen BIOS – järjestelmään**. BIOS on koneen emolevyn ohjelmisto, joka sallii joko **MBR/Legacy** tai **EFI asennukset** tai - joissakin koneissa - molemmat. Tarkista, että olet valinnut vain toisen (MBR/Legacy tai UEFI), mutta **et missään tapauksessa** molempia. UEFI on vastaava emolevyn ohjelmisto ja se sallii UEFI asennukset.

Jos teit muutoksen, **tallenna tämä BIOS -asetusten muutos**. Jos tämä muutoksen tallennus (esim. 'F10 Save and Exit') ohjaa sinut takaisin koneen käynnistykseen, avaa kone uudelleen BIOS -järjestelmään ja jatka ao. kohdasta b.

**b.) Etsi BIOS -valikoista 'Secure Boot' ja 'Fast Boot' -asetukset** (= Pikakäynnistys), ne molemmat tulivat Windows 8:n mukana. Etsi näitä rauhassa, koska eri laitevalmistajien eri BIOS:ien eri versioissa ko. asetukset ovat usein eri paikoissa. Katso onko ne asetettu päälle

(enabled) Windowsia varten. Jos ne on asetettu päälle, niin **asetat ne molemmat pois päältä (disabled). Tallenna tämä BIOS -asetusten muutos.**

Jos tämä muutoksen tallennus ohjaa sinut takaisin koneen käynnistykseen, avaa kone uudelleen BIOS -järjestelmään ja jatka ao. kohdasta c.

Jotkut Linuxit hyväksyvät Secure Boot:n, Arch Linux pohjaiset jakelut eivät sitä hyväksy. Kts. kohta 5.1.

c.) **Etsi BIOS -valikoista koneen käynnistysjärjestys: Siinä on ensimmäisenä koneen nykyinen kovalevy**, jossa on nyt Windows. **Muuta tätä käynnistysjärjestystä niin, että kone käynnistyy ensin USB -asennustikulta.** Eri BIOS -järjestelmät nimittävät asennustikkua eri tavoin: 'USB -kovalevy', USB -tikun oikea nimi jne. Varmista, että **USB-asennustikku** on BIOS:n ilmoittamien koneen eri laitteiden keskinäisen käynnistysjärjestyksen **pinossa ylimpänä (jonossa ensimmäisenä)**. Tämä vie usein hetken aikaa ja on joskus kokeilua vaativa tehtävä, koska eri koneiden eri BIOS:t nimittävät nämä käynnistysjonossa olevat laitteet eri tavoin. **Kun valmista, tallenna myös tämä BIOS -asetusten muutos. Poistu BIOS:sta ja käynnistä kone, niin Linuxin perusasennus alkaa.**

Huom. Joissakin koneissa (esim. jotkut HP läppärit, HP pöytäkoneet) jokaisen käynnistysjärjestyksen voi määrittää erikseen → **Esc** → **BIOS -menu** → **Käynnistysjärjestys** → **USB -drive (siis ei Hard Drive)**. Mutta useimmissa koneissa sen määrittäminen onnistuu vain BIOS:n sisältä ja silloin **tämä BIOS -asetusten pysyvät muutos on tallennettava erikseen.**

d.) Linuxin koko asennuksen jälkeen voit rauhassa palata koneen BIOS:iin ja testata, josko asennettu Linux järjestelmä käynnistyy, kun laitat BIOS:n **'Fast Boot'** -asetus (Pikakäynnistys) päälle (enabled) ja tallentanut ko. muutoksen. Jos koneen Linux käynnistyy ja jos se käynnistyy nyt nopeammin, niin voit jättää BIOS:n Fast Boot -asetuksen (Pikakäynnistys) voimaan (enabled).

e.) Samalla voit muuttaa BIOS:n käynnistysjärjestykseen kohdassa c. tallennetun käynnistysjärjestyksen pysyvän muutoksen takaisin alkuperäiseen, eli kovalevy on pinossa ylimpänä. Se saattaa hieman nopeuttaa käynnistystä sekä hidastaa asiattomien pääsyä omalla asennustikullaan koneeseen.

**2.4.3 Nykyiset Linuxien asennusohjelmat (kuten Calamares, Anaconda jne.) sisältävät usein 2 osaa: kokeiluosan (ns. live-osa) ja asennusosan.** Kokeiluosan avulla voit tutustua asennustikulle ladatun Linuxin tärkeimpiin ominaisuuksiin ilman, että asennat sen vielä. Jos se ei tunnu sopivalta, kokeile jotain toista Linuxia.

**Huom. Heti kokeilu- ja asennusohjelman käynnistyttyä valitaan ensin kokeilu- ja asennusohjelman kieli → **suomi**, asennettavan Linux -järjestelmän käyttökieli → **suomi**, sekä näppäimistön asettelu → **suomalainen, ei kuolleita näppäimiä.****

Kun kokeilun tulos on selvä, voit joko lopettaa kokeilun tai - jos haluat - voit siirtyä asennusosaan → jos haluat siirtyä asennusosaan → valitse **'Install xyz' / 'Asenna xyz'** → siitä käynnistyy valitun järjestelmän xyz perusasennus.

**2.4.4 Kokeilun (kohta 2.4.3) jälkeen voit alustaa koneen kovalevyn** esim. asennusohjelman Levyt (Disks) -sovelluksella, joko **MBR** tai **GPT muotoon**. GPT muotoa suositellaan a.) kaksois- tai monikäyttökoneille ( dual- ja multiboot asennukset, kts kohta 6.), koska GPT muodossa olevan

kovalevyn osioiden myöhempi lisääminen on joustavampaa kuin traditionaalinen MBR muodossa olevan levyn osiointi (partitioning) sekä b.) koska GPT muodossa olevalle levyllä voi tallentaa suurempia (yli 4 GB) tiedostoja.

**2.4.5** Kun / jos kokeilun (kohta 2.4.3) tulos on selvä ja olet alustanut kovalevyn (kohta 2.4.4.) ja haluat asentaa ko. järjestelmän, paina 'Asenna Ubuntu' tai 'Asenna Linux Mint' painiketta' tai 'Asenna xyz' ja järjestelmän varsinainen automaattinen **perusasennus** alkaa. Huom. Linux -järjestelmien asennusohjelma osaa myös itse alustaa kovalevyn.

- Suorita Linuxin **perusasennus** näiden ohjeiden mukaisesti:

**Ubuntu:** <https://ubuntu-fi.org/ohjeet-ja-tuki/asentaminen/>

**Katso 2.4.3:n huomautus punaisella.**

Jos asennusohjelma kysyy haluatko asentaa päivitykset ja multimediat jo perusasennuksen yhteydessä → klikkaa 'kyllä'.

**Linux Mint:** <https://fi.101-help.com/linux-mint-aloittelijan-opas-ja-ammattilaisvinkkejaa7532ee48c> → kohta 'Linux Mintin asentaminen'

**Katso 2.4.3:n huomautus punaisella.**

Linuxin perusasennuksen alussa asennusohjelma kysyy yleensä haluatko ladata päivitykset ja multimediat jo perusasennuksen yhteydessä → klikkaa → **kyllä**.

Sitten kun asennusohjelma kysyy, haluatko **salata koneen koko kovalevyn** salasanalla:

<https://arhivo.com/fi/chapters/3748-how-to-encrypt-a-filesystem-with-luks-passphrase--linux-hi>

Jos haluat luoda koko kovalevyn salauksen se (Luks salausta) on tehtävä tässä vaiheessa: .

Jos kovalevyn salausta on tarjolla, niin suositellaan valittavan:

- '**lvm + salausta**' kts. <https://linuxconfig.org/linux-lvm-logical-volume-manager>;
- '**swap osiona**' kts. <https://linuxvox.com/blog/linux-partition-swap/> sekä <https://linuxize.com/post/create-a-linux-swap-file/> sekä
- **ext4 tiedostojärjestelmä** kts. <https://en.wikipedia.org/wiki/Ext4>

Huom1. Kovalevyn salaustavaimen (**LUKS** -avaimen) ja pääkäyttäjän (ylläpitäjän) salasanat voi muuttaa myöhemmin. LUKS yleistiedot: <https://www.cyberciti.biz/security/howto-linux-hard-disk-encryption-with-luks-cryptsetup-command/> → **Kts. kohta 3.**

Huom2. Linux Mintin asennuksen yhteydessä kysytään, haluatko salata vain Koti -kansion sisältö (eli vain kaikki omat työt). Mikäli ei jo valittu em. koko kovalevyn **lvm + salausta** -vaihtoehtoa **suositellaan ainakin Koti- kansion salaamista.**

**2.4.6 Perusasennuksen jälkeen** suositellaan, että kone ensin sammutetaan ja asennustikku irrotetaan koneesta. Sitten kone käynnistetään uudelleen.

Nyt BIOS:n käynnistysjärjestyksestä voi - halutessaan - muuttaa koneen käynnistymään vain sen kovalevyltä. Tämän muutoksen voi tehdä myöhemminkin.

Jos koneen nettiyhteys (LAN tai wifi) on päällä, niin uudelleen käynnistyksen jälkeen kannattaa ladata ja asentaa koneelle kaikki päivitykset, joita käyttöjärjestelmä tarjoaa perusasennuksen jälkeen ja käynnistää kone sitten taas uudestaan.

Tämän jälkeen on syytä kytkeä ensin jakelun **Palomuuri** päälle. Jos Palomuuri -sovellusta ei löydy asennetuista sovelluksista, niin ei tullut jakelun perusasennuksen ohjelmiston yhteydessä ja se on syytä erikseen a.) ladata joko ko. jakelun '**Ohjelmistot – Lisää ja poista tietokoneen ohjelmistoja**' -sovelluksesta tai **Päätteellä** (Konsolilla), esim. Ubuntussa ja Linux Mintissä se on komennolla **sudo apt install gufw** ja b.) asettaa se päälle → klikkaa Palomuurin kuvaketta → anna pääkäyttäjän salasana ja c.) klikkaa Palomuuri päälle → odota hetki ja varmistut, että se jäi päälle → d.) sulje Palomuuri -sovellus, niin se jää päälle ja toimimaan taustalla.

**2.4.7** Tee seuraavaksi järjestelmän **Asetuksista** järjestelmään mieleisesi käyttö- ja ulkonäköasetukset.

Tämän jälkeen perusasennus on valmis ja voit turvallisesti siirtyä kohtaan **2.5**.

**2.5 Perusasennuksen jälkeen** suositellaan seuraavia **lisäasennuksia ja -asetuksia**:

Eri Linux käyttöjärjestelmien /-jakelujen luomat ja ylläpitämät **lisäohjelmien ja -sovellusten kirjastot** (repositories) tarjoavat hyvin laajan valikoiman erilaisia **lisäsovelluksia**.

Lisäsovellukset ja -ohjelmat voi ladata ja asentaa perusasennuksen jälkeen tai myöhemmin joko kirjastoista (kts. 2.5.1) tai ajamalla päätteellä lataus- ja asennuskomento (kts. 2.5.2) .

**2.5.1** Etsi ja lataa lisäsovelluksia koneesi käyttöjärjestelmän tarjoamasta sovellusten kirjastosta (eri järjestelmissä tästä käytetään samasta asiasta eri nimityksiä': Ubuntu: 'Ubuntu Software'; Linux Mint: 'Ohjelmistohallinta') ko. sovellukset ja asenna ne sieltä.

**A. Ubuntu sovelluskirjasto** otetaan käyttöön ajamalla Päätteellä ensin komento **sudo snap refresh** ja sitten **sudo snap install snap-store** → se luo '**Ubuntu Software**' -nimisen painikkeen, josta ko. kirjasto avautuu: siinä on 3 välilehteä: etsi uusia → avaa välilehti 'Tutki; jo asennetut → avaa välilehti 'Asennetut'; päivityksiä saatavilla → avaa välilehti 'Päivitykset', jos tässä on \* -merkki otsikon yläkulmassa.

**B. Linux Mint:n sovelluskirjasto** avataan klikkaamalla jo perusasennuksen luomaa **Ohjelmistohallinta** -painiketta → josta ko. kirjasto avautuu: siinä on etusivulla 2 osaa '**Esittelyssä**' ja '**Luokat**' sekä oikeassa yläkulmassa '**hampurilais**' -**painike**, josta avautuu 5-rivinen hakemisto: a.) 'Näytä asennetut sovellukset' (tarkoittaa lisäsovellukset); b.) 'Päivitä pakettiluettelo' (päivittää sovelluslistan välimustin); c.) 'Ohjelmälähteet' → valitse 'Viralliset ohjelmälähteet' → valitse 'Pääpalvelin' → valitse lähimmän peilipalvelimen maa → Ruotsi → valitse sieltä esim. 'Bahnhof'; d.) Asetukset → 2 alavalikkoa: 'Hakuun liittyvät valinnat' ja 'Flatpak-ohjelmisto'; d.) Tietoja.

**C. Näiden Linux -jakeluiden kirjastojen kautta** jaetaan myös **Flathub.org kirjaston Flatpak -ohjelmistoja**. Se toimii niin, että ensin tietokoneelle latautuu ja asentuu **Flatpak – 'hiekkalaatikko'** ('sandbox') - niminen kontti (container), jonka sisään haluttu flatpak -lisäsovellus tai -ohjelma ja kaikki sen vaatimat ohjelmakirjastot latautuvat ja asentuvat. 'Hiekkalaatikko' on eristetty muista Linux ohjelmista. **Edut:** 'Hiekkalaatikkoon' ladatuilla ohjelmilla ei ole riippuvuuksia Linuxissa oleviin muihin ohjelmiin. **Haitat:** Kukin 'Hiekkalaatikon' sovellus ja sen ohjelmistokirjastot vie aika paljon koneen levytilaa. Flatpak -ohjelmia on usein moitittu

toimimaattomuudesta. Kts. lisää esim. <https://docs.flathub.org/docs/category/for-users> ja <https://itsfoss.com/what-is-flatpak/> ja <https://ostechnix.com/why-flatpak-apps-use-so-much-disk-space/>.

**2.5.2** Lisäohjelmat ja -sovellukset voi ladata ja asentaa myös **ajamalla päätteellä** komento **sudo apt install xyz** (= xyz on ohjelman nimi vain pienillä kirjaimilla), eli esimerkiksi **sudo apt install gufw gnote gparted keepassxc seahorse screenfetch screenshot** -> tämä komento lataa ja asentaa koneelle em. **paksulla punaisella fontilla tähän esimerkkiin** kirjoitetut 7 sovellusta ko. Linux jakelun omasta kirjastosta, mikäli ne eivät kuuluneet jo perusasennuksen pakettiin.

Lisää **Linux – komennoista** kts. esim. <https://www.linux.fi/wiki/Komentorivikomennot> ja <https://fi.linux-console.net/?p=10166#gsc.tab=0> Tästä teemasta netissä on paljon sivustoja.

**2.5.3 Käynnistä asennettu palomuuuri** (se vaatii salasanan).

**2.5.4** Tarkista asennuksessa tulleen **swap -osion** (partition) **tai -tiedoston** (file) koko ja herkkyys: aja päätteellä ensin komento **free -h** → näyttää RAM (random access memory) muistin koon ja mahdollisen swap – osion (partition) tai -tiedoston (file) koon xx Gt. Aja päätteellä **swapon --show**, niin saat tietää, onko se swap -osio vai zram -tiedosto. Tässä se on 8 Gt kovalevyn osio:

| NAME      | TYPE      | SIZE | USED | PRIO |
|-----------|-----------|------|------|------|
| /dev/sda4 | partition | 8G   | 0B   | -2   |

ja tässä se on 2 Gt zram tiedosto:

```
~ >>> swapon --show
```

| NAME      | TYPE | SIZE | USED | PRIO |
|-----------|------|------|------|------|
| /swapfile | file | 2G   | 0B   | -2   |

Swap:n koko tulisi olla vähintään 50% RAM:n koosta, pelikoneissa 100%. Tässä alla esimerkkejä swap tiedoston koon ja swappiness -arvon (herkkyys) säätämiseen päätteellä perusasennuksen jälkeen:

**\* Tee 2 Gt swap-faili ja säädä swappiness arvoon -> 25**

```
~ >>> free -h
```

|       | total | used  | free  | shared | buff/cache | available |
|-------|-------|-------|-------|--------|------------|-----------|
| Mem:  | 3,8Gi | 1,7Gi | 462Mi | 189Mi  | 1,6Gi      | 1,7Gi     |
| Swap: | 0B    | 0B    | 0B    |        |            |           |

**Tässä Swap:n koko on 0. Näin tehdään 2 Gt swap tiedosto:**

```
~ >>> sudo fallocate -l 2G /swapfile
```

```
[sudo] käyttäjän salasana:
```

```
~ >>> sudo chmod 600 /swapfile
```

```
~ >>> sudo mkswap /swapfile
```

```
Setting up swapspace version 1, size = 2 GiB (2147479552 bytes)
```

```
ei nimiötä, UUID=88b17c84-09c8-4f18-8913-7388625f8083
```

```
~ >>> sudo swapon /swapfile
```

```
~ >>> swapon --show
```

| NAME      | TYPE | SIZE | USED | PRIO |
|-----------|------|------|------|------|
| /swapfile | file | 2G   | 0B   | -2   |

```
~ >>> sudo sysctl vm.swappiness=25
```

```
vm.swappiness = 25
```

\* Suurena swap file 511M → 2G, jos asennuksessa on tullut liian pienikokoinen swap -tiedosto, esim 511M ja säädä sen swappiness arvoon → 25

```
~ >>> sudo swapoff /swapfile
~ >>> sudo fallocate -l 2G /swapfile
[sudo] käyttäjän salasana:
~ >>> sudo chmod 600 /swapfile
~ >>> sudo mkswap /swapfile
Setting up swapspace version 1, size = 2 GiB (2147479552 bytes)
ei nimiötä, UUID=88b17c84-09c8-4f18-8913-7388625f8083
~ >>> sudo swapon /swapfile
~ >>> swapon --show
NAME      TYPE SIZE USED PRIO
/swapfile file  2G  0B  -2
~ >>> sudo sysctl vm.swappiness=25
vm.swappiness = 25
```

2.5.5 Mikäli koneessa on SSD -tyyppinen kovalevy → käynnistä fstrim.timer ajamalla päätteellä komento `sudo systemctl enable fstrim.timer`

2.5.6 Lokitietojen maksimikoon rajoitus: Avaa pääte ('konsoli') ja aja sillä komento `sudo nano /etc/systemd/journald.conf` → etsi auenneesta tiedostosta rivi `#SystemMaxUse=` → poista rivin alusta `#` -merkki ja lisää rivin loppuun `50M` niin, että rivi näyttää tältä `SystemMaxUse=50M` Kun tämä muutos ja lisäys on tehty, paina Ctrl+O (eli O kuten Oulu) ja paina sitten Enter → poistu nano -editorista painamalla Ctrl+X. Voit tarkistaa tuliko oikein ajamalla uudestaan `sudo nano /etc/systemd/journald.conf` --> jos se on OK, poistu nano -editorista painamalla Ctrl+X.

Voit tarkistaa paljonko tähän mennessä lokitiedostoihin on kertynyt aineistoa ajamalla Pääteillä komennon `du -s -h /var/log/journal`. Jos niihin on jo ennen tämän rajoituksen asettamista kertynyt yli 50M, niin tämän asetetun määrän (50M) ylittävä vanhin data pyyhkiytyy pois seuraavissa koneen käynnistyksissä eikä siten kuormita kovalevyn tilaa enää.

2.5.7 Asennetun **nettiselaimen** (esim Firefox) turvallisuuden määrittely ja mainosten esto: asenna vähintään nämä **laajennukset**: Avaa Firefox → hae 'hampurilaisvalikko oikealla yläkulmassa → 'Avaa sovellusvalikko' → avaa 'Laajennukset ja teemat' → etsi ja lataa **uBlock Origin** ja aseta sen 'Hallitse' → 'Suoritus yksityisissä ikkunoissa' → klikkaa 'Salli'. Muita suositeltuja laajennuksia ovat mm. **Adblock Plus**, **Disconnect**, **Privacy Badger** sekä Linux työpöytäsi integraatio (kuten **Gnome Shell -integraatio**, **Plasman Intergration**) ja asennettuja salasananamagereita tukevat laajennukset (**Bitwarden salasanahallinta** ja/tai **KeePassXC-Browser**). Aseta myös näihin on suoritus yksityisissä ikkunoissa.

**Nettiselaimen hakukoneeksi** suositellaan yksityisyyttä kunnioittavat **Qwant** (Ranska), **Startpage** (Hollanti) tai **DuckDuckGo** (USA).

2.5.8 **Sähköpostiohjelman** (esim. Thunderbird, Evolution, Geary jne) käynnistys ja määrittely + omien sähköpostitilien liittäminen tähän ohjelmaan. Huomaa että, jos s-posteissasi on ollut IMAP -asetus, niin s-postisi on tallennettu s-postipalvelusi palvelimilla (serveilla); jos s-posteissasi on ollut POP -asetus, niin s-postisi on tallennettu vain koneellesi ja ne on ennen Linuxin asennusta varmuuskopiota ulkoiselle levyille / tikulle.

Gmail ja siellä olevien osoitteiden kytkeminen esim. Thunderbirdiin käy gmailin omilla tunnuksilla ja kytkennän varmentamiseen tarvitaan kannettavaa puhelintasi.

Entinen Telian pp-inet.fi on nyt **inet** ja sen ohjeet esim. Thunderbirdia varten → <https://www.inet.fi/faq> → kts. kohta → ”Käytän sähköpostiohjelmaa tai sovellusta. Mitä asetuksia minun tulisi käyttää?”.

**2.5.9 Salasanamanagerin asennus:** Suositellaan Bitwarden tai KeePassXC sovelluksia, joista suositellaan KeePassXC, koska se on maksuton ja rajaton ja siinä on mm. kätevä salasanojen vaikeusasteen eli entropian (= epäjärjestyksen suuruuden) mittari. Hyvän salasanan entropian tulisi olla yli 100.

Molempiin on saatavilla 2 -vaiheinen tunnistautuminen (2FA): Bitwardenissa se toimii netin kautta (ohjeet: <https://bitwarden.com/help/setup-two-step-login/> ) ja KeePassXC on tietokantasovellus, joka toimii vain koneessasi ilman nettiyhteyttä ja siihen kannattaa lisätä heti käyttöönoton yhteydessä salasanan lisäksi joko oma **avaintiedosto** (key file) tai käyttää erillisiä Youbikey tai OnlyKey varmennetikkuja.

- Jos a.) valitset KeePassXC:n ja jos b.) asennetun Linuxin käyttöjärjestelmän ikkunointijärjestelmä on **Wayland** ja jos c.) haluat, että KeePassXC suorittaa nettipalvelujesi käyttäjänimen ja salasanojen automaattisen täytön, niin aja päätteellä komento

**sudo nano /usr/share/applications/org.keepassxc.KeePassXC.desktop** → etsi auenneesta tiedosta rivi **Exec=keepass %f** ja lisää siihen tämä tässä **vihreällä merkitty lisäteksti Exec=env QT\_QPA\_PLATFORM=xcb keepass %f** . Kun tämä lisäys on tehty, paina Ctrl+O (eli O kuten Oulu) ja paina Enter → poistu ohjelmasta painamalla Ctrl+X. Voit tarkistaa tuliko muutos oikein → aja päätteellä uudestaan sama komento

**sudo nano /usr/share/applications/org.keepassxc.KeePassXC.desktop** --> jos se on OK, poistu päätteeltä, eli paina Ctrl+X.

**2.5.9.1 Tärkeiden tiedostojen synkronointi pilvipalvelussa:** mm. KeePassXC tietokannan synkronointi onnistuu esim näissä: <https://itsfoss.com/install-dropbox-ubuntu/> tai <https://mega.io/syncing> tai <https://blog.otterlord.dev/posts/proton-drive-rclone/>

**2.5.10 Pelit:** Koneen teknisestä tasosta riippuen Linuxeilla voi pelata hyvin monia pelejä. Niitä löytyy joko ko. Linuxin omasta ohjelmakirjastosta tai **Steam + Proton Plus alustalta**, kts. **’How to Play Games on Linux: A Beginner’s Guide’** → <https://www.howtogeek.com/how-to-play-games-on-linux-a-beginners-guide/>

Jos tarvis, niin tämän kohdan 2.5. eri tehtävien (2.5.1 ... 2.5.10) suorittamiseen voit pyytää yksityiskohtaisempia ohjeita erikseen tai kysyä niistä ko. jakelun käyttäjäfoorumilta.

**2.6 Windows sovelluksien käyttö Linuxeissa:** Kaikkia Windowsille tehtyjä sovellusohjelmia ei ole valmiiksi käännetty Linuxiin, joskin niiden määrä kasvaa. Linuxiin voi asentaa Win -alustan (kääntäjä /compatibility layer), jolla aika monet - mutta ei ihan kaikki - Windowsille tehdyt sovellukset toimivat Linuxeissa:

- Wine -alustan (-kääntäjän) asennusohjeet Linuxiin:  
<https://www.geeksforgeeks.org/linux-unix/how-to-use-wine-on-linux/>

- Wine -alustalla toimivat Windows sovellukset → katso tietokanta: <https://appdb.winehq.org/>

Huom. Jos jotkut näistä tietokannassa olevista Windows sovelluksista voivat edellyttää, että UEFI koneiden BIOS:n Secure Boot toiminto tulee olla päällä. Voit kokeilla nykyistä Linux UEFI

asennustasi kytkeällä BIOS:ssa Secure Bootin ensin päälle ja tarkistamalla sitten käynnistyykö Linux. Jos se ei käynnisty, kytke Secure Boot pois päältä ja käynnistä Linux uudestaan.

### 3. Pääkäyttäjän / Ylläpitäjän tehtäviä kaikkien asennusten ja asetusten jälkeen - tietoturvan ylläpitämiseksi:

Pidä koneesi ja omat tiedostosi hyvässä ja turvallisessa kunnossa näin:

- **Lataa päivitykset** sitä mukaa kun niitä on koneeseen automaattisesti tarjottu (internetin kautta)
- **Varmista** aina, että lataat koneellesi ohjelmia ja sovelluksia ja niiden päivityksiä **vain niiden virallisista lähteistä**
- **Aseta** kaikille koneen kautta käyttämillesi palveluille **omat vahvat salasanat**. Suositeltavaa on ottaa käyttöön **2 -vaiheinen tunnistautuminen** ('two-factor authentication', 2FA; tai '2-step authentication') **kaikkiin sellaista tarjoaviin nettipalveluihin**. Huom. kännykän tekstiviestipalveluun perustuva 2 -vaiheinen tunnistautuminen on todettu heikoimmaksi.
- **Pidä salasanat** on turvallisesti säilössä esim. turvallisessa pilvessä ja ainakin tärkeimmät myös omassa vihkossa.
- **LUKS -salausavaimen muutos**: Ohje: <https://www.cyberciti.biz/security/how-to-change-luks-disk-encryption-passphrase-in-linux/>. Kts. Liite 1.
- **LUKS -salausavaimen lisäys (esim. toiselle tai vierailevalle käyttäjälle)**: <https://access.redhat.com/solutions/230993> tai <https://blog.ummit.dev/posts/linux/tools/luks/luks-add-key-or-verify/> Kts. Liite 2.
- **Lisätyn LUKS -salausavaimen poisto**: <https://www.cyberciti.biz/security/howto-linux-hard-disk-encryption-with-luks-cryptsetup-command/> → kts artikkelin lopussa → komento: **cryptsetup luksRemoveKey /dev/xvdc** + Tämä vaatii antamaan vanhan salasanan.
- **Pääkäyttäjän/ylläpitäjän salasanan muutos** Linux → Asetukset → Järjestelmä → Käyttäjät → Avaa lukitus → Pääkäyttäjä/Ylläpitäjä → ..
- **Muiden käyttäjien lisäys / poisto**: Linux → Asetukset → Järjestelmä → Käyttäjät → Avaa lukitus → Pääkäyttäjä/Ylläpitäjä → tässä samassa Asetusten paikassa Pääkäyttäjä /Ylläpitäjä voi lisätä muita käyttäjiä ja poistaa niitä. Huom. Lisätyille pysyville tai tilapäisille muille käyttäjille Pääkäyttäjä / Ylläpitäjä voi luoda omat LUKS -salasanat, enintään 7 kpl. Lisäksi heille tulevat sovellukset, esim Firefox nettiselain, Thunderbird s-posti jne., tulee Pääkäyttäjän 'virittää' erikseen. **Lisätyn LUKS -salasanan poisto: Kts edellä.**
- **Käytä salasanamanageria** → suositellaan **Bitwarden** ( <https://bitwarden.com/> ) ja/tai **KeePassXC** ( <https://keepassxc.org/> ) sovelluksia.
- **Tee säännöllisesti** omien töiden **varmuuskopiot** pilvipalveluun ja/tai ulkoisille kovalevyille, mutta mieti ensin millaista varmuuskopiostrategiaa aiot ja voit suorittaa pitemmällä tähtäimellä. [ Hyvänä strategiana pidetään ns. **3-2-1 sääntöä**, eli tehdään säännöllisesti, esim. kerran kuukaudessa, varmuuskopio on 3:na kappaleena 2:lla eri tekniikalla (esim. omat levyt SSD ja HDD

tai oma levy + turvallinen pilvi, esim. Mega (Uusi Seelanti), Box (USA), Proton (Sveitsi), Cozy (Ranska) ja joista 1:tä varmuuskopiota säilytetään muista erillään turvallisessa paikassa. ]

- **Nettireititin (kiinteä verkon ja mobiiliverkon): Vaihda** tehtaan/myyjän reitittimeen liimaama salasana **omaksi vahvaksi salasanaksi**. Sammuta nettireititin vähintään kerran vuorokaudessa ja käynnistä se uudestaan, näin sen välimuistista 'pyyhkiytyvät' pois sinne mahdollisesti kertyneet hakkeriyritysten tiedot, joita en ko. tahot enää hyödyntää uusissa yrityksissään.

- Nämä samat asiat koskevat myös kännykkääsi.

**4. Lopuksi:** Koska tätä asiakokonaisuutta voi kuvata ja lähestyä niin monelta eri kantilta, suositellaan, että jos havaitset tässä ohjeessa asia- tai kirjoitusvirheitä tai huonoa (epäselvää) suomea tai mitä tahansa lisätietoja tai tarkennuksia vaativia asioita, niin lähetä siitä tämän lähettäjälle viesti.

Linuxeissa on hyvää myös se, että voi kokeilla yhtä tapaa ja jos erehtyy, niin voi kokeilla toista tapaa tai toista Linuxia, kunhan vaan pitää omat varmuuskopiot päivitettyinä.

## **5. Windows 11 + Linux kaksoiskäyttö -ja monikäyttöjärjestelmät (dual boot ja multi boot systems) – yksi tai useampi kovalevy**

Ennen kaksoiskäyttö -ja monikäyttöjärjestelmät (dual boot ja multi boot systems) asennuksiin ryhtymistä asentajan tulee hallita kovalevyn osiointin (partitioning) perusteet. Kts esim <https://tecnobits.com/fi/miten-kiintolevy-osioidaan-Windows-11%3Ass%C3%A4/> <https://www.lifewire.com/how-to-partition-a-hard-drive-2626081> ja [https://en.wikipedia.org/wiki/Disk\\_partitioning](https://en.wikipedia.org/wiki/Disk_partitioning)

**Windows 11:n kovalevyllä varaamaa tilaa supistetaan. Ohjeet löytyy netistä. Vapautuneeseen levytilaan voi asentaa Secure Bootia tukevan Linuxin tai muutaman Linuxin.**

**Jos koneessa on useampi levy, helpointa on pitää Windows 11 omalla levyllään ja asentaa muille levyille Linuxeja. Ohjeet löytyy netistä.**

**5.1 UEFI koneiden Secure Boot (SB):** Windows 8:sta alkaen Microsoft on suositellut laitetasolla (firmware) toimivan Microsoftin kehittämän ja ylläpitämän SB:n käyttöä tukemaan Windowsien turvallista käynnistymistä, mutta se ei ole ollut pakollista (kts. UEFI/Secure Boot asiasta tarkemmin esim. <https://www.minitool.com/lib/secure-boot.html> ). **Windows 11:sta alkaen SB on pakollinen, koska pakollinen TPM2.0 turvapiiri vaatii sen.**

**5.2 SB:a on pakko käyttää, kun samaan tietokoneeseen, joko samalle kovalevylle tai erillisille kovalevyille, on asennettu Windows 11 + joku tai joitakin em. kohtien 1.1, 1.2 ja 1.3 Linuxeista** (ns. dual boot tai multiboot järjestelmät). Kohtien 1.1, 1.2 ja 1.3 Linux -järjestelmissä on Microsoftin allekirjoittama ns. 'shim -käynnistyslataaja' ('shim bootloader') ja se toimii koneen UEFI laitteiston ja Linuxin käynnistyslataajan välissä ja tukee niiden SB:n käyttöä. SB luo – teoriassa - myös näiden Linuxien käynnistykseen lisäturvaa. Kts. esim. <https://wiki.ubuntu.com/UEFI/SecureBoot>.

**5.3 Kohdan 1.4 Arch Linux käyttöjärjestelmiin voi tehdä SB:n jälkiasennuksen itse, mutta, kuten seuraavasta linkistä näkyy, se ei ole aivan helppo tehtävä, kts.** [https://wiki.archlinux.org/title/Unified\\_Extensible\\_Firmware\\_Interface/Secure\\_Boot](https://wiki.archlinux.org/title/Unified_Extensible_Firmware_Interface/Secure_Boot). Toinen SB:n

keino on mennä BIOS:iin ja kytkeä ensin SB pois päältä ja käynnistää vasta sitten sellainen Linux, joka ei tue SB:a ja kytkeä SB takaisin päälle, ennen kuin palaa Windows 11:een.

## 6. Linux + Linux kaksoiskäyttö -ja monikäyttöjärjestelmät (dual boot ja multi boot systems) – lyhyt esitys

Tässä juttua - lyhyesti - vain erilaisia Linux -järjestelmiä sisältävien kaksoiskäyttö -ja monikäyttöjärjestelmien (dual boot ja multi boot systems) asennuksien peruseräpäätteistä. Eri käyttöjärjestelmillä saattaa olla hieman näistä poikkeavia erilaisia toteutuksia, joita sitten sovelletaan niiden asennuksissa.

Ensiksi pitää selvittää koneen BIOS:ssa, onko koneessa ns. **legacy** vai **UEFI** -käynnistys. Jos koneen BIOS sallii valita molemmat, niin valitaan **joko** legacy **tai** UEFI -käynnistys ja suoritetaan sen mukainen asennus.

### 6.1 Legacy koneet – yksi kovalevy – useita Linux järjestelmiä

**A.** Aluksi koneen kovalevy on hyvä alustaa **GPT muotoon** asennustikun Levyt – sovelluksella. GPT muoto sallii 126 osion luomisen. Samalla Levyt -sovelluksella jatketaan ja luodaan kaikille koneen järjestelmille **yhteinen tietovarasto-osio** (suositus), jonka koko on esim 80 – 160 Gt, ext4 tiedostojärjestelmä, tämä osio on syystä salata luks salauksella, luks = Linux Unified Key Setup, kts esim. [https://en.wikipedia.org/wiki/Linux\\_Unified\\_Key\\_Setup](https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup) tai <https://itsfoss.com/luks/>. Mikäli tätä yhteistä tietovarastoa ei haluta luoda, kohtaa A. ei suoriteta, vaan siirrytään seuraavaan kohtaan E.

Kun koneen eri Linux järjestelmät asennetaan samalle kovalevylle, niin niiden asennusohjelman **manuaalisella** (ei automaattisella) **osioinnilla** luodaan:

**B. levyn ensimmäiselle Linux järjestelmälle 2 osiota (partition):** eli **osio 1.)** 600 – 1000 MiB /**boot** -osio, ext4 tiedostojärjestelmä; **osio 2.)** 35 – 60 GiB / **(root) -osio**, ext4 tiedostojärjestelmä; tämä osio tai vain sen alainen /Koti – kansio ( /home -folder ) on syystä salata luks salauksella, luks = Linux Unified Key Setup, kts esim. [https://en.wikipedia.org/wiki/Linux\\_Unified\\_Key\\_Setup](https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup) tai <https://itsfoss.com/luks/>. Huom. Linux Mintin asennusohjelmassa on oma oivallinen /Koti -kansion salausominaisuus. Tämän jälkeen asennetaan ensimmäinen järjestelmä.

#### 6.1.B.1 Lisäys:

Jotkut Linux -järjestelmät - kuten esim. Manjaro - suosittelevat, että legacy koneessa olevaan GPT alustettuun levyyn luodaan 1.) ensin **8 Mt alustamaton (unformatted) osio** ja 2.) käyttöjärjestelmää varten **/root -osio**.

#### 6.1.B.2 Lisäys:

Mikäli legacy koneen emolevyn ei hyväksy GPT muotoon alustettua kovalevyä, asennettu Linux -järjestelmä ei ehkä käynnisty. **Siirry silloin kohtaan E., eli alusta kovalevy ensin MBR muotoon ja asenna Linux -järjestelmä siihen.**

**C.** levyn ensimmäiselle Linux järjestelmälle voi luoda myös oman /home -osion MBR -alustetun kovalevyn 3:een osioon ja salata se luks salauksella. Tällöin / (root) -osion koko voi olla pienempi, esim 25 - 35 GiB.

**D.** Levyn muille järjestelmille luodaan kullekin sen asennusohjelmalla manuaalisesti **yksi uusi osio, eli sen oma / (root) -osio + ko. järjestelmän oma swap tiedosto**. Tämän järjestelmän /Koti -kansio (/home -folder) on syytä suojata luks salauksella.

Kunkin Linux -järjestelmän asennusvaiheessa luodaan sen oma sisäinen ohitustiedosto (swap-file), jonka koko on 50 – 100% koneen RAM- muistin koosta. Jos ko. uuden järjestelmän asennusohjelma ei luo swap -tiedostoa, sen voi luoda myös asennuksen jälkeen. Swap tiedoston kokoa voi suurentaa asennuksen jälkeen sille varatun (osion) tilan puitteissa, kts kohta 2.5.4.

Kovalevyn loppuun suositellaan jätettäväksi noin 5-6 MiB tyhjä ('varaamaton') tila.

**E.** Mikäli kovalevyä ei alusteta GPT -muotoon eikä levyille luoda kohta A:n mukaista yhteistä tietovarastoa, silloin levy **alustetaan MBR muotoon**. Se sallii vain **4 ensisijaista osiota** (primary partition tai primary volume) . Näistä neljän (4.) osion voi muuttaa laajennetuksi (extended volume) osioksi, jonka alle voi tehdä ala-osioita (sub-volumes) ja asentaa niihin toisen, kolmannen jne. Linux – järjestelmän. Vaikka tämän alustuksen tekisi GPT -muotoon, niin ensimmäisen järjestelmän asennusohjelma **saattaa todeta** koneen legacy -koneeksi ja alustaa levyn MBR -muotoon, jos ei ole ensin tehty, kuten kuvattu kohdassa A.

Kun koneen eri Linux järjestelmät asennetaan samalle MBR -alustetulle kovalevyille, niin asennusohjelman **manuaalisella** (ei automaattisella) **osioinnilla** luodaan:

**F. levyn ensimmäiselle Linux järjestelmälle 2 osiota (partition):** eli **osio 1.)** 600 – 1000 MiB /**boot** -osio, ext4 tiedostojärjestelmä; **osio 2.)** 35 – 60 GiB / (root) -osio, ext4 tiedostojärjestelmä; tämä osio tai vain sen alainen /Koti – kansio ( /home -folder ) on syytä salata luks salauksella, luks = Linux Unified Key Setup, kts esim. [https://en.wikipedia.org/wiki/Linux\\_Unified\\_Key\\_Setup](https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup) tai <https://itsfoss.com/luks/>. Huom. Linux Mintin asennusohjelmassa on oma oivallinen /Koti -kansion salausominaisuus. Tämän jälkeen asennetaan ensimmäinen järjestelmä.

**G.** levyn ensimmäiselle Linux järjestelmälle voi luoda myös oman /home -osion MBR -alustetun kovalevyn 3:een osioon ja salata se luks salauksella. Tällöin / (root) -osion koko voi olla pienempi, esim 25 - 35 GiB.

**H.** Muiden Linux -järjestelmien asennusta varten muutetaan MBR -alustetun kovalevyn 4. osio laajennetuksi (extended) asennusohjelman manuaalisella osioinnilla ja luodaan sen alle ala-osioita (sub-volumes), joihin ko. muut järjestelmät asennetaan. Muille järjestelmille tehdään joko yksi (1) osio tai – jos ko. järjestelmän asennusohjelma sallii – toinen /home (= /Koti) -osio, joka salataan luks salauksella.

Kunkin Linux -järjestelmän asennusvaiheessa luodaan sen oma sisäinen ohitustiedosto (swap-file), jonka koko on 50 – 100% koneen RAM- muistin koosta. Jos ko. uuden järjestelmän asennusohjelma ei luo swap tiedostoa, sen voi luoda myös asennuksen jälkeen. Swap tiedoston kokoa voi suurentaa asennuksen jälkeen sille varatun (osion) tilan puitteissa, kts kohta 2.5.4.

Kovalevyn loppuun suositellaan jätettäväksi noin 5-8 Mt tyhjä ('varaamaton') tila.

**I.** Kovalevyille ensiksi asennetun Linux-järjestelmän käynnistysvalikossa näkyy aluksi vain tämä ensiksi asennettu Linux -järjestelmä. Muut asennetut Linux -järjestelmät saadaan näkymään tässä samassa käynnistysvalikossa seuraavasti:

Avataan levyn ensimmäinen Linux -järjestelmä ja ajetaan sen Päätteellä komento **sudo nano /etc/default/grub** (tai **/grub2** – eri järjestelmissä tämä on joko grub tai grub2) ja aseta sillä OS\_PROBER seuraavasti → poista riviltä **#GRUB\_DISABLE\_OS\_PROBER=false** sen mahdollinen # -etumerkki → jolloin sen oikea muotoilu on tämä:  
**GRUB\_DISABLE\_OS\_PROBER=false** ---» tallenna tämä muutos painamalla Ctrl+O + Enter ja poistu editorista Ctrl+X.

Tämän jälkeen **päivitä alkulatausohjelma grub** (kts alla):

Mikäli ko riviä ei ole tässä grub -tiedotossa , niin asenna os\_prober ajamalla ko. komento Päätteellä.

### **Grub (tai grub2:n) -alkulatausohjelman päivityskomennot eri järjestelmille:**

Debian, Ubuntu,  
Linux Mint:

sudo update-grub

Archlinux, Manjaro,  
EndeavourOS:  
**tai**

sudo grub-mkconfig -o /boot/grub/grub.cfg t  
sudo grub2-mkconfig -o /boot/grub2/grub.cfg

openSUSE:

sudo grub2-mkconfig -o /boot/grub2/grub.cfg

--» tämän jälkeen käynnistä kone uudelleen --» nyt ensiksi asennetun järjestelmän käynnistys- eli grub -valikossa näkyy tämä järjestelmä sekä sen alla muut tämän valikon kautta käynnistyvät ko. kovalevyllä olevat Linux -järjestelmät.

## **6.2 Legacy koneet – useita kovalevyjä – useita Linux järjestelmiä**

Ensin tulee suunnitella, mitä Linux -järjestelmiä asennetaan koneen eri kovalevyille.

Kun jollekin kovalevyllä asennetaan sen ensimmäinen, toinen (tai kolmas jne.) Linux -järjestelmä, tulee kaikkien muiden kovalevyjen kaapelit ensin irrottaa. Näin asennettavien uusien järjestelmien **käynnistysosiot** asentuvat varmasti vain samalle kovalevyllä kuin ko. uusi järjestelmäkin.

A. Koneen yksi kovalevy on hyvä ensin alustaa GPT -muotoon asennustikun Levyt – sovelluksella ja luoda siihen **koneen kaikkien levyjen** järjestelmien **yhteinen tietovarasto**, joka on suojattu luks kryptauksella.

Jos tälle samalle (GPT muotoon alustetulle) kovalevyllä, jossa on koneen kaikkien järjestelmien yhteinen tietovarasto, asennetaan useita Linux järjestelmiä, niin toimitaan kuten kohdassa 6.1.A, 6.1.B, 6.1.C ja 6.1.D, eli asennukset aloitetaan tekemällä ensimmäisen järjestelmän asennusohjelman manuaalisella (ei automaattisella) osiinnilla ja jatketaan järjestelmien perusasennuksella.

B. Muille MBR -alustetuille kovalevyille asennukset tehdään 6.1.E, 6.1.F, 6.1.G ja 6.1.H mukaisesti.

Kun asennukset on tehty, kone sammutetaan, koneen virtajohto ja mahdollinen akku irrotetaan ja käynnistetään kone pari kertaa, jotta se saadaan varmasti jännitteettömäksi. Sitten kiinnitetään muiden kovalevyjen kaapelit, ja käynnistetään kone uudestaan.

Haluttu kovalevy valitaan koneen BIOS ohjelmasta.

### 6.3 UEFI koneet – yksi kovalevy – useita Linux järjestelmiä

Aluksi koneen kovalevy(t) tulee alustaa GPT asennustikun Gparted tai Levyt – sovelluksella muotoon. GPT muoto sallii 126 osion luomisen. Jos koneen eri Linux järjestelmät asennetaan samalle kovalevylle, niin asennusohjelman manuaalisella (ei automaattisella) osioinnilla ja asennuksella luodaan:

**A. kullekin Linux järjestelmälle 3 osiota (partition):** eli osio 1.) 512 - 600 Mt **/boot/efi** osio, fat32 tiedostojärjestelmä + **boot lippu**; osio 2.) 600 – 1000 Mt **/boot** osio, ext4 tiedostojärjestelmä; osio 3). 35 – 60 Gt / **(root) osio**, ext4 tiedostojärjestelmä; tämä 3. osio on syystä salata luks salauksella, luks = Linux Unified Key Setup, kts esim.

[https://en.wikipedia.org/wiki/Linux\\_Unified\\_Key\\_Setup](https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup) tai <https://itsfoss.com/luks/> .

**B.** Kaikille levyn järjestelmille **yhteinen ohitusosio (swap-osio):** jonka koko on 50 – 100% koneen RAM- muistin koosta, linux-swap tiedostojärjestelmä. Tämän jälkeen asennetaan ko. levyn ensimmäinen järjestelmä.

**C.** Levyn tilansäästämiseksi suositellaan, että kaikille levyn järjestelmille luodaan **yhteinen tietovarasto-osio**. Tämä osio luodaan joko jo asennetun järjestelmän tai seuraavaksi asennettavan järjestelmän USB-asennustikun Levyt- (Disks-) sovelluksella. Osion koko on esim 80 – 160 Gt, ext4 tiedostojärjestelmä. Tämä osio on syystä salata luks salauksella.

Paras tapa tehdä UEFI kaksoiskäyttö- ja monikäyttöjärjestelmiä (dual boot tai multi boot systems) yhdelle levylle on suorittaa em. tehtävät A., B. ja C. levyn ensimmäiselle Linux -järjestelmälle ja sitten asentaa vapaaseen tilaan lisää muita Linux -järjestelmiä suorittamalla niiden osalta vain A. kohdan tehtävät (kolmeen vain ko. järjestelmää koskevaan osioon).

Kovalevyn loppuun on syytä jättää n 5-8 Mt tyhjä ('varaamaton') tila.

**D.** Kovalevylle ensiksi asennetun Linux-järjestelmän käynnistysvalikossa näkyy aluksi vain tämä ensiksi asennettu Linux -järjestelmä. Muut asennetut Linux -järjestelmät saadaan näkymään tässä samassa käynnistysvalikossa seuraavasti: kts. kohta 6.1.I.

### 6.4 UEFI koneet – useita kovalevyjä – useita Linux järjestelmiä

Kun jollekin kovalevylle asennetaan ensimmäinen, toinen (tai kolmas jne.) Linux -järjestelmä, tulee muiden kovalevyjen kaapelit ensin irrottaa. Näin asennettavien uusien järjestelmien käynnistysosiot asentuvat varmasti vain samalle kovalevylle kuin asennettava järjestelmäkin.

Jos useita Linux järjestelmiä asennetaan samalle kovalevylle, niin toimitaan kuten kohdassa 6.3.A, 6.3.B, 6.3.C ja 6.3.D, eli asennukset tehdään asennusohjelman manuaalisella (ei automaattisella) osioinnilla ja järjestelmän perusasennuksella.

Kun perusasennukset on tehty, kone sammutetaan, sen virtajohto/akku irrotetaan ja käynnistetään kone, jotta se saadaan jännitteettömäksi. Vasta sitten kiinnitetään muiden kovalevyjen kaapelit, ja käynnistetään kone uudestaan.

Riippuen koneen emolevyn UEFI tai BIOS/UEFI ohjelmasta **haluttu kovalevy** valitaan joko UEFI:n käynnistysjärjestys -valikon kautta tai EFI -valikon kautta. **Haluttu järjestelmä** valitaan

ko. avautuvan levyn ensimmäisen Linux -järjestelmän käynnistys- eli grub- valikosta, sitten kun ko. levyn ensimmäiselle järjestelmälle on avattu kohdan 6.1.I tehtävien mukaisesti näkymä muihinkin levyille asennettuihin järjestelmiin.

## **7. Lisäoppaat** – pyydä s-postitse:

- Ohje .iso -tiedoston aitouden tarkistamiseen\_ver1.0.pdf
- Manjaro Linuxin perusasennus ja ohjeita pesuasennuksen jälkeen\_ver.1.0.pdf
- Archlinuxin asennus skriptiltä\_ver.1.0.pdf

# Miten muutan LUKS salauksen salausavaimen Linuxissa

Linkki: <https://www.cyberciti.biz/security/how-to-change-luks-disk-encryption-passphrase-in-linux/>

Kirjoittaja: Vivek Gite Last updated: January 6, 2021 – mukailtu suomenkos Kp

Aluksi pitää hankkia salattujen tiedostojärjestelmien sijaintitiedot.

## Vaihe 1.) Tehdään kysely Linux järjestelmän /etc/crypttab tiedostoon

Tiedosto /etc/crypttab sisältää kuvailun LUKS salatuista tiedostojärjestelmistä ja näkymän cat komennolla:

```
sudo cat /etc/crypttab
```

Tässä se, mitä minä näin itse:

```
sda3_crypt UUID=42e50ed0-5055-45f5-b1fc-0f54669e6d1f none luks,discard>
```

Eli, minulla salattuna on sda3\_crypt. Sinun järjestelmässäsi saatat nähdä toisenlaisen nimityksen, kuten "md1\_crypt for RAID-1 protected LUKS disk encryption."

Nyt meillä on tieto osiosta ('partition', toinen nimi on: 'laitteesta - device') ja voimme etsiä sda3 osion osiointimallin komennolla:

```
sudo fdisk -l /dev/sda
```

Komentoni sudo fdisk -l /dev/sda3 tuotti tuloksen:

Disk /dev/sda: 931.5 GiB, 1000204886016 bytes, 1953525168 sectors

Disk model: CT1000MX500SSD1

Units: sectors of 1 \* 512 = 512 bytes

Sector size (logical/physical): 512 bytes / 4096 bytes

I/O size (minimum/optimal): 4096 bytes / 4096 bytes

Disklabel type: gpt

Disk identifier: 1BB1DDD0-47F9-48FB-AA29-69D6A74F4D91

| Device    | Start   | End        | Sectors    | Size   | Type             |
|-----------|---------|------------|------------|--------|------------------|
| /dev/sda1 | 2048    | 1050623    | 1048576    | 512M   | EFI System       |
| /dev/sda2 | 1050624 | 1550335    | 499712     | 244M   | Linux filesystem |
| /dev/sda3 | 1550336 | 1953523711 | 1951973376 | 930.8G | Linux filesystem |

Varmista, että merkitset em. komentoon oikein sen osion oikean nimen, tässä sda3, joka on sinun järjestelmässäsi.

## Vaihe 2.) Haetaan LUKS salatun osion ylätunniste

Aja seuraava komento saadaksesi selville tietoa sinun salatusta /dev/sda3 osiosta:

```
sudo cryptsetup luksDump /dev/sda3
```

Minun LUKS salatun osion ylätunnisteen tie<https://www.cyberciti.biz/security/how-to-change-luks-disk-encryption-passphrase-in-linux/dot>:

```

LUKS header information
Version:      2
Epoch:       4
Metadata area: 16384 [bytes]
Keyslots area: 16744448 [bytes]
UUID:        42e50ed0-5055-45f5-b1fc-0f54669e6d1f
Label:       (no label)
Subsystem:   (no subsystem)
Flags:       (no flags)

Data segments:
 0: crypt
    offset: 16777216 [bytes]
    length: (whole device)
    cipher: aes-xts-plain64
    sector: 512 [bytes]

Keyslots:
 0: luks2
    Key:        512 bits
    Priority:    normal
    Cipher:     aes-xts-plain64
    Cipher key: 512 bits
    PBKDF:      argon2i
    Time cost:  7
    Memory:     1048576
    Threads:    4
    Salt:       fc 9d b7 e0 ec 06 d0 b1 47 09 61 6f c1 73 f9 51
                b7 ff 9b 6b 44 a0 2b c5 dd 5a c4 7e 46 28 c3 62
    AF stripes: 4000
    AF hash:    sha256
    Area offset: 32768 [bytes]
    Area length: 258048 [bytes]
    Digest ID:  0

Tokens:
Digests:
 0: pbkdf2
    Hash:       sha256
    Iterations: 136107
    Salt:       40 82 65 fc cf e1 24 d3 0d b8 85 07 13 c7 dd a1
                03 52 6a b9 04 b8 6d 23 4a d1 90 89 cb 96 a7 ca
    Digest:     5b d0 10 56 e4 9a ff e1 eb 14 2a fb 4d 85 ba c3
                a7 75 fa fa 6c 24 cc 01 b0 9c 34 dd 48 98 1a d9

```

Tästä näemme, että minulla on vain yksi salausavain, joka on salausavaimen tilassa slot 0 :ssa, mutta monista järjestelmistä saattaa löytyä jopa 8 salausavainta, jotka ovat salausavaimien tiloissa slot 0 ... slot 7. Siksi vaiheessa 3 näemme miten määritellään sinun LUKS salausavaimen tila (slotti).

### Vaihe 3.) Selvitetään, minkä paikan ([slot:in](#)) Linuxin asennusohjelma on määritellyt sinulle

Tämän selvittämiseksi ajetaan seuraava komento:

Komennon syntaksi: `sudo cryptsetup --verbose open --test-passphrase /path/to/dev/`  
**Esimerkiksi:** `sudo cryptsetup --verbose open --test-passphrase /dev/sda3`

Tämä komento kertoo, missä [slot:ssa](#) LUKS salausavain sijaitsee:

Enter passphrase for /dev/sda3:  
 Key slot 0 unlocked.  
 Command successful.

### Vaihe 4.) Vaihetaan kovalevyn LUKS salausavain Pääteen komennolla

Edellä olemme hakeneet tiedot LUKS salausavaimen päivittämiseen / muuttamiseen. Huomaa, että salausavain muistuttaa tavallista salasanaa, mutta se on turvallisuussyistä yleensä sitä pidempi. Komennon muoto (syntaksi) on

```
sudo cryptsetup luksChangeKey /dev/sda3 -S 0
```

Kirjoita aluksi nykyinen salausavain ja paina Enter. Mikäli kirjoitit salausavaimen oikein, pääset muuttamaan sen kirjoittamalla uuden salausavaimen kahteen kertaan seuraavasti:

```
Enter passphrase to be changed:
Enter new passphrase:
Verify passphrase:
```

#### Vaihe 5.) Varmista uusi salausavain

Käynnistä Linux käyttöjärjestelmä uudestaan tai aja Pääteellä uuden salausavaimen simulaatio komennolla:

```
sudo cryptsetup --verbose open --test-passphrase /dev/sda3
```

## Miten voit käyttää graafista Gnome -työpöydän 'Levyt' -sovellusta salausavaimen muuttamiseen:

Linuxin uudet kehittäjät ja käyttäjät saattavat pitää Pääteen komentojen käytön monimutkaisiksi. Linuxin käyttäjät voivat em. komentojen sijaan käyttää Gnome -työpöydän Levyt -sovellusta (= Disks)

Gnome -työpöydän Levyt -sovellus ja se avautuu joko Sovellukset -kansion kuvakkeesta tai Pääteeltä komennolla `$ gnome-disks`.

Kun Levyt -sovellus on avattu, sen vasemman reunan valikosta voi valita ko. kovalevyn sekä valita siltä se LUKS suojattu osio, jonka salausavainta halutaan muuttaa. Klikkaa levykuvan vasemmassa alalaidassa olevaa avoimen lukon kuvaa (jon päälle tulee teksti 'Avaa ...') ja avaa ko. osion LUKS -salaus sen nykyisellä salausavaimella. Sitten voi muuttaa tämän salausavaimen toiseen klikkaamalla levykuvan vasemmassa alalaidassa olevaa kahden hammasrattaan kuvaketta → valitse avautuvasta valikosta 'Vaihda tunnuslause ...' → se avaa **uuden valikon**, joka pyytää kirjoittamaan ensin nykyisen salausavaimen ja sitten 2 kertaan uuden salausavaimen sekä näyttää jos uusi salausavaimesi on heikko; samoin tässä valikossa kirjoitettujen salausavainten merkit saa näkymään ruksaamalla 'Näytä tunnuslauseet'. Uusi salausavain on vahva, kun sen mittari muuttuu vihreäksi ja se sanoo Strong'. Vahvista muutos valitsemalla 'Muuta'. **Tämän jälkeen lukitse ko. kovalevyn osio takasin, jolloin ko. osion sisällä oleva lukon kuva on suljettu sekä levykuvan vasemmassa alalaidassa on taas avoimen lukon kuva.** Poistu vasta sitten tästä sovelluksesta.

## Yhteenveto

Edellä kuvattiin LUKS salausavaimen päivittäminen tai muuttaminen Pääteellä ja graafisella sovelluksella. Tässä muutettiin vain sinulle osoitetun [slot:n](#) salausavain. LUKS:ssa on myös pääavain (master key), jota ei voida muuttaa ilman uudelleen kryptaamista. LUKS:n pääavainta käytetään LUKS kontin (container) salauksen avaamiseen ilman salausavainta ja ilman LUKS -otsikkoa. Eli, mikäli pääavain on murrettu, koko kovalevyn osio on poistettava sen sisältöön pääsyn estämiseksi. Suosittelen vahvasti, että luet LUKS:n dokumentaation netissä tai kirjoittamalla Pääteellä seuraavan ohjeistus komennot (manual command):

```
$ man cryptsetup
$ man crypttab
```

Tämä osa 3. osa tätä 5 osan artikkeleita koskein LUKS salausta (alla ko. artikkelien aiheet ja niiden linkit):

#### 1. Linux Hard Disk Encryption With LUKS

<https://www.cyberciti.biz/security/howto-linux-hard-disk-encryption-with-luks-cryptsetup-command/>

#### 2. Backup and restore LUKS header on Linux

<https://www.cyberciti.biz/security/how-to-backup-and-restore-luks-header-on-linux/>

#### 3. Change LUKS disk encryption passphrase on Linux

<https://www.cyberciti.biz/security/how-to-change-luks-disk-encryption-passphrase-in-linux/>

#### 4. Unlock LUKS using Dropbear SSH keys remotely in Linux

<https://www.cyberciti.biz/security/how-to-unlock-luks-using-dropbear-ssh-keys-remotely-in-linux/>

#### 5. Add/enable LUKS disk encryption with keyfile on Linux

<https://www.cyberciti.biz/hardware/cryptsetup-add-enable-luks-disk-encryption-keyfile-linux/>

## Miten lisään uuden LUKS salausavaimen olemassa olevaan Linuxin LUKS asennukseen

Linkki: <https://forum.mxlinux.org/viewtopic.php?t=69270>

Huom. Alla olevat kohdat punaisella ovat vain tämän ohjeen ymmärtämisen helpottamista varten.

**Kohta 1. Etsi ensin minkä asennetun Linux osiossa on LUKS -salaus ajamalla komento:**

```
sudo cat /etc/crypttab
```

```
sda3_crypt UUID=42e50ed0-5055-45f5-b1fc-0f54669e6d1f none luks,discard>
```

eli tässä se on esimerkiksi **sda3**.

**Toinen tapa todeta tämä on avata Gparted -sovellus ja katsoa mikä osio on salattu, tai – jos sinulla on Linuxissa Gnome -työpöytä → avaa sen Levyt -sovellus ja katso mikä osio on salattu.**

**Kohta 2. Aja sitten nykyisen salausavaimen testi:**

Aja ensin:

```
sudo cryptsetup luksDump /dev/sda3 ==> Testaa sitten em. osion LUKS jo olemassa oleva salausavain ajamalla
```

```
sudo cryptsetup --verbose open --test-passphrase /dev/sda3
```

```
Enter passphrase for /dev/sda3:
Key slot 0 unlocked.
Command successful.
```

Tämä testi kertoo, että:

- sda3:lla on salaus ja
- sda3:lle annettu salausavain on oikea

**Kohta 3. Tarkista, mitkä sda3 osion LUKS -salausavainten paikat on jo varattuja ajamalla**

```
sudo cryptsetup luksDump /dev/sda3 ==> Tulos ==> tässä alla esimerkiksi:
```

” LUKS header information for /dev/sda3

```
Version:          1
Cipher name:      aes
Cipher mode:      xts-plain64
Hash spec:        sha256
Payload offset:   4096
MK bits:          512
MK digest:        95 a .....
MK salt:          7d .....
                  47 g.....
MK iterations:    97814
UUID:             478f523 .....
```

### Key Slot 0: ENABLED

```
Iterations:       15 ...06 (muutettu)
Salt:             xyz123 (muutettu)
                  zyx123 (muutettu)
Key material offset: 8
AF stripes:       4000
```

### Key Slot 1: ENABLED

```
Iterations:       15 ....26 (muutettu)
Salt:             xyz123 (muutettu)
                  xyz123 (muutettu)
Key material offset: 8
AF stripes:       4000
```

Key Slot 2: DISABLED

Key Slot 3: DISABLED  
Key Slot 4: DISABLED  
Key Slot 5: DISABLED  
Key Slot 6: DISABLED  
Key Slot 7: DISABLED

Tämä testi kertoo lisätiedon, että:

- sda3 osiolla salausavaimen paikat (slotti) **slot 0 ja slot 1 on jo varattu** ensimmäistä ja toista salausavainta varten ja
- siksi sda3:lla on vielä **vapaana 6 paikkaa (slot 2 ..slot 7) uusia salausavaimia varten**

#### Kohta 4. Lisää uusi salausavain automaattisesti seuraavaan vapaaseen paikkaan

Tässä lisätään automaattisesti uusi salausavain em. sda3 osion uuteen paikkaan (slotiin 2) seuraavasti:

**sudo cryptsetup -v luksAddKey /dev/sda3**

Enter any existing passphrase:

(Kirjoita jokin olemassa oleva salausavain => tässä kirjoitettu slot 0:n salausavain)

Key slot 0 unlocked.

(Ja siksi slotti 0 on nyt avattu)

Enter new passphrase for key slot:

(Kirjoita UUSI salausavain)

Verify passphrase:

(Varmista UUSI salausavain)

Key slot 2 created.

(Luotiin UUSI salausavain paikkaan (slotti) slot 2, joka oli seuraava vapaana oleva ja lähimpänä slotti 0:aa oleva salausavaimen paikka)

Command successful.

Tulos: Nyt käytössäsi on 2 salausavainta: yksi (alkuperäinen) paikalla slot 0 ja toinen (uusi) paikalla slot 2.

#### Kohta 5. Tarkista vapaat paikat ajamalla

**sudo cryptsetup luksDump /dev/sda3** ==> ja saat tulokseksi:

”LUKS header information for /dev/sda3

Version: 1  
Cipher name: aes  
.... (muutettu)  
.... (muutettu)  
MK iterations: 97814  
UUID: 478f523.....

##### Key Slot 0: ENABLED

Iterations: 15 ...06 (muutettu)  
Salt: xyz123 (muutettu)  
zyx123 (muutettu)  
Key material offset: 8  
AF stripes: 4000

##### Key Slot 1: ENABLED

Iterations: 15 ....26 (muutettu)  
Salt: xyz123 (muutettu)  
xyz123 (muutettu)  
Key material offset: 8  
AF stripes: 4000

##### Key Slot 2: ENABLED

Iterations: 15 ....26 (muutettu)  
Salt: xyz123 (muutettu)  
xyz123 (muutettu)  
Key material offset: 8  
AF stripes: 4000

Key Slot 3: DISABLED  
Key Slot 4: DISABLED  
Key Slot 5: DISABLED  
Key Slot 6: DISABLED  
Key Slot 7: DISABLED

Eli, nyt sda3:ssa 3 paikkaa (slot 0, slot 1 ja slot 2) on nyt varattu ja 5 paikkaa on vielä vapaana.

## Miten poistan LUKS salausavaimen olemassa olevasta Linuxin LUKS asennuksesta

<https://unix.stackexchange.com/questions/60971/how-to-remove-luks-encryption>

Mikäli Linux asennuksessa LUKS salausavaimia on enemmän kuin yksi (1), tarpeettoman salausavaimen voi poistaa komennolla **cryptsetup luksRemoveKey** – vähintään 1 pitää jättää.

### 1. Ensin katsotaan missä sda3 -osion LUKS slotissa on salausavain:

**Komento:** `sudo cryptsetup luksDump /dev/sda3`

```
[AB@ax ~]$ sudo cryptsetup luksDump /dev/sda3
[sudo] AB-käyttäjän salasana:
```

Tulos:

```
...
Keyslots:
  0: luks2
    Key:        512 bits
  ...
  1: luks2
    Key:        512 bits
```

Eli sda3 -osion **kahdessa LUKS -slotissa** on salausavain (**slot0 ja slot1**) ja tiedämme mitkä ne ovat.

### 2. Poistetaan salausavain slotista 1 (ja pidetään slot0:n salausavain):

Ensin testataan, että olemme poistamassa oikeaa (poistettavaksi valittua) salausavainta:

`sudo cryptsetup --verbose open --test-passphrase /dev/sda3`

```
[AB@ax ~]$ sudo cryptsetup --verbose open --test-passphrase /dev/sda3
```

```
[sudo] AB-käyttäjän salasana:
```

No usable token is available.

Kirjoita salasanalause kohteelle /dev/sda3:                      --> Kirjoitimme tähän slot1:n salausavaimen

**Key slot 1 unlocked.**

**Command successful.**

```
[AB@ax ~]$
```

Nyt tiedämme missä slotissa on poistettava salausavain ja mikä se on.

### 3. Poistamme valitun salausavaimen osiosta sda3:

**Komento:** `sudo cryptsetup -v luksRemoveKey /dev/sda3`

```
[AB@ax ~]$ sudo cryptsetup -v luksRemoveKey /dev/sda3
```

```
[sudo] AB-käyttäjän salasana:
```

**Kirjoita poistettava salasanalause:**                      --> Kirjoitimme tähän slot1:n salausavaimen

Key slot 1 unlocked.

Keyslot 1 is selected for deletion.

Key slot 1 removed.  
Command successful.  
[AB@ax ~]\$

#### 4.0 Tarkistamme poistamisen tuloksen kahteen kertaan:

##### 4.1 Tarkistus 1 →

```
sudo cryptsetup luksDump /dev/sda3
```

Tulos:

...

Keyslots:

0: luks2

Key: 512 bits

Eli nyt vain slot0:ssa on salausavain jäljellä.

##### 4.2 Tarkistus 2 → Tarkistamme, että meillä on tallessa sda3 -osion slot0:n oikea salausavain:

```
[AB@ax ~]$ sudo cryptsetup --verbose open --test-passphrase /dev/sda3
```

[sudo] AB-käyttäjän salasana:

No usable token is available.

Kirjoita salasanalause kohteelle /dev/sda3:

--» Kirjoitimme tähän slot0:n salausavaimen

Key slot 0 unlocked.

Command successful.

[AB@ax ~]\$

Eli nyt tiedämme sad3 -osion slot0:n salausavaimen. Pidä se varmassa tallessa!