Guide til kryptering med TrueCrypt

Om TrueCrypt

TrueCrypt er et open source, gratis og multi-platform krypteringsprogram. Det virker til Linux, Windows og Mac. Det kan hentes på deres officielle hjemmeside.

Indledning

At bruge TrueCrypt kan være lidt teknisk, men denne guide har til hensigt at guide dig igennem opsætning og kryptering af dine drev, så nemt og smertefrit som muligt. Det skal siges at der altid er en risiko for at tingene ikke går som ventet, så før du kryptere et drev med hjælp fra denne guide, skal du have en kopi af de data du ikke vil miste (skulle uheldet være ude). TrueCrypt fungere ved at man kryptere en harddisk, og når den er krypteret så "mounter" man den til et andet drevbogstav.

Kan du svare JA til 1 eller flere af nedstående punkter, skal du **ikke** anvende denne guide:
- Har du mere end 1 styresystem installeret?
- Ønsker du kun at kryptere enkelte filer / mapper, og IKKE et helt drev eller en partition?

Forberedelser

- Hent seneste version her og installer det.

Der er en dansk sprogpakke tilgængelig, den bruger jeg dog ikke i denne guide. Kan hentes her.

- Start TC via genvejen på dit skrivebord - programmet ser således ud når du åbner det.

Programmet SKAL startes som administrator! Højreklik evt og vælg Kør som administrator.

Kryptering af system-drev

Denne guide dækker KUN kryptering af drevet Windows starter fra!
For ALLE andre drev-typer, se denne guide

Opsætning af kryptering

- Gå op i **System** -> **Encrypt System Partition/Drive**
- Vælg **Normal mode** & **Encrypt the Windows system partition**

Får du en besked om at du kun har en partiton, trykker du bare **No**

- Tryk **Next** til du skal indtaste dine password.
- Indtast et password og tryk **Next**

Mht længde og styrke anbefaler jeg mindst 8 tegn, og en sammensætning af store og små bogstaver, samt specielle tegn.

- Bevæg musen rundt for at generere tilfældige data. Jo længere tid jo bedre.

Får du en fejl nu? Så genstart programmet - og kør det med administrator rettigheder!

- TC vil nu oprette en Rescue Disc (imagefil). Du skal trykke **Browse** og gemme den på skrivebordet.

Filnavnet er ligegyldigt, men for at gøre det nemt bør filnavnet slutte med .iso

- TC vil nu brænde disken ud. Gør det, eller snyd den.

Du snyder den ved at åbne ISO-filen med MagicISO, Daemon Tools, osv. Du bør gemme ISO-filen, da det er din eneste måde at dekryptere drevet på hvis Windows en dag ikke starter op.

- Når Imagefilen er brænd ud / mounted, trykker du **Next** til TC spørger om **Wipe Mode**.
- Ved Wipe Mode skal du vælge **None** (Det går væsentligt hurtigere!) - Tryk **Next**.

Benytter du Wipe, vil TC overskrive den sektor der krypteres, før den skriver dine data til sektoren. Det er IKKE formatering af drevet!

Du er nu klar til at begynde SELVE krypteringen af dit systemdrev. Trykker du Test på næste side, installeres de ting der er nødvendige for at dit krypterede drev kan bootes, og derefter genstartes din PC. Dette gøres for at sikre sig at de ting der installeres rent faktisk fungere (det er ikke fedt at kryptere sit drev, for så at finde ud af at det ikke kan boote).

Tryk på Test, og der kommer et vindue frem. **Gem den tekst således at du har den liggende, i fald du ikke kan starte din PC igen!** Ligeledes, **lad være** med at genstarte før du har din Rescue Disc liggende et sted - om ikke andet således at du kan brænde en kopi! Når din PC genstarter, bør du møde denne skærm. Der indtaster du bare dit password.

Tryk Ok, og din PC genstarter. Du kan ikke afbryde den genstart, og du kan ikke udsætte den når først den er sat i gang, så gem dine ting først.

Selve krypteringen

Når din PC er genstartet korrekt, kan selve krypteringen begynde.

Du vil blive mødt med denne besked, som fortæller dig hvad vi allerede ved - nemlig at testen gik godt. Du kan nu trykke Encrypt eller Defer. Defer vil udsætte krypteringen, og Encrypt siger vist sig selv. Når krypteringen starter, ser det således ud.

Det er vigtigt at du ikke genstarter din PC imens krypteringen er igang. Du risikere at du ikke kan starte op igen!

Kryptering af ANDRE drev

Vil du kryptere dit boot-drev istedet, eller har du ikke TrueCrypt installeret? Så se her.

Inden du starter!

- Skift ikke drevbogstav imens programmer der er afhængige af det kører.
- Hvis din PC crasher imens du kryptere et drev, mister du IKKE data.
- Et drev behøver IKKE en formatering for at blive krypteret (det går dog hurtigst).
- Kryptere du data i RAID anbefaler jeg at det er et hardware raid! TC understøtter software raids, meeen..
- Vil du kryptere UDEN formatering, SKAL dine drev være NTFS. Se her hvordan du konvertere fra FAT32 til NTFS.
- Det er NEMMEST at bruge samme kode til ALLE drev (det er sikrest at have forskellige, men har du kun 1, skal du kun indtaste 1 kode ved opstart af Windows)

Krypteringen af dine drev

- Åbn TrueCrypt (husk at starte det som administrator)
- Gå op i **Volumes** -> **Create New Volume**.
- Vælg **Encrypt a non-system partition/drive** og **Standard TrueCrypt volume**
- Tryk **Select Device** og vælg den **partition** (IKKE harddisk) du vil kryptere og tryk OK. Den kan kendes på sit drevbogstav.

- Er drevet **100% TOMT** vælger du Create encrypted volume **and format it**, ellers vælger du den nederste Encrypt partition in place.

Valgte du at formatere og så kryptere:

Quote:

> - Under encryption options trykker du bare Next (det er nogle tekniske indstillinger omkring hvordan dine data krypteres)
> - TrueCrypt viser dig størrelse fysiske placering af drevet du kryptere. Verificer at det er det rigtige drev, og tryk next.
> - Indtast et password og tryk **Next**. Der er intet om keyfiles i denne guide (det kommer aldrig).
> Mht længde og styrke anbefaler jeg mindst 8 tegn, og en sammensætning af store og små bogstaver, samt specielle tegn.
> - Sæt hak i **Quick Format** og flyt musen i 5 - 10 sek. Tryk derefter **Format**. ALLE DINE DATA PÅ DREVET SLETTES!!!
>
> Glemte du at sætte hak ved Quick Format? Så har du nok fortrudt det nu. Bare tryk Abort, og lav det om.

Valgte du at kryptere uden formatering:

Quote:

> - Under encryption options trykker du bare Next (det er nogle tekniske indstillinger omkring hvordan dine data krypteres)
> - Indtast et password og tryk **Next**. Jeg har ikke lavet understøttelse for keyfiles i denne guide, og det kommer aldrig.
> Mht længde og styrke anbefaler jeg mindst 8 tegn, og en sammensætning af store og små bogstaver, samt specielle tegn.
> - Bevæg musen rundt for at generere tilfældige data (5 - 10 sek er helt fint). Tryk Next.
> - Vælg None ved Wipe Mode. Det overskriver hver sektor X antal gange, før dine data skrives til sektoren.
> Det formatere IKKE dit drev, men det mangedobler tiden en kryptering tager!
> - Tryk Next og derefter Encrypt.
> Tryk Defer nede i højre hjørne for at udsætte krypteringen (hvis du skal genstarte, etc).
> Du kan ikke bruge drevet før det er 100% krypteret, men du mister ikke data ved at udsætte!

Gentag overstående for alle de drev du vil kryptere!

Bevaring af drevbogstaver.

Når en partition eller harddisk er krypteres med TrueCrypt, skal den loades ("mountes") før det kan bruges. Når den loades via TrueCrypt, får den et drevbogstav tildelt på ny (Drev X), og vil derfor ikke bruge samme drevbogstav som før (Drev Y). Drev Y er nu krypteret, men hvis der stadig er et drevbogstav tildelt, vil det blive vist under Denne Computer, selvom det ikke kan læses af Windows, da det er krypteret. Drev X kan dog læses, da det er det TrueCrypt-loadede drev. Et eksempel kan ses her, hvor min USB-pen på 1.9 GB er tilgængelig i ukrypteret form (Drev H), samt i krypteret form, loadet via TrueCrypt (Drev L). Drev H kan Windows ikke bruge til noget som helst, hvorimod drev L kan ses som en hvilken som helst andet harddisk. At bevare drevbogstaver går ud på at fjerne drevbogstavet fra drev H, således at der kun er drev L tilbage. TrueCrypt benytter den fysiske placering (Harddisk 5Partition 1) til at finde disken, og ikke drevbogstavet.

1. Højreklik på Denne Computer og vælg Administrer // Manage

2. I vinduet der åbner vælger du Diskhåndtering // Disk Management ude til venstre.
3. Derefter højreklikker du et drev og vælger Skift drevbogstav og sti // Change Drive Letter and Paths
4. I vinduet der åbner markere du drevbogstavet og trykker Fjern // Remove og Ja // Yes.
Fjern drevbogstavet for alle drev der er krypteret. Får du denne fejl skal du lukke programmer der bruger disken, eller genstarte.

Adgang til krypterede drev:

- Åbn TrueCrypt. Højreklik på det drevbogstav hvortil du ønsker din krypterede harddisk tilknyttet.
- Fra menuen der kommer frem vælger du **Select Device and Mount**.
- I vinduet der åbner vælger du din harddisk, og indtaster koden.
- Gentag dette for alle krypterede drev der skal mountes/loades

Tips & Tricks (Avanceret opsætning)

Nogle indstillinger gør TC bedre / nemmere at bruge, hvis indstillet korrekt. De vil blive gemmengået her.

Auto-mount af drev ved boot

Har du et drev krypteret du ikke booter fra, kan du få dem åbnet automatisk når Windows er startet. Det gøres således:

- Åbn TC og mount alle de drev du ønsker auto-mounted ved opstarten af Windows.
- Gå op i **Volumes** og vælg **Save Currently Mounted Volumes as System Favorites**

De mountede volumes er nu dine favoritter, og det gør at vi kan få dem auto-mounted

- Gå op i **Settings** og vælg **System Favorite Volumes**
- Sæt hak i den øverste box (og den nederste hvis du vil) - Tryk OK bagefter.

Har du mere end 1 drev som favorit-drev, og bruger alle drev samme kode, bør du også gøre disse ting:

- Gå op i **Settings** og vælg **Preferences**
- Sæt hak ved Cache password in driver memory og tryk Ok.

Tilbage til toppen