Lokal lagring og bruk av sensitive data

Are Edvardsen, SKDE

2017-09-11

Innhold

Figurer

Forord

Introduksjon

Analyse av sensitive og tidsavgrensede data inngår som en del av de praktiske oppgaven SKDE har. Egenskapene til slike data vil typisk være at de kun skal nås av en begrenset og definert gruppe av brukere samt at de effektivt må kunne slettes ved gyldighetsperiodens utløp. Dette gir noen spesielle utfordringer når brukere samtidig skal kunne arbeide effektiv og dele slike data seg imellom. Typisk for analysevirksomhet er også at det genereres store mengder avledede data i form av ulike analysedatasett. Slike avledede data må også kunne slettes effektivt når gyldighetsperioden utløper.

Dette dokumentet beskriver hva brukeren skal gjøre for kunne ta i bruk den infrastruktur som er etablert ved SKDE for slike formål.

Leserveiledning

Målgruppen for denne brukermanualen er analysemedarbeidere og personer med teknisk ansvar ved SKDE som skal ha befatning med sensitive og tidsavgrensede data. Dokumentet kan også brukes som en beskrivelse av de sikkerhetstiltak som er gjort ved SKDE. I så fall må det sees i sammenheng med annen utfyllende dokumentasjon som SKDE sin sikkerhetsinstruks og internkontrollrutiner. Referanser til navn, filnavn, filstier, aksjonspunkter og lignende i teksten er *uthevet*.

I tillegg er det gjort uthevinger der det er budskap i tilgrensende tekst som er særlig verdt å merke seg:

Utfyllende opplysninger, men som ikke er vesentlig for å følge brukerveiledningen.

Utheving av et viktig moment.

Et vesentlig budskap som om det blir misforstått innebærer en fare.

Dokumenthistorie

Brukerveiledningn ble opprinnelig utviklet i forbindelse med formell etablering av sikkerhetsinstruks og internkontrollrutiner ved SKDE. Gjeldende versjon av brukermanual for sikring av data (lagring og sletting)

ved lokal lagring er et tatt ut fra en større sammenheng som også omhandlet sikker sentralisert lagring (*Sarkofag*). Sikker sentralisert lagring skulle ivareta behovet for samarbeid (om data) mellom personer særlig hos analyseenheten ved SKDE. Ved innføring og bruk av sentraliserte *SAS* servere falt dette behovet bort.

Metoden for sikring av data på lokale lagringsmedier var opprinnelig basert på programvaren *TrueCrypt*. På et tidspunkt ble videre utvikling og vedlikehold av *TrueCrypt* stanset og trygg framtidig bruk kunne derfor ikke garanteres. Siden *TrueCrypt* var i utsrakt bruk av mange ble teknologien videreført av andre aktører men da under navnet *VeraCrypt*. De hos SKDE som fra før har brukt *TrueCrypt* vil gjenkjenne det meste som beskrives i denne brukermanualen.

Gjeldende status for dokumentet er versjon 0.9 som ligger til godkjenning hos ledergruppa ved SKDE. Are Edvardsen har ansvar for innarbeiding av nødvendige endringer fortløpende. Det er også mulig for andre å (foreslå) endringer direkte i dokumentet ved "pull requests" gjennom GitHub[1].

[1] `https://github.com/areedv/docSens/`

Kapittel 1

Infrastruktur

Den tekniske infrastrukturen som er etablert ved SKDE går i grove trekk ut på å behandle data på kryptert form både hva angår lagring og transport. I tillegg fins det en egen sikkerhetsinstruks som alle ansatte på SKDE skal etterleve. Sikkerhetsinstruksen regulerer også spesifikt hvordan ansatte med tilgang til sensitive og tidsavgrensede data skal forholde seg dette i sitt arbeid.

Bruk av den tekniske infrastrukturen forutsetter tilgang til SKDE sitt interne datanettverk. Ansatte på SKDE som er satt opp med hjemmekontor (VPN/Citrix) vil kunne nå denne infrastrukturen også utenfor SKDE sine kontorlokaler.

1.1 Lokal bruk

Hver bruker skal benytte verktøy som muliggjør kryptert lagring av data på eget/lokalt lagringsmedium slik som harddisk, minnepinne, CD-plater og lignende. Nøkkelen som benyttes til kryptering skal være tydelig definert slik at sletting av denne kan benyttes som en metode for effektiv sletting av lokale data.

1.2 Sikkerhetsinstruksen ved SKDE

SKDE har en egen sikkerhetsinstruks som skal styre hvordan de ansatte skal forholde seg for å ivareta de sikkerhetskrav som gjelder for virksomheten. Her er det også beskrevet rutiner for arbeid med sensitive data, herunder også data med tidsavgrensning og dermed krav til sletting. Stabsleder ved SKDE er ansvarlig for sikkerhetsinstruksen og at denne etterleves.

Hver person som skal jobbe med tidsavgrensede data må i forkant av utleveringen skrive under en egenerklæring som bekrefter at slike data er mottat. Ved gyldighetsperiodens slutt signeres et nytt felt i samme erklæring som bekreftelse på at data er slettet i henhold til de prosedyrer som sikkerhetsinstruksen gir. Alle egenerklæringer oppbevares ved stabsenheten og vil inngå som en del av virksomhetens dokumentasjon på egne sikkerhetstiltak.

Kapittel 2

Brukerveiledning

En forutsetning for effektivt analysearbeid vil ofte være å kunne jobbe med data på lokal datamaskin. Når dette gjelder sensitive data skal disse krypteres ved lagring også hos brukeren. Dette er en forutsetning for å gi en tilstrekkelig beskyttelse mot uautorisert innsyn i data, for eksempel ved tyveri, og som et tiltak for rent praktisk å kunne slette alle data når disse har en begrenset gyldighetsperiode.

2.1 Oppsett og bruk av kryptering på lokale lagringsmedier

Lagring av sensitive data på egen datamaskin eller andre lokal lagringsmedier (*e.g.* CD, minnepinne) skal skje kryptert slik at den bare kan leses av den som har riktig nøkkel. Sensitive data vil derfor ikke kunne falle uvedkommende i hende hvis lagringsmediet kommer på avveie ved for eksempel tap eller tyveri. I tillegg vil man kunne oppnå effektiv sletting av data ved at respektiv nøkkel slettes.

Flere vertøy kan brukes for å oppnå lokal kryptering av data. Her er det tatt utgangspunkt i VeraCrypt[1]

2.1.1 Last ned og installér VeraCrypt

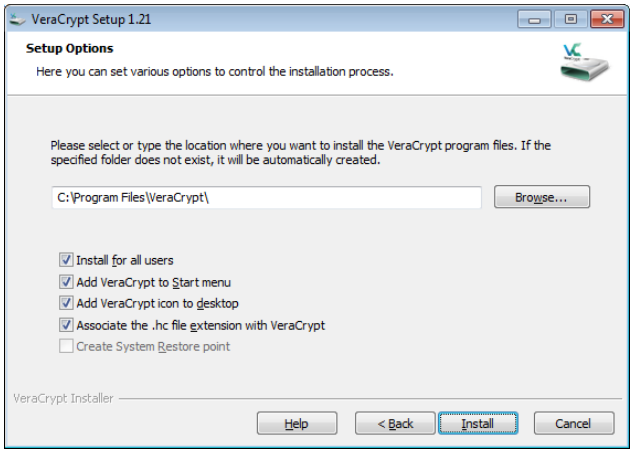
VeraCrypt er fri og åpen programvare og kan lastes ned gjennom lenken som er angitt her[2]. Velg riktig variant i forhold til ønsket operativsystem, her vist for *Windows 7/Vista/XP/2000* med versjon 1.21 av *VeraCrypt*.

Intallasjon av *VeraCrypt* krever adminstratorrett til datamaskinen som installasjonen foretas på. Hvis man fra før ikke har (lokal) administratortilgang er man nødt til å be HNIKT om hjelp til installasjonen

Kjør den nedlastede fila og godta lisensvilkårene. I det neste vinduet velges *Install* og trykk deretter på *Next*. Vinduet vist i figure 2.1 skal da komme opp:

Installasjonsprogrammet foreslår en plassering av programmet, og med mindre det fins gode grunner til å gjøre det motsatte, godta det som er valgt. Avhengig av de privilegier man har som bruker av sin egen datamaskin, kan man velge å installer *VeraCrypt* for alle brukere (første avkryssningsalternativ i Figur 2.1). Trykk deretter *Install*. Om alt gikk riktig for seg får man et nytt vindu med teksten "VeraCrypt has been successfully installed". Trykk *OK*.

[1] https://veracrypt.codeplex.com/
[2] https://veracrypt.codeplex.com/



Figur 2.1: Installasjon av VeraCrypt.

Det er mulig det ved slutten av installasjonen gis tilbud om å lese dokumentasjon på *VeraCrypt*, og det er vel anvendt tid å gjøre. Ved seinere behov fins denne dokumentasjonen tilgjengelig på nettsida[3] der programmet lastes ned fra.

2.1.2 Oppsett av VeraCrypt

VeraCrypt kan benyttes på mange vis, og denne veilednigen er ikke uttømmende men beskriver typisk bruk ved SKDE. Ved behov utover dette må man lese tilgjengelig dokumentasjon samt konferere med andre brukere.

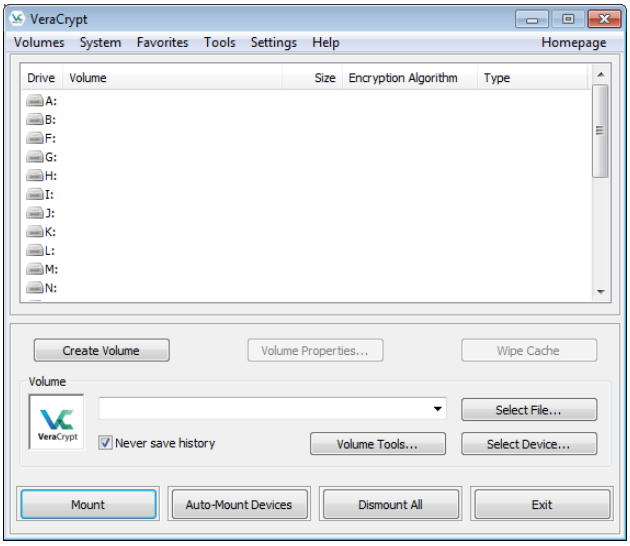
Etter riktig oppsett av *VeraCrypt* krypteres informasjon ved å lagre data til en disk som *VeraCrypt* har satt opp. *VeraCrypt* kaller dette for et *volum* eller *diskvolum* og vil for eksempel i *Windows* framstå som hvilken som helst annen disk med en egen bokstav (*e.g. I:*). Det som skjer under oppsett av et *VeraCrypt* volum er at ei fil med definert størrelse blir satt av på et angitt lagringsmedie. *VeraCrypt* kaller denne fila for en kryptert filkontainer og det er denne fila som inneholder krypterte data. Ved oppstart monterer *VeraCrypt* denne fila som et volum som det da er mulig å skrive til (lagre) og lese fra (åpne).

Følgende viser et oppsett av en kryptert disk på 100 Mb (i mange tilfeller vil det være behov for å sett av mer plass). Ved oppstart av *VeraCrypt* vil man se vinduet vist i figur 2.2.

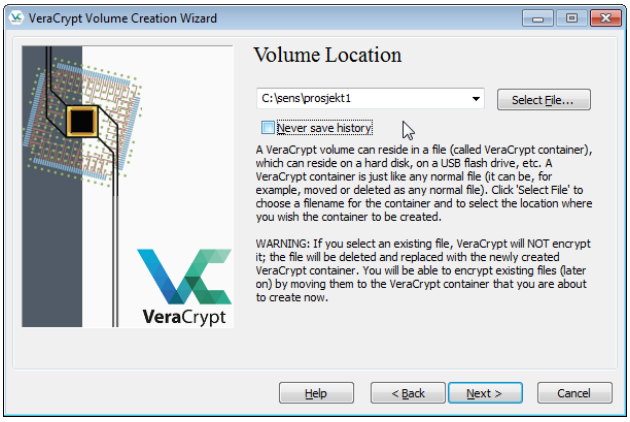
Trykk på *Create volume*. I påfølgende vindu (ikke vist) velges *Create an encrypted file container* og trykk *Next*. I vinduet deretter velg *Standard VeraCrypt volume* og trykk *Next*. Da skal man se vinduet vist i figur 2.3.

Her definerer man den krypterte filkontaineren, i dette tilfellet *C:\sens\prosjket1*. Fjern avkryssing for *Never save history* og trykk *Next*. I det påfølgende vinduet, trykk *Next* uten å endre på det som installasjonsprogrammet har foreslått av innstillinger.

Kryptoalgoritmen som benyttesom standard i *VeraCrypt* er *AES-256* som gir god nok beskyttelse for sensitive data som SKDE er befatning med. Det er derfor ingen grunn til ikke å velge standard instilling her.



Figur 2.2: Oppsett av ny kryptert disk.



Figur 2.3: Oppsett av kryptert filkontainer.

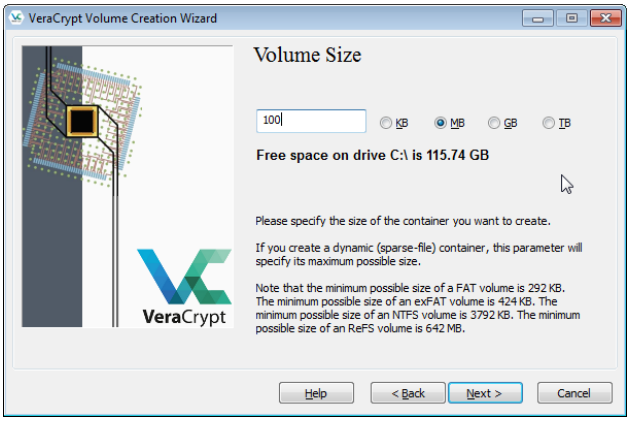
Deretter angis størrelsen på det nye krypterte diskvolumet, eksempelvis slik det er vist i 2.4.

Trykk *Next*. I påfølgende vindu velger (og bekrefter) man et sterkt passord (åtte tegn bestående av store og små bokstaver, tall og spesialtegn) og krysser av for *Use keyfiles* slik det er vist i 2.5.

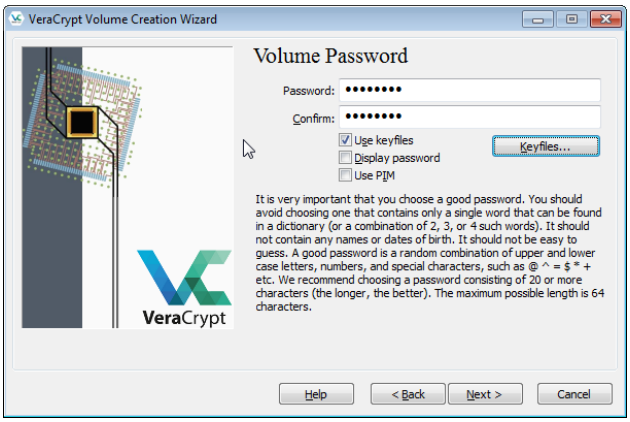
Trykk på *Keyfiles...*. I det neste vinduet (ikke vist) trykker man på *Generate Random Keyfile...*. Følg installasjonsveilederen for å lage nøkkelfila som deretter lagres på et egnet sted.

Ta godt vare på nøkkelen. Om den endres eller mistes, så vil alle data som er kryptert ved hjelp av denne nøkkelen være tapt for alltid. Ikke la nøkkelen ligge på samme lagringsmedie som de krypterte data. En god plassering av nøkkelen vil for SKDE sine ansatte være på personlig område på nettverksdisk (*P:*). Da er nøkkelen skilt fra data (som ligger på på lokal disk) samt at den er bedre sikret i forhold til tap som for eksempel ved diskfeil.

Trykk *Close* i vinduet *VeraCrypt - Keyfile Generator* (ikke vist). Tilbake i vinduet *VeraCrypt - Keyfiles* (ikke vist), trykk *Add files...* og velg deretter nøkkelfila som nettopp ble laget og trykk *OK*. Tilbake i vinduet vist i 2.5, trykk *Next*.



Figur 2.4: Definisjon av volumstørrelse



Figur 2.5: Definisjon av passord.

Som standard brukes oppgitt passord som utgangspunkt for kryptovariabel i *VeraCrypt*. Ved en slik tilnærming vil et vanlig stertkt passord (åtte tegn bestående av store og små bokstaver, tall og spesialtegn) være utilstrekkelig for å oppnå en sterk nok kryptering. Dette vil man nå kunne få en advarsel om, men så lenge en nøkkelfil og et stertkt passord er definert kan man ignorere denne advarselen.

I det nest vinduet velger man *FAT* under *Filesystem* og trykker *Format* slik vist i 2.6.

Når filkontaineren er ferdig formatert vil man få en bekreftelse på at dette er gjennomført slik vist i 2.7.

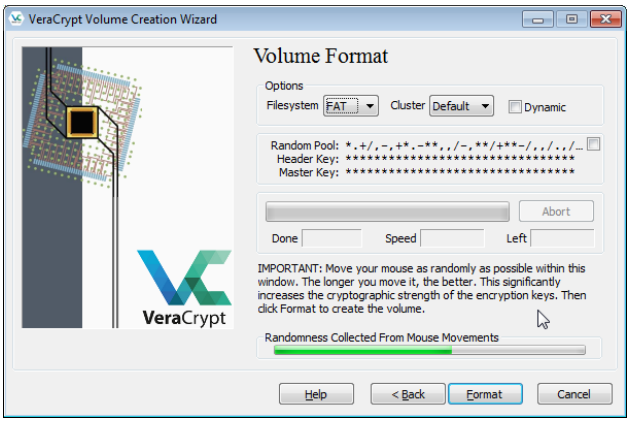
Trykk *OK* og deretter *Exit* i det neste vinduet.

2.1.3 Oppstart av VeraCrypt

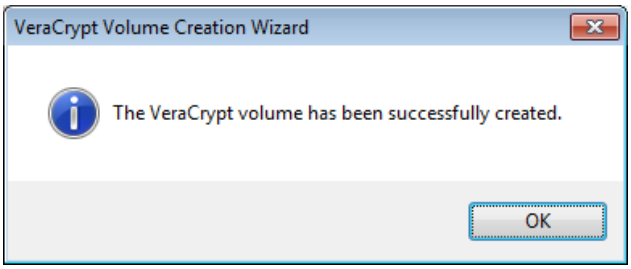
Start programmet *VeraCrypt* og angi stasjonsbokstav (*i.e.* monteringspunkt) og tilhørende filkontainer slik det er vist i 2.8. Her er stasjonsbokstav angitt som *I:* og fikontainer er *C:\sens\prosjekt1*.

Trykk på *Mount*. Deretter angis passord og nøkkelfil slik det er vist i figur 2.9.

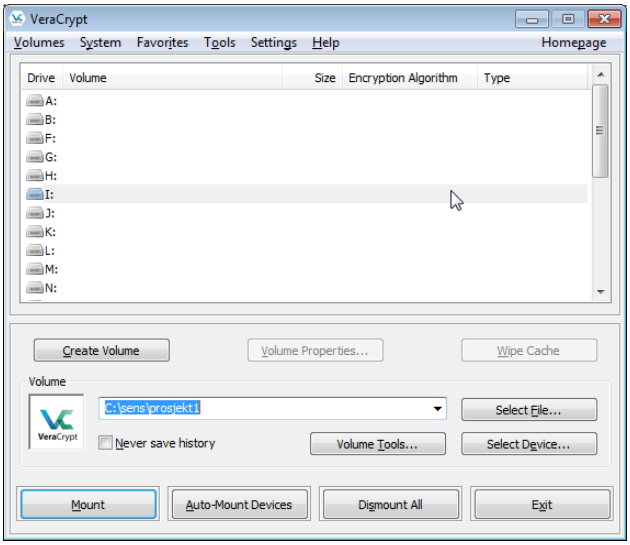
Når man trykker *Keyfiles…* vil man i neste vindu (ikke vist) velges riktig nøkkelfil ved å trykke på *Add files…*. Trykk deretter *OK*. Tilbake i vinduet vist i figur 2.9 trykker man *OK*. Deretter skal man kunne se at en ny disk er lagt til (figur 2.10).



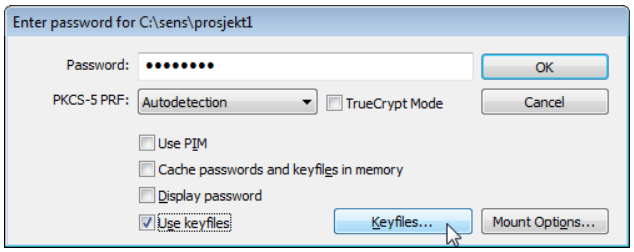
Figur 2.6: Formatering av diskvolum.



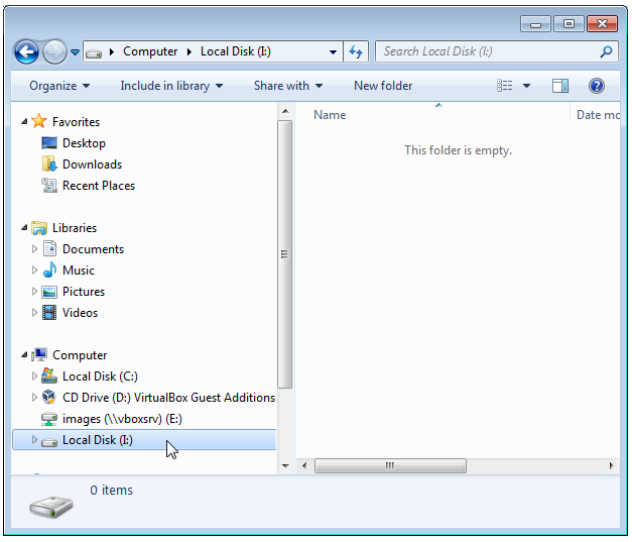
Figur 2.7: Formatering av OK.



Figur 2.8: Montering av diskvolum



Figur 2.9: Definisjon av passord og nøkkelfil

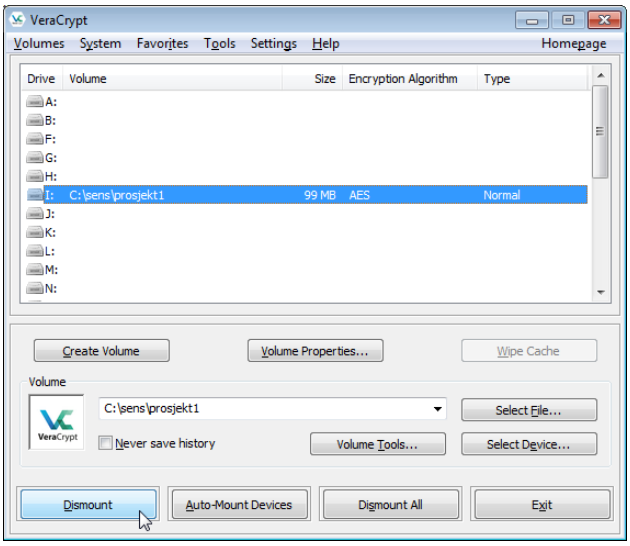


Figur 2.10: Kryptert diskvolum er satt opp.

Det nye *VeraCrypt* diskvolumet er nå klart til bruk, på samme vis som hvilken som helst annen disk. Alle filer som skrives hit, i dette tilfellet *I:*, vil krypteres før de lagres og filer som leses herfra dekrypteres før de åpnes.

For å gjøre diskvolumet utilgjengelig må det avmonteres. Merk aktuell stasjonsbokstav og trykk på *Dismount* slik det er vist i figur 2.11.

Oppsett og bruk vil være tilsvarende om man ønsker å bruke *VeraCrypt* til å kryptere data på andre lagringsmedier, som for eksempel en minnepinne. For bruk av minnepinne vil det være uhensiktsmessig å benytte en separat nøkkel, men da må man velge et passord som gir mer beskyttelse og som er i henhold til de anbefalinger *VeraCrypt* gir. Sletting av data på minnepinne må derfor også håndteres særlig siden det ikke fins noen nøkkel som kan slettes. Her bør man prøve seg frem og spør gjerne andre med erfaring fra bruk av *VeraCrypt*.



Figur 2.11: Avmontering av diskvolum.