Slutrapport Krypteringstjänster

SUNET Inkubator Dokument 12/14/12 Joakim.nyberg@umu.se

INNEHÅLLSFÖRTECKNING

1 INLEDNING

1.1 SAMMANFATTNING

SUNET Inkubator projektet kryptering har utrett hur lärosäten kan skydda information från att intressenter utan tillåtelse ska kunna få tillgång till sekretess skyddad information. På marknaden finns det ett stort utbud av produkter och tjänster för detta.

Ett problem är vilken tillverkare man litar på då man ska kryptera sin skyddsvärda information? Eller om det garanteras att produkten inte innehåller funktioner som kan vara skadliga?

Den här slutrapporten innehåller rekommendationer som rör hanteringen av kryptering vid svenska lärosäten.

Huvudaktiviteter i projektet har varit att genomföra en kartläggning rörande vilka behov av kryptering som finns på svenska lärosäten, göra en teknisk genomlysning av möjliga verktyg för kryptering, testa de intressanta verktygen och metoderna samt ta fram rekommendationer

Kartläggningen genomfördes för att få större kunskap om behovet av kryptering ute på lärosätena. Detta visade att merparten av dom som deltog i enkäten anser att skydd av data som kommer på avvägar och konkurrerande verksamhet är det som är mest intressant att skydda sig mot. Enkäten visade också på att man bör fokusera skyddet på fil nivå och inte databaser, även att prioritera skyddet på klient nivå.

Nyckelhanteringen lyfts också fram som mycket viktigt för att återställa informationen om användaren förlorar sin nyckel. När man tittar på olika lagringstjänster så är det tydligt att man vill ha en så brett stöd som möjligt.

1.2 DEFINITIONER AV BEGREPP

FIPS 140-? Standard utfärdad av National Institute of Standards and Technology (NIST) för hur kryptografiska moduler skall vara skyddade. Det finns fyra nivåer:

1) Lägsta nivån. Inga speciella krav på fysiskt skydd. Motsvarar ett kryptografiskt kort i en PC eller kryptografisk programvara.

2) Modulen skall vara förseglad så att det märks om någon försökt bryta sig in i den. Rollbaserad autentisering.

3) Förutom 2) skall modulen också vara svår att öppna. Lösenord och PIN-koder skall nollställas om modulen öppnas. Lösenord och PIN-koder skall överföras via separat port.

4) Högsta nivån. Förutom 3) skall modulen vara extra svår att öppna. Lösenord och PIN-koder nollställs så fort modulen öppnas. Modulen skall även klara onormala temperaturer, spänningar etc. Moduler på denna nivå är lämpliga att användas i fysiskt oskyddade miljöer.

KSU KSU-system är avsedda att användas för skydd av information som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400).

Genom att svenska myndigheter ställer kraven och även granskar säkerheten i produkterna får KSU systemen ett kvitto på att de t.ex. utför de funktioner de är

avsedda för och att det inte finns massa dolda fel i produkten.

KSU får däremot inte användas för uppgifter som rör rikets säkerhet. Det ersätter med andra ord inte dagens signalskyddssystem.

NIST National Institute of Standards and Technology i USA.

PCIe Peripheral Component Interconnect Express, en seriell expansionsbuss för datorer.

PGP Pretty Good Privacy, ett program för kryptering och dekryptering. Används ofta för signering och kryptering av e-post.

PKCS Public Key Cryptography Standards, en grupp standarder publicerade av RSA. PKCS#11, även kallad Cryptoki, är ett API för hårdvarubaserade säkerhetsobjekt som smarta kort etc.

SSH Secure Shell, ett kryptografiskt nätverksprotokoll för säker datakommunikation, fjärrinloggning och fjärrexekvering av kommandon mellan två datorer.

SSL Secure Sockets Layer, en föregångare till Transport Layer Security (TLS). Kryptografiskt protokoll för säker datakommunikation över Internet. Använder X.509 certifikat.

1.3 Mål

Det finns fyra delmål:

1. Genomföra en kartläggning angående vilka behov rörande kryptering finns på svenska lärosäten.
2. Gör en teknisk genomlysning av möjliga verktyg för krypterings möjligheter.
3. Genomför en POC över intressant metod.
4. Ta fram dokumenterade rekommendationer för kryptering.

1.4 Tidplan

Projektet startas 2014-02-01 och avslutas 2014-12-12

1.5 Kostnader

Aktiviteter	Resurs	Budget 2014(timmar)
Utredningsarbete	Joakim Nyberg	
Genomlysning verktyg	Joakim Nyberg, Einar Hillbom & Erik Johansson	
POC	Joakim Nyberg	
Totalt		400

1.6 Dokumentation

- Fastställd projektplan
- Statusrapporter

- Slutrapport

1.7 REFERENSER

[1] How To Encrypt Directories/Partitions With eCryptfs On Debian Squeeze (2011) [www] <http://www.howtoforge.com/how-to-encrypt-directories-partitions-with-ecryptfs-on-debian-squeeze> Hämtad 2014-03-14
[2] *eCryptfs* (2012) [www] <http://ecryptfs.org/> Hämtad 2014-03-14
[3] Yubikey NEO and OpenPGP [www] http://www.yubico.com/2012/12/yubikey-neo-openpgp/ Hämtad 2014-03-25.
[4] GPG4Win [www] http://www.gpg4win.org/ Hämtad 2014-03-25.
[5] TrueCrypt (2014-01-14) [www] <http://www.truecrypt.org/> Hämtad 2014-02-07.
[6] Martin Stout. Comparison of Cloud and Backup Options for TrueCrypt containers (2013-10-09) [www] <http://martinstutenglish.wordpress.com/2013/10/09/comparison-of-cloud-and- backup-options-for-truecrypt-containers/> Hämtad 2014-02-07.
[7] Boxcryptor [www] <https://www.boxcryptor.com> Hämtad 2014-02-07.
[8] Mellisa Tolentino. 5 Tools to Encrypt Files for Dropbox, Salesforce, Office365 + More (2013-09-25) [www] <http://siliconangle.com/blog/2013/09/25/5-tools-to- encrypt-files-for-dropbox-salesforce-office365-more/> Hämtad 2014-02-10.
[9] Paul Niemeyer. The Most Secure Cloud Storage Providers That Respect Your Privacy (2013-09-16) [www] <http://www.cloudstoragereviews.org/secure-cloud- storage/> Hämtad 2014-02-10.
[10] Ashutosh KS. Top 10 Online Storage Solutions With Encryption [www] <http://www.hongkiat.com/blog/online-storage-with-encryption/> Hämtad 2014-02-10.
[11] Hardware Encrypted Secure Drives [www] <http://www.apricorn.com/products/hardware-encrypted-drives.html/> Hämtad 2014-02-07.

2 ORGANISATION

2.1 UPPDRAGSGIVARE

Inkubator är uppdragsgivare och Per Hörnblad kontaktperson

2.2 REFERENSGRUPP

Gruppen består av ett antal representanter från svenska för lärosätena.

HUGO LANDGREN	CHALMERS
DAVID HEED	ÖREBRO UNIVERSITET
TORBJÖRN WICTORIN	UPPSALA UNIVERSITET

JOHANNES HASSMUND	LINKÖPINGS UNIVERSITET
PER HÖRNBLAD	UMEÅ UNIVERSITET
MAGNUS PERSSON	LUND UNIVERSITETET

2.3 PROJEKTGRANSKARE

Projektgranskning sker av Per Hörnblad, IT-arkitekt, Umeå universitet

2.4 PROJEKTLEDARE

Projektledare är Joakim Nyberg, IT-stöd och systemutveckling, ITS, Umeå universitet

2.5 RESURSPERSONER

Einar Hillbom – ITS, Umeå universitet

Erik Johansson – ITS, Umeå universitet

David Heed – Örebro universitet

Hugo Landgren – Chalmers universitet

3 GENOMFÖRANDE

3.1 KARTLÄGGNING OCH BEHOVS ANALYS AV KRYPTERINGSTJÄNSTER VID LÄROSÄTEN

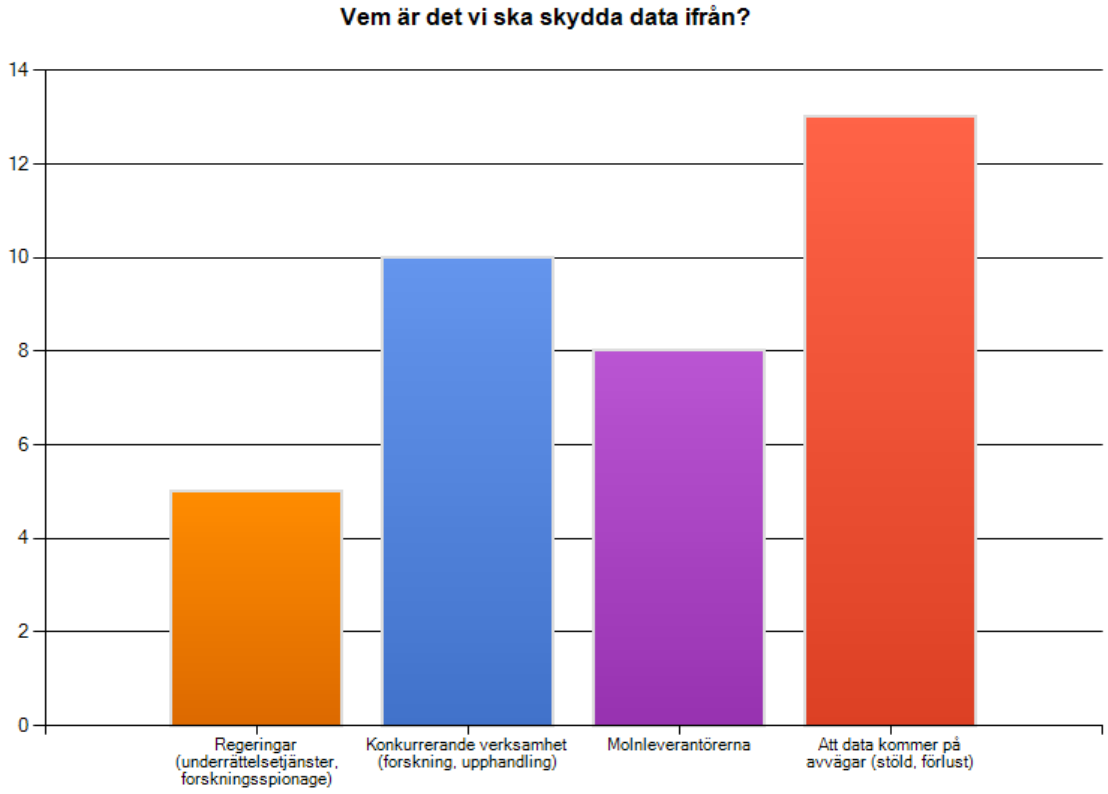
Enkäten skickades ut till IT-chefer vid svenska lärosäten.

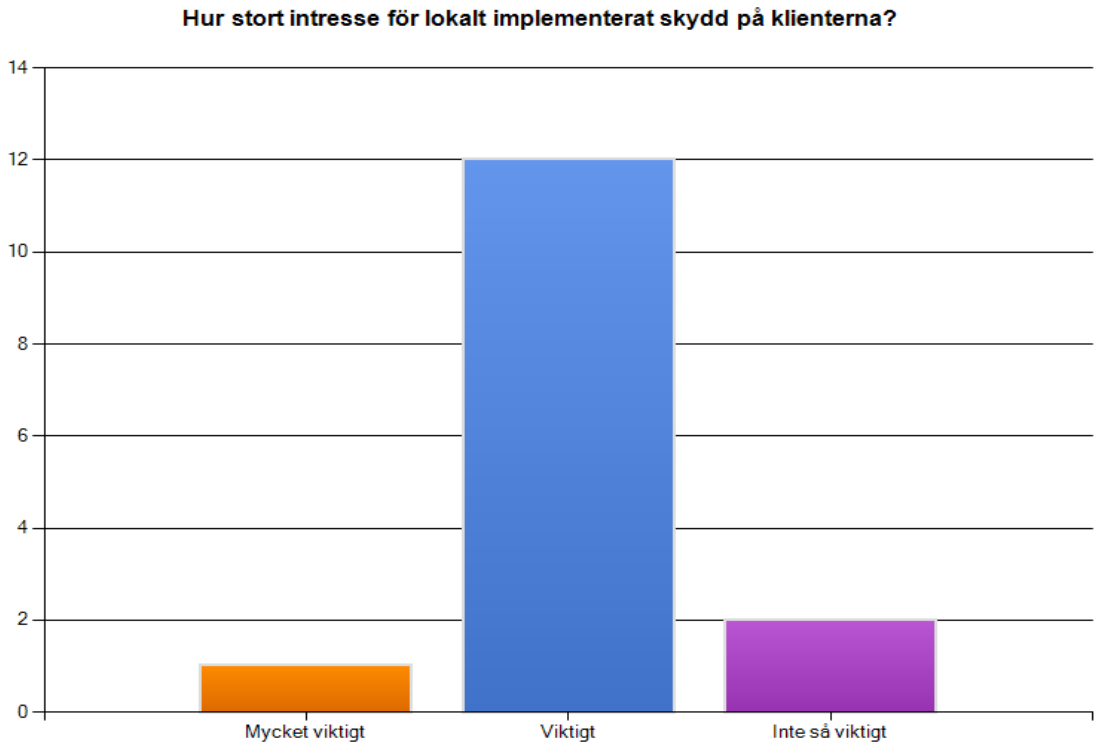
Elva lärosäten svarade på enkäten:

1. Blekinge Tekniska Högskola
2. Chalmers
3. Handelshögskolan i Stockholm
4. Högskolan i Borås
5. Högskolan i Gävle
6. Karlstads universitet
7. Karolinska Institutet
8. Lunds universitet
9. Stockholms universitet
10. Södertörns högskola
11. Umeå universitet

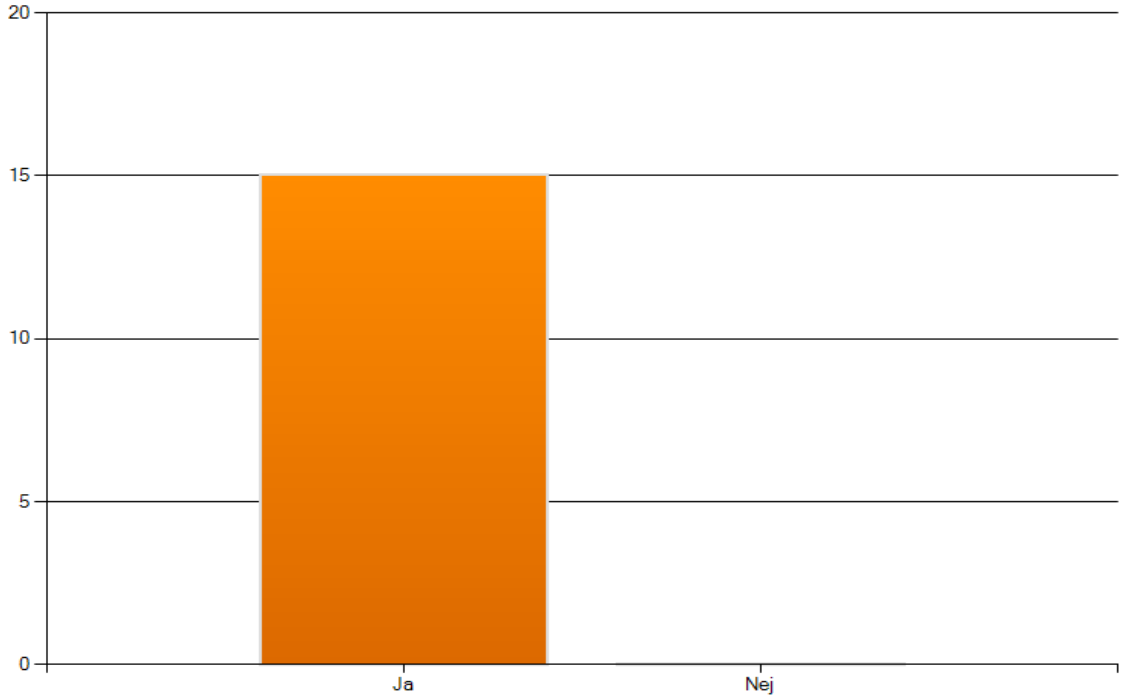
3.2 RESULTATET AV ENKÄTEN SOM SKICKADES UT

Här följer en sammanställning av de frågor som enkäten innehåller.

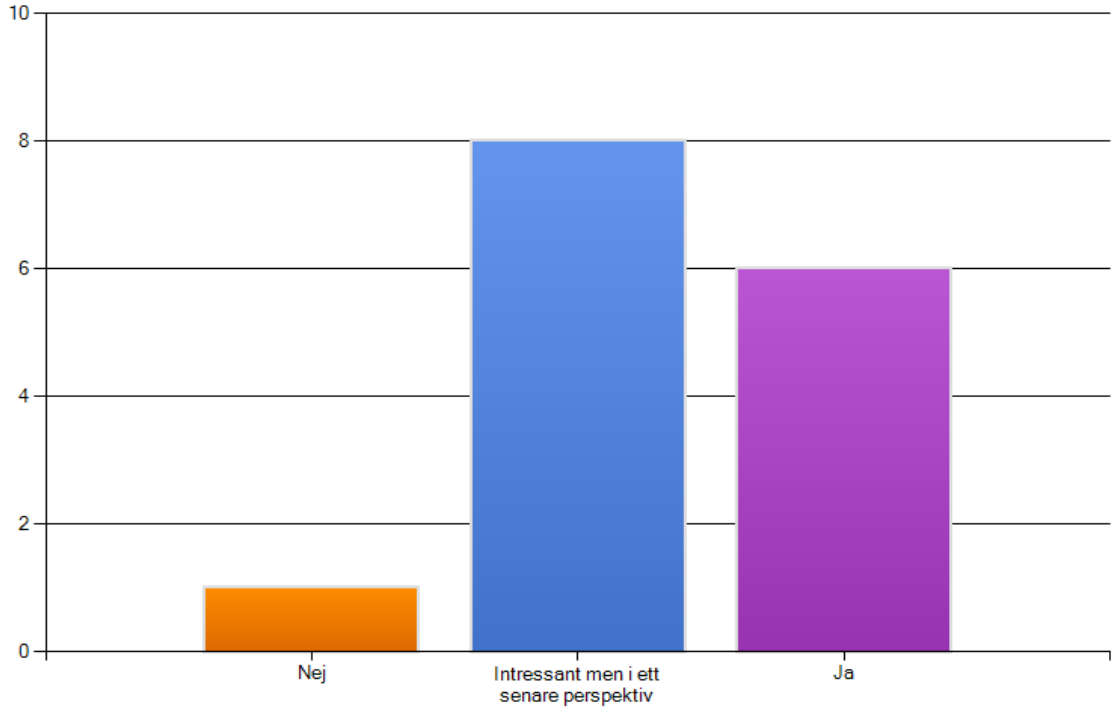


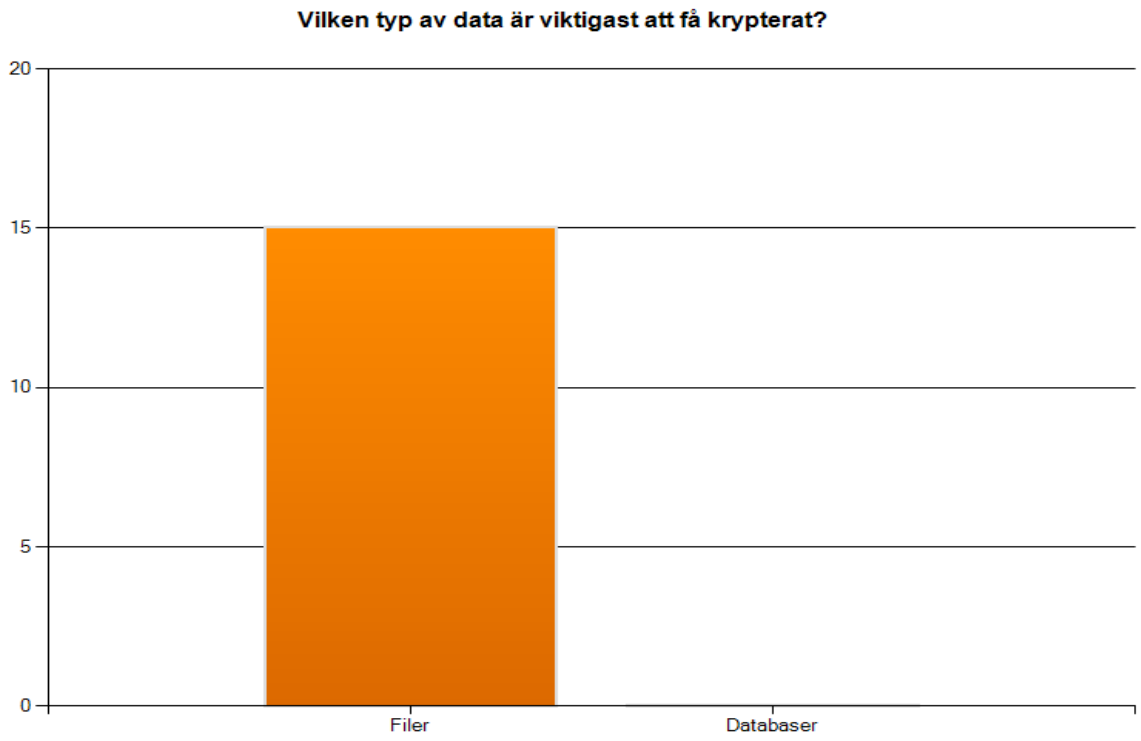


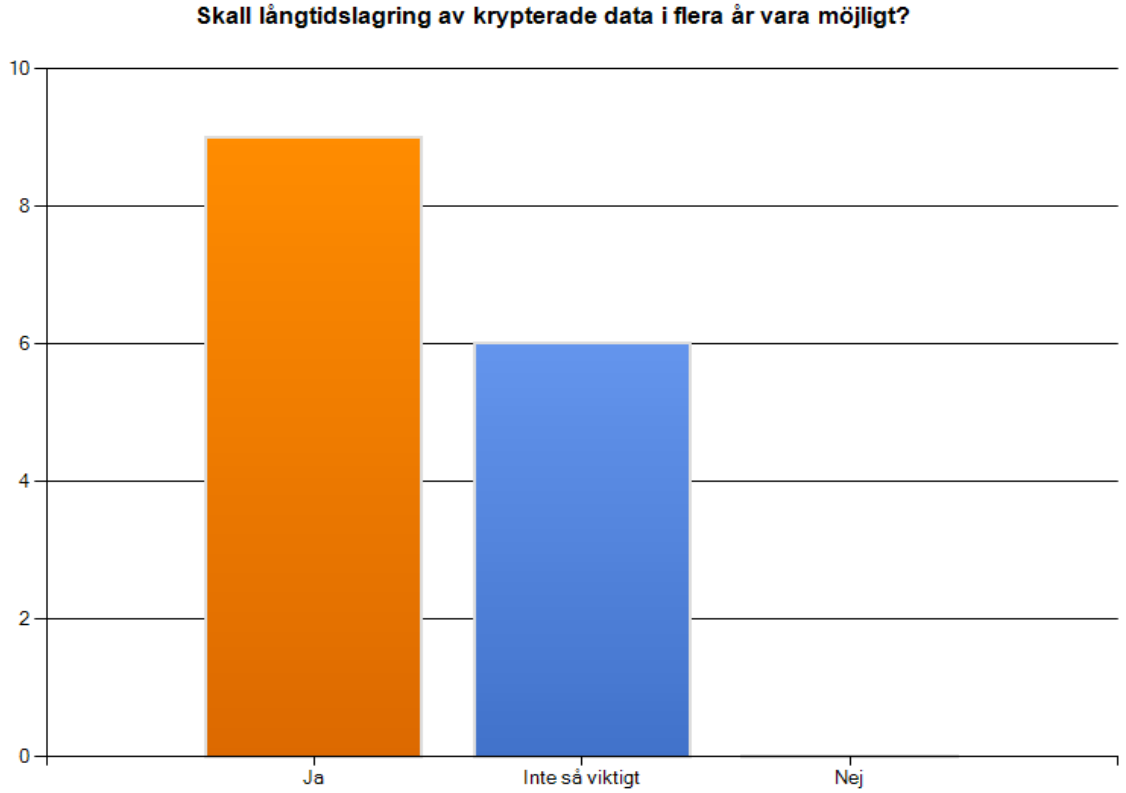
Är det viktigt att ta fram en hantering för att centralt lagra nycklar (glömt lösenord)?

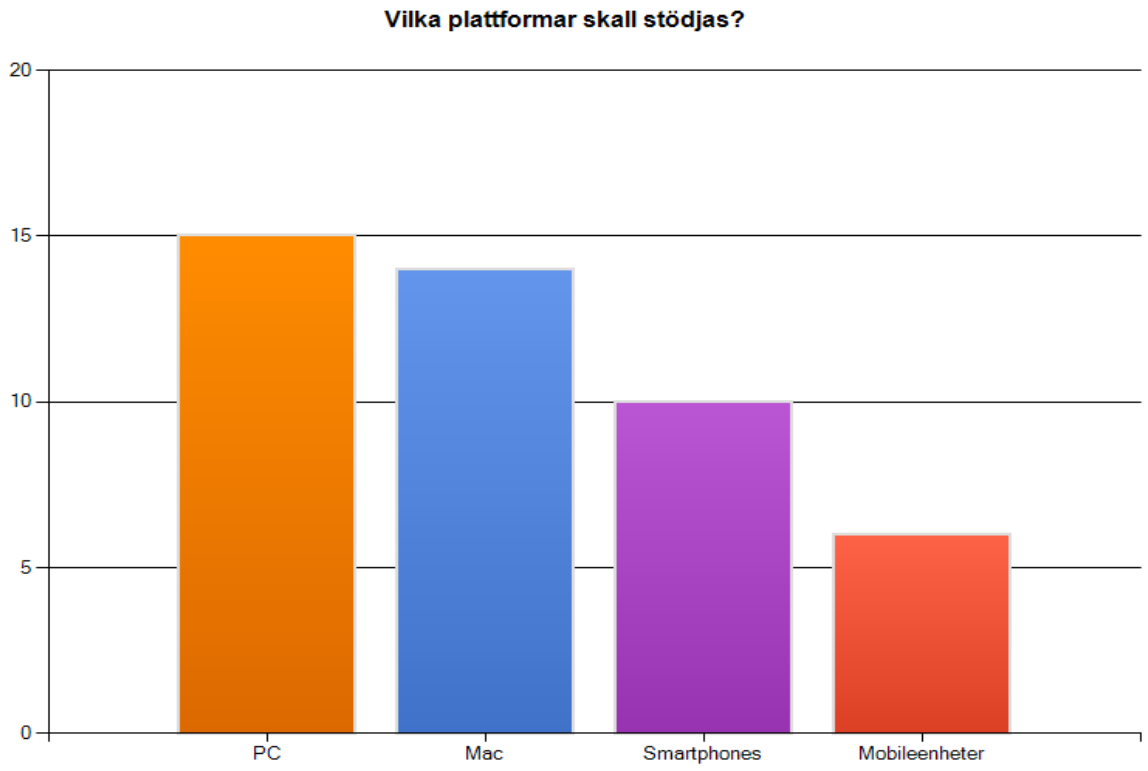


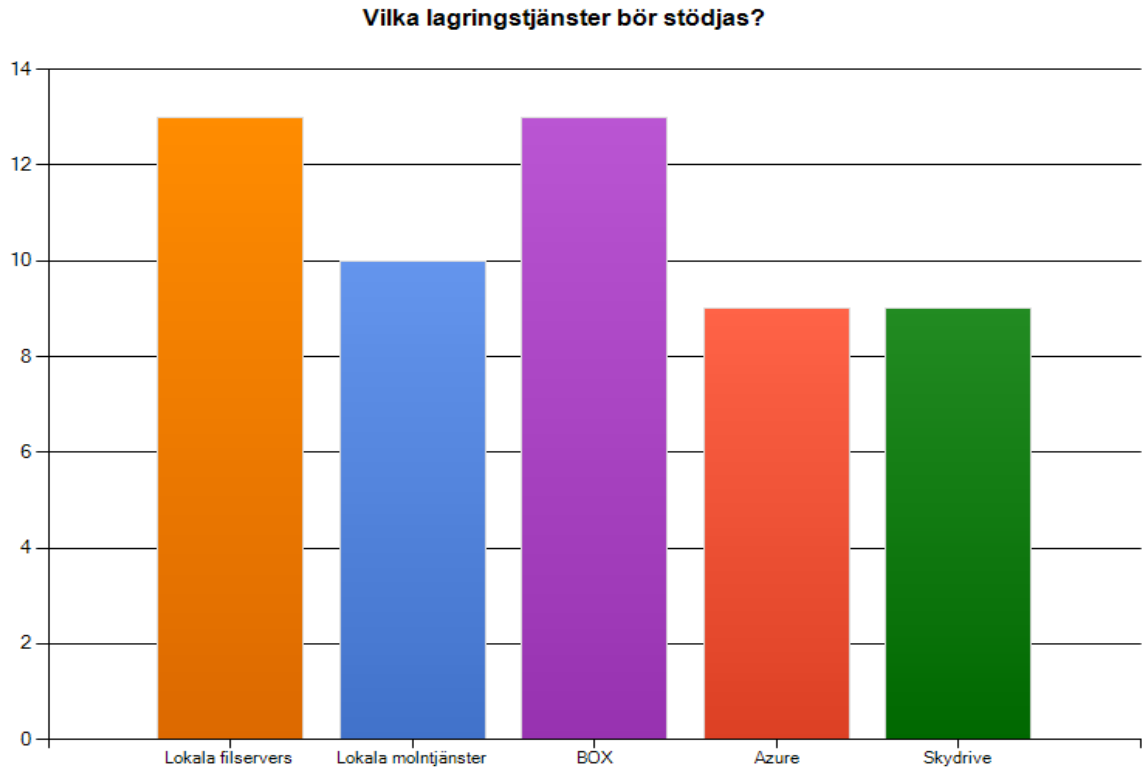
Är det intressant med en central administrationshantering med gruppolicys mm så att institutionen kan styra vad som skall vara krypterat och inte?

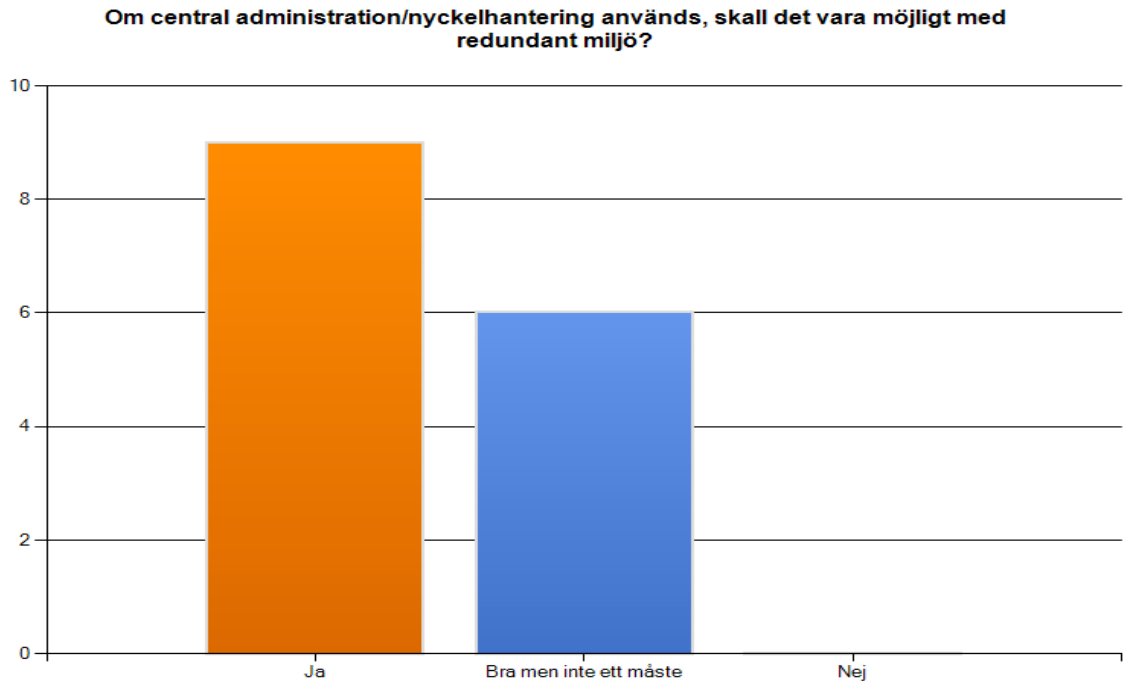



Vilken typ av data är viktigast att få krypterat?
20
15
10
5
0
Filer
Databaser


Skall långtidslagring av krypterade data i flera år vara möjligt?
10
8
6
4
2
0
Ja
Inte så viktigt
Nej


Vilka plattformar skall stödjas?
20
15
10
5
0
PC
Mac
Smartphones
Mobileenheter


Vilka lagringstjänster bör stödjas?
14
12
10
8
6
4
2
0
Lokala filservers
Lokala molntjänster
BOX
Azure
Skydrive



Skriv gärna hur ni ser på en lägsta nivå för en krypteringstjänst, och vilken vision vi bör sträva mot

- Följ vedertagna rekommendationer (Ecrypt-II och NIST)
- Vi vill skydda relevant data från otillåten tillgång.
- Skall hjälpa oss att uppfylla kraven i ISO27000 och vara så enkelt att användare kan hantera det utan avancerad utbildning. Koppla gärna till TERENA personliga cert. Central nyckelhantering eller huvudnyckel är ett måste eftersom användare kommer att glömma/bli av med nycklar.
- Förstår inte ordet "nivå". Den skall inte kunna kringgås av en individuell gärningsman eller sättas ur spel av lokalt kontos ändringar. Gäller det hårddiskkrypto måste bootloader kunna skyddas. Gäller det kryptot i sig själv skall Blowfish, AES256 eller bättre kunna stödjas.

Övriga tjänster (ge förslag)

- virtuella enheter som kan flyttas som separata filer med nyckelutbyte

Övriga synpunkter

- Stöd även Linux som är en av våra officiella plattform
- Ett val för den enskilde borde finnas att kunna köra med centralt administrerade nycklar eller i egen regi. De legala aspekterna borde även utredas!!

- Kanske intressant att erbjuda alternativa produkter i en gemensam upphandling. Fillagring i molnet ställer andra krav än e-post eller hårddisks-kryptering. Med lokalt implementerat skydd svarade jag för diskkrypto. Om det avser att nyckelgenerering sker lokalt så är det av yttersta vikt.

3.2.1 Slutsatser och diskussioner

Merparten av dom som deltog i enkäten anser att skydd av data som kommer på avvägar och konkurrerande verksamhet är det som är mest intressant att skydda sig mot. Enkäten visade också på att man bör fokusera skyddet på fil nivå och inte databaser, även att prioritera skyddet på klient nivå.

Nyckelhanteringen lyfts också fram som mycket viktigt för att möjliggöra restore av data om användaren förlorar sin nyckel. När man tittar på vilka lagringstjänster så är det tydligt att man vill ha en så brett stöd som möjligt.

Baserat på detta underlag beslutade projektgruppen att test och utvärdera flera olika krypteringsmöjligheter.

4 PRODUKTGENOMGÅNG AV LOKALT IMPLEMENTERBARA LÖSNINGAR

4.1 INLEDNING

Detta kapitel beskriver de testade produkterna och tar fram styrkor och svagheter. Målet med utredningen är att belysa de olika produkternas styrkor och svagheter och komma med en rekommendation om hur kryptering ska hanteras inom dom olika lärosätena.

Problemställning:

De faktorer som undersökts är:

- Hur fungerar krypteringen?
- Vilka operativsystem stöds?
- Hur enkel är den att använda?
- Krävs installation av programvara?
- Kan flera dela på det krypterade materialet?
- Kan man återställa borttappade nycklar?
- Hur fungerar lösningen tillsammans med molntjänster?
- Fungerar det med mobila enheter som surfplattor och smarta telefoner?

Utifrån enkäten så kunde slutsatser dras vilka produkter som används inom svenska lärosäten och hur de används. Utifrån detta så valdes några produkter som finns tillgängliga på marknaden idag.

1. Microsoft BitLocker.
2. Ecryptfs.
3. Yubikey NEO och OpenPGP.

4. TrueCrypt.
5. AXcrypt.
6. BoxCryptor.
7. Generella krypteringslösningar för moln
8. Tutus Filkrypto – ”KURIR”.
9. Krypterad USB-disk

Utifrån enkäten så drogs även slutsatsen att nyckelhanteringen var av stort intresse. Utifrån det så valde vi att titta på olika sätt hur man kan skydda nycklarna.

1. Nyckelhantering

4.2 MICROSOFT BITLOCKER

4.2.1 Sammanfattning

Bitlocker är en mjukvarukryptering som funnits inbyggd i Windows sedan Vista Enterprise/Ultimate, och kan användas för att kryptera hårddiskar och USB-minnen. Krypteringsnycklarna sparas som standard på ett kompatibelt TPM-chip i datorn, alternativt på ett USB-minne. Vid central hantering sparas även krypteringsnycklar i AD eller dedikerad MBAM-server(Microsoft Bitlocker Administration)

Bitlocker kan implementeras på olika sätt, manuellt av den enskilde användaren eller centralt styrt och påtvingande. I fallet med manuell installation kan policys appliceras via AD för att bestämma hur användaren får använda tjänsten och vart nycklarna ska sparas. För denna utredning har vi valt att installera Bitlocker Administration(MBAM). MBAM-servern lagrar krypteringsnycklarna från samtliga klienter och erbjuder en webbportal med självbetjäning för återställning. Rapporteringsfunktionen samlar in och presenterar status på dom klienter som hanteras.

4.2.2 Tester

Bitlocker har för denna rapport testats på Windows:

- Windows 8.1

MBAM-servern har för denna rapport testats på Windows:

- Windows server 2012 R2

4.2.3 Införande och uppföljning

Vid UmU har man valt att använda MBAM för att få full kontroll över krypteringen. MBAMs rapporteringsfunktion kommer även att kopplas mot befintlig SCCM-server för att bli en del i vår regelbundna övervakning och uppföljning.

Initialt kommer endast supportpersonal att ha tillgång till webportalen för återställning av krypteringsnycklar.

4.2.4 Autentisering

Det finns två olika kombinationer att använda för att låsa upp en Bitlocker-klient som använder sig av TPM, med eller utan PIN-kod. Med PIN-kod så måste denna anges vid uppstart innan operativsystemet startas. PIN-kod ger en högre säkerhet men högre risk att användaren glömmer bort den och misslyckas med att logga in i datorn. Vi har valt att använda enbart TPM då detta påverkar användaren minimalt och inte tillför några extra steg vid inloggning.

4.2.5 Risker

En risker som har identifierats under tester visar att det finns metoder att dekryptera BitLocker om en angripare kommer över ett system som inte är ner stängt (viloläge skyddar inte), eftersom Bitlocker sparar information i minnet som kan nyttjas för att dekryptera hårddisken.

4.2.6 Slutsatser och diskussioner

Genom att nyttja Bitlocker tillsammans med MBAM-servern så har det visat sig att man kan hantera diskkrypteringen centralt på ett mycket enkelt sätt när det gäller Windows system. Genom att MBAM-servern lagrar alla krypteringsnycklar får man även en bra central hantering för att återställa nycklar. Risken att en angripare ska kunna extrahera ut information ur minnet för att dekryptera disken ser man som liten eftersom angriparen måste komma åt systemet fysiskt och systemet måste vara minst i viloläge för att inte systemet ska tömma minnet.

4.3 KRYPTERING MED ECRYPTFS

4.3.1 Sammanfattning

Denna undersökning visar hur man kan kryptera filer i Linux med hjälp av eCryptfs (Enterprise Cryptographic File) [1-2] som finns inbyggt i Linux-kärnan och hur man kan migrera de krypterade filerna till en annan Linux-dator. Har funnits med sedan version 2.6.19 av Linux Kernel, Ubuntu sedan version 9.04.

4.3.2 Tester

Versioner på testsystemet:

- ecryptfs-utils 75-8.el5
- CentOS release 5.9 (Final)

4.3.3 Administration/användarhantering

Installera **ecryptfs-utils**

```
# yum install ecryptfs-utils
```

Versioner på testsystemet:

- ecryptfs-utils 75-8.el5
- CentOS release 5.9 (Final)

Skapa en krypterad katalog:

```
# mkdir /data/secret
# mount -t ecryptfs /data/secret/ /data/secret/
Select key type to use for newly created files:
 1) openssl
 2) passphrase
 3) tspi
Selection: 2
```

```
Passphrase: ********
Select cipher:
 1) aes: blocksize = 16; min keysize = 16; max keysize = 32 (loaded)
 2) blowfish: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
 3) des3_ede: blocksize = 8; min keysize = 24; max keysize = 24 (not loaded)
 4) twofish: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
 5) cast6: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
 6) cast5: blocksize = 8; min keysize = 5; max keysize = 16 (not loaded)
Selection [aes]: <Enter>
Select key bytes:
 1) 16
 2) 32
 3) 24
Selection [16]: <Enter>
Enable plaintext passthrough (y/n) [n]: <Enter>
Attempting to mount with the following options:
  ecryptfs_unlink_sigs
  ecryptfs_key_bytes=16
  ecryptfs_cipher=aes
  ecryptfs_sig=a48f46b6781af204
WARNING: Based on the contents of [/root/.ecryptfs/sig-cache.txt],
it looks like you have never mounted with this key
before. This could mean that you have typed your
passphrase wrong.

Would you like to proceed with the mount (yes/no)? : yes
Would you like to append sig [a48f46b6781af204 ] to
[/root/.ecryptfs/sig-cache.txt]
in order to avoid this warning in the future (yes/no)? : yes
Successfully appended new sig to user sig cache file
Mounted eCryptfs
```

Kolla hur det ser ut i **mount**:

```
# mount
...
/data/secret on /data/secret type ecryptfs (rw,ecryptfs_sig=a48f46b6781af204
,ecryptfs_cipher=aes,ecryptfs_key_bytes=16,ecryptfs_unlink_sigs)
```

Kopiera filer till katalogen:

```
# cp /etc/hosts /data/secret/
# cp /etc/passwd /data/secret
# ls -l /data/secret/
total 8
-rw-r--r-- 1 root root  469 Mar 14 13:25 hosts
-rw-r--r-- 1 root root 2478 Mar 14 13:25 passwd
```

Kontrollera att filerna går att läsa:

```
# cat /data/secret/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1               localhost.localdomain localhost
...
```

Avmontera katalogen och kontrollera att filerna inte går att läsa:

```
# umount /data/secret
# cat /data/secret/hosts
□#□o□#[□□PYE□豎&Z□##"3DUfw`R□□:□Q
...
```

Montera katalogen på nytt:

```
# mount -t ecryptfs /data/secret /data/secret
Select key type to use for newly created files:
 1) openssl
 2) passphrase
 3) tspi
Selection: 2
Passphrase: ********
Select cipher:
 1) aes: blocksize = 16; min keysize = 16; max keysize = 32 (loaded)
 2) blowfish: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
 3) des3_ede: blocksize = 8; min keysize = 24; max keysize = 24 (not loaded)
 4) twofish: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
 5) cast6: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
 6) cast5: blocksize = 8; min keysize = 5; max keysize = 16 (not loaded)
Selection [aes]: <Enter>
Select key bytes:
 1) 16
 2) 32
 3) 24
Selection [16]: <Enter>
Enable plaintext passthrough (y/n) [n]: <Enter>
Attempting to mount with the following options:
  ecryptfs_unlink_sigs
  ecryptfs_key_bytes=16
  ecryptfs_cipher=aes
  ecryptfs_sig=a48f46b6781af204
Mounted eCryptfs
```

Kontrollera att filen åter går att läsa:

```
# cat /data/secret/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
```

```
127.0.0.1               localhost.localdomain localhost
...
```

För att slippa svara på alla frågor kan man skapa en .rc-fil:

```
# cat /root/.ecryptfsrc
key=passphrase
ecryptfs_sig=a48f46b6781af204
ecryptfs_cipher=aes
ecryptfs_key_bytes=16
ecryptfs_passthrough=n
```

Nu behöver man bara ange lösenordet:

```
# mount -t ecryptfs /data/secret /data/secret
Passphrase: ********
Attempting to mount with the following options:
  ecryptfs_unlink_sigs
  ecryptfs_key_bytes=16
  ecryptfs_cipher=aes
  ecryptfs_sig=a48f46b6781af204
Mounted eCryptfs
```

4.3.4 Montering på annan dator

Katalogen /data/secret avmonterades och den nu krypterade katalogen flyttades till en annan dator via en tar-fil. Den nya datorn hade följande versioner:

- ecryptfs-utils 82-6.el6_1.3
- CentOS release 6.3 (Final)

Dessutom kopierades filerna

- /root/.ecryptfs/sig-cache.txt
- /root/.ecryptfsrc

Katalogen monterades:

```
# mount -t ecryptfs /data/secret /data/secret
Passphrase: ********
Enable filename encryption (y/n) [n]: <Enter>
Attempting to mount with the following options:
  ecryptfs_unlink_sigs
  ecryptfs_key_bytes=16
  ecryptfs_cipher=aes
  ecryptfs_sig=a48f46b6781af204
Mounted eCryptfs
```

Eftersom den andra datorn hade en nyare version av eCryptfs så fanns ytterligare en option som man måste besvara:

```
Enable filename encryption (y/n) [n]: <Enter>
```

Man fick lägga till den i /root/.ecryptfsrc för att slippa frågan:

```
key=passphrase
ecryptfs_sig=a48f46b6781af204
ecryptfs_cipher=aes
ecryptfs_key_bytes=16
ecryptfs_passthrough=n
ecryptfs_enable_filename_crypto=n
```

4.3.5 Slutsatser och diskussioner

Det är relativt enkelt att skapa en krypterad katalog med eCryptfs i Linux men man är begränsad till Linux. Den krypterade filen går dock att flytta mellan olika Linux-servrar. Eftersom möjligheten har funnits ett bra tag och många Linux tekniker kan eCryptfs så är det den bästa alternativet när det gäller kryptering i och mellan Linux system. Enkelt och beprövat.

4.4 YUBIKEY NEO OCH OPENPGP

4.4.1 Sammanfattning

Yubikey NEO

Yubikey NEO [3] har JavaCard och en inaktiverad OpenPGP applet. I detta dokument visas hur man aktiverar OpenPGP applet i en Yubikey NEO, hur man skapar ett nyckelpar och hur man sedan kan kryptera/dekryptera en fil. Som PGP-program används Kleopatra i GPG4Win [4]. Man har bara tre försök, sedan förstörs Yubikey NEO. Testade även att använda Yubikey NEO i en Linuxdator till vilken man exporterade nycklarna. Det gick bra att kryptera en fil med den publika nyckeln men inte att dekryptera. pcscd krävs på Linux-datorn för att använda OpenPGP applet och det kan vara något med detta som ställer till det. Som vanligt är det problem med Linux, open source och smarta kort.

4.4.2 Administration/användarhantering

Laddade hem konfigureringsprogrammet från

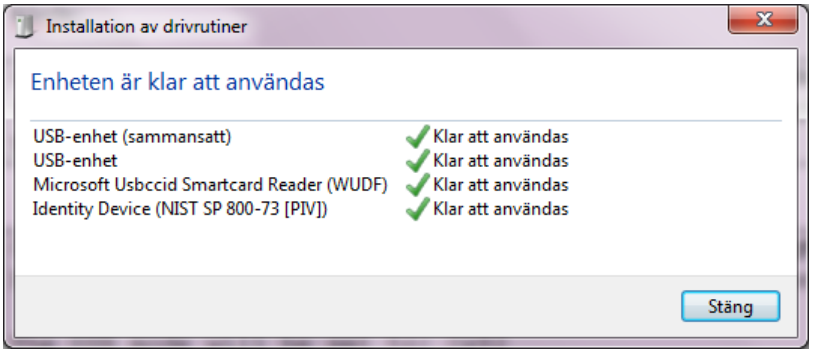
http://opensource.yubico.com/yubikey-personalization/releases.html

Stoppade in Yubikey NEO och körde:

```
>cd C:\Users\eihi0001\Downloads\ykpers-1.15.1-win64\bin
C:\Users\eihi0001\Downloads\ykpers-1.15.1-win64\bin>ykinfo -v
version: 3.2.0
```

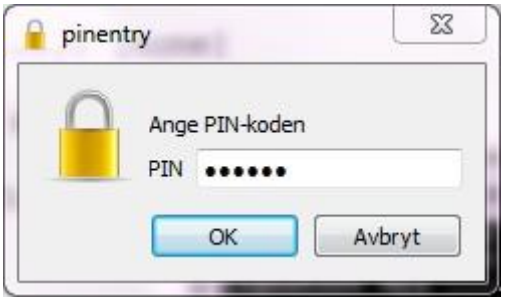
```
C:\Users\eihi0001\Downloads\ykpers-1.15.1-win64\bin>ykpersonalize    -m82

Firmware version 3.2.0 Touch level 1285 Program sequence 1

The USB mode will be set to: 0x82
```

Nya drivrutiner installerades automatiskt:



Genererade nyckelpar

```
C:\Users\eihi0001\Downloads\ykpers-1.15.1-win64\bin>gpg --card-edit


Application ID ...: D2760001240102000000000000010000
Version ..........: 2.0

Manufacturer .....: test card
Serial number ....: 00000001

Name of cardholder: [inte instõllt]
Language prefs ...: [inte instõllt]
Sex ..............: ej angiven

URL of public key : [inte instõllt]
Login data .......: [inte instõllt]
Signature PIN ....: tvingad

Key attributes ...: 2048R 2048R 2048R
Max. PIN lengths .: 127 127 127

PIN retry counter : 3 3 3
Signature counter : 0
Signature key ....: [none]
Encryption key....: [none]
Authentication key: [none]
General key info..: [none]
gpg/kort> generate
```



```
Specificera hur lõnge nyckeln skall vara giltig.
         0 = nyckeln blir aldrig ogiltig
      <n>  = nyckeln blir ogiltig efter n dagar
      <n>w = nyckeln blir ogiltig efter n veckor
```

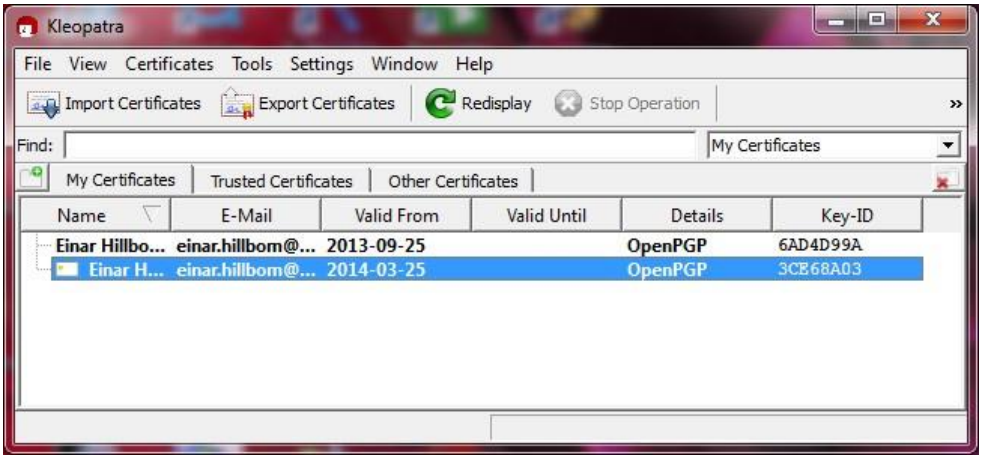
```
F÷r hur lÕng tid ska nyckeln vara giltig? (0)
Nyckeln gÕr aldrig ut

Stõmmer detta? (j/N) j


GnuPG beh÷ver konstruera en anvõndaridentitet f÷r att identifiera din
nyckel.


Namn: Einar Hillbom

E-postadress: einar.hillbom@umu.se

Kommentar:

Du valde f÷ljande ANV—NDAR-ID:

    "Einar Hillbom <einar.hillbom@umu.se>"


—ndra (N)amn, (K)ommentar, (E)post eller (O)k/(A)vsluta? O


gpg: nyckeln 3CE68A03 õr markerad med f÷rbehÕllsl÷st f÷rtroende
den publika och den hemliga nyckeln õr skapade och signerade.
```

Man bör backa upp den publika nyckeln. Den privata nyckeln går ej att exportera så man måste se till att man har en klartextbackup av filer man krypterar.

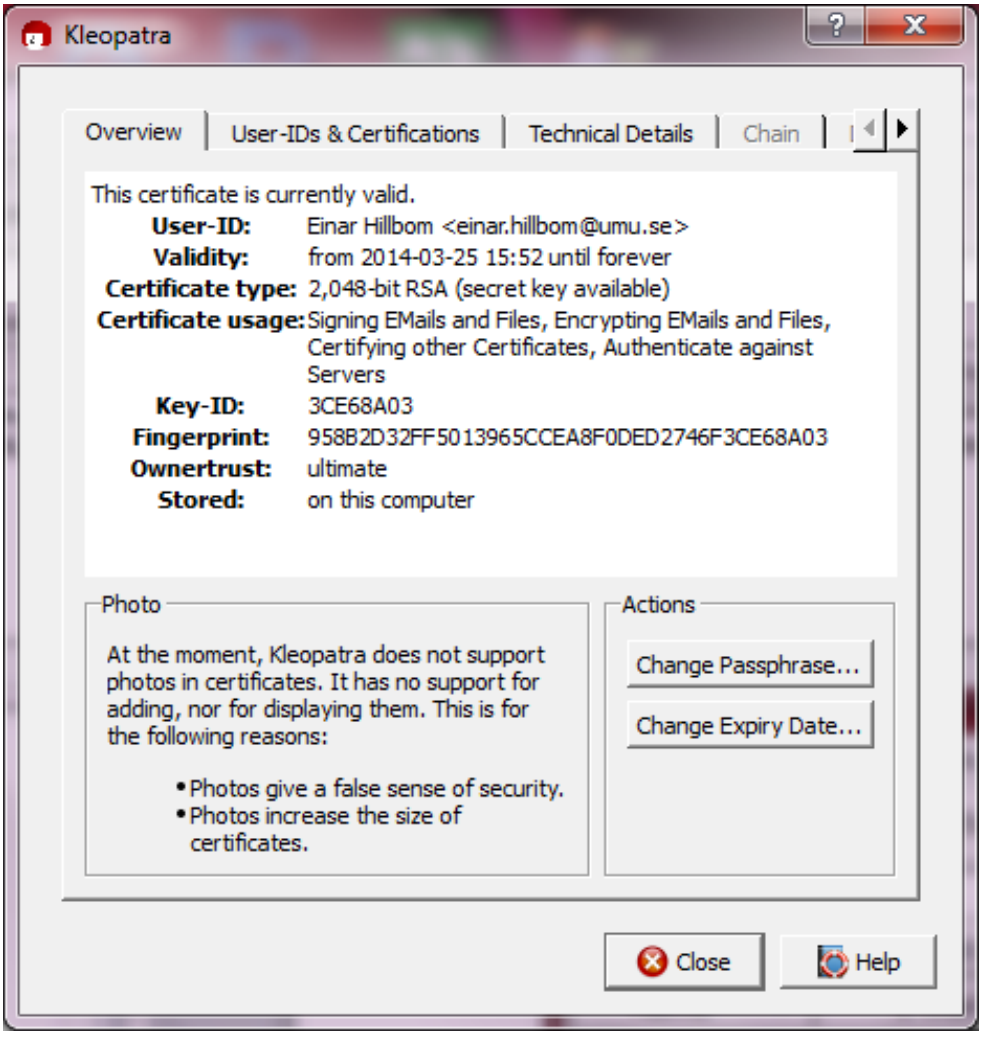
Bytte PIN-kod samt Admin PIN-kod:

```
C:\Users\eihi0001\Downloads\ykpers-1.15.1-win64\bin>gpg    --change-pin

gpg: OpenPGP-kort nr. D2760001240102000000000000010000 identifierades


1 - change PIN
2 - unblock PIN
3 - change Admin PIN
4 - set the Reset Code
Q - quit


Vad võljer du? 3

PIN changed.


1 - change PIN
2 - unblock PIN
3 - change Admin PIN
4 - set the Reset Code
Q - quit


Vad võljer du? Q
```

Starta Kleopatra:



Studera den nyligen genererade nyckeln.



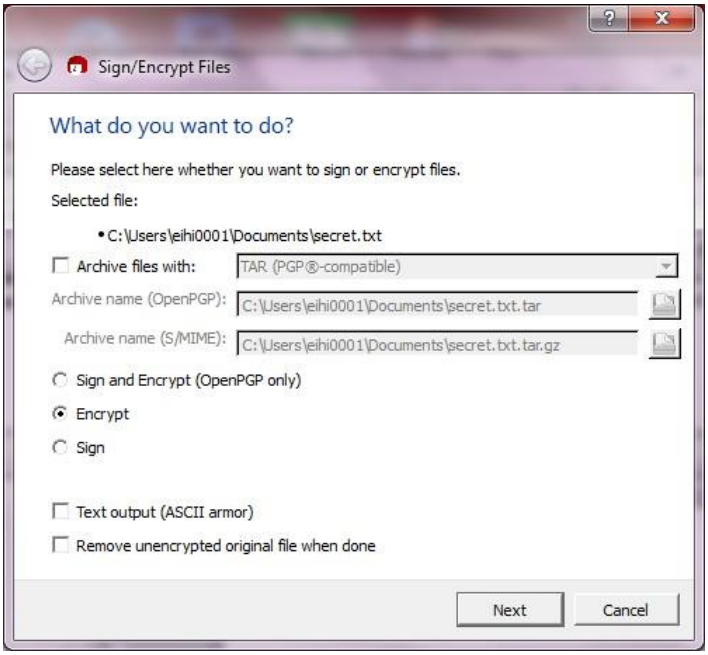
Kryptering

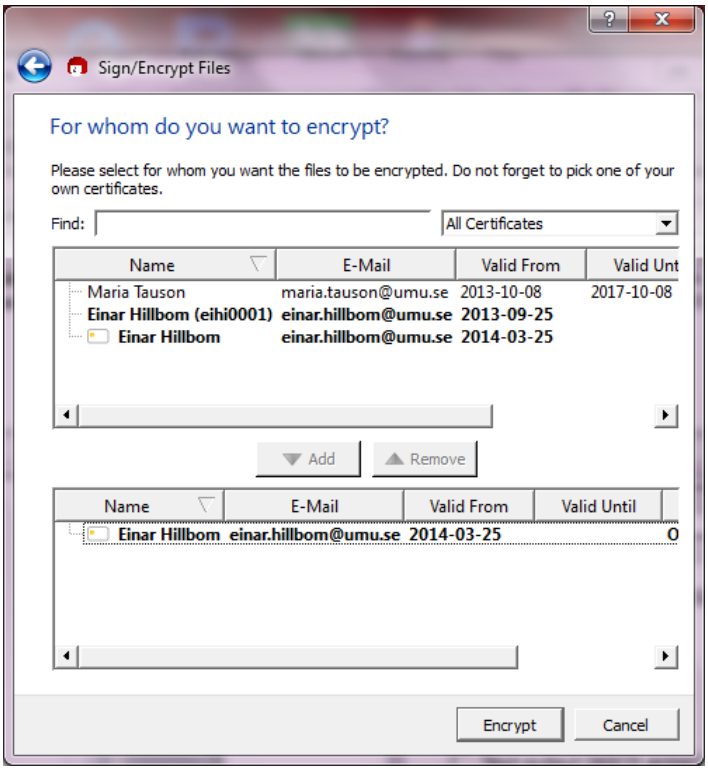
Skapade filen secret.txt:

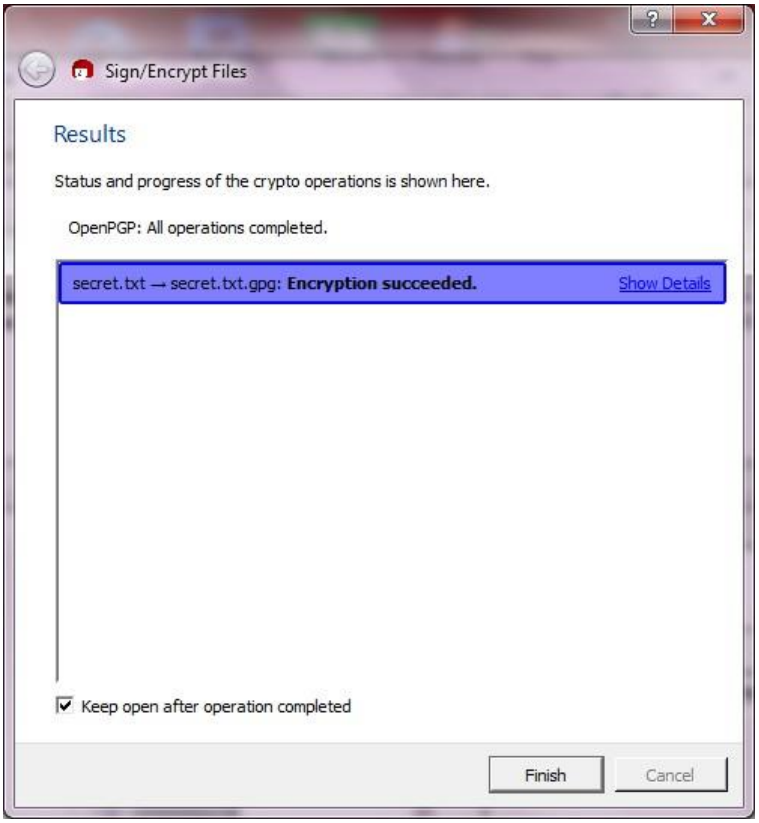
```
2014-03-25
```

```
Detta är en jäkligt hemlig fil.
```

I Kleopatra:



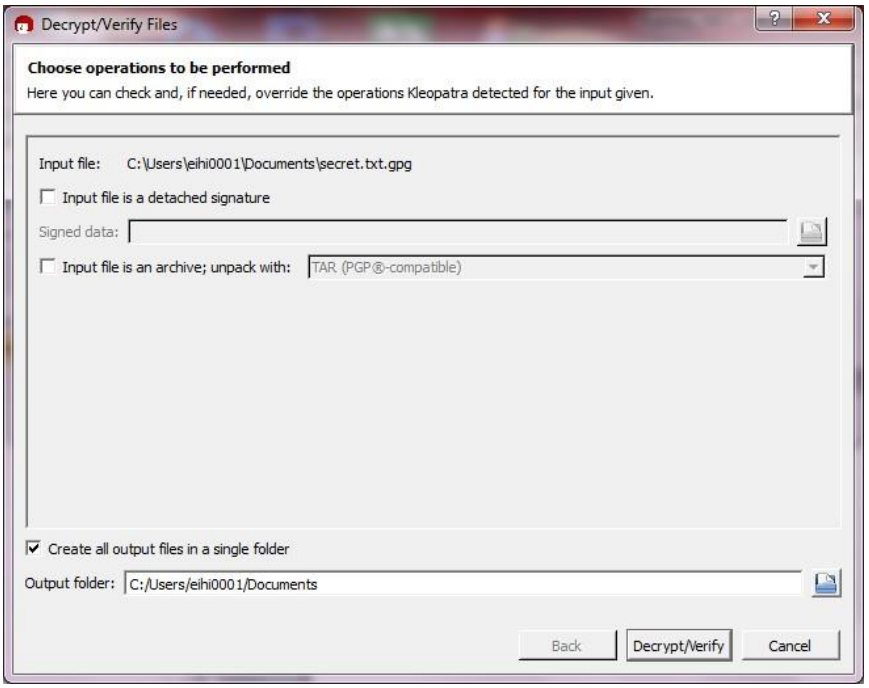

Sign/Encrypt Files
For whom do you want to encrypt?
Please select for whom you want the files to be encrypted. Do not forget to pick one of your own certificates.
Find:
All Certificates
Name
E-Mail
Valid From
Valid Unt
Maria Tauson
maria.tauson@umu.se
2013-10-08
2017-10-08
Einar Hillbom (eihi0001)
einar.hillbom@umu.se
2013-09-25
Einar Hillbom
einar.hillbom@umu.se
2014-03-25
Add
Remove
Name
E-Mail
Valid From
Valid Until
Einar Hillbom
einar.hillbom@umu.se
2014-03-25
Encrypt
Cancel

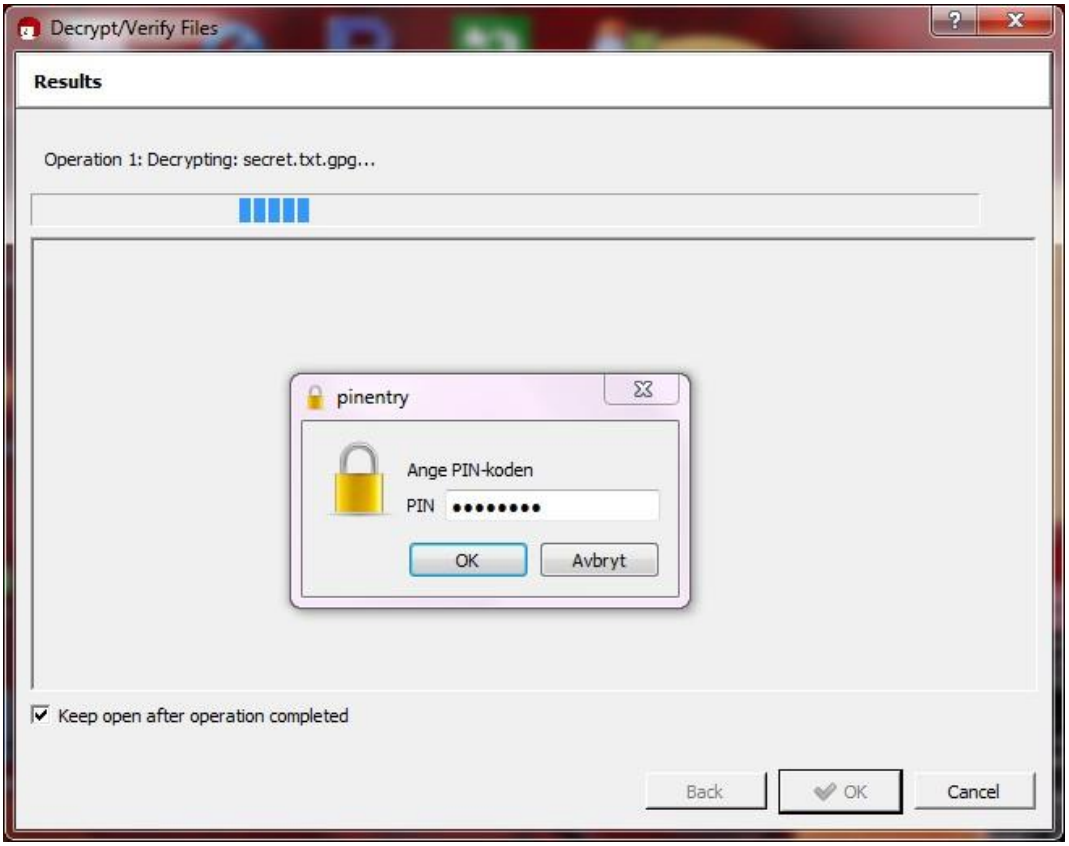


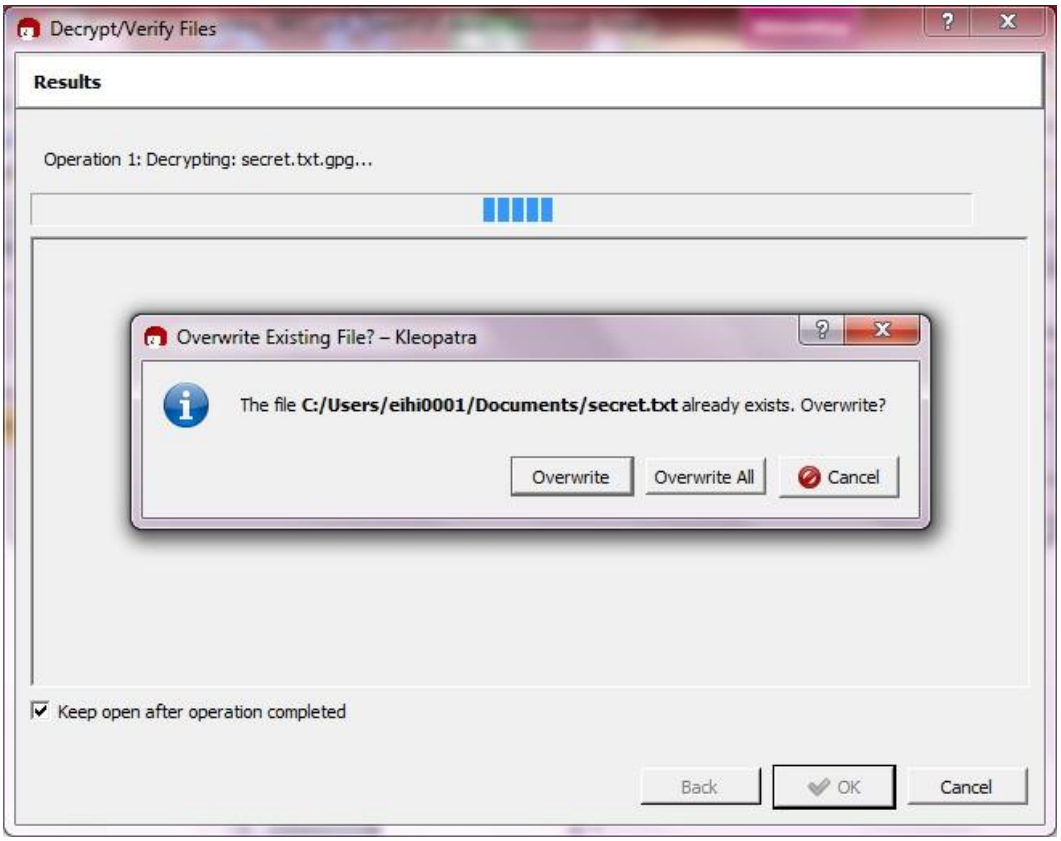
secret.txt.enc:

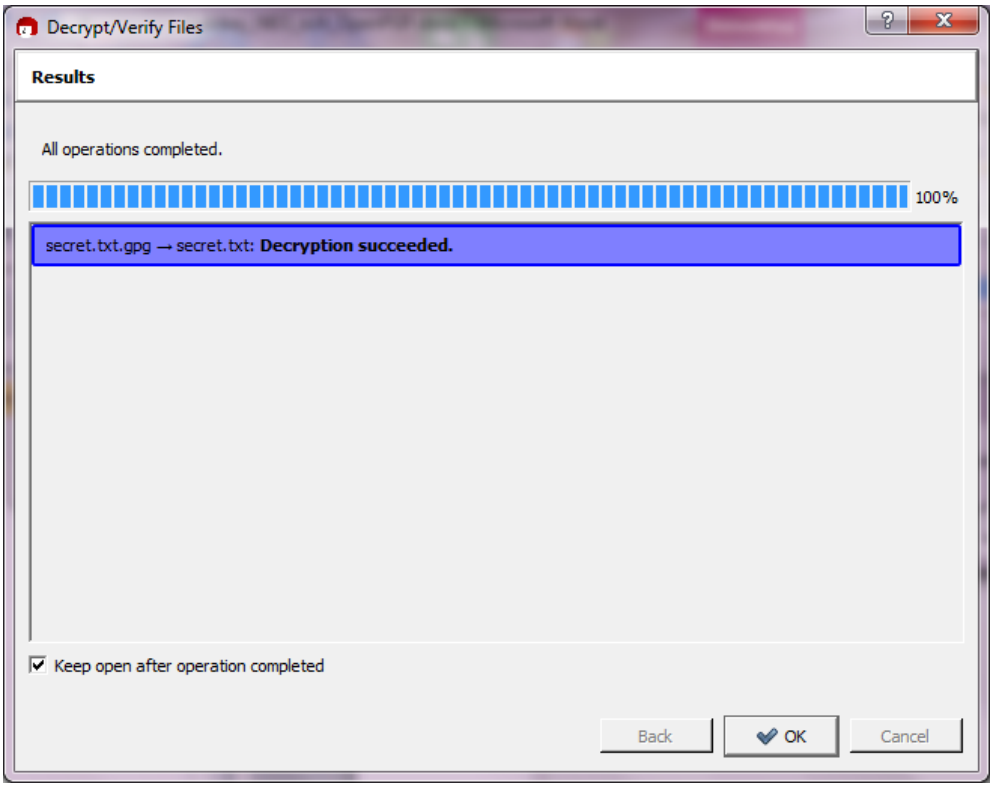
```
…_____k|qHÿ_LŸn¹áŽ2ígÊEÿp%.ÿ(Q□l«…dHÂ.
*) p!QXqÁP/2
```

Dekryptering






Decrypt/Verify Files
Results
Operation 1: Decrypting: secret.txt.gpg...
Overwrite Existing File? – Kleopatra
The file C:/Users/eihi0001/Documents/secret.txt already exists. Overwrite?
Overwrite
Overwrite All
Cancel
Keep open after operation completed
Back
OK
Cancel


Decrypt/Verify Files
Results
All operations completed.
100%
secret.txt.gpg → secret.txt: Decryption succeeded.
Keep open after operation completed
Back
OK
Cancel

GnuPG i Linux

När man stoppade in Yubikey NEO i en Linux-maskin och körde

```
$ gpg --list-keys
```

Så såg man inga av de nycklar som skapats. Vid genereringen skapas en stub i nyckelringen (den privata nyckeln kan ej exporteras). För att få över nycklarna till Linux-maskinen exporterades både den privata (stub) och den publika nyckeln från Windows-datorn med Kleopatra. Dessa importerades i GnuPG på Linux-datorn med:

```
$ gpg --import neo_public.asc
gpg: key 3CE68A03: public key "Einar Hillbom <einar.hillbom@umu.se>"
imported
gpg: Total number processed: 1
gpg:               imported: 1   (RSA: 1)

$ gpg --allow-secret-key-import --import neo_secret.gpg
gpg: key 3CE68A03: secret key imported
gpg: key 3CE68A03: "Einar Hillbom <einar.hillbom@umu.se>" not changed
gpg: WARNING: key 3CE68A03 contains preferences for unavailable
gpg:          algorithms on these user IDs:
gpg:          "Einar Hillbom <einar.hillbom@umu.se>": preference for cipher
algorithm 1
gpg: it is strongly suggested that you update your preferences and
gpg: re-distribute this key to avoid potential algorithm mismatch problems

Set preference list to:
     Cipher: AES256, AES192, AES, CAST5, 3DES
     Digest: SHA1, SHA256, RIPEMD160
     Compression: ZLIB, BZIP2, ZIP, Uncompressed
     Features: MDC, Keyserver no-modify
Really update the preferences? (y/N) y
gpg: detected reader `Yubico Yubikey NEO OTP+CCID 00 00'
gpg: signatures created so far: 6

Please enter the PIN
[sigs done: 6]
gpg: pcsc_transmit failed: insufficient buffer (0x80100008)
gpg: apdu_send_simple(0) failed: invalid value
gpg: signing failed: invalid argument
gpg: update_keysig_packet failed: invalid argument

Key not changed so no update needed.
gpg: Total number processed: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
```

Något verkar ha gått snett vid importen av den privata nyckeln.

Det gick bra att kryptera en fil men man lyckades inte dekryptera den:

```
$ gpg -r 3CE68A03 -e yub.txt

gpg: 1F714819: There is no assurance this key belongs to the named user


pub  2048R/1F714819 2014-03-25 Einar Hillbom <einar.hillbom@umu.se>
 Primary key fingerprint: 958B 2D32 FF50 1396 5CCE  A8F0 DED2 746F 3CE6

8A03

      Subkey fingerprint: 1E2B A261 C44F 6975 A8BD  44C9 6B7C 1306 1F71

4819


It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.


Use this key anyway? (y/N) y
```

För att man skall kunna använda Yubikey NEO krävs att man kör **pcscd** på datorn och troligen är det något problem med denna. Som vanligt är det massor med problem när det gäller Linux, open source och smarta kort. Suck!

Filen som krypterats på Linux-datorn gick att dekryptera med Kleopatra på Windows-datorn

4.4.3 Slutsats och diskussioner

Det går att använda en Yubikey NEO för att lagra GPG-nycklar för kryptering men det kan vara besvärligt, särskilt i Linuxmiljö. Om man tappar bort sin Yubikey NEO eller råkar generera om nycklarna i den så kan man inte längre läsa de filer man krypterat. Man måste alltid ha en klartext-backup.

4.5 TRUECRYPT

(Tyvärr så är utvecklingen stoppad i år på denna produkt, så vi rekommenderar ej denna produkt)

Avknoppningar på TrueCrypt finns:

VeraCrypt:

http://www.esecurityplanet.com/open-source-security/veracrypt-a-worthy-truecrypt-alternative.html

CipherShed:

http://www.esecurityplanet.com/open-source-security/truecrypt-getting-a-new-life.html

---

4.5.1 Sammanfattning

Truecrypt (http://www.truecrypt.org/) [5] är ett open-source krypteringsprogram som kan laddas ner gratis.

TrueCrypt utför kryptering och dekryptering on-the-fly, dvs data krypteras just innan det sparas och dekrypteras strax efter det lästs. Dekrypterat data sparas aldrig på disk utan lagras bara temporärt i minnet (RAM). Användaren behöver inte agera på något sätt utan de krypterade diskarna eller katalogerna används precis som normala diskar och kataloger.

Om datorn slås av eller om disken avmonteras måste användaren montera den virtuella disken igen vilket innebär att lösenordet måste anges på nytt.

Rekommenderad längd på lösenordet är 20-64 tecken och man bör blanda små och stora bokstäver, siffror och specialtecken.

Det går att köra TrueCrypt i ”portable mode”, dvs utan att först installera programmet. Man kan skapa en ”traveler disk” som både innehåller den krypterade volymen och TrueCrypt. På så vis har man allt som behövs på USB-disken eller USB-stickan.

Lösenordet kan ersättas med en nyckelfil. Metoden gör det möjligt att använda smarta kort och andra fysiska säkerhetstokens som stödjer PKCS#11. Det går att dela på tillgången till en krypterad volym genom att varje användare har samma nyckelfil men olika lösenord till sina PKCS#11-kort där filen lagras.. Slutligen kan man ha en lösning där samtliga användare måste presentera sina nyckelfiler innan volymen kan monteras. Man kan även skapa TrueCrypt-volymer på CD och DVD.

Den rekommenderade metoden för att göra en backup av en TrueCrypt-volym är att skapa en ny TrueCrypt-volym som är minst lika stor som den volym som skall backas upp och montera både original-volymen och backup-volymen. Sedan kopierar man filerna från originalet till backupen.Om en bit i en TrueCrypt-fil ändras så förstörs bara ett 16 bytes block, resten skall gå att läsa.

Om man vill kunna återställa nyckeln ifall användaren tappat bort lösenordet kan man göra en kopia av volym-headern efter att TrueCrypt-containern skapats. Därefter låter man användaren ändra lösenord. Om användaren sedan tappar bort sitt lösenord kan man återställa den ursprungliga volym-headern och volymen går att montera med det första lösenordet.

Att använda Truecrypt i en molntjänst innebär vissa svårigheter. Normalt används en synkroniseringsagent som synkroniserar användarens dator med molnet. Om en TrueCrypt-volym används kommer de flesta agenter att behöva föra över hela TrueCrypt-filen, som oftast är stor, för varje liten ändring. Man måste också se till att tidsstämplarna för TrueCrypt-filen sätts rätt så att synkroniseringsagenten upptäcker ändringar. Martin Stout har gjort en del tester [6] dock ej på Box.net.

TrueCrypt kan användas för att:

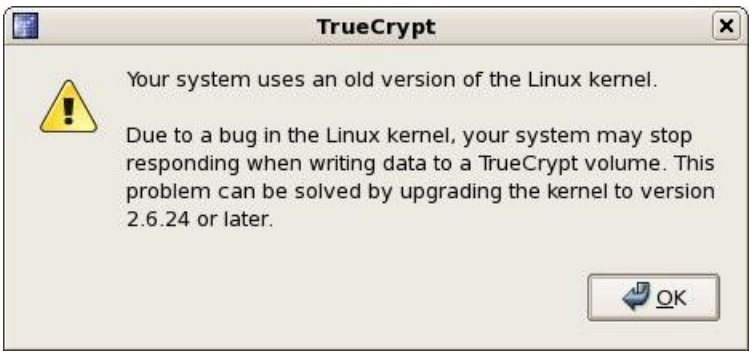
- Skapa en krypterad virtuell disk inuti en fil
- Kryptera en partition eller disk som inte innehåller operativsystemet
- Följande krypteringsalgoritmer stöds (samtliga med 256 bitars nyckel):
    - AES
    - Serpent
    - Twofish
    - AES-Twofish
    - AES-Twofish-Serpent
    - Serpent-AES
    - Serpent-Twofish-AES Följande hashalgoritmer stöds:
    - RIPEMD-160
    - SHA-512
    - Whirlpool

4.5.2 Tester

Truecrypt har för denna rapport testats på Windows och Linux:

- Truecrypt 7.1a på CentOS 5.9
- Truecrypt 7.1a på Windows 7 Enterprise

Linuxkärnans version var 2.6.18 vilket gav upphov till en varning i Truecrypt:



I Windows kan en användare utan administrativ behörighet montera/avmontera en krypterad volym och läsa/skriva till den samt skapa virtuella diskar. Detta förutsätter dock att en administratör först installerat TrueCrypt. Utan administrativ behörighet kan man inte skapa krypterade partitioner, skapa NTFS-volymer, installera/avinstallera TrueCrypt, byta lösenord/nyckelfiler eller köra TrueCrypt i ”portable mode”.

4.5.2.1 Linux

I Linux krävs root-behörighet för att montera en krypterad volym. Man kan kringgå detta genom att ex.vis använda sudo:

user ALL=NOPASSWD: /usr/bin/truecrypt

Säkerheten kan dock bli lidande.

Två virtuella volymer skapades, privat.tc med lösenord samt delad.tc utan lösenord men med en nyckelfil med namnet delad.key (det fanns inga PKCS11-enheter att testa PIN-kodskyddad nyckelfil med). Filen delad.tc sparades på ett USB-minne som ett FAT-filsystem.

En tredje TrueCryptvolym,masterkey.tc, skapades och med hjälp av ”Tools-Backup Volume Header” så skapades en kopia av headern till filen masterkey.bak. Därefter byttes lösenordet med ”Volumes-Change Volume Password”. Detta för att efterlikna situationen där en administratör skapar en TrueCrypt-volym åt en användare som sedan får välja ett eget lösenord men där administratören sparar en masternyckel. Sedan användes ”Tools-Restore Volume Header” där det ursprungliga lösenordet fick anges. Därefter kunde volymen monteras med det usprungliga lösenordet.

4.5.2.2 Windows

USB-minnet med filen delad.tc som skapades i Linux flyttades till Windows-datorn och monterades med hjälp av nyckelfilen delad.key. En fil kopierades till den virtuella disken varefter USB-minnet åter monterades i Linux-datorn. Filen gick bra att läsa i Linux.

Filen delad.tc (100 MB) lades i ”My Box Files/Default Sync Folder”. Det tog ca 15 min att synkronisera mot Box.net. Filen i synk-mappen monterades sedan i TruCrypt. I ”Settings-Preferences avbockades ”Preserve modification timestamp of file containers”. Några bildfiler kopierades till den monterade volymen. Efter att volymen avmonterats i TrueCrypt startade synkroniseringen som tog 14 minuter.

4.5.3 Slutsatser och diskussioner

Det är enkelt att skapa virtuella, krypterade volymer både i Linux och i Windows då bägge har grafiska interface.

Det går att dela på en krypterad volym med hjälp av nyckelfiler i stället för lösenord. Man bör dock lagra nyckelfilen på en PIN-kodsskyddad enhet som stödjer PKCS11, ex.vis ett smart kort eller en säkerhetstoken, annars är säkerheten inte mycket bättre än om man delar på lösenordet. Har man PIN-kodsskyddade smarta kort kan varje användare ha en egen PIN-kod till sitt kort.

Det går bra att använda samma TrueCrypt-fil både i Linux och Windows under förutsättning att filsystemet är kompatibelt.

Det är möjligt att skapa en masternyckel till en TrueCrypt-volym. Om användaren glömmer bort sitt lösenord kan man återställa lösenordet till det som ursprungligen sattes.

Det går att ha TrueCrypt-containern i molnet men det innebär vissa svårigheter [6]. Det gick att köra mot Box.net men synkroniseringen tog alldeles för lång tid eftersom hela TrueCrypt-containern fick synkroniseras även efter små ändringar.

4.6 AxCrypt

4.6.1 Sammanfattning

AxCrypt är en öppen källkod filkryptering programvara för Windows. Det kan enkelt integreras med Windows för att komprimera, kryptera, dekryptera, lagra, skicka och arbeta med enskilda filer.

AxCrypt använder Advanced Encryption Standard med 128-bitars nycklar i Cipher Block Chaining-läge med en "random" IV för datakryptering, men om du vill uppnå den nivå av säkerhet måste du ge det 128 bitar av verkligt "slumpmässiga" uppgifter.

Det enklaste och säkraste sättet att göra detta är att låta AxCrypt generera en nyckel-fil för dig. Högerklicka på den mapp där du vill ha den, och välj 'AxCrypt | Gör Key-fil ". Detta kommer att skapa en liten textfil med en stark nyckel. Lagra filen på en diskett eller USB-minne till exempel, och hålla det hemligt och separat från dina filer.

Skriv alltid din nyckel-fil eller lösenordsfras och insättning på ett säkert ställe! Om du förlorar det, är alla dokument som krypterats med den permanent. Det finns inga genvägar och inget sätt att dekryptera utan den.

Använda lösenordsfras, detta motsvarar ungefär 10 "slumpmässiga" ord. Använd inte meningsfulla meningar och absolut inte kända eller ens obskyra citat!

Genom att införa variationer om fallet, liksom icke-alfabetiska tecken kan du minska antalet ord som behövs. Det är inte rekommenderat att använda mindre än fem ord.

Om du använder ett helt slumpmässigt urval av övre och gemena bokstäver och siffror, behöver du minst 22 tecken för att uppnå 128 bitar säkerhet.

Den fragmentering, eller avtorkning, inslag i AxCrypt kan du radera filer på ett sätt som gör det omöjligt att återställa innehållet med undeletion programvara. Men det finns några varningar:

Namnet på filen, liksom storleken, kan återvinnas.
Om filen har visats eller redigeras med ett program som skapar tillfälliga kopior av innehållet (till exempel Microsoft Office kan), kan dessa tillfälliga kopior fortfarande vara tillgänglig för undeletion på din hårddisk.

Plattformsstöd/Tjänster:

• Windows 2003/XP/Vista/2008/7/8 32- and 64-bit compatible.

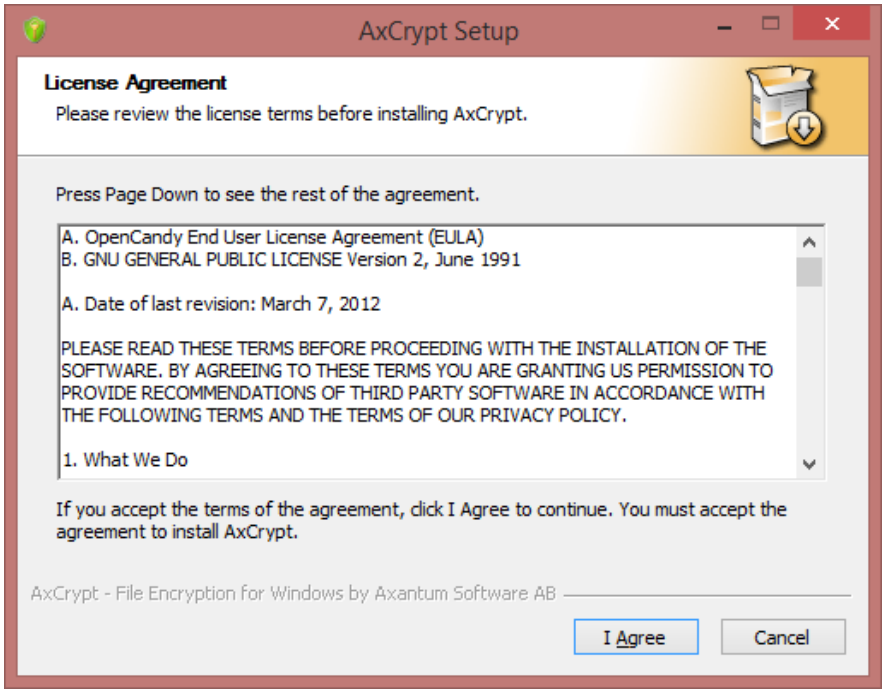
4.6.2 Tester

AxCrypt har för denna rapport testats på Windows:

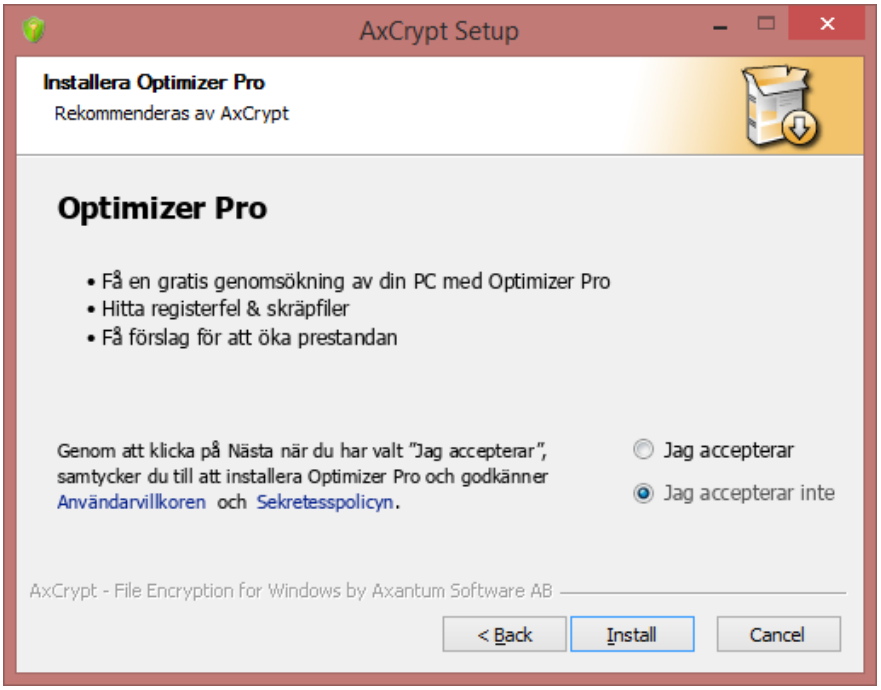
- Windows 8
- Windows 7

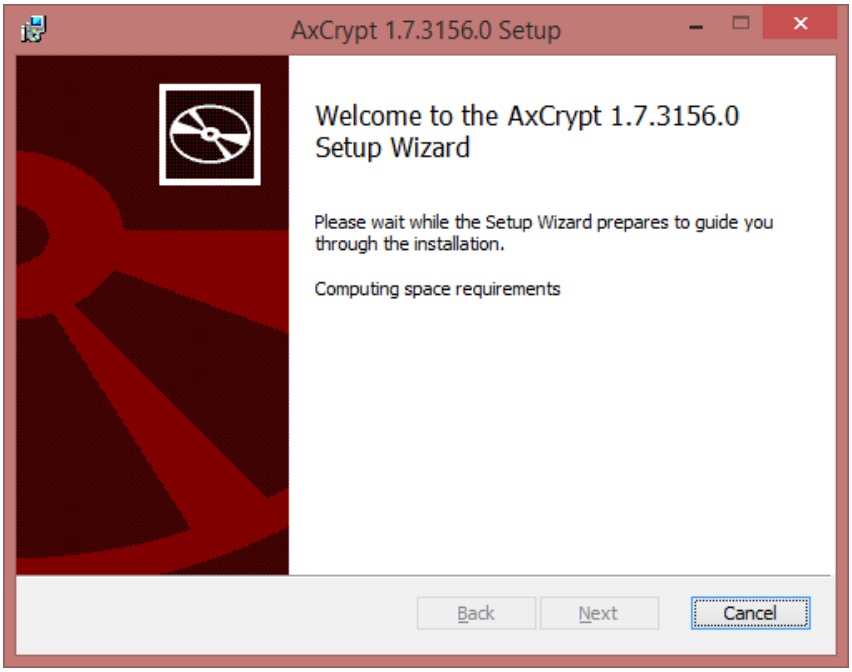
4.6.3 Administration/användarhantering

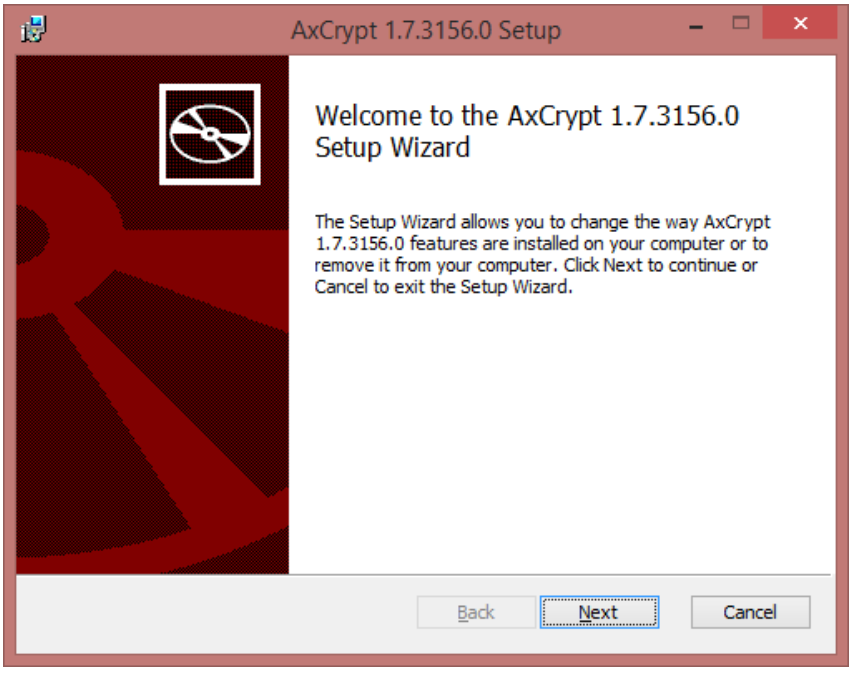
Enkel installation

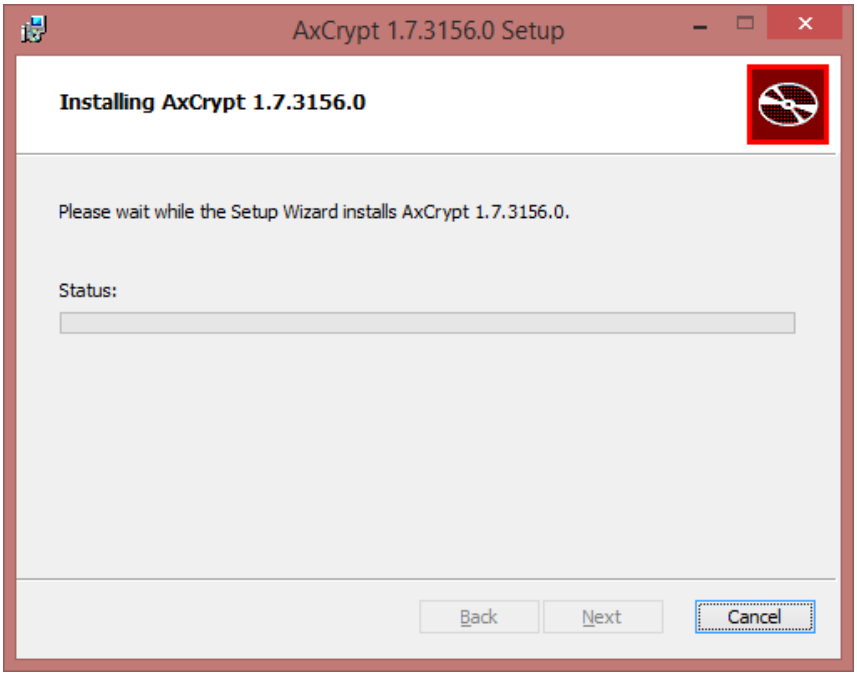


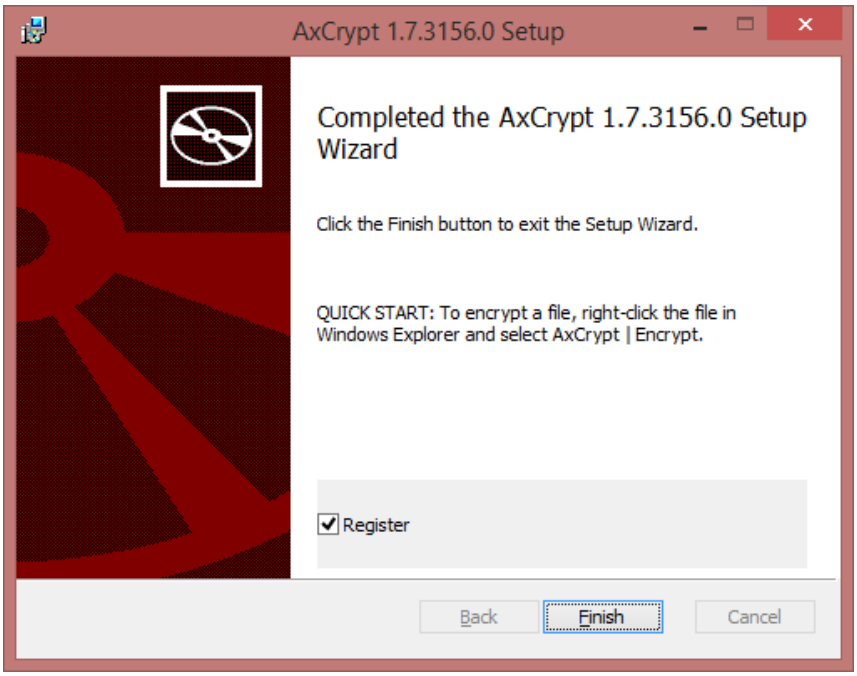
Obs! viktigt välj ”Jag accepterar inte” eftersom man inte vill installera någon annan produkt i detta skede.



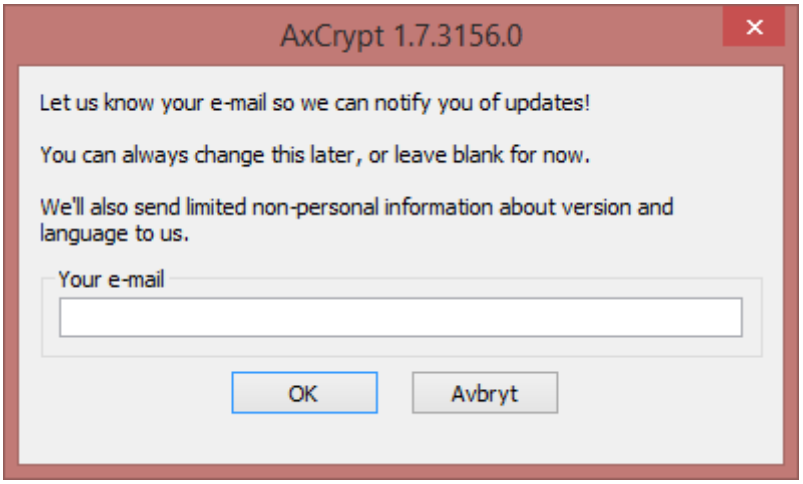

AxCrypt 1.7.3156.0 Setup
Welcome to the AxCrypt 1.7.3156.0 Setup Wizard
Please wait while the Setup Wizard prepares to guide you through the installation.
Computing space requirements
Back
Next
Cancel


AxCrypt 1.7.3156.0 Setup
Welcome to the AxCrypt 1.7.3156.0 Setup Wizard
The Setup Wizard allows you to change the way AxCrypt 1.7.3156.0 features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel





Obs! lämna blankt.



4.6.4 Slutsatser och diskussioner

AxCrypt får anses som en krypterings applikation som är enkel att använda men med hänsyn att den endast använder sig av 128-bitars nyckel när vissa använder 256-bitar. Produkten är Free vilket innebär att man inte med säkerhet veta vad mer som följer med i applikationen men så kan det vara även med kommersiella produkter. Framtida utveckling av produkten kan också ifrågasättas.

http://www.axantum.com/axcrypt

4.7 BoxCryptor

4.7.1 Sammanfattning

Boxcryptor, https://www.boxcryptor.com/en/ [7], är ett krypteringsprogram som används tillsammans med molntjänsters synkroniseringsagenter. Innan filerna sparas i molnet krypteras dom och får ändelsen .bs. Vid nerladdning från molnet dekrypteras filerna med ändelsen .bs som sedan tas bort. Det är således bara förändrade filer som synkroniseras. Nackdelen med gratisversionen av Boxcryptor är att filnamnen fortfarande är läsbara.

4.7.2 Administration/användarhantering

Filerna krypteras med asymmetrisk RSA kombinerat med symmetrisk 256-bitars AES.

Köper man ett företagspaket finns möjligheten att aktivera masternycklar så att användarna kan få nya nycklar ifall dom tappas bort. Man kan även sätta policys rörande minsta längd på lösenord etc.

Man kan antingen använda en lokal nyckelfil som skyddas av ett lösenord eller använda ett Boxcryptor-konto. Använder man en lokal nyckelfil kan man inte använda Boxcryptor på mobila enheter eller dela filer med andra användare. För testet valdes en lokal nyckelfil.

Efter installation av Boxcryptor var det bara att lägga filerna i ”My Box Files/Default Sync Folder” och efter en kort stund fanns de på konto i Box.net. Filerna gick ej att läsa med en webbläsare.

Boxcryptor har mobila appar för Windows, Mac OS X, iOS, Android, Windows Phone, Windows RT, Blackberry 10, and Google Chrome.

Plattformar som stöds

	Windows	Mac OS X	Android	iOS
Dropbox	✔	✔	✔	✔
Google Drive	✔	✔	✔	✔
Microsoft SkyDrive	✔	✔	✔	✔
Box	✔	✔	✔	✔
SugarSync	✔	✔	✔	✔
Telekom Cloud	✔	✔	✔	✔
TrendMicro SafeSync	✔	✔	✔	✔
Strato HiDrive	✔	✔	✔	✔
GMX MediaCenter	✔	✔	✔	✔
Web.de Smartdrive	✔	✔	✔	✔
CloudMe	✔	✔	✔	✔
Cubby	✔	✔	✔	✔
Livedrive	✔	✔	✔	✔
Yandex Disk	✔	✔	✔	✔
CloudSafe	✔	✔	✔	✔
Cloudwatt-box	✔	✔	✔	✔
Filespots	✔	✔	✔	✔
Egnyte	✔	✔	✔	✔
Local Storage	✔	✔	✔	✘
SpiderOak	✔	✔	✘	✘
Wuala	✔	✔	✘	✘
Ubuntu One	✔	✘	✘	✘

4.7.3 Slutsatser och diskussioner

Boxcryptor kan vara ett alternativ om man använder Box. En nackdel är att man tappar förhandsgranskningen av filerna eftersom Box inte kan läsa de krypterade filerna. Man är tvungen att hämta hem filerna till sin egen dator och titta på dom där.

4.8 TUTUS FILKRYPTO – ”KURIR”

4.8.1 Sammanfattning

KURIR är under godkännande av Försvarets materielverk för att få godkänt som KSU.

Kryptering och dekryptering kan enkelt göras genom att dra och släppa filerna till Kurir applikationen. Men all funktionalitet finns också tillgängliga från menyerna i programmet.

Applikationen kan beroende på serienumret användas i ett fullständigt läge eller ett begränsat läge. I det begränsade läget inte kan användaren skapa krypteringsnycklar. Serienummer kan också användas för att skapa slutna användargrupper som bara kan kryptera filer sinsemellan.

Kurir ger följande säkerhetsfunktioner:

- Kryptering av filer
- Skydd av filer
- Dekryptering av filer
- Integritet kontroll av filer

4.8.2 Kryptering av filer

Filerna krypteras med symmetriska algoritmen AES i CBC-läge med en 256-bitars nyckel, för att säkerställa sekretess för information undertiden den lagras och/eller under sändning. De

kryptografiska nycklarna väljs av användaren ur en nyckellista eller med standard nyckeln. När en fil krypteras av Kurir resulterar det i en * .xml-fil som innehåller ytterligare information om vilken nyckel (id) användes för att kryptera filen, tid när filen krypterades, filnamnet av original filen, och den krypterade informationen.

4.8.3 Skydd av filer

För att upptäcka förlust av integritet datafiler och nycklar, används en nyckel hash funktion över varje chiffer som genereras av Kurir. Algoritmen som används är HMAC- SHA256 - ett meddelande autentiseringsfunktion använder en 256-bitars nyckel och en SHA-256 hash funktion. Nyckeln som används för att beräkna HMAC är en 256-bitars nyckel som endast används för detta ändamål. Därför måste även denna nyckel delas mellan krypteringsparter, förutom att dela respektive kryptering/dekrypteringsnyckel.

4.8.4 Dekryptering av filer

Kurir ser till att endast de användare som besitter rätt nyckel, eller känner till lösenordet associerad med nyckeln, kan läsa krypterad fil.

4.8.5 Integritet kontroll av filer

Denna funktion möjliggör potentiell förlust av integritet datafiler och nycklar att detekteras genom att validera de knappat hash värdena före dekryptering. Algoritmen som används är HMAC-SHA256 - ett meddelandes autentiseringsfunktion använder en 256-bitars nyckel och en SHA-256 hash funktion. Nyckeln som används för beräkning av HMAC är en 256-bitars nyckel som skapas för detta ändamål. Denna nyckel måste delas mellan de kommunicerande parterna, förutom att dela med sig av respektive kryptering/dekryptering nyckel.

4.8.6 Nyckel hantering

Nyckelhantering är en process för att hantera en hel livscykel för kryptografiska nycklar från generering genom distribution till arkivering och destruering.

- Nyckel generering
    - Nyckel härledning: De nycklar som används för att skydda krypterade Key stores kommer från lösenord som matats in av användarna.
    - Data fil krypteringsnycklar: Endast symmetriska AES nycklar med en nyckellängd på 256 bitar genereras av Kurir.
- Importera/Exportera nycklar: För att utbyta nycklar mellan olika användare kan nycklarna exporteras inom lösenordskyddade, krypterade nyckelfiler som skapats av en Kurir användaren. Å andra sidan, kan dessa nycklar endast importeras i Kurir av en användare som känner till lösenordet.
- Nyckel lagring: Alla nycklar lagras i lösenordskyddade krypterad key storages.
- Säker radering implementeras genom att Kurir skriver över filer med slumpmässiga data som genereras av datorn. Denna funktion används i nödfall om man måste tas bort Kurir data omedelbart.

4.8.7 Tester

AxCrypt har för denna rapport testats på Windows:

- Windows 7
- Windows 8
- Windows 8.1

4.8.8 Administration/användarhantering

4.8.8.1 Starta Kurir

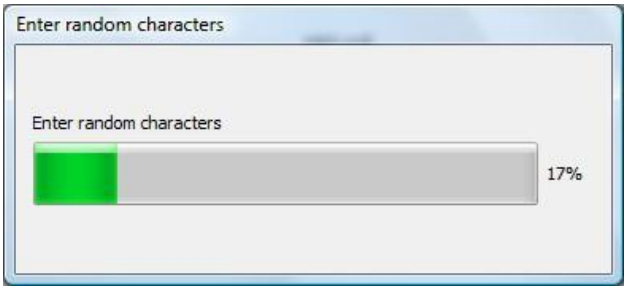
Kurir programmet startar lite annorlunda första gången du kör applikation, jämfört med resten av tiderna.

Första gången du startar Kurir efter installationen

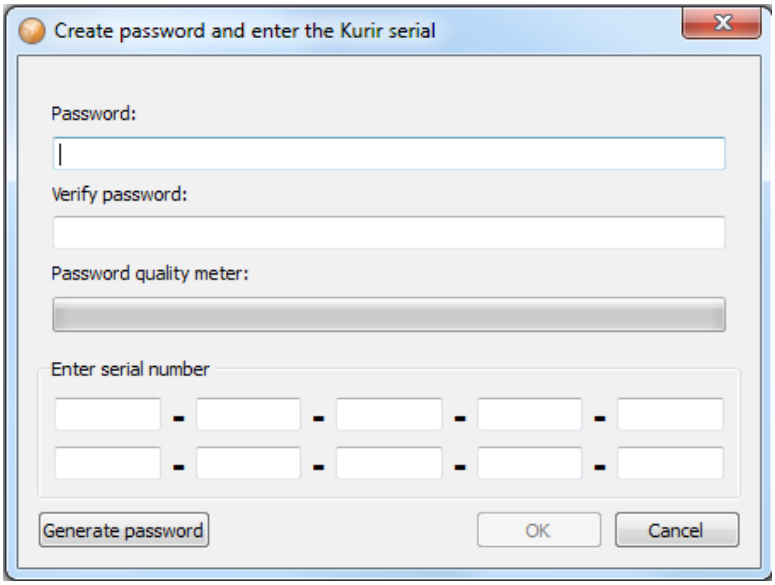
För att starta Kurir programmet för första gången:

Dubbelklicka på ikonen Kurir på skrivbordet.

Dialogrutan "Enter slumpmässiga tecken" öppnas.



1. Ange slumpmässiga tecken tills fältet är fullt (100%) och dialogrutan stängs.
2. Lösenord och serienummer fönstret öppnas.



3. Skriv in det lösenord du vill använda i fältet Lösenord.

Lösenordskvalitetsmätare fältet indikerar kvaliteten på lösenord. Kvalitets tabells fält måste fyllas innan du har ett giltigt lösenord.

3. Skriv in lösenordet en gång till i fältet Bekräfta lösenord.

Tips! Om du inte vill skapa ett lösenord själv, kan du klicka på Generera lösenord-knappen för att automatiskt generera ett lösenord.

4. Ange serienumret för Kurir.

Du är nu inloggad och kan börja använda applikation.

För att starta Kurir för andra gången (och resten av tiden):

1. Dubbelklicka på ikonen Kurir på skrivbordet. Uppstarten dialogen för Kurir öppnas.

2. Ange ditt lösenord i fältet Lösenord: och klicka på OK.

Kurir startar och du kan börja använda programmet.

Obs! Om du av någon anledning, måste du radera alla nycklar i Kurir, kan du använda Emergency radering knappen i startdialogruta.

4.8.8.2 Programfönster

Kurir programfönster innehåller fyra menyer, tre mappar och ett dokument dokumentförstörare.

Mappar

De tre mappar innehåller följande:

- Filer - Innehåller de krypterade/dekrypterade filerna.
- Nycklar - Innehåller Keystores och krypteringsnycklar som skapats av användaren.
- Logg – Logg information på händelser i Kurir

Menyer
De fyra menyerna innehåller följande alternativ:

- Arkiv - Denna meny innehåller Kryptera fil, Kryptera mapp, dekryptera, Skriv över, Kryptera med gamla formatet (1,0) och Exit alternativ.
- Nycklar - Denna meny innehåller Emergency radera, Exportera nyckel, Byt namn på nyckel, skapa nyckeln, Import nycklar, Byta nyckel lösenord och keystores alternativ.
- Inställningar - Denna meny innehåller Visa filer, Visa-filer i kombination, Visa filer åtskilda, Visa nycklar, Visa keystores, alltid på topp, och språkalternativ.
- Om - Denna meny visar information om Kurir programmet.

4.8.8.3 Dokumentförstörare

Med dokumentförstörare kan du ta bort filer som du inte vill behålla. Detta görs genom att skriva över informationen flera gånger.

Obs! Beroende på det underliggande filsystemet, och lagringsmediet används, kan du inte vara säker på att dokumentförstörare lyckas skriva över lagrad information. Även om Kurir lyckas skriva över information, kommer en analys av den magnetiska ytan av skivan ofta kunna återställa informationen.

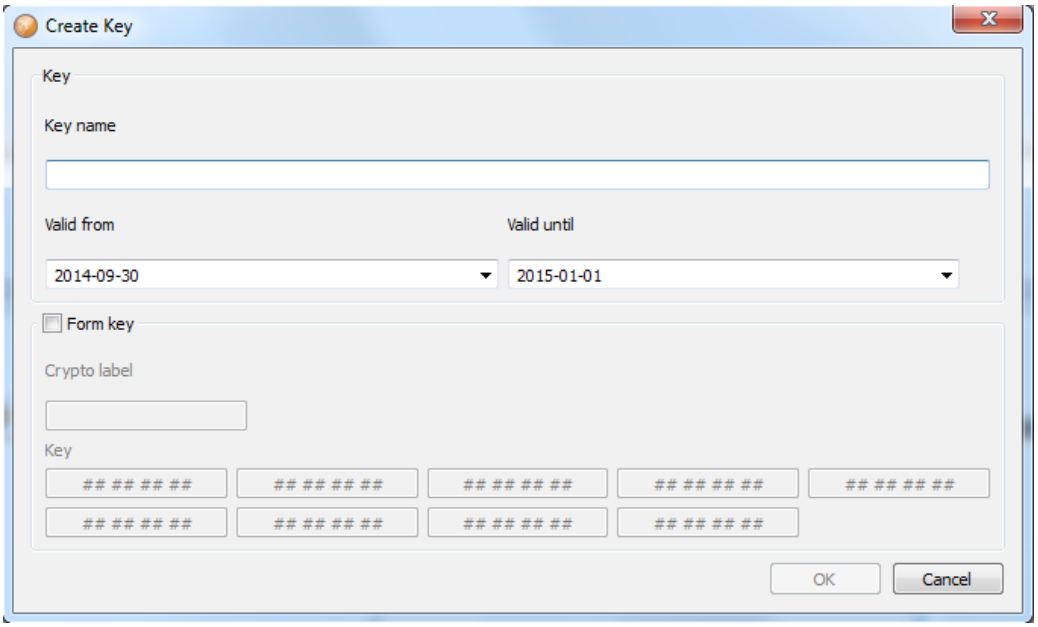
4.8.8.4 Krypteringsnycklar

Obs! Nycklar kan inte skapas om du kör den begränsade versionen av Kurir.

Skapa en nyckel

För att generera en nyckel:

1. Klicka på Keys menyn och välj alternativet Skapa nyckeln. Dialogrutan "Skapa nyckel" öppnas.

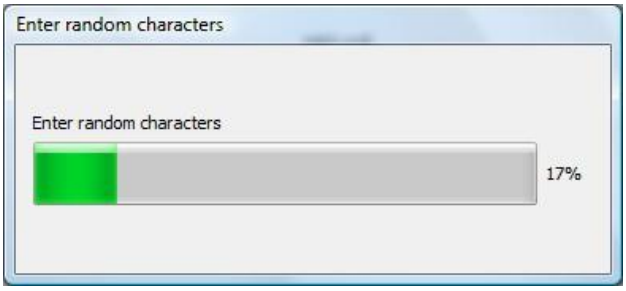


2. Ange nyckelnamn du vill använda i Key namnfältet.

3. Välj start- och slutdatum för tidsintervallet under vilken du vill att nyckeln ska vara giltigt.

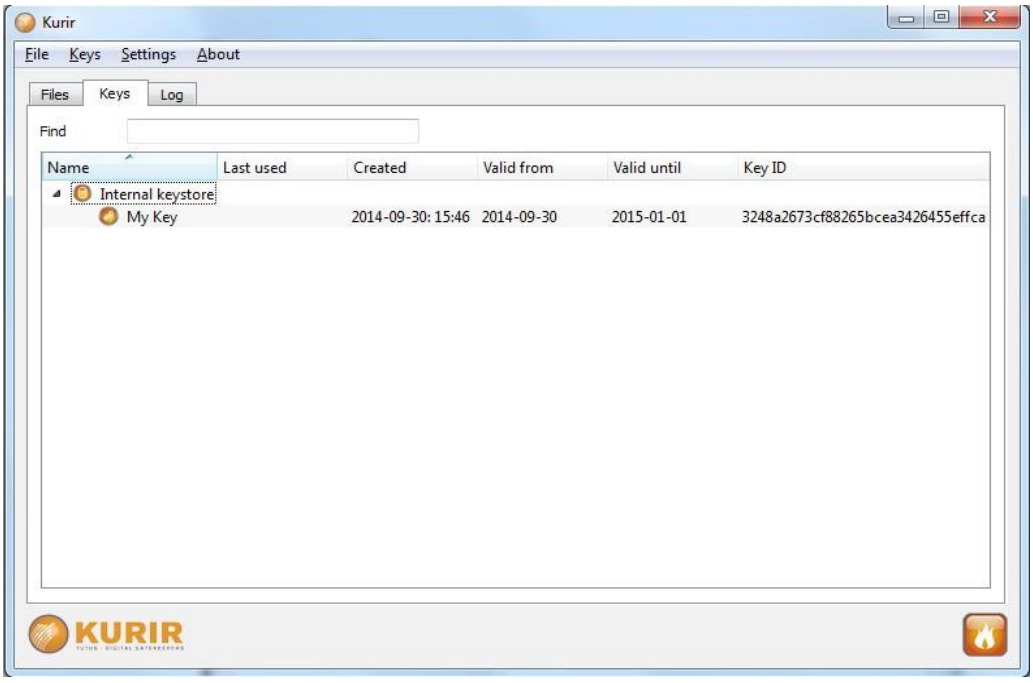
4. Klicka på OK.

Dialogrutan "Enter slumpmässiga tecken" öppnas.



5. Ange slumpmässiga tecken tills fältet är fullt (100%) och dialogrutan stängs.

Nyckeln är noterat i mappen Keys tillsammans med information om när nyckeln skapades, start- och slutdatum för giltighetstiden samt nyckel-ID.



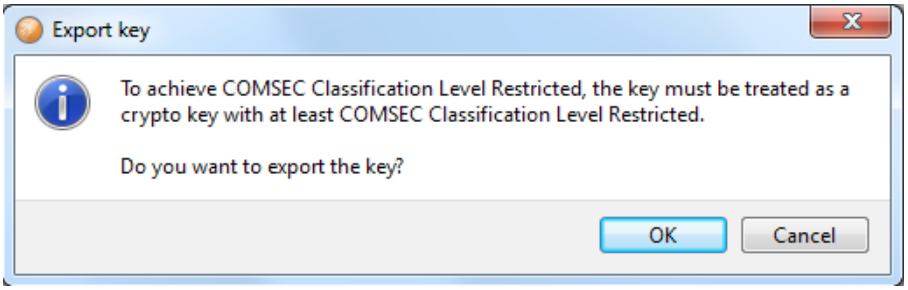
Exporterande nycklar

Du måste exportera nyckeln till den andra parten.

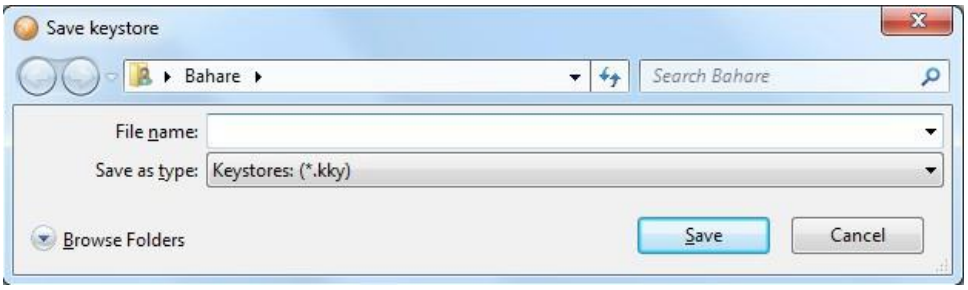
För att exportera nycklar:

1. Välj nyckeln (er) som du vill exportera, högerklicka, eller klicka på Keys menyn och välj alternativet Exportera nyckel.

En bekräftelse fråga, där du kan välja om du är säker på att du vill ex- port den valda nyckeln (er) eller inte, visas.



2. Klicka på OK om du är säker på att du vill exportera nyckeln (s). Dialogrutan "Spara-nyckel" öppnas.



3. Ange ett filnamn som du själv väljer, välj nyckelbehållare typ i Filformat listrutan, och klicka på Spara.

Dialogrutan "Ange lösenord" öppnas.

4. Ange det lösenord du har kommit överens om att använda i fältet Lösenord.

Lösenordskvalitetsmätare i botten av dialogrutan visar kvaliteten på det angivna lösenordet. Hela Mätaren måste fyllas innan du har ett giltigt lösenord.

Kvaliteten på lösenord har fått betyget baseras på följande regler:

»Lösenordet måste bestå av minst 7 tecken.

»Lösenordet kommer att ha en lägre kvalitet rating om den innehåller upprepade kombinationer, t.ex. ababcabab.

»Lösenordet kommer att ha en högre kvalitet rating om den innehåller ESC, övre och små bokstäver, siffror och specialtecken som utropstecken (!), Citationstecken ("), dollartecken ($), etc.

5. Kontrollera lösenordet genom att ange det igen i Bekräfta lösenord: fält och klicka på OK.

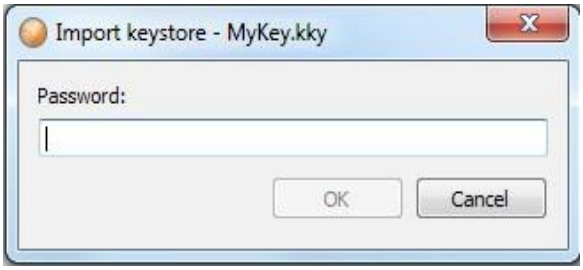
En nyckel med filändelsen * .kky finns nu i den valda mappen.

Importera nycklar

För att importera nycklar:

1. Klicka på Keys menyn och välj sedan alternativet Importera nycklar.

2. Bläddra till den mapp där nyckeln ligger välja tangenten och klicka på Öppna. Dialogrutan "Importera nyckelbehållare" öppnas.



3. Ange det lösenord du har kommit överens om att använda och klicka på OK.

4.8.8.5 Keystore

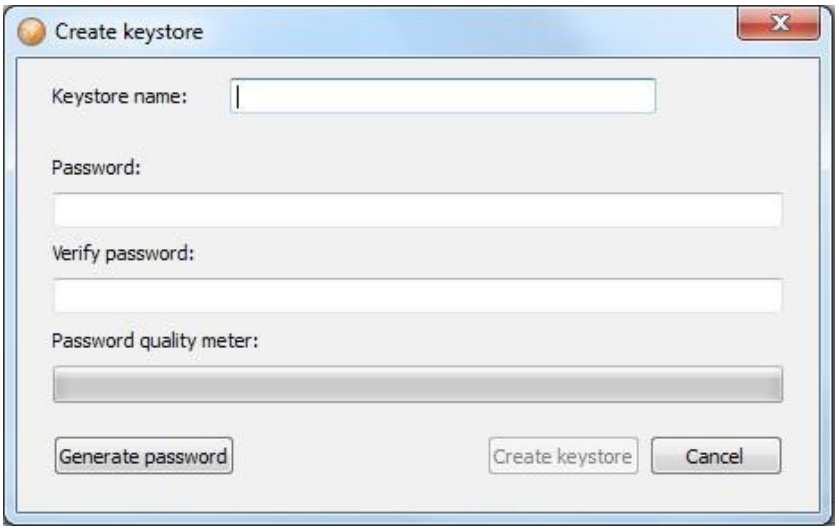
Om du inte vill importera nyckeln (s), men håll dem i en extern mapp eller i en extern media, såsom en USB datalagringsenhet, kan du skapa genväg till nyckeln (er) genom att lägga till keystore.

Skapa en keystore

För att skapa en keystore:

1. Klicka på Keys menyn, välj alternativet keystore, och sedan skapa nya keystore.

Den "Skapa keystore" dialogruta öppnas.



2. Skriv in ett namn för keystore i Keystore namnfältet.

3. Skriv in lösenordet du har valt att använda i fältet Lösenord.

4. Kontrollera lösenordet genom att ange det igen i Bekräfta lösenord: fält, och klicka på knappen Skapa keystore.

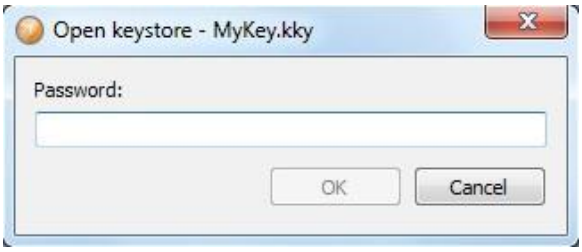
Keystore är nu skapad.

Lägga till en keystore

För att lägga till en keystore:

1. Klicka på Keys menyn, välj alternativet keystore, och sedan Lägg keystore.

2. Bläddra till den mapp där nyckeln ligger välja nyckeln och klicka på Öppna. Dialogrutan "Öppna keystore" öppnas.



3. Ange det lösenord du har kommit överens om att använda och klicka på OK.

Emergency erase

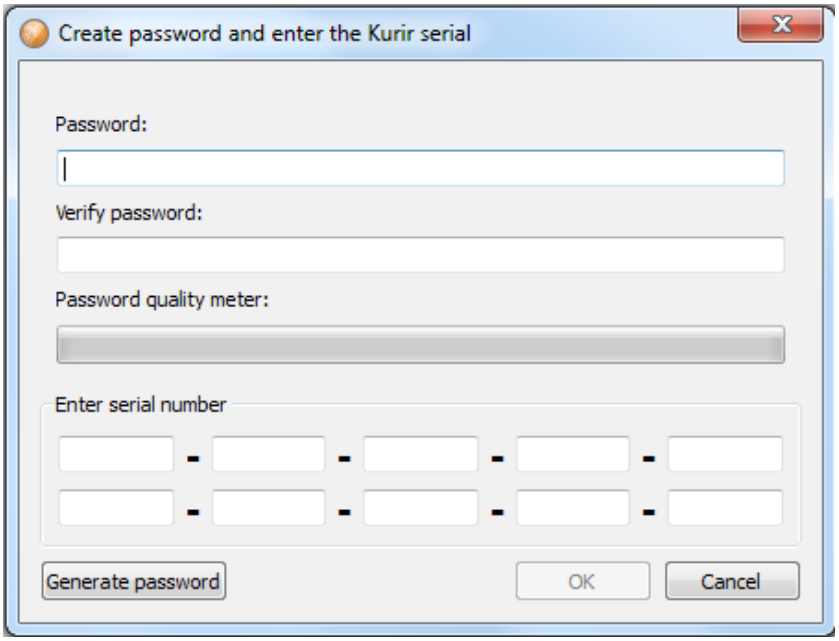
Om du av någon anledning, måste du radera alla keystore, nycklar och filer i Kurir programmet, kan du använda Emergency erase:

1. Klicka på Keys menyn och välj alternativet Emergency erase. Dialogrutan "Emergency erase" visas.

2. Klicka på Ja om du är säker på att du vill fortsätta med borttagningen.

3. Alla filer, nyckelbehållare och nycklar bifogas Kurir nu raderas.

4. Dialogrutan "Skapa lösenord och ange Kurir seriella" visas, där du måste ange ett nytt lösenord samt serienumren, återigen.



5. Ange lösenordet du har valt att använda i fältet Lösenord.

6. Kontrollera lösenordet genom att ange det en gång till i fältet Verifiera lösenord.

7. Ange serienumret för Kurir i löpnummer fält och klicka

OK.

Kurir programfönstret är nu aktiv. Du är nu inloggad och kan använda programmet igen.

Obs! När du använder Emergency raderingsalternativet så raderas bara data för den inloggade användaren ej för övriga användare.

Kryptering och dekryptering

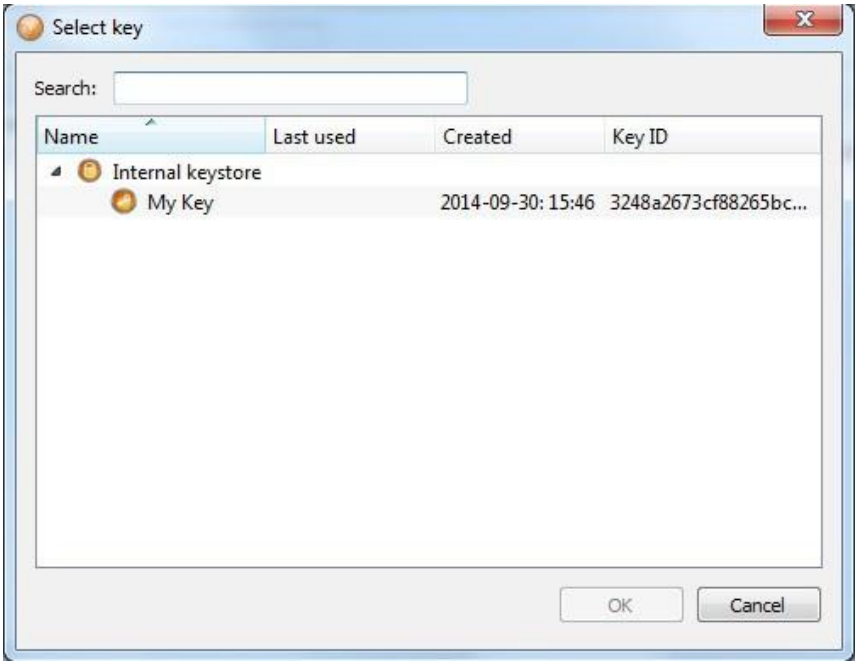
När du har skapat en gemensam nyckel, kan du börja kryptera och dekryptera dokument eller mappar. Kryptering och dekryptering kan göras genom att använda både menyerna eller dra och släppa.

Kryptera filer och mappar

Kryptera filer:

1. Dra och släpp eller använd verktygets menyer.

Dialogrutan "Välj nyckel" öppnar upp.



2. Välj den nyckel du vill använda och klicka på OK.

Den krypterade filen eller mapp visas nu i mappen Files tillsammans med nyckeln ID som används och tid för skapande.

3. Dra och släpp den krypterade filen eller mapp till platsen där du vill ha den lagrad.

4.8.9 Dekryptera filer eller mappar

När du får en krypterad fil eller mapp, måste du dekryptera den för att kunna öppna och visa innehållet.

Att dekryptera filer:

1. Dra och släpp filen eller mapp du vill dekryptera på Kurir applikation.

Förutsatt att du har tillgång till nyckeln krävs, är filen eller mappen dekrypterade och vissas i mappen Files.

2. Dra och släpp den dekrypterade filen eller mappen till den plats du vill lagra den på.

3. fil (er) kommer att tas bort från mappen Files vid byte av lagringsplats och kan nu öppnas och visas direkt från den lagrade mappen.

4.8.10 Slutsatser och diskussioner

Kurir upplevs som en relativt enkel applikation för att kryptera data och stödet för svenska som språk underlättar också för ovana användare. Kurir applikationen har ett mycket bra och logiskt gränssnitt som gör det enkelt att använda. Kurir ger också möjligheten att ha flera skyddade keystores som underlättar om man jobbar i olika uppdrag dvs. en keystore för varje uppdrag. Eftersom produkten kommer att bli klassad som KSU så betyder det att vi kan till stort lita på produkten att den är ren från oönskade bakdörrar mm. Kan vi inte lita på vår egen stat som i många fall är vår arbetsgivare så kan vi nog inte lita på någon annan produkt heller.

4.9 E-MAIL KRYPTERING

När en person begär ett Terena-certifikat för email-signering skapas det ett nyckelpar automatiskt i webbläsaren varefter den publika nyckeln signeras av Terena vilket bildar ett S/MIME-certifikat. När någon vill skicka ett krypterat mail till denna person krypterar han med den publika nyckeln i certifikatet och mottagaren kan läsa mailet med sin privata nyckel. För att få tag på mottagarens certifikat räcker det ofta med att mottagaren tidigare skickat ett signerat mail.

Om personen slarvar bort sina nycklar och certifikat kan han enkelt skaffa ett nytt Terena-certifikat och fortsätta signera sina mail som om inget hade hänt. Han kan däremot inte läsa de krypterade mail han fått tidigare såvida han inte sparat undan dom i klartext.

4.9.1 Slutsatser och diskussioner

Projektet har testat att kryptera mail med Outlook och Terena certifikat med blandat resultat. Idag känns det inte som helt stabilt och felsökningen vid problem är svår. Ett problem är att användarna använder olika mail klienter som hanterar krypteringen lite olika men även supportkostnaden ökar om man har flera olika klienter. Ska man använda denna teknik enbart i sin egen domän där man har samma klienter och versioner så är möjligheten mycket större att få en fungerande lösning. När projektet har pratat med andra experter på marknaden så rekommenderar dom att man krypterar den känsliga delen med en tredjeparts produkt och skickar med den krypterade filen som bilaga.

4.10 GENERELLA KRYPTERINGSLÖSNINGAR FÖR MOLN

4.10.1 Sammanfattning

Om man använder sig av en okrypterad molnlagringstjänst kan man installera ett krypteringsprogram som krypterar filerna innan de kopieras till molnet. Användaren får själv installera programmet och hålla reda på krypteringsnycklarna. CipherCloud är mer avancerat där det också finns möjlighet att använda sig av en extern nyckelserver om den stödjer KMIP.

Exempel på krypteringsprogram [10]:

Produkt	Länk	Noteringar
CipherCloud	http://www.ciphercloud.com/	Ca £60/år och användare. Kan använda en extern nyckelserver. Amerikanskt företag
Boxcryptor	https://www.boxcryptor.com/en	74€/år och användare. Tyskt företag.
Viivo	http://www.viivo.com	$120/år och användare. Amerikanskt företag (PKWare).
Cloudfogger	http://www.cloudfogger.com/en/	Gratis tills vidare. Tyskt företag.

4.10.2 Krypterade molntjänster

En del molntjänster krypterar innehållet på sina lagringsytor men eftersom vissa hanterar krypteringsnycklarna själva så kan de också komma åt innehållet. Ett bättre alternativ är att krypteringen sker lokalt på den egna datorn innan filerna skickas iväg till molnet. Detta kräver dock installation av extra programvara och hantering av krypteringsnycklar för användaren. Tappas nycklarna bort är filerna i molnet oläsbara.

Exempel på molnlagring med lokal kryptering [8][9].

Produkt	Länk	Noteringar
SpiderOak	https://spideroak.com/	$100/år för 100 GB. Amerikanskt företag.
Wuala	http://www.wuala.com/	€389 för 100 GB och 5 användare. Schweiziskt företag.
IDrive	http://www.idrive.com/	Backuplösning. $50/år för 100 GB. Amerikanskt företag.
Comodo Online	https://www.ccloud.com/	$96/år för 100 GB. Amerikanskt företag.
CloudSafe	https://secure.cloudsafe.com	$80/år för 50 GB. Tyskt företag.
TeamDrive	http://www.teamdrive.com	50€/år för 2 GB. För 50 GB extra kostar det 250€/år för obegränsat antal användare. Tyskt företag
SafeMonk	https://www.safemonk.com	$79/år och användare för upp till 100 användare. För Dropbox. Amerikanskt företag(SafeNet)

5 KRYPTERAD USB-DISK

5.1.1 Sammanfattning

Idag finns det flera olika tillverkare och varianter av krypterade USB-diskar och USB-minnen, dom är enkla att använda och har börjat komma ner i pris vilket gör dom prisvärda.

Den USB-disk som testats är en Aegis Padlock DT - USB 3.0 Desktop Drive på 4 TB [11].

Aegis Padlock DT

Den använder 256-bitars AES-kryptering och fungerar med de flesta operativsystem som Windows, Mac och Linux. Den kräver separat strömförsörjning. Priset är $389.00. Disken har ett administratörslösenord och upp till fem användarlösenord. Det finns dock ingen uppdelning av disken utan ett korrekt lösenord ger tillgång till hela disken. Lösenorden består av 6-16 siffror. Man kan sätta en timeout på 5, 10 eller 20 minuter så att disken kopplar bort sig själv automatiskt. Som default är ingen timeout aktiverad.

Efter sex misslyckade försök att låsa upp disken slutar disken att svara och man måste tillfälligt koppla bort den från datorn. Detta upprepas för fyra misslyckade upplåsningar. Har man inte lyckats låsa upp disken efter 10 försök måste man slå av enheten, hålla in knapp 5 medan man slår på den igen. Därefter ger man en särskild upplåsningskod (samma för alla diskar). Nu kan man göra ytterligare 10 upplåsningsförsök. Efter totalt 20 misslyckade försök måste disken fabriksåterställas, partitioneras och omformateras.

Det finns möjlighet att lägga in en kod som förstör krypteringsnyckeln (Self Destruct Password) som kan användas om någon försöker tvinga användaren att låsa upp den. Informationen på disken är därefter omöjlig att återställa.

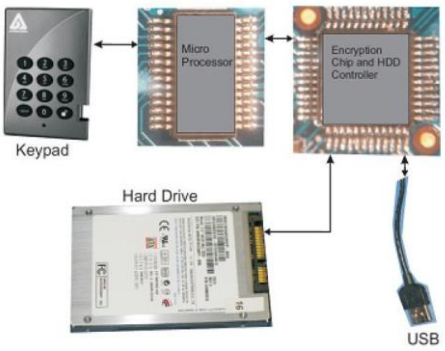
Om disken går sönder är innehållet förlorat så backup bör göras till en annan krypterad hårddisk.

Det finns även mindre USB-diskar, lämpliga att ha med på resor. Dessa har inbyggd USB-kabel och kräver inte extra strömförsörjning.

Aegis Padlock - USB 3.0Det finns även USB-minnen med tangentbord [11].

Aegis Secure Key

Att använda den krypterade hårddisken är väldigt enkelt bara man kommer ihåg lösenordet och hur man slår in det. Att ta en 120 GB kopia av hårddisken på en bärbar Windows-dator innebar inga problem. Disken gick sedan lika enkelt att montera i en Linuxdator där diskkopian kunde analyseras.



AES-nyckeln sitter i krypteringskretsen och är ej tillgänglig för användaren.

5.1.2 Slutsatser och diskussioner

Dom tester som utförts har visat att krypterade USB-diskar och USB-minnen som man köper färdiga från leverantörer är enkla att hantera och har en bra prisbild. Man bör välja FIPS 140 nivå 2 eller högre eftersom dom är mycket svårare att försöka bryta sig in i. Viktigt att tänka på att dom kan bli korrupta om som vilken hårddisk som helst och då gäller det att man har original data på någon annan plats.

6 NYCKELHANTERING

6.1 SYFTE

Syftet med denna punkt är att presentera en inledande orientering i världen av nyckelhantering, nyckelservrar och hårdvarubaserade säkerhetsmoduler.

6.2 PROBLEMSTÄLLNING

Vad innebär nyckelhantering och vad använder man nyckelhanteringsservrar till? Vad är en HSM (Hardware Security Module) och vad använder man dom till?

6.3 AVGRÄNSNING

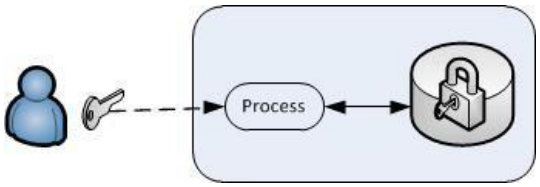
I de fall specifika produkter presenterats har det gjorts ganska översiktligt. Läsaren förutsätts ha en viss kunskap om symmetrisk resp. asymmetrisk kryptering och hur nycklarna används.

6.4 METOD

Einar Hillbom har studerat ett antal publikationer från NIST, letat efter diverse information på Internet samt läst om några tillverkares produkter.

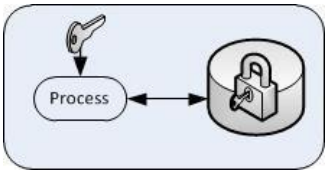
6.5 NYCKELHANTERING

Om man har information som är krypterad på en server, ex.vis SSH-nycklar, filer, databaser etc, finns det alltid en nyckel någonstans för att komma åt denna information. Hanteringen av dessa nycklar är ofta ett bekymmer. När det gäller de privata nycklarna för en servers SSL-kommunikation är dessa oftast okrypterade för att servern skall kunna starta automatiskt utan att någon manuellt måste knappa in ett lösenord. I andra fall finns nyckeln/lösenordet i klartext i skript och konfigurationsfiler.



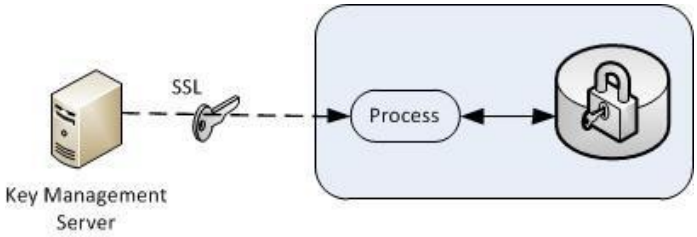
Manuell nyckelhantering

Använder man en manuell nyckelhantering måste nyckeln förvaras säkert, ex.vis på ett USB-minne som förvaras i ett kassaskåp. Varje gång servern eller processen startas om måste man mata in nyckeln. Om användaren tappar bort nyckeln är informationen oåtkomlig om ingen backup av nyckeln finns.



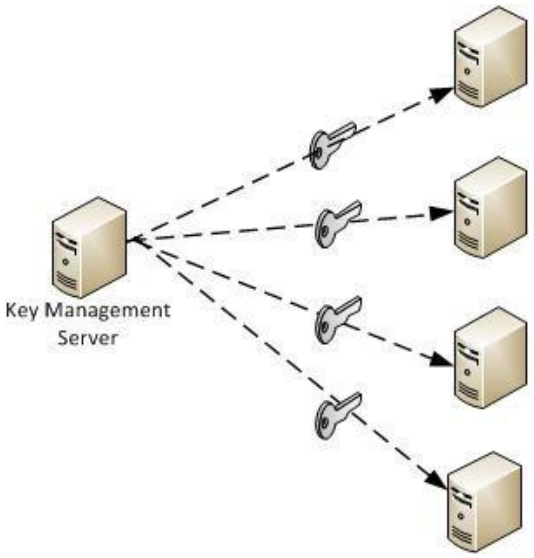
Nyckeln förvarad på servern

Vanligt är att nyckeln finns lagrad på servern så att processen och servern kan startas om utan manuellt ingripande. Om någon hackar sig in i datorn är risken stor att både databasen och nycklarna stjäls. Nyckeln kan också återfinnas i backuper som ofta hanteras av annan personal.



Nyckelhanteringsserver

Med en nyckelhanteringsserver (KMS) så lagrar man nycklarna i denna. KMS kan bl.a. generera, lagra, rotera och revokera nycklar. Oftast kan den hantera symmetriska nycklar (ex.vis AES), asymmetriska nycklar (ex.vis RSA), certifikat och andra säkerhetsobjekt. En del KMS kan även kontakta en CA för att få certifikat utfärdade efter att nycklarna skapats. En KMS kan ofta även hantera olika policys ex.vis lösenords komplexitet mm.



En nyckelserver kan hantera många servrars nycklar

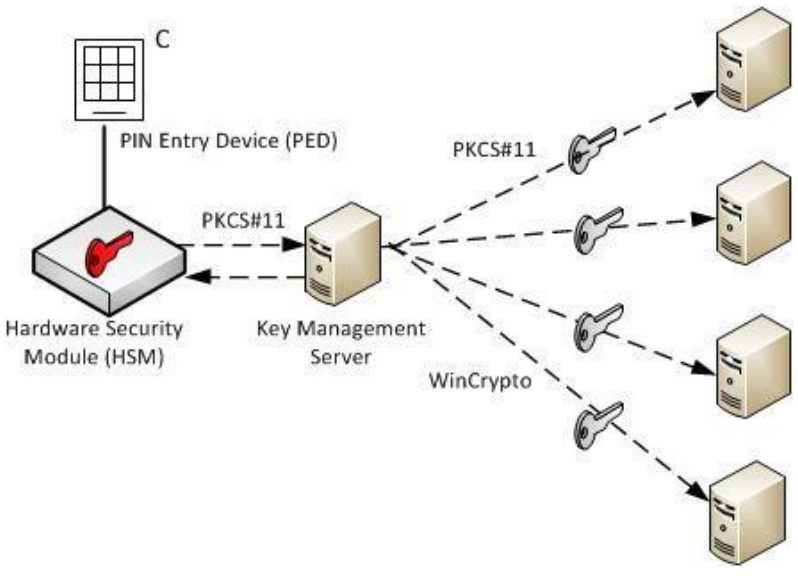
Eftersom KMS innehåller många nycklar som absolut inte får komma på avvägar måste databasen med dessa krypteras. Då får man återigen ett problem med hur huvudnyckeln till denna databas skall hanteras, man kan ju inte gärna lägga den på servern.

Det stora problemet med nyckelservrar är skyddet av nycklarna. Enligt NIST SP 800- 57 har man tre val för att skydda huvudnycklarna:

- Använd HSM
- Lås in nycklarna i ett kassaskåp
- Lagra huvudnyckeln på servern men kryptera den med en Key-Encryption-Key (KEK).

Dock måste KEK skyddas på något sätt.

Den fysiska lösningen med kassaskåp är ett billigare alternativ men kräver att nyckeln matas in varje gång applikationen startas. Någon måste finnas på plats och knappa in nyckeln varje gång servern startas om.



Användning av HSM

Genom att lagra huvudnycklarna i en HSM kan man skydda dessa från kopiering och stöld. Genom att låta HSM sköta de kryptografiska operationerna behöver inte KMS ha tillgång till själva huvudnyckeln. För att låsa upp HSM kan man ex.vis använda ett tangentbord anslutet till en separat port.

6.6 NYCKELSERVRAR

6.6.1 Sammanfattning

En nyckelserver, eller Key Management Server, har som uppgift att hålla reda på kryptografiska nycklar:

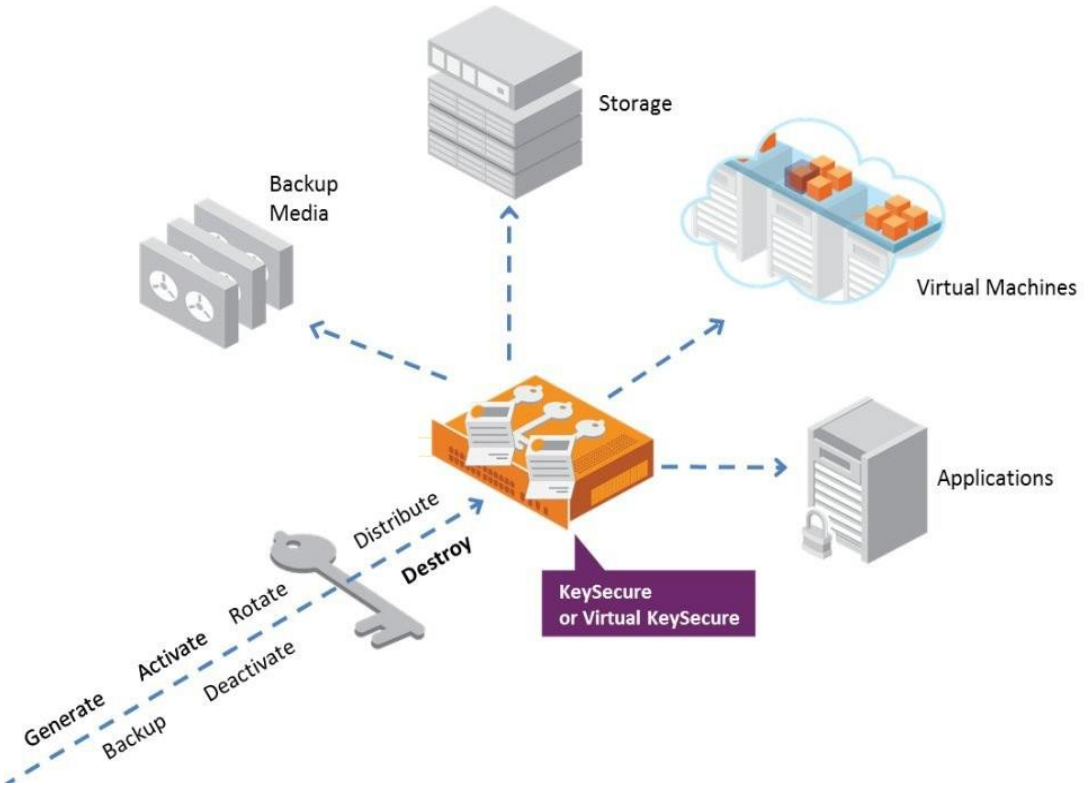
- Skapa nycklar
- Backup av nycklar
- Aktivering av nycklar
- Inaktivering av nycklar
- Rotering av nycklar
- Distribution av nycklar
- Radering av nycklar

Ofta kan de även hantera policys, rollbaserad auktorisation mm.

6.6.2 PGP Key Management Server

PGP Key Management Server har en licensavgift på ca $140/år och användare i små volymer. Det verkar dock finnas en särskild prissättning för skolor och myndigheter.

6.6.2.1 Safenet KeySecure



SafeNet KeySecure Model Comparison

Feature	KeySecure k460	KeySecure k150	KeySecure k150v
Max keys	1,000,000	25,000	25,000
Max concurrent clients per cluster	1,000	100	100
Redundant hot-swap HDs & Power	Yes	No	N/A
FIPS 140-2 Level 3	Yes (Luna HSM)	No	N/A
Luna HSM Management	SafeNet Luna SA & PCI		
SafeNet ProtectV and ProtectApp	Yes	Yes	Yes
SafeNet StorageSecure	Yes	No	No
Brocade SAN Switch (BES)	Yes	No	No
SafeNet Third-party Integration Support	HP ESL G3, Quantum Scalar Series(i6000, i500 & i40/80), NetApp NSE, Hitachi VSP, Amazon Web Services S3, DropBox, Google Cloud Storage, Google Drive		
Partner Integration Support (requires ProtectApp)	CipherCloud, Perscesys, PKZip, Sepaton VTL, ServiceMesh , Viasat		

6.6.2.2 Oracle Key Manager 3

Avsedd för Java applikationer, Oracles databaser och bandbackup. Kan förses med Sun Crypto Accelerator PCIe för att uppnå FIPS 140-2 Level 3.

Oracle Key Manager 3

6.6.2.3 Thales keyAuthority

Stödjer KMIP.

Skyddsklass: FIPS 140-2 Level 3

Cryptographic algorithms supported:

- AES (128, 192, 256)
- XTS AES (128, 256)
- EME2 AES (128, 256)
- CCM 128 AES 256
- GCM 128 AES 256
- CBC AES 256 HMAC SHA (1, 256, 512)
- XTS AES 256 HMAC SHA 512
- XCB AES (128, 256)
- TDES
- RSA 2048 (Key wrapping, exchange, agreement and log signing)

- AES 256 (key wrapping of material stored on disk and authenticated using HMAC SHA 512 for Group Keys)

Exempel på applikationer som stöds:

- Brocade Encryption Switch and FS8-18 Encryption Blades for DCX Chassis
- IBM encryption-ready tape (TS-Series) and disk (DS-Series) storage line products

Thales keyAuthority

6.6.3 Hardware Security Modules (HSM)

När man lagrar kryptografiska nycklar i en nyckelservers databas måste dessa krypteras för att skyddas. De nycklar som används för denna kryptering får ej lagras på servern utan läggs i en separat hårdvara, HSM. Om någon lyckas hacka sig in i nyckelservern och ladda ner databasen är den oanvändbar utan fysisk tillgång till HSM.

De flesta HSM stödjer generering av och signering med RSA- och DSA-nycklar. För att kommunicera med HSM används oftast:

- PKCS#11 - en öppen RSA-standard.
- OpenSSL engine - en plugin för OpenSSL
- Microsoft CryptoAPI - Används enbart i Windows-system. Det brukar finnas en separat port för administrationen av en HSM.

Det fysiska skyddet är ofta specificerat som FIPS 140-2 Level 1...4. För att ex.vis uppfylla FIPS 140-2 Level 2 är modulen är förseglad så att det skall märkas om någon försökt öppna den.

Det finns inget standardiserat sätt att göra backup av en HSM. Många tillverkare har egna metoder för detta.

De mer avancerade HSM kan ofta förses med ett tangentbord för upplåsning. Detta brukar kallas för PED-Auth (PIN Entry Device) till skillnad från PW-Auth (Password).

Hardware Security Modules finns i flera olika former:

- Software tokens
    - Lågt pris
    - Kan lagra stora mängder nycklar mm
    - Antal kryptografiska operationer per sekund begränsas av datorns hårdvara
    - Lägre säkerhet då nycklarna inte skyddas av hårdvara
    - Kan användas som HSM för teständamål
    - SoftHSM är ett exempel som tillhandahålls av OpenDNSSEC.

- Smarta kort och USB tokens
    - Lågt pris (< 5000 kr/enhet)
    - Portabla
    - Begränsad lagringskapacitet för nycklar (< 20 RSA nyckelpar)
    - Begränsad eller ingen support för symmetriska kryptografiska algoritmer
    - Begränsat antal kryptografiska operationer per sekund Exempel)
    - Exempel
        - YubiHSM från Yubico. Kostar 3499 kr plus moms på http://www.dustin.se. Avsedd för validering av Yubikeys men kan i viss utsträckning användas för autentisering ex.vis i Linux-system.

YubiHSM

        - CryptoStick (https://www.crypto-stick.com). Under utveckling. Fungerar med Outlook, TrueCrypt, Thunderbird, Evolution, GnuPG m.fl. Mer för personligt bruk.

CryptoStick

Thales nShield Edge

- Kryptografiska acceleratorer
    - Finns som PCI-kort och separata enheter
    - Högt pris (25.000 - 300.000 kr/enhet)
    - Ej portabla
    - Optimerade för kryptografiska operationer och ej för nyckellagring
    - Hög kapacitet för symmetriska och asymmetriska kryptografiska operationer.
- Traditionella hårdvarubaserade moduler
    - Finns som PCI-kort och separata enheter
    - Högt pris (25.000 - 300.000 kr/enhet)
    - Ej portabla
    - Stor lagringskapacitet för kryptografiska nycklar (tusentals RSA-nycklar eller mer)
    - Kryptografisk accelerator Exempel)

SafeNet Luna PCI-E

- SafeNet [3] Luna PCI-E
  - PCI-kort som stoppas in i datorn
  - Kommunicerar med PKCS#11, Java (JCA/JCE), Microsoft CAPI och CNG, OpenSSL.
  - Pris ca $5000-$6000.

SafeNet Luna SA

- SafeNet [3] Luna SA
  - En separat enhet
  - Kommunicerar med PKCS#11, Java (JCA/JCE), Microsoft CAPI och CNG, OpenSSL
  - Pris ca $20.000.

Thales nShield Connect [5]

6.7 SLUTSATSER OCH DISKUSSIONER

Nyckelhanteringssystem och säkerhetsmoduler utgör en komplex värld. Ofta används dom för speciella ändamål som bandbackup, certifikathantering etc. där man har stora krav på säkerhet. Kunderna är ofta banker, kreditkortsföretag, myndigheter etc.

Eftersom säkerhetskraven är stora och produkterna måste uppfylla en mängd standarder och certifieringar blir dom dyra.

Generella system är svåra att hitta, det verkar som om man normalt köper hela lösningar från ett företag. Nyligen har dock ett flertal företag enats om en standard för kommunikationen mellan nyckelservrar och klienter - Key Management Interoperability Protocol (KMIP) som sköts av OASIS.

7 SAMMANFATTNING ÖVER DOM TESTADE PRODUKTERNA

Det har blivit allt viktigare att skydda informationen man har på sin dator eller i en molntjänst. Datorer, USB-diskar och USB-minnen kan stjälas och NSA eller molnadministratörer kan komma åt filerna i molnet.

I den här undersökningen har några enklare sätt att kryptera information testats: BitLocker, Ecryptfs, TrueCrypt, AXcrypt, Boxcryptor, Kurir och krypterad USB-disk. Dessutom har exempel på ett antal generella krypteringsprogram för molnlagring samt krypterade molntjänster listats.

BitLocker: Är målet är att höja säkerheten på den enskilda klienten och skydda data mot stöld eller förlust så är BitLocker för Windows system ett bra alternativ. BitLocker ger en bra central kontroll med övervakning. BitLocker ger en bra krypteringsgrund om man vill ha en sådan för sin Windows miljö.

Ecryptfs: Det är relativt enkelt att skapa en krypterad katalog med eCryptfs i Linux men man är begränsad till Linux. Den krypterade filen går dock att flytta mellan olika Linux-servrar.

Yubikey NEO levereras med en OpenPGP Applet men man måste först aktivera YubiKey NEO's Smartcard interface (CCID) med programmet ykpersonalize. Därefter kan man generera ett nyckelpar med gpg och använda Yubikey:n för att kryptera med gpg. Att tänka på är att man inte kan backa upp den privata nyckeln. Om man tappar sin Yubikey eller av misstag råkar generera om nyckelparet så kan man inte längre komma åt sina krypterade filer. Av den anledningen måste man alltid ha en klartext-backup.

TrueCrypt: Tyvärr så stoppades utvecklingen av denna produkt under året med anvisningar att man inte skulle använda applikationen mer, anledning varför saknas. TrueCrypt passar bäst för kryptering på den egna datorn eller ansluten USB- disk/USB-minne. Det fungerar också för fildelningstjänster baserade på NFS, CIFS, SAMBA eller liknande. TrueCrypt är mindre lämpligt för molntjänster som bygger på att en agent synkroniserar innehållet på datorn med innehållet i molnet eftersom hela containerfilen för det mesta måste överföras även om man bara ändrat i en fil.

AxCrypt: Får anses som en krypterings applikation som är enkel att använda men med hänsyn att den endast använder sig av 128-bitars nyckel när vissa använder 256-bitar. Produkten är Free vilket innebär att man inte med säkerhet veta vad mer som följer med i applikationen men så kan det vara även med kommersiella produkter. Framtida utveckling av produkten kan också ifrågasättas.

Boxcryptor: Tillhör en familj av krypteringsprogram för molnlagring. Här sker krypteringen av enskilda filer i samband med att de synkroniseras med molnet. Fungerar med många olika molntjänster och kan även användas på mobila enheter. Dock krävs att man lagrar sina nycklar i ett konto hos Boxcryptor för att man skall kunna dela filerna med andra och för att kunna använda mobila enheter. I annat fall räcker det med att använda en lösenordskyddad nyckelfil som sparas på datorn.

Kurir: Upplevs som en relativt enkel applikation för att kryptera data och stödet för svenska som språk underlättar också för ovana användare. Kurir applikationen har ett mycket bra och logiskt gränssnitt som gör det enkelt att använda. Kurir ger också möjligheten att ha flera skyddade keystores som underlättar om man jobbar i olika uppdrag dvs. en keystore för varje uppdrag. Eftersom produkten kommer att bli klassad som KSU så betyder det att vi kan till stort lita på produkten att den är ren från oönskade bakdörrar mm. Kan vi inte lita på vår egen stat som i många fall är vår arbetsgivare så kan vi nog inte lita på någon annan produkt heller.

E-mail kryptering: Känns inte som helt stabilt och felsökningen vid problem är mycket svår. I dom senaste versionerna i Outlook så ska vissa funktioner ske med automatik men under testerna har det visat sig att det inte alltid funkar på klienterna och eftersom det ska ske med automatik så är informationen mycket bristfällig vilket försvårar felsökningen markant. I samtal med säkerhetsleverantörer så använder dom själva inte funktionen utan kryptera data och skickar med den som bifogad fil istället. Intrycket är att vi får vänta tills funktionen förbättrats innan man gör någon större implementation.

Krypterade USB enheter används när man ska skydda stora mängder data som bara används lokalt. Då är en krypterad USB- disk ett enkelt och säkert alternativ.

Nyckelhanteringssystem och säkerhetsmoduler utgör en komplex värld. Ofta används dom för speciella ändamål som bandbackup, certifikathantering etc. där man har stora krav på säkerhet. Kunderna är ofta banker, kreditkortsföretag, myndigheter etc.

Eftersom säkerhetskraven är stora och produkterna måste uppfylla en mängd standarder och certifieringar blir dom dyra.

Generella system är svåra att hitta, det verkar som om man normalt köper hela lösningar från ett företag. Nyligen har dock ett flertal företag enats om en standard för kommunikationen mellan nyckelservrar och klienter - Key Management Interoperability Protocol (KMIP) som sköts av OASIS [4]. Om man väljer att använda manuell nyckelhantering måste backupen av nyckeln förvaras säkert, ex.vis på ett USB-minne som förvaras i ett kassaskåp och gärna på två olika minnen pga. kan bli fel på USB-minnen. Det viktigaste att tänka på är att spara en kopia/backup av master nyckeln så man kan återskapa det krypterade data om användaren förlorar sin nyckel eller lösenord.

Krypterade USB enheter används när man ska skydda stora mängder data som bara används lokalt. Då är en krypterad USB- disk ett enkelt och säkert alternativ.

8 SLUTORD OCH REKOMMENDATIONER

Projektet kan sammanfatta att kryptering i en större implementation när det gäller Windows miljö så rekommenderar vi BitLocker eftersom den är enkel att införa och underhålla. En viktig sak att tänka på i valet av BitLocker är att det finns ”avancerade” metoder att dekryptera Bitlocker men om skyddet är till för skydda data från att bara någon som kommit över en disk ska enkelt kunna läsa den så fungerar Bitlocker bra. Vill man skydda mycket skyddsvärd information behövs det starkare skydd än Bitlocker.

När det gäller högre krav på kryptering så är det Kurir som vi rekommenderar eftersom den är snart är KSU godkänd, har man bråttom så går det att köra den tidigare versionen Filkrypto som också är KSU godkänd. Kurir kräver kort inlärnings period för användarna.

Om man väljer manuell nyckelhantering måste backupen av nyckeln förvaras säkert, ex.vis på ett USB-minne som förvaras i ett kassaskåp.

Under projektets gång hamnade vi ofta i diskussion om krypteringspolicy och Nyckelhantering. Här måste varje lärosäte själv ta fram en krypterings policy som är anpassat för dom själva. När vi kommer till nyckelhantering så är det även här viktigt att varje lärosäte själv beslutar hur man ska hantera detta. Frågor som förknippades med dessa områden var Skydd av nycklar, bortglömt lösenord, vad man får kryptera och vad man inte får kryptera mm.