

LÄR DIG KRYPTERING.....	2
KRYPTERING OCH NYCKLAR – VAD ÄR DET?.....	3
KRYPTERA MEDDELANDEN.....	3
PC: HÄMTA HEM OCH INSTALLERA GNUPG.....	4
SKAPA NYCKLAR.....	6
TESTA NYCKLARNAS.....	9
TA EMOT EN KRYPTERAD FIL.....	13
KRYPTERA ETT MEDDELANDE TILL NÅGON ANNAN.....	14
MAC: HÄMTA HEM OCH INSTALLERA GNUPG.....	15
SKAPA NYCKLAR.....	18
TESTA NYCKLARNAS.....	21
TA EMOT EN KRYPTERAD FIL.....	22
KRYPTERA ETT MEDDELANDE TILL NÅGON ANNAN.....	23
DAGS FÖR THUNDERBIRD.....	24
STÄLL IN POP3.....	26
MEN NÄR SKULLE VI BÖRJA KRYPTERA...?.....	26
STÄNG AV HTML.....	28
SKRIV ETT MEDDELANDE.....	29
TA EMOT ETT KRYPTERAT MEDDELANDE.....	30
SIGNERA ETT MEDDELANDE.....	30
ATT KONTROLLERA ETT SIGNERAT MEDDELANDE.....	30
STÄNG AV FÖRHANDSGRANSKNING.....	32
SIGNERADE DOKUMENT.....	32
KRYPTERA DATORN.....	32
TRUECRYPT.....	33
BITLOCKER.....	37
FILEVAULT.....	38

Digitalt källskydd – en introduktion

Det här dokumentet om kryptering är extramaterial som hör ihop med Internetguiden "Digitalt källskydd – en introduktion" av Sus Anderson, Fredrik Laurin och Petra Jankov. Hela boken, och mer extramaterial, finns att ladda ned kostnadsfritt här: www.iis.se/guider



Lär dig kryptering

I den här guiden går vi igenom hur du krypterar enstaka dokument, hur du skickar krypterade meddelanden och hur du krypterar hela din hårddisk.

Först kommer vi att gå igenom litet allmänt om kryptering. Om du vill gå direkt till installationerna, se nedan under "Kryptera meddelanden".

För bara några år sedan var kryptering fortfarande ganska komplicerat, och det krävdes ett ganska stort mått av datorvana för att överhuvudtaget ge sig in på det. Idag följer möjligheten att kryptera med när du köper en ny Mac, och det finns med i de dyrare varianterna av Microsofts operativsystem. Många av de usb-stickor som finns i handeln har ett krypteringsprogram inbyggt, så det enda du behöver göra själv är att välja ett tillräckligt komplicerat lösenord, och sedan lägga de dokument du vill skydda i rätt mapp. För den som är nybörjare är nog det lättaste att börja med att just använda krypterade usb-minnen för den information som är känslig.

Även om det finns krypteringsmetoder som är väldigt säkra i sig är det viktigt att komma ihåg att kryptering inte löser allt. En stark kryptering är som att ha ett superlås på dörren. Men det hjälper inte om du lämnar fönstren öppna och ställer fram en stege – du löper ändå risk för inbrott. Om du inte tänkt igenom hur du handskas med dina dokument – såväl innan du krypterar dem som när du sedan öppnat dem igen – kan krypteringen i princip bli meningslös. Filer kan ha sparats i temporära mappar, och de kan gå att återskapa även om de blivit raderade.

Om du skickar ett krypterat e-postmeddelande kan visserligen inte vem som helst läsa vad som stod i det. Men i vissa fall kan just det faktum att någon skickar krypterad information vara tillräcklig för att skapa misstankar. En person som skickar krypterade mejl från sin arbetsplats till en redaktion kommer sannolikt bli misstänkt för att läcka hemligheter, även om ingen annan än journalisten kan läsa vad som faktiskt står i e-brevet.

Det är därför viktigt att du tänker igenom hur du jobbar, och lär dig hur olika program och din dator fungerar innan du ger dig på att kryptera riktigt känsliga saker. Alla detaljer kommer vi inte att gå igenom här. Innan du känner att du har någorlunda kläm på det kan det vara bättre att använda gamla, analoga metoder: skicka pappersbrev, eller träffas och överlämna informationen på något ställe där ingen kan tjuvlyssna.

Innan du börjar kryptera behöver du också ha bra rutiner för att skapa säkerhetskopior – som naturligtvis också bör vara krypterade, eller förvaras inlåsta, exempelvis i ett kassaskåp. Undvik säkerhetskopiering till molntjänster. Ifall du

fulldiskkrypterar din dator och inte har en återställningsnyckel är du körd; det finns ingen ångra-knapp.

Kryptering och nycklar – vad är det?

Kryptering är en metod för att förvandla information till oläslig rappakalja. Genom komplicerade matematiska algoritmer går det att skapa krypterade meddelanden som är extremt svåra att knäcka.

När du krypterar din hårddisk eller ett använder ett usb-minne med förinstallerade krypteringsprogram behöver du egentligen inte fundera så mycket på hur det hela fungerar; allt är färdigpaketerat från början, och det svåraste du behöver göra är att hitta på ett lösenord som ingen annan kan lista ut. Normalt brukar man rekommendera lösenord på tio – 14 tecken. Men handlar det om att säkra allt du gör, genom att du fulldiskkrypterar din hårddisk, eller att spara ditt livs scoop, bör lösenordet ha minst 23 tecken och gärna 30. Programmet TrueCrypt tillåter lösenord på upp till 64 tecken. Läs om att konstruera lösenord i guiden Digitalt källskydd.

När du ska utbyta krypterad information med andra ska du använda en metod som har två nycklar. Den ena låser och den andra öppnar – bara låsnyckeln kan kryptera ett meddelande, men framför allt: bara upplåsningsnyckeln kan dekryptera det.

Det fiffiga med den här metoden är att du kan lämna ut låsnyckeln till hela världen. Vem som helst kan då skicka ett hemligt meddelande till dig. Även om någon annan får tag i meddelandet kan den personen inte läsa det, eftersom den enda kända nyckeln, låsnyckeln, aldrig kan öppna något. Enda sättet att komma åt meddelandet är genom att använda den andra nyckeln. Om du skyddar den med ett starkt lösenord är krypteringen mycket säker.

Den här metoden kallas för asymmetrisk kryptering, eftersom nycklarna är olika. Den nyckel som krypterar kallas för publik nyckel, eftersom den kan göras allmänt tillgänglig. Du kan ha den som slutkläm i dina e-postmeddelanden, eller lägga ut den på någon nyckelserver på Internet – då kan andra lätt hitta hur de ska skicka krypterad e-post till dig. Men den publika nyckeln kan aldrig låsa upp något. Inte ens den som skickar meddelandet kan läsa det när det blivit krypterat med din publika nyckel. Den nyckel som du sedan låser upp med kallas för din privata eller hemliga nyckel.

Kryptera meddelanden

För att kryptera e-post behövs ett par olika program. Dels ett program som sköter själva krypteringen, dels ett e-postprogram som gör krypteringen enkel.

I den här guiden installeras tre komponenter:

- programpaketet GnuPG. Det kan du också använda för att kryptera enstaka dokument.
- e-postprogrammet Thunderbird
- insticksprogrammet Enigmail, som kopplar ihop Thunderbird med GnuPG.

Det finns flera olika standardmetoder för kryptering. Vi kommer att använda OpenPGP. Det bygger på programmet PGP, Pretty Good Privacy, som skapades i början av 1990-talet. I OpenPGP används öppen källkod. Tekniken är alltså transparent och kan granskas.

En annan standard heter S/MIME, och den finns inbyggd i flera stora e-post-system.

En skillnad mellan de båda metoderna är hur man verifierar nycklar. OpenPGP bygger på att andra användare går i god för varandra. Med S/MIME är det en ackrediterad organisation som säkerställer certifikat.

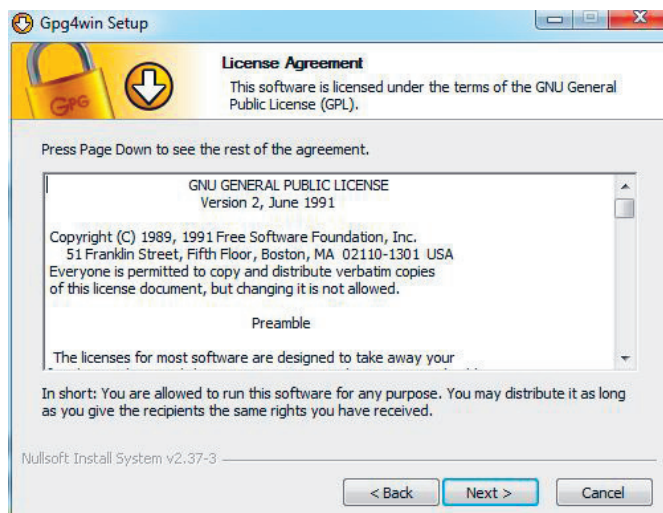
PC: hämta hem och installera GnuPG

1. Gör en säkerhetskopia på din dator. Ifall något går snett kan du gå tillbaka och återställa din dator.
2. Ladda hem programmet från <http://www.gpg4win.org>. Ladda helst hem det själv. Kör bara programmet om du är säker på att du fått det från en säker källa. Om du får det på en cd, usb-sticka eller laddar ned det någon annanstans ifrån kan det vara en manipulerad version.
3. Stäng alla andra program.
4. Dubbelklicka på filnamnet. I den här guiden har vi laddat ned version 2.1.0.

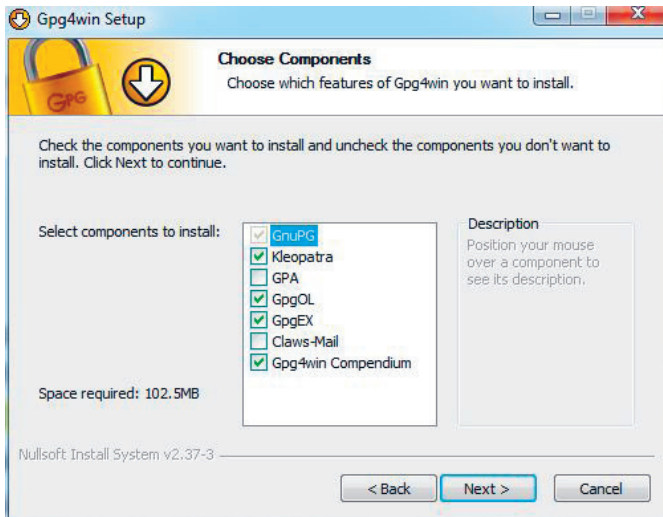


Namn	Senast ändrad	Typ
Gammalt	2012-10-11 14:14	Filmapp
gpg4win-2.1.0	2012-09-21 11:27	Program

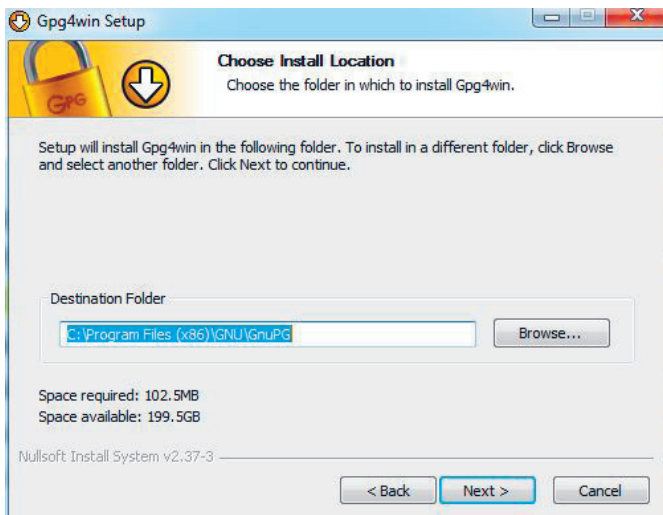
5. När du får upp välkomstrutan klickar du på "Next".
6. Nästa sida innehåller licensavtalet. Det rör framför allt den som vill utveckla programmet eller sprida det vidare. Men även om det mesta inte berör dig: gör det till en vana att alltid skumma igenom licensavtal. Om du accepterar villkoren klickar du på "Next".



7. I nästa steg kan du välja och välja bort delar av installationen. Som normalanvändare kan du låta förinställningarna vara. Klicka på "Next".



8. I nästa steg väljer du var programmet ska installeras. Förslaget är normalt bra. Klicka på "Next".



9. I nästa steg kan du välja om du vill ha genvägar till programmet från skrivbordet eller startmenyn. Det kan vara praktiskt att ha genvägarna i startmenyn. Klicka på "Next".
10. Du kan välja vad mappen för programmet ska heta. Om du är nöjd med rubrikförslaget väljer du "Install".
11. Nu installeras programmet. Det tar någon minut.
12. Beroende på vad du har för inställningar i din brandvägg och ditt antivirusprogram kan du få upp en varning om programmet dirmngr.exe. Programmet är till för att hantera dina certifikat och nycklar. Acceptera detta. Klicka på "Tillåt" eller motsvarande i ditt program.
13. När installationen är klar klickar du på "Next".
14. Nu får du upp en ruta om att definiera S/MIME-certifikat. Hoppa över den så länge. Klicka i rutan "Root certificate defined of skip configuration". Om du senare vill använda S/MIME-certifikat kan du göra de inställningarna då. Instruktioner hittar du via startmenyn i Gpgwin4 och välj "Documentation". Klicka på "Next" och i nästa ruta "Finish".
15. Ibland behöver datorn startas om för att installationen ska bli helt genomförd.

Skapa nycklar

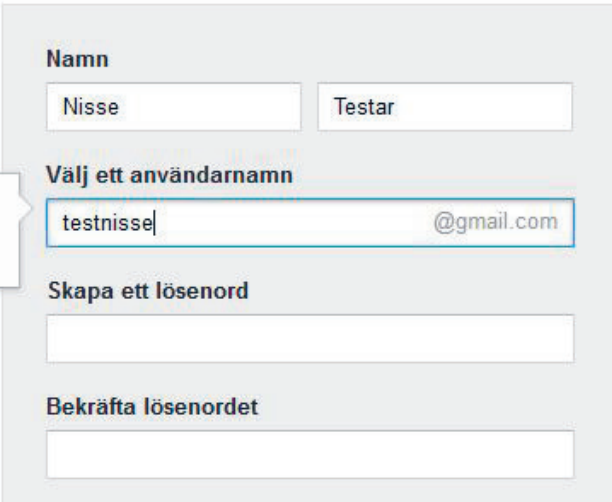
Nu behöver du dina egna nycklar, för att du ska kunna kryptera material, och för att andra ska kunna skicka krypterade meddelanden till dig.

Öppna programmet Kleopatra.

Beroende på hur din brandvägg och ditt antivirusprogram fungerar kan du få varningar för att ett antal program körs igång. Acceptera dem.

Programmet hanterar dina nycklar. Till att börja med är listan tom, eftersom du ännu inte har några.

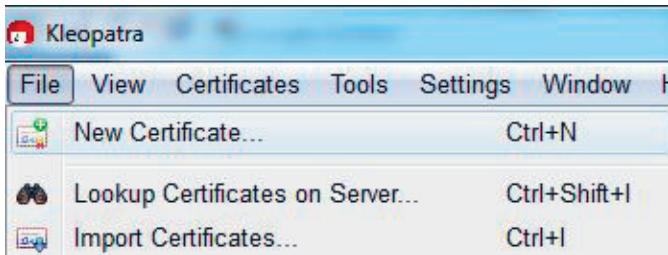
1. Skapa en test-epostadress. Även om du bara gör en testnyckel första gången måste du göra det med en fungerande e-postadress. Du kan exempelvis skapa en testadress på gmail som du bara använder till detta.



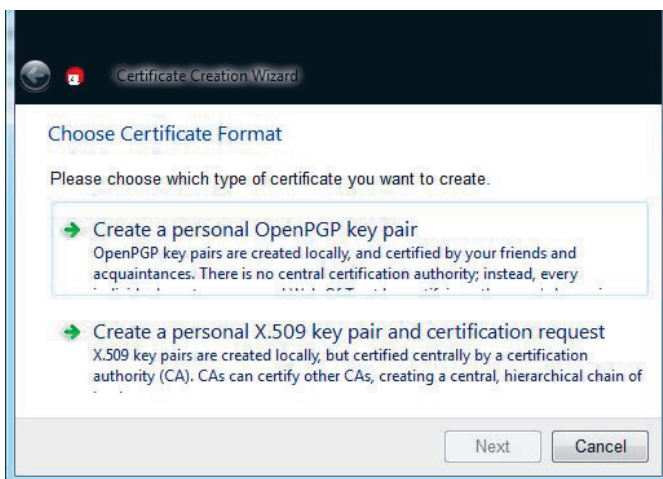
The image shows a dialog box for creating a key in Kleopatra. It has the following sections:

- Namn**: Two text boxes containing "Nisse" and "Testar".
- Välj ett användarnamn**: A text box containing "testnisse" and a dropdown menu showing "@gmail.com".
- Skapa ett lösenord**: A text box for entering a password.
- Bekräfta lösenordet**: A text box for confirming the password.

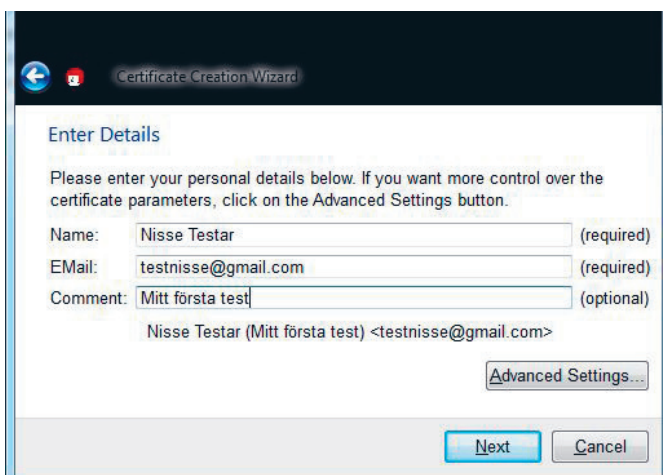
2. När du har en e-postadress: gå till Kleopatra, menyn "File" och välj "New Certificate".



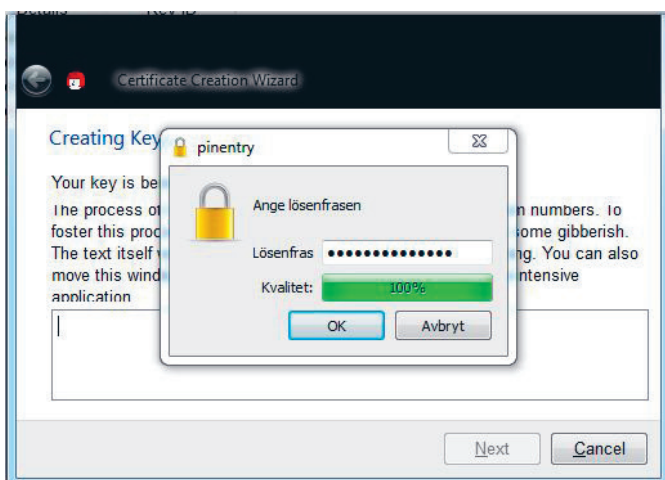
3. Välj "Create personal OpenPGP key pair".



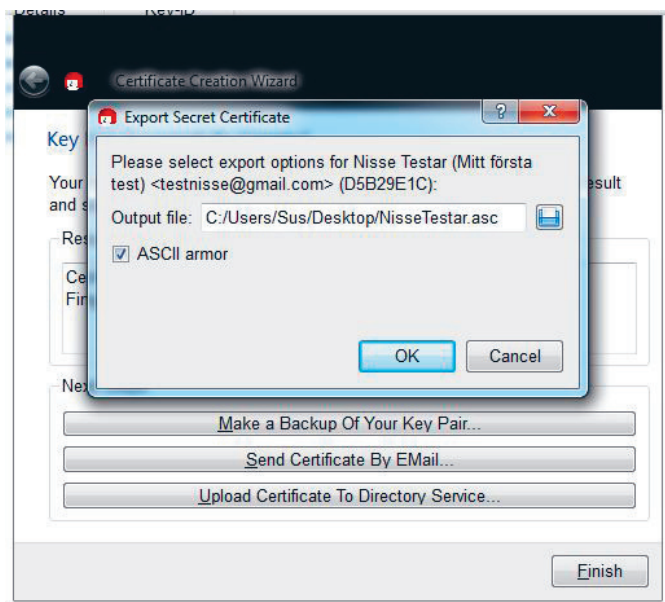
4. Ange namn och e-postadress som nyckeln ska vara kopplad till. Klicka på "Next".



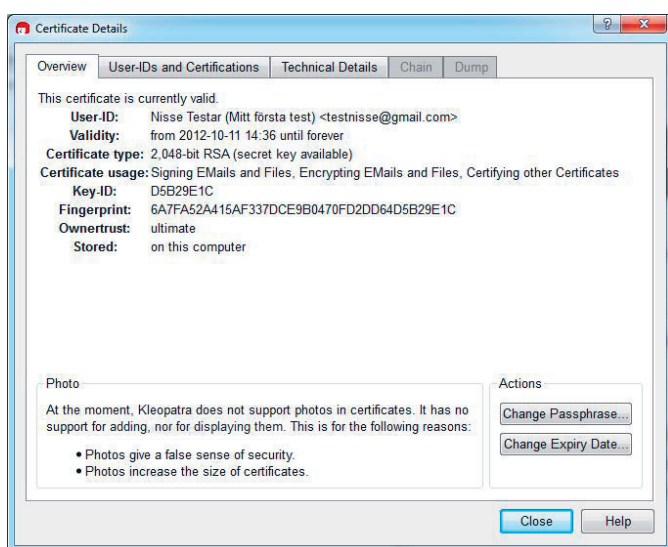
5. Kontrollera att uppgifterna stämmer. Om de är det väljer du "Create Key".
6. Nu ska du skapa ett lösenord till din privata, hemliga nyckel. Det här lösenordet måste vara mycket starkt. Ju längre lösenord, desto mindre risk att någon kan knäcka det, och komma åt din privata nyckel. Vill du ha hög säkerhet bör du sikta på 16 – 19 tecken. Du bör använda siffror, stora och små bokstäver och specialtecken som !#%&. Om du inte gör det kommer du att få en varning.



7. Att skapa nycklarna kommer att ta några minuter. Sedan får du upp en ruta med ett 40 tecken långt "fingeravtryck", som är ditt unika id-nummmmer. Ofta används bara de åtta sista tecknen, som är tillräckliga som identifiering. Du behöver inte komma ihåg ditt fingeravtryck. Det sparas i programmet Kleopatra.
8. Innan du går vidare ska du spara en säkerhetskopia av ditt nyckelpar.
Välj "Make a Backup Copy Of Your Key Pair". Kryssa i rutan för "ASCII armor" om du huvudsakligen ska använda krypteringen för e-post. Backupfilen får då ändelsen .asc. Välj var filen ska sparas.



- Spara till en cd eller usb-sticka, och förvara den sedan på ett säkert ställe – helst ett kassaskåp eller i ett bankfack. Undvik att först spara den på datorn och sedan flytta den.
9. Radera säkerhetskopian helt från datorn, ifall du sparat den där. Observera att det INTE räcker att slänga filen i papperskorgen. För att den verkligen ska vara borta måste papperskorgen vara tömd och raderad med ett överskrivningsprogram. Läs mer i XL-guiden om radering >>.
 10. Du kan också skapa en kopia av din privata nyckel genom att gå in i menyn "File" och sedan "Export Secret Keys". Observera att den här exporten ALDRIG får användas när du ska skicka din nyckel till någon annan. I så fall kan andra också komma åt allt ditt krypterade material.
 11. Avsluta nyckelguiden. I huvudmenyn i Kleopatra ska nu ett nytt certifikat finnas i listan "My Certificates". Om du dubbelklickar på det får du veta mer. Du hittar bland annat hela ditt fingeravtryck och vad certifikatet kan användas till.



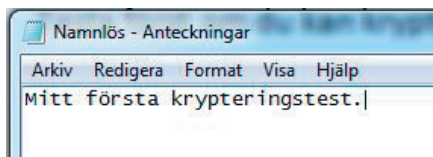
Testa nycklarna

Nu kan du börja testa dina nycklar och sedan att skicka krypterade meddelanden. Tänk på att det är viktigt att du känner dig trygg med hur dina program fungerar innan du börjar använda dem till att överföra känsliga meddelanden.

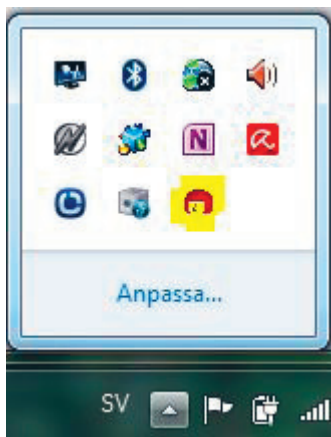
Se till att du har Kleopatra öppet.

Testa först om du kan kryptera en textsnuitt.

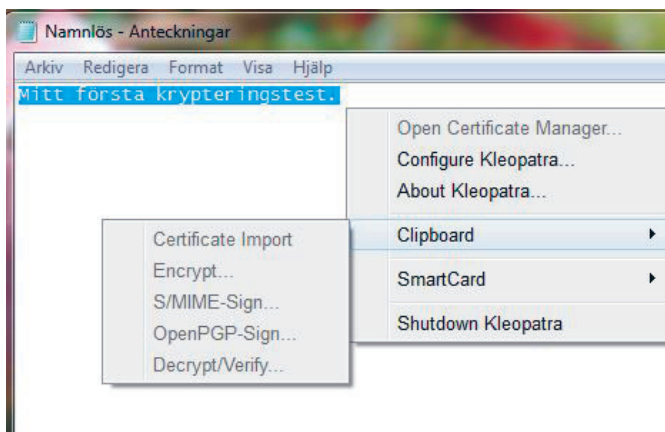
1. Öppna programmet Anteckningar, Word Pad eller motsvarande, där du kan arbeta med ren, oformaterad text.
2. Skriv en kort text.



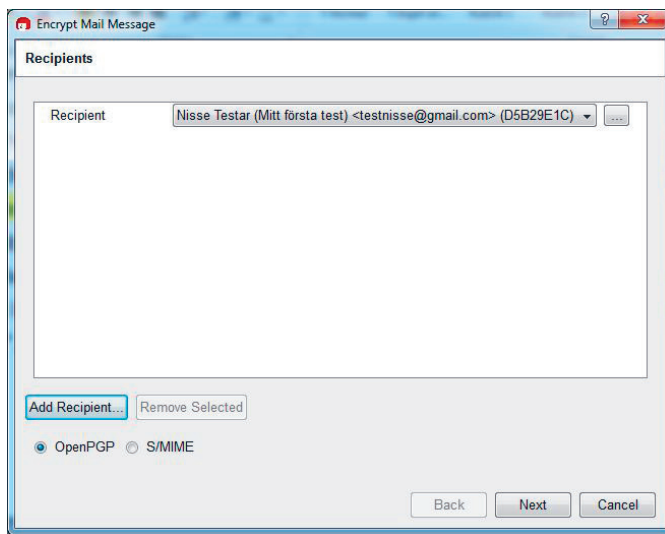
3. Markera hela texten och kopiera den. Nu finns texten i urklippshanteraren i din dator.
4. Högerklicka på Kleopatra-ikonen i menyn längst ned till höger på skärmen.



5. Välj "Clipboard" och sedan "Encrypt".



6. I rutan "Recipients" låter du "OpenPGP" vara markerat och klickar på "Add Recipient...". Du får nu en lista över alla dina sparade mottagare. Välj det certifikat du nyss skapade och klicka på "Next".



7. Nu har texten i urklippet krypterats. Öppna ett nytt dokument i textredigera-
ren. Klistra in texten.

Den kommer nu att se ut ungefär så här:

```
-----BEGIN PGP MESSAGE-----  
Version: GnuPG v2.0.17 (MingW32)  
  
hQEMAwKMSsupndKfAQf/TaoXJHg91snSq50/XLcCmYGonMfSA0EG-  
TrEUfvGbdH08  
  
jz3wNMkt4oTHxa9ikQ7P3MnUvQCit6xhPUaR1R9ytYHgq+15/4yFEvTf  
oGIicF1k  
  
VZh2qKVrEInw7nF34XNdQzEHbNIh4/lDEa/cVrp/COkTaxi-  
DIcFmd33XKxylBADy  
  
x/NM/D4u  
  
=fmk2  
  
-----END PGP MESSAGE-----
```

Du kan nu spara den här filen, exempelvis på ett usb-minne. Du kan också klistra in den i ett e-postmeddelande. Din hemliga text kan inte läsas utan tillgång till din privata nyckel.

Ett annat sätt att kryptera din text är att först spara den okrypterade texten i ett dokument, exempelvis med namnet "texten.txt". I Kleopatra går du in i menyn "File" och sedan "Sign/Encrypt Files". Dubbelklicka på "texten.txt", och markera att det är du själv som är mottagare.

När du sedan vill titta på din text gör du på samma sätt fast tvärtom:

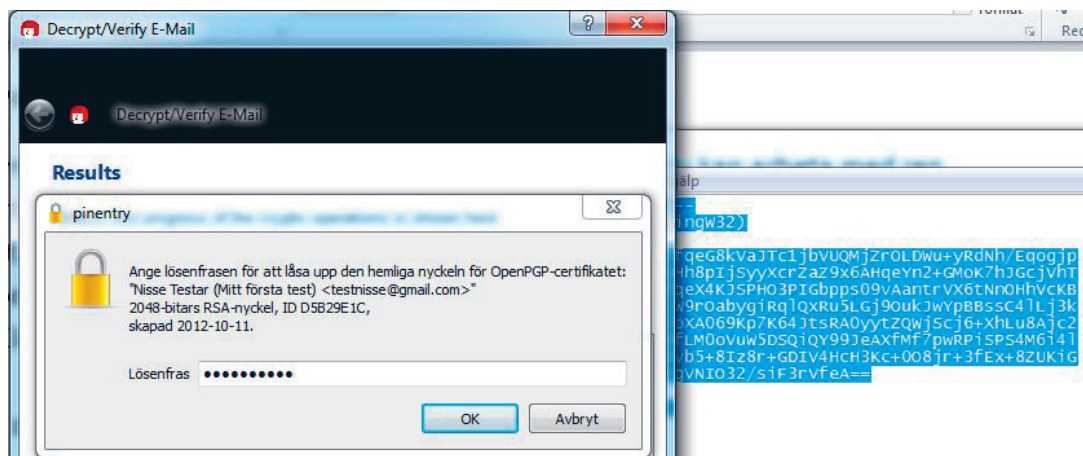
Kopiera den krypterade texten till ett urklipp – hela texten, från

-----BEGIN PGP MESSAGE-----

till

-----END PGP MESSAGE-----

Högerklicka på Kleopatrasymbolen, välj "Clipboard" och "Decrypt/Verify" och ange ditt lösenord.



När dekrypteringen är färdig trycker du på "Finish". Bry dig inte om att det står "No Signatures found". Du har nu den dekrypterade texten i urklippet, och kan klistra in den i ett dokument.

Du kan också dekryptera en fil, på motsvarande sätt som du krypterade den.

Just nu hanterar vi bara testdokument. Men när du sedan krypterar och avkrypterar dokument med känsligt innehåll bör du vara försiktig med de filer som är okrypterade. Spara dem inte på datorn hur som helst, och se till att de raderas ordentligt. Läs mer om säker radering i guiden Digitalt källskydd.

Ta emot en krypterad fil

Än så länge har du bara krypterat för eget bruk. Men du vill antagligen också utbyta krypterad information med andra.

Ett första test kan du göra med en testrobot som heter Adele. När du känner dig trygg med hur det funkar kan du testa på någon riktig person – men gör ännu inte någonting skarpt; be inte någon skicka något till dig som är känsligt på riktigt, och skicka inte själv någonting innan du har full koll på hur dina program fungerar!

Adele är en dator som kan skicka e-postsvar på rudimentära krypteringsförsök. Börja med att testa om du kan ta emot en krypterad fil.

För att Adele ska kunna kryptera meddelanden som du ska kunna läsa behöver hon din publika nyckel. Den får du fram i Kleopatra genom att markera ditt certifikat och sedan välja "Export certificates".

Kontrollera *noga* att det bara är den publika nyckeln som exporteras, och inte hela certifikatet. Du kan se det i rutan "Filformat" i dialogrutan som dyker upp. Där ska det stå "Open PGP Certificates". Det föreslagna namnet är ditt fingeravtryck, men du kan kalla filen något i stil med DittNamn.asc.

Filnamn:	6A7FA52A415AF337DCE9B0470FD2DD64D5B29E1C
Filformat:	OpenPGP Certificates (*.asc *.pgp *.pgp)

Du kan nu öppna dokumentet som skapats – antingen med ett textredigeringsprogram eller med din webbläsare.

Kontrollera noga att texten inleds med

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

Och slutar med

```
-----END PGP PUBLIC KEY BLOCK-----
```

Nu ska du skicka nyckeln till Adele. Du kan kopiera hela texten och lägga den direkt i ett e-postmeddelande. Du kan också skicka den fil du nyss skapade som bilaga i ett e-postmeddelande. Skicka det till adressen adele-en@gnupp.de. Du behöver inte ange något ämne.

Det är dock viktigt att meddelandet är i rent textformat. I Outlook ställer du in det i menyn "Formatera text", där du väljer "Oformaterad text". I Gmail finns valet "Vanlig text".

Observera att den e-postadress som du angav när du skapade certifikatet måste stå som avsändare i e-postmeddelandet. Om du gjort ett testcertifikat måste du alltså skicka detta meddelande från e-postkontot som har rätt adress!

Efter en liten stund får du ett svar från Adele. Om allt blivit rätt har du fått ett krypterat meddelande. Du dechiffrerar det på samma sätt som du gjorde med den text du själv krypterade tidigare.

Om Adele klagar på att hon inte fått någon publik nyckel av dig kan det bero på att ditt e-postmeddelande inte är i rent textformat. Kontrollera inställningarna i ditt e-postprogram.

Det finns insticksprogram för en rad e-postprogram som kan sköta kryptering och dekryptering på ett smidigt sätt. Till Outlook finns GpgOL. Vi kommer dock att installera e-postprogrammet Thunderbird och tillägget Enigmail, som är en beprövad lösning med öppen källkod.

Kryptera ett meddelande till någon annan

För att du ska kunna skicka ett meddelande till Adele, som bara hon kan läsa, behöver du hennes publika nyckel. Den bör du ha fått i det testmeddelande du just dekrypterat.

Först måste du importera den till Kleopatra.

Om du fått nyckeln som en bilagd fil sparar du den, exempelvis på skrivbordet. Om du fått nyckeln i ett e-postmeddelande kopierar du hela texten – från

```
---BEGIN PGP PUBLIC KEY BLOCK---
```

till och med

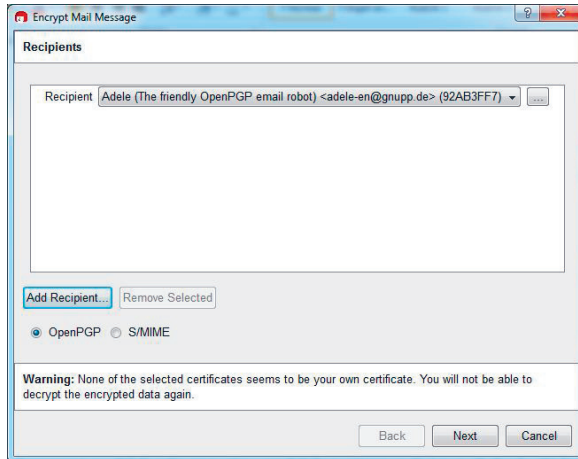
```
---END PGP PUBLIC KEY BLOCK---
```

Texten kopierar du in i en textredigerare. Spara filen med ett lämpligt namn och ändelsen .asc eller .gpg om det är en OpenPGP-nyckel – och det är det ifall du fått den av Adele. Ifall det är en nyckel för S/MIME – även kallat X.509 – ska filens namn sluta på .pem eller .der.

Nu ska nyckeln importeras till Kleopatra. Välj "File" och sedan "Import Certificate". Du kommer nu att ha Adeles nyckel i din nyckelknippa. Du hittar den i fliken "Imported Certificates".

När du fått in Adeles publika nyckel i Kleopatra kan du skapa ett meddelande till henne. Öppna en textredigerare, skriv en text och kopiera den. Högerklicka på Kleopatra-symbolen i skärmens nedre högra hörn, välj "Clipboard" och "Encrypt". När du ska välja mottagare går du in på fliken "Other Certificates" och väljer Adeles certifikat.





När programmet krypterat klart klistrar du in texten i ett e-postmeddelande. Skicka det till Adele. Efter en stund får du ett svar. Om du har lyckats är det ett krypterat meddelande, som visar att Adele tagit emot det som du hade skickat.

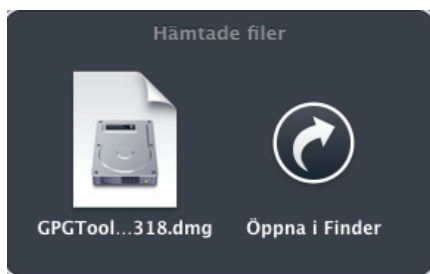
Du kan nu skicka krypterad information till Adele – eller någon som du tror är Adele. När det kommer till praktiska tillämpningar är det minst lika viktigt att du har koll på vem du skickar ditt meddelande till, som att du gjort rätt när du krypterar. Vem som helst kan skapa en nyckel, och fejka en e-postadress. Något mer om hur du ska hantera de frågorna kommer senare i guiden.

Mac: hämta hem och installera GnuPG

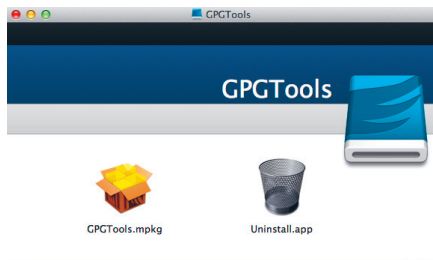
Kör bara programmet om du är säker på att du fått det från en säker källa. Ladda helst hem det själv från <http://gpgtools.com>. Om du får det på en cd, usb-sticka eller laddar ned det någon annanstans ifrån kan det vara en manipulerad version.

Stäng alla andra program.

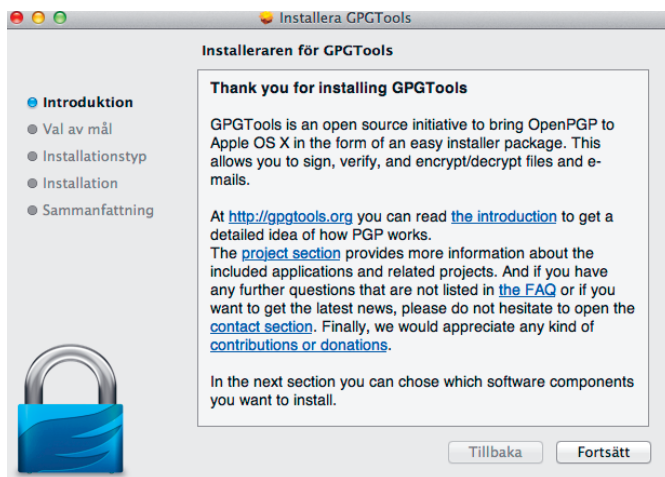
Dubbelklicka på den fil du laddat hem. I den här guiden har vi laddat ned version 2012.03.18.



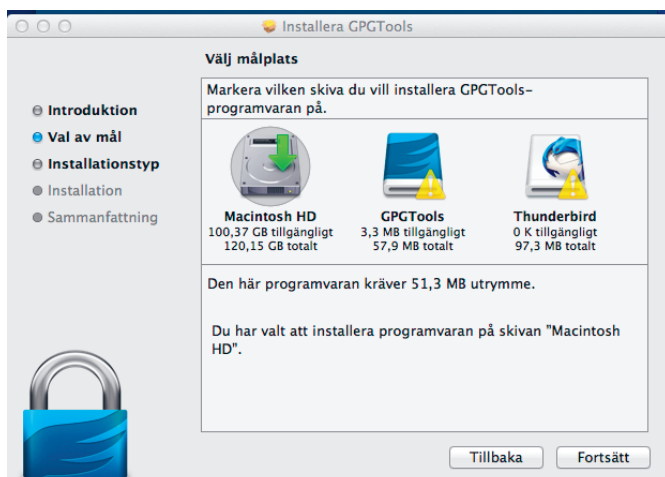
Klicka på installationspaketet



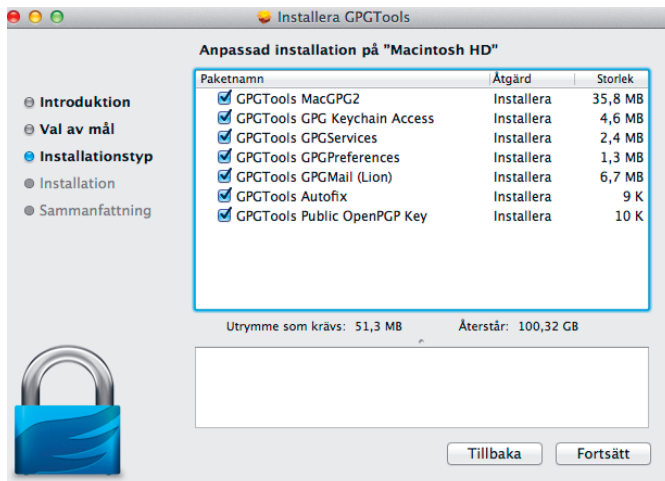
Nästa sida innehåller licensavtalet. Det rör framför allt den som vill utveckla programmet eller sprida det vidare. Men även om det mesta inte berör dig: gör det till en vana att alltid skumma igenom licensavtal. Om du accepterar villkoren klickar du på "Next".



I nästa steg väljer du var programmet ska installeras. Förslaget är normalt bra. Klicka på "Fortsätt" och sedan "Installera".



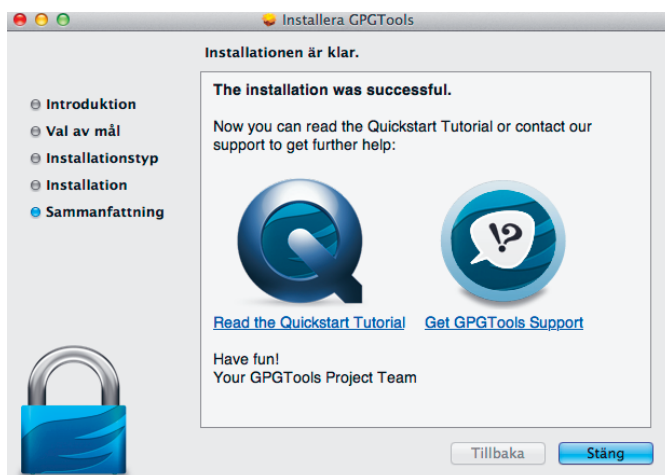
Om du får upp en ruta om vilka komponenter som ska vara med låter du förvalet stå.



Nu installeras programmet. Det tar någon minut.

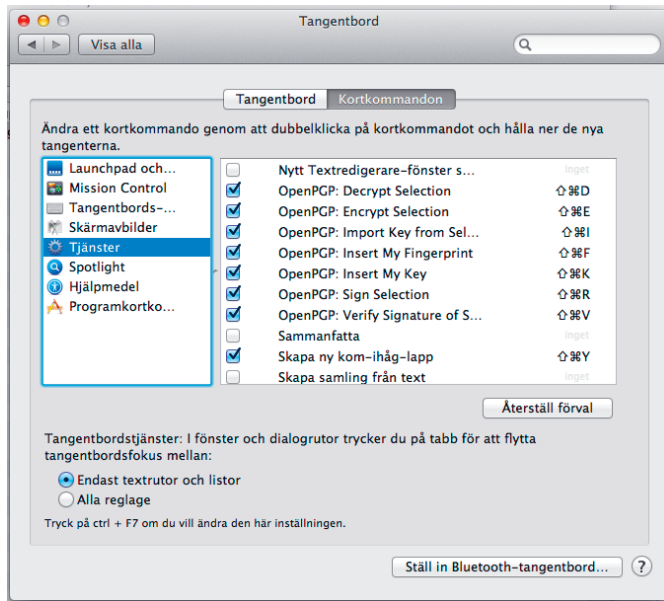
Beroende på vad du har för inställningar i din brandvägg och ditt antivirusprogram kan du få upp en varning om programmet dirmngr.exe. Programmet är till för att hantera dina certifikat och nycklar. Acceptera detta. Klicka på "Tillåt" eller motsvarande i ditt program.

När installationen är klar klickar du på "Stäng".



Nu får du upp en ruta om att skapa nycklar. Hoppa över det så länge. Avsluta installationen.

Du kan behöva aktivera ett antal tjänster för att allt ska fungera. Gå in under "Systeminställningar", "Tangentbord" och välj "Tjänster". I listan skrollar du ner till de rader som gäller PGP och kryssar för alla rutorna.



Skapa nycklar

Nu behöver du dina egna nycklar, för att du ska kunna kryptera material, och för att andra ska kunna skicka krypterade meddelanden till dig.

Öppna programmet GPG Nyckelhanteraren.

Beroende på hur din brandvägg och ditt antivirusprogram fungerar kan du få varningar för att ett antal program körs igång. Acceptera dem.

Programmet hanterar dina nycklar. Till att börja med är listan tom, eftersom du ännu inte har några.

Även om du bara gör en testnyckel första gången måste du göra det med en fungerande e-postadress. Du kan exempelvis skapa en testadress på gmail som du bara använder till detta.



Namn

Nisse Testar

Välj ett användarnamn

testnisse @gmail.com

Skapa ett lösenord

Bekräfta lösenordet

Klicka på den första nyckelikonen, som heter "Ny".

Ange namn och e-postadress som nyckeln ska vara kopplad till. Klicka på "Skapa nyckel".



Skapa nytt nyckel-par.

Fullständigt namn: Nisse Testar

Epostadress: testnisse@gmail.com

Upload key after generation

► Advanced options

Avbryt Skapa nyckel

Nu ska du skapa ett lösenord till din privata, hemliga nyckel. Det här lösenordet måste vara mycket starkt. Ju längre lösenord, desto mindre risk att någon kan knäcka det, och komma åt din privata nyckel. Vill du ha hög säkerhet bör du sikta på 16 – 19 tecken. Repetera lösenordet.

Pinentry Mac

Ange lösenfrasen

Lösenfras

Show typing

Cancel OK

Att skapa nycklarna kommer att ta några minuter. När ditt nya certifikat är klart får du upp det i nyckelhanteraren.

Innan du går vidare ska du spara en säkerhetskopia av ditt nyckelpar.

Markera din nya nyckel. Klicka på "Exportera". Som förval har den fått namn i form av det id-nummer som du fått. Du kan döpa om den till ditt namn. Välj var filen ska sparas. Spara till en cd eller usb-sticka, och förvara den sedan på ett säkert ställe – helst ett kassaskåp eller i ett bankfack. Undvik att först spara den på datorn och sedan flytta den.

Klicka i kryssrutan "Tillåt export av hemliga nycklar". Observera att den här exporten *aldrig* får användas när du ska skicka din nyckel till någon annan. I så fall kan andra också komma åt allt ditt krypterade material. Klicka på "Spara".

Spara som: NisseTestar.asc

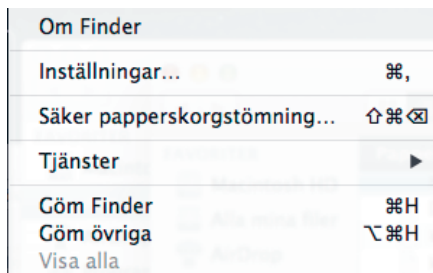
Plats: NO NAME

Format: ASCII

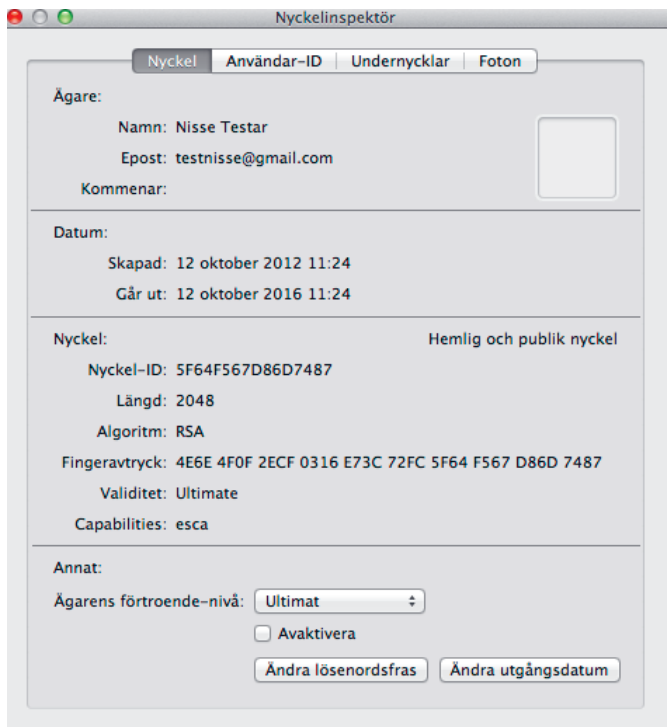
Tillåt export av hemliga nyckla

Avbryt Spara

Radera säkerhetskopian helt från datorn, ifall du sparat den där. Observera att det *inte* räcker att slänga filen i papperskorgen. För att den verkligen ska vara borta måste papperskorgen vara tömd och raderad med ett överskrivningsprogram. Använd funktionen ”Säker papperskorgstömning”.



Om du nu dubbelklickar på ditt nya certifikat får du veta mer. Du hittar bland annat hela ditt fingeravtryck, som ibland används som identifiering för att hitta nycklar. Oftast används dock bara id-numret, som är de åtta sista tecknen i fingeravtrycket.



Testa nycklarna

Nu kan du börja testa dina nycklar och sedan att skicka krypterade meddelanden. Tänk på att det är viktigt att du känner dig trygg med hur dina program fungerar innan du börjar använda dem till att överföra känsliga meddelanden.

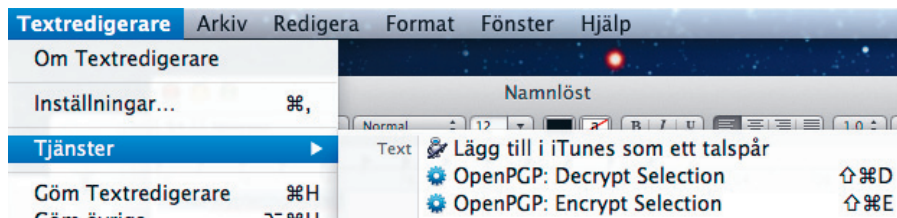
Testa först om du kan kryptera en textsnut.

Öppna programmet Textredigerare, där du kan arbeta med ren, oformaterad text.

Skriv en kort text.

Markera hela texten.

Gå in i huvudmenyn "Textredigerare". Välj "Tjänster" och sedan "OpenPGP: Encrypt Selection".



I rutan "Choose Recipients" klickar på kryssrutan för ditt eget certifikat. Klicka bort markeringen vid "Add to Recipients". Klicka på "OK".

Nu har texten i urklippet krypterats. Texten kommer nu att se ut ungefär så här:

```
-----BEGIN PGP MESSAGE-----
```

```
hQEMAwKMSsupndKfAQf/TaoXJHg91snSq50/XLcCmYGonMfSA0EG-  
TrEUfvGbdH08
```

```
jz3wNMkt4oTHxa9ikQ7P3MnUvQCit6xhPUaR1R9ytYHgq+15/4yFEvTf  
oGIicF1k
```

```
VZh2qKVrEInw7nF34XNdQzEHbNIh4/lDEa/cVrp/COkTaxi-  
DlCFmd33XKxylBADy
```

```
x/NM/D4u
```

```
=fmk2
```

```
-----END PGP MESSAGE-----
```

Du kan nu spara den här filen, exempelvis på ett usb-minne. Du kan också klistra in den i ett e-postmeddelande. Din hemliga text kan inte läsas utan tillgång till din privata nyckel.

Ett annat sätt att kryptera din text är att först spara den okrypterade texten i ett dokument, exempelvis med namnet "texten.txt". Markera filen i Finder. Gå in i menyn "Finder" och välj sedan "Tjänster" och "OpenPGP: Encrypt File". I rutan som öppnas markerar du att det är du själv som är mottagare.

När du sedan vill titta på din text gör du på samma sätt fast tvärtom:

Kopiera den krypterade texten till ett urklipp – hela texten, från

```
-----BEGIN PGP MESSAGE-----
```

till

```
-----END PGP MESSAGE-----
```

Gå in i menyn "Textredigerare", välj "Tjänster" och "OpenPGP: Decrypt" och ange ditt lösenord.

Du kan också dekryptera en fil, på motsvarande sätt som du krypterade den.

Just nu hanterar vi bara testdokument. Men när du sedan krypterar och avkrypterar dokument med känsligt innehåll bör du vara försiktig med de filer som är okrypterade. Spara dem inte på datorn hur som helst, och se till att de raderas ordentligt.

Ta emot en krypterad fil

Än så länge har du bara krypterat för eget bruk. Men du vill antagligen också utbyta krypterad information med andra.

Ett första test kan du göra med en testrobot som heter Adele. När du känner dig trygg med hur det funkar kan du testa på någon riktig person – men gör ännu inte någonting skarpt; be inte någon skicka något till dig som är känsligt på riktigt, och skicka inte själv någonting innan du har full koll på hur dina program fungerar!

Adele är en dator som kan skicka e-postsvar på rudimentära krypteringsförsök. Börja med att testa om du kan ta emot en krypterad fil.

För att Adele ska kunna kryptera meddelanden som du ska kunna läsa behöver hon din publika nyckel. Den får du fram i GPG Nyckelhanterare genom att markera ditt certifikat och sedan välja "Exportera".

Kontrollera NOGA att det bara är den publika nyckeln som exporteras, och inte hela certifikatet. Kontrollera att kryssrutan "Tillåt export av hemliga nycklar" INTE är ikryssad. Du kan kalla filen något i stil med DittNamn.asc

Du kan också öppna dokumentet som skapats – antingen med ett textredigeringsprogram eller med din webbläsare.

Kontrollera noga att texten inleds med

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

Och slutar med

```
-----END PGP PUBLIC KEY BLOCK-----
```

Nu ska du skicka nyckeln till Adele. Du kan kopiera hela texten och lägga den direkt i ett e-postmeddelande. Du kan också skicka den fil du nyss skapade som bilaga i ett e-postmeddelande. Skicka det till adressen `adele-en@gnupp.de`. Du behöver inte ange något ämne.

Det är dock viktigt att meddelandet är i rent textformat. I gmails webbgränssnitt finns valet "Vanlig text".

Observera att den e-postadress som du angav när du skapade certifikatet måste stå som avsändare i e-postmeddelandet. Om du gjort ett testcertifikat måste du alltså skicka detta meddelande från e-postkontot som har rätt adress!

Efter en liten stund får du ett svar från Adele. Om allt blivit rätt har du fått ett krypterat meddelande. Kopiera in meddelandet i ett textdokument. Du dechiffrerar det på samma sätt som du gjorde med den text du själv krypterade tidigare.

Om Adele klagar på att hon inte fått någon publik nyckel av dig kan det bero på att ditt e-postmeddelande inte är i rent textformat. Kontrollera inställningarna i ditt e-postprogram.

Det finns insticksprogram för en rad e-postprogram som kan sköta kryptering och dekryptering på ett smidigare sätt. Vi kommer dock att installera e-postprogrammet Thunderbird och tillägget Enigmail, som är en beprövad lösning med öppen källkod.

Kryptera ett meddelande till någon annan

För att du ska kunna skicka ett meddelande till Adele, som bara hon kan läsa, behöver du hennes publika nyckel. Den bör du ha fått i det testmeddelande du just dekrypterat.

Om du fått nyckeln som en bilagd fil sparar du den, exempelvis på skrivbordet. Om du fått nyckeln i ett e-postmeddelande kopierar du hela texten – från

```
---BEGIN PGP PUBLIC KEY BLOCK---
```

till och med

```
---END PGP PUBLIC KEY BLOCK---
```

Texten kopierar du in i en textredigerare. Spara filen med ett lämpligt namn och ändelsen .asc eller .gpg om det är en OpenPGP-nyckel – och det är det ifall du fått den av Adele.

Nu ska nyckeln importeras till nyckelhanteraren. Välj ”Importera” och dubbelklicka sedan på filen du just skapade. Du kommer nu att ha Adeles nyckel i din nyckelknippa.

När du fått in Adeles publika nyckel kan du skapa ett meddelande till henne. Öppna en textredigerare, skriv en text och markera den. Gå in i menyn ”Textredigerare”, välj ”Tjänster” och ”OpenPGP: Encrypt Selection”.

När du ska välja mottagare väljer du Adeles certifikat. När programmet krypterat klart klistrar du in texten i ett e-postmeddelande. Skicka det till Adele. Efter en stund får du ett svar. Om du har lyckats är det ett krypterat meddelande. När du dekrypterat det ser du om Adele har lyckats ta emot det som du hade skickat.

Du kan nu skicka krypterad information till Adele – eller någon som du tror är Adele. När det kommer till praktiska tillämpningar är det minst lika viktigt att du har koll på vem du skickar ditt meddelande till, som att du gjort rätt när du krypterar. Vem som helst kan skapa en nyckel, och fejka en e-postadress. Något mer om hur du ska hantera de frågorna kommer senare i guiden.

Dags för Thunderbird

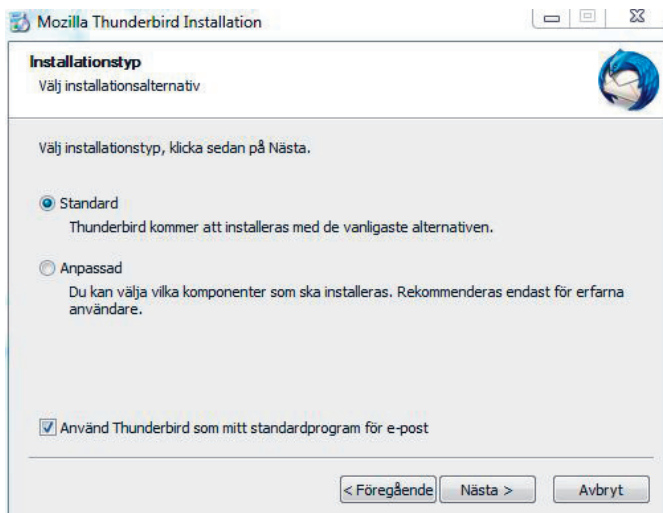
Nu har du byggt en bra grund för din fortsatta kryptering. Du kan kryptera enskilda texter och skicka enkla meddelanden.

Men att böka med krypteringen av e-post som vi gjort hittills är omständligt. Flera e-postprogram kan hjälpa dig att kryptera direkt, om du har rätt tillägg.

En väl beprövad lösning med öppen källkod är e-postprogrammet Thunderbird med tillägget Enigmail, och den här guiden hjälper dig att installera det du behöver.

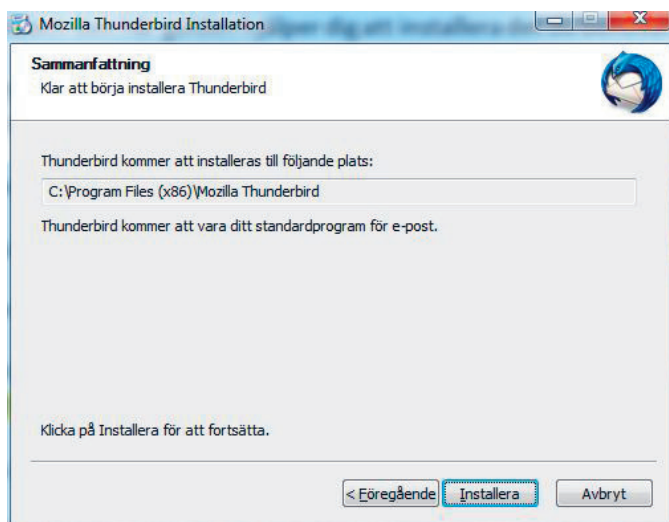
Thunderbird finns för såväl Mac som PC. Skärmdumparna nedan är från PC, version 16.0.1, men installationen på Mac är i princip likadan.

Ladda hem Thunderbird från <http://www.mozilla.org/sv-SE/thunderbird/>
Kör installationsprogrammet för Thunderbird.



Välj standardinstallation.

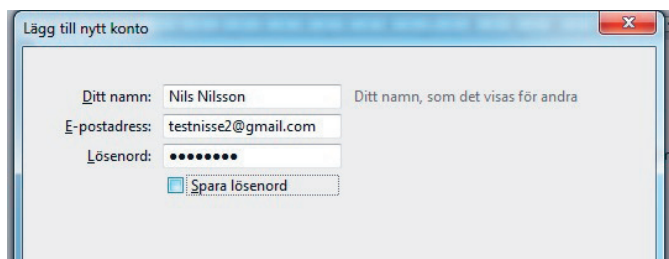
I nästa steg väljer du var programmet ska installeras. Förslaget är normalt bra. Klicka på "Installera".



Avsluta installationen och kör igång programmet.

Nu ska du skapa ett konto för den e-postadress du tidigare gjort i ordning certifikat för. Det kan vara bra att ha den krypterade e-posten på ett separat konto. Ifall du ibland kör krypterat och ibland okrypterat med din vanliga e-post är risken stor att du plötsligt skickar ett okrypterat svar i en tidigare krypterad konversation. Om du råkar göra det innebär det att hela konversationen, med alla inkluderade svar, går iväg öppet.

Hoppa över förslaget från Thunderbird att skapa en adress på gandi eller hover. Fyll i dina kontouppgifter. Tag bort förvalet att Thunderbird ska spara ditt lösenord.



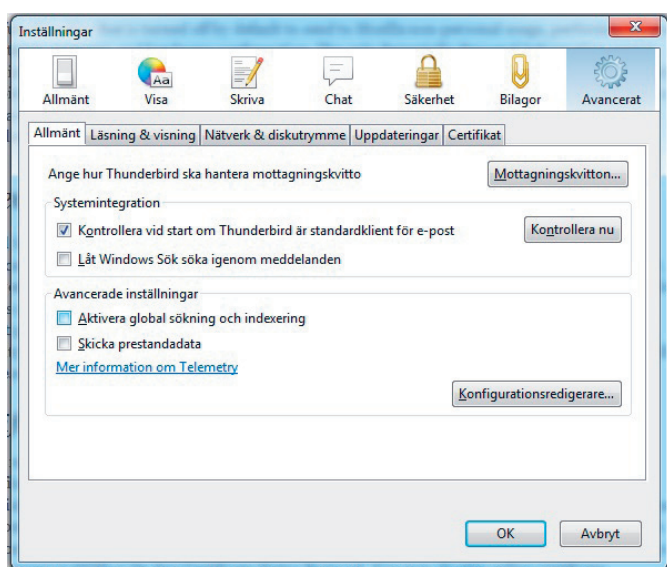
Om du vill ha kvar alla mejl på e-postservern ska du nu välja att det ska vara ett IMAP-konto. Om du inte vill att e-posten ska ligga kvar hos leverantören, utan att

de alltid ska tankas hem till din dator väljer du ruta att det ska vara ett POP3-konto. Du måste dock i så fall senare även göra en annan inställning.

Nu har du skapat ett e-postkonto.

Avaktivera att prestandadata skickas iväg.

På PC: På Gå in i menyn "Verktyg", och välj "Inställningar". Gå in på fliken "Avancerat" och sedan fliken "Allmänt". Kryssrutan "Skicka prestandadata" ska vara avmarkerad.



På Mac: På Gå in i menyn "Thunderbird", och välj "Inställningar". Gå in på fliken "Avancerat" och sedan fliken "Allmänt". Kryssrutan "Skicka prestandadata" ska vara avmarkerad.

Ställ in POP3

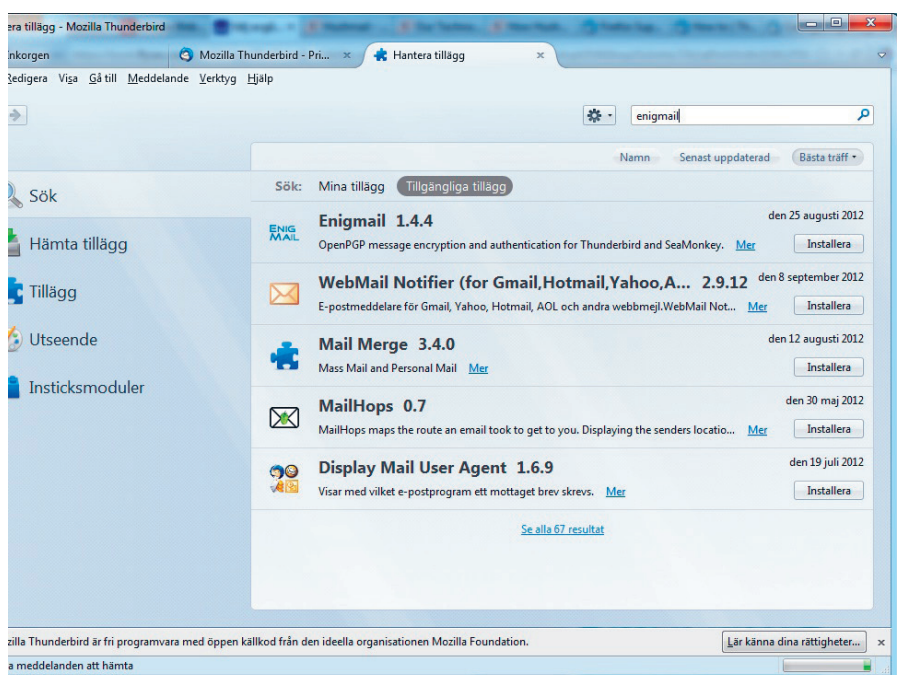
Om du vill att dina meddelanden tas bort från e-postservern, så att du bara hantarerar dem i din egen dator, skulle du ställa in ditt e-postkonto att använda POP3. För att aktivera detta går du nu in under menyn "Verktyg", sedan "Kontoinställningar". Klicka på "Serverinställningar" i vänstermenyn. På den undre hälften i rutan finns en kryssruta som heter "Lämna kvar meddelanden på servern". Avmarkera den.



Men när skulle vi börja kryptera...?

Nu är det dags att installera det tillägg i Thunderbird som hanterar krypteringen, nämligen Enigmail.

Gå in i Thunderbird, menyn "Verktyg", "Tillägg" och skriv in "Enigmail" i sökrutan. När du hittat det klickar du på "Installera".



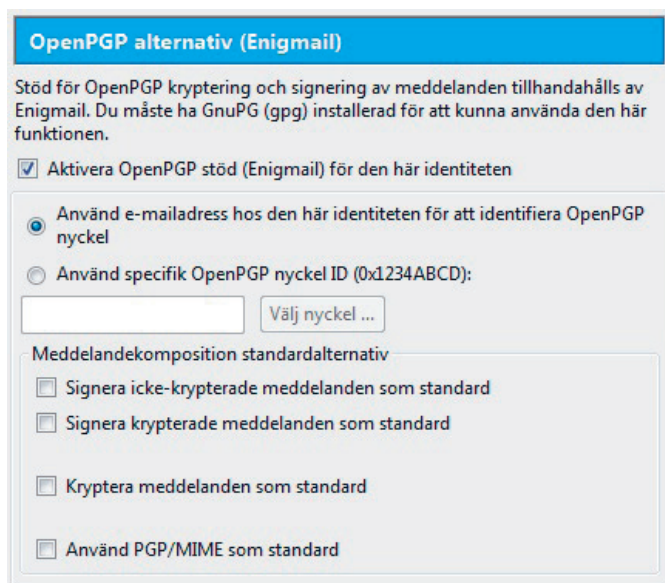
Enigmail installeras då när du startar om Thunderbird. Välj att göra det på en gång.

När Thunderbird startats om ska menyraden nu även innehålla menyn "OpenPGP". Gå in i undermenyn "Inställningar".

Om allt blivit rätt ska sökvägen till din GnuPG-installation framgå i rutan som kommer upp. Annars kommer du att få en varning. Har du kollat att installationen fungerar bör detta dock inte hända nu.

I samma ruta finns en möjlighet att ändra den tid programmet ska komma ihåg ditt lösenord. Om du vill sitta länge och skicka och ta emot krypterade meddelanden kan det kanske vara irriterande om du måste ange lösenordet om och om igen. Men det är en balansgång att ställa in en lagom tid. Tänk dock på att "ingången" till dina krypterade mejl kommer att vara öppen under denna tid efter varje gång du angett lösenordet. För att radera lösenordet ur programminnet – exempelvis om du ska hämta kaffe eller gå på lunch – stänger du programmet.

Gå in i menyn "Verktyg", och välj "Kontoinställningar". I vänstermenyn finns nu raden "Open PGP Security". Klicka på den.



Markera kryssrutan "Aktivera OpenPGP stöd (Enigmail) för den här identiteten". (Bry dig inte om sårskrivningen. Formuleringen är något annorlunda på Mac). Låt valet "Använd e-mailadress hos den här identiteten för att identifiera OpenPGP nyckel" vara ikryssat. Ifall du senare skaffar flera nycklar för samma användare ska du specificera vilken nyckel du vill använda till ett visst e-postkonto.

Du kan välja att signera och kryptera alla dina meddelanden här. Eftersom du troligen inte har PGP-nycklar till alla dina kontakter bör du inte välja att kryptera allt. Att signera meddelanden fungerar dock alltid, och kan vara en bra idé om du vill försäkra dig och dem du mejlar med att innehållet inte manipulerats på vägen.

Stäng av html

Du bör stänga av användningen av HTML, det språk som används för att layouta bland annat webbsidor men även e-post. Krypteringen kan störas av HTML. Men HTML och bilder kan också användas för att kontrollera ditt beteende – exempelvis när du sedan går in på en webbsida eller hur du vidarebefordrar e-brevet. Därför bör du helst inte tillåta HTML alls, och bara köra med rena textmeddelanden. Du kan också välja att bara stänga av användningen medan du ska skicka krypterade meddelanden.

Välj menyn "Verktyg", "Kontoinställningar", "Skriva och adressera", och avmarkera kryssrutan "Skriv meddelanden i HTML-format".

Skriv ett meddelande

Dags att skicka ett krypterat meddelande.

Klicka på "Skriv". Du får nu upp ett tomt e-postformulär. Förslagsvis börjar du med att testa på testroboten Adele, adele-en@gnupp.de.

Du kan nu skriva ditt meddelande som vanligt. Tänk dock på att det bara är själva texten i e-postmeddelandet som kommer att krypteras. Såväl mottagare, avsändare som ärenderad överförs okrypterat. Det innebär att om obehöriga snappar upp meddelandet kan de se vem som kommunicerat med vem, ert ärende – och att ni skickar krypterade meddelanden till varandra.

När du skrivit ditt meddelande tittar du i meddelanderutans nedre högra hörn. Där finns två små ikoner: en penna och en nyckel. Om du vill att meddelandet ska krypteras klickar du på nyckeln. Den lilla symbolen ska nu bli gul.

Klicka på "Skicka".

Ifall den mottagare du angett redan finns med bland de personer som du har en publik nyckel till kommer nu meddelandet att skickas iväg.

Ifall du inte har mottagarens publika nyckel kommer Thunderbird att klaga över att mottagaren inte finns. Välj "Ladda ned saknadenycklar". Programmet kommer då att ansluta till en nyckelservrar, som samlar publika nycklar, och leta efter den e-postadress du angett där. Om e-postadressen hittas markerar du den och skickar ditt meddelande.

Alla lägger dock inte upp sina publika nycklar på nyckelservrar. Du måste då lägga in den manuellt i ditt program. Du kanske hittar den som en bilaga i ett e-postmeddelande från personen, eller så kanske den ligger som ett textblock i meddelandet.

Thunderbird känner av PGP-nyckeln och föreslår att den ska importeras. Gör det genom att klicka på "Dekryptera".

Ifall du fått nyckeln på något annat sätt – om den exempelvis finns på en webbsida – kopierar du hela texten från

```
---BEGIN PGP PUBLIC KEY BLOCK---
```

till och med

```
---END PGP PUBLIC KEY BLOCK---
```

Gå sedan in i Thunderbird-menyn "OpenPGP", och välj "OpenPGP nyckelhantering". I rutan du får upp går du in i menyn "Redigera" och väljer "Importera nycklar från klippbordet". När du har alla nödvändiga nycklar kan du skicka meddelandet.

Det går bra att skicka ett meddelande till flera mottagare på en gång, men du måste ha allas publika nycklar. Det fungerar inte att skicka krypterat till några men inte alla mottagare.

Det fungerar inte heller att lägga in en dold kopia till någon; Enigmail lägger in alla mottagare i ett PGP-block som alla kan se. Även om det finns sätt att ta sig runt detta är det sannolikt enklare att skicka en separat mejlkopia till dem som du inte vill ska synas bland mottagarna.

Ta emot ett krypterat meddelande

När du fått ett meddelande som är krypterat kommer programmet att känna av det och fråga efter ditt lösenord. När du skrivit in det visas meddelandet i klartext. I överdelen av meddelandet kommer det att finnas en rad som talar om att det är ett dekrypterat meddelande. I nedre högra hörnet finns också en gul nyckelsymbol.

Om du trycker på "Svara" kommer Thunderbird automatiskt att välja att det ska vara ett krypterat svar. Du ser det genom att nyckelsymbolen i nedre högra hörnet är gul. Kontrollera noga att du inte råkat stänga av krypteringen, eftersom det innebär att svaret skickas okrypterat – och då har dina tidigare vedermödor varit förgäves.

Signera ett meddelande

Ibland kan det vara bra att kunna verifiera att ett e-brev verkligen kommer från en viss person, och inte minst: att det inte blivit manipulerat sedan du skickade det. Signeringen kan också komma till nytta om du inte har mottagarens öppna nyckel. Du kan visserligen inte kryptera meddelandet, men mottagaren kan i alla fall verifiera att det som kommit fram är detsamma som det du skickade. Signeringen görs med din privata nyckel, och mottagaren kan kontrollera att signeringen är korrekt med hjälp av din publika nyckel.

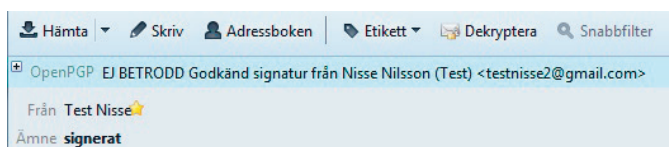
I Thunderbird sätter du på signeringen genom att trycka på den lilla pennan bredvid nyckeln i nedre högra hörnet av ett e-postmeddelande.

Att kontrollera ett signerat meddelande

När du fått ett signerat meddelande från någon ska du kontrollera att signeringen stämmer.

Till att börja med behöver du avsändarens publika nyckel. Den kanske avsändaren har skickat med i meddelandet, eller så har du fått den på annat sätt.

När du får ett signerat meddelande i Thunderbird från någon som redan finns i din nyckellista kommer överdelen av meddelandet att vara grönt.



Om det står "Godkänd signatur från ..." är allt bra.

Det kan också stå "EJ BETRODD Godkänd signatur från...". Att signaturen är godkänd innebär att den är tekniskt ok – ingen har manipulerat meddelandet på vägen. Att det står "EJ BETRODD" kan antingen innebära att avsändaren verkligen inte är betrodd. Eller så är det bara så att varken du eller någon annan har verifierat att den här avsändaren är den som den ger sig ut för att vara.

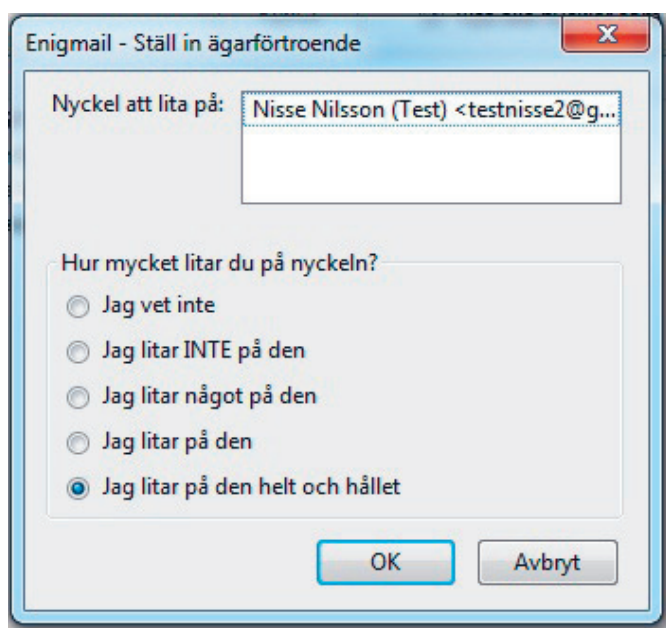
Om du helt säkert vet att en nyckel i din lista är skapad av den person du tror – du kanske har fått id-numret till nyckeln personligen – kan du ställa in det i din nyckelhanterare.

Om du får upp felmeddelanden i rött i meddelandets överkant när du öppnar det kan meddelandet ha manipulerats. Men du behöver inte få stora skälvan för att du får det meddelandet – ibland förändras meddelanden på vägen utan att det är en medveten manipulation. Ett exempel kan vara om avsändaren skickar meddelanden i html-format, något som inte alltid hänger med hela vägen.

Om du får ett felmeddelande bör du i alla fall be avsändaren skicka meddelandet på nytt. Meddelanden bör vara i rent textformat när de ska signeras.

Du behöver vara medveten om att signeringen inte ger 100-procentig säkerhet. Vem som helst kan skapa en nyckel, och kan använda en godtycklig e-postadress. Skumma Nisse kan skapa e-postadressen FredrikR@regeringen.se och skapa nycklar för den. Du kan därmed få ett e-brev som är korrekt signerat – eftersom det inte manipulerats på vägen och det har skickats med en signatur som stämmer överens med e-postadressen. Men det är fortfarande ingen garanti för att det kommer från Sveriges statsminister.

För att du inte själv hela tiden ska behöva kontrollera varenda publik nyckel du stöter på använder GnuPG ett nät av pålitliga signaturer – web of trust. Du kan själv verifiera att rätt nyckel hänger ihop med rätt människa när du träffar någon, och du kan markera det i dina egna inställningar. Du kan också låta dina inställningar gå ut till allmänheten. Sedan utnyttjar du kedjor av tilltro – om du litar på Anna som litar på Bertil, kan du också lita på Bertil.



Vill du lära dig mer om verifiering av nycklar kan du göra det i GnuPG-handboken <http://www.gnupg.org/gph/en/manual.html>.

Stäng av förhandsgranskning

Det finns skadliga program som aktiveras bara genom att du förhandsgranskar e-postmeddelanden i ditt e-postprogram. Du bör därför stänga av förhandsgranskningen om du vill ha hög säkerhet. Gå in under menyn "Visa", sedan "Layout" och se till att "Förhandsgranskning" inte är förbockad. Du kan också trycka på "F8" på tangentbordet.

Om du får ett meddelande från en okänd avsändare och med ett ärende som verkar suspekt ska du överhuvudtaget inte öppna det, utan radera det direkt. En del angrepp sker genom att kod aktiveras när du öppnar ett e-postmeddelande. Andra går via bilagor. Var alltid vara försiktig med att öppna bilagor som du inte vet vad de innehåller och alldeles särskilt om de kommer från en okänd avsändare.

Signerade dokument

Precis som man kan signera e-postmeddelanden, för att så gott det går försäkra sig om att rätt person ligger bakom det och att det inte manipulerats på vägen, går det också att signera filer.

När du tar emot en signerad fil behöver du ha avsändarens publika nyckel. Om du inte redan har den importerar du den i Kleopatra eller GPG Nyckelhanterare på samma sätt som tidigare.

Du behöver också en signaturfil, en fil med ändelsen.sig. Lägg den filen i samma mapp som den fil du vill verifiera.

Gå till den fil du vill kontrollera.

På PC: Högerklicka på filen. I listan som kommer upp väljer du "Egenskaper". Gå sedan in på fliken "Digitala signaturer". Dubbelklicka på raden där signaturen står. I rutan du får upp ska det framgå att

signaturen är OK.

På Mac: Markera filen du vill kontrollera i Finder. Högerklicka. Längst ned i menyn finns valet "Tjänster". Välj OpenPGP: Verify Signature of File". Du ska nu få upp ett meddelande som säger "Signed by...". Ifall verifieringen misslyckats får du varningen "Verification FAILED".

Kryptera datorn

Genom att kryptera din dator hindrar du angripare från att komma åt dina dokument. Att kryptera är något helt annat än att bara skapa ett lösenord för att logga in. Ett sådant lösenord hindrar den som råkar promenera förbi din dator att titta i den. Men det krävs ingen högre datautbildning för att ta sig förbi lösenordet – det kan räcka att skruva isär datorn och koppla in sig mot hårddisken från en annan dator.

Krypterar du dina data går de inte att läsa utan att knäcka krypteringen. Det kräver betydligt mer av den som är ute efter dina data, och har du en stark kryptering är det möjligen organisationer som svenska FRA eller amerikanska NSA som kan knäcka den.

Du kan välja att bara kryptera en del av datorn, eller hela. En fördel med att fulldiskkryptera din dator är att du inte behöver fundera så mycket. Allt krypteras. Om du väljer att bara kryptera vissa filer kan det du krypterat ibland plockas fram i klartext ändå, genom att återskapa raderade dokument eller genom att plocka fram temporära filer. Är datorn fulldiskkrypterad kommer allt det här krypteras också.

En annan fördel med att kryptera allt är att du inte behöver tänka på att dina data kanske plötsligt får ett annat värde. Dokument som till en början verkade helt oförarliga kanske plötsligt blir de som kan peka ut en viktig källa.

Däremot behöver du fortfarande vara försiktig när du skickar iväg filer till någon annan, eller lägger över dem till någon annan dator i ett nätverk. Filerna är bara krypterade så länge de ligger på den krypterade datorn.

En fördel med att bara kryptera en del av hårddisken är att du kan få det att se ut som att du inte har några krypterade data alls på datorn. Den krypterade delen kan gömmas i en fil, som du kan ge ett fullständigt oskyldigt namn – och som verkar vara oläsbar för den som tillfälligtvis försöker öppna den. Det här är inget som lurar ett proffs – men de kommer likväl inte att komma åt dina data utan att först knäcka ditt lösenord.

Om du har krypterad information på ett usb-minne och öppnar den på någon annans dator måste du också tänka på att inte spara filerna där, eftersom de då kommer att ligga öppna och okrypterade.

På en Windowsdator finns programmet Bitlocker för att kryptera hela hårddisken eller delar, partitioner. På alla nya Macar finns krypteringsprogrammet FileVault inbyggt.

Du kan också installera ett program med öppen källkod. I den här guiden får du hjälp att installera programmet TrueCrypt och skapa en virtuell hårddisk.

Truecrypt

TrueCrypt är ett krypteringsprogram som använder öppen källkod. Programmet är gratis.

I den här guiden går vi igenom hur du skapar en krypterad liten ”låda”. TrueCrypt kan dock också användas för att kryptera en del av hårddisken – en partition – hela hårddisken, eller läggas på exempelvis ett usb-minne.

Det finns stora fördelar med att kryptera hela hårddisken, som vi beskrivit ovan. Men också risker. Därför kan det vara bra att börja med en enklare variant. I den installation du gör i den här guiden kommer bara en del av datorn att vara krypterad.

Den här lösningen kan räcka ganska långt – du skapar en enhet som krypteras, och sedan ser du bara till att lägga de filer som ska vara krypterade i den enheten.

Men det gäller att komma ihåg att filer som lagras någon annanstans på datorn först, och sedan flyttas till den krypterade enheten, kan återskapas i okrypterat skick. Du bör alltså tänka igenom hur du hanterar dina dokument. Ställ in olika program så att de sparar dokument direkt på den krypterade enheten. Och se till att ha ett bra program för att radera filer som du slängt. Ett exempel kan vara Ccleaner. Läs mer här >> På Mac finns alternativet Säker papperskorgstömning. Du kan gå in under "Finder" och "Inställningar", "Avancerat" och välja "Töm papperskorgen säkert".

När din enhet är krypterad kommer den att ligga sparad som en fil på datorn. Vill du vara extra hemlig kan du byta namn på filen, exempelvis så att den har ändelsen .avi. Då ser det ut som om det skulle vara en film – men om man försöker visa filmen kommer det inte gå.

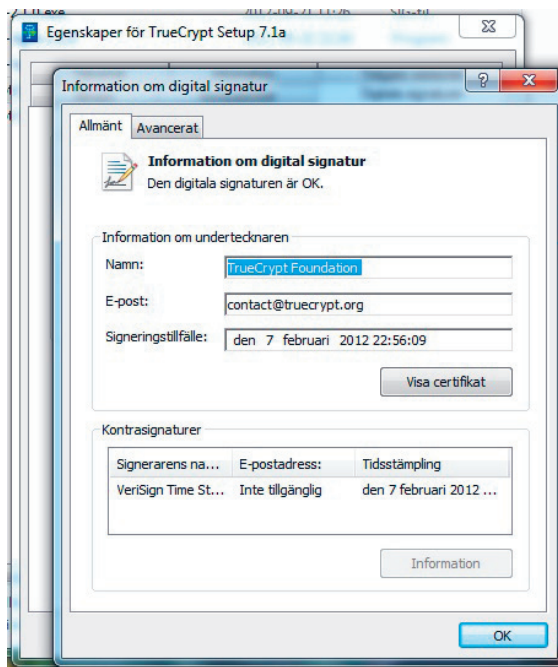
Detta kommer inte att lura en expert, som ser att du har TrueCrypt installerat. Men för den som bara kollar din dator litet snabbt går det inte att se att du har krypterat material, och inte var du har det.

När filen är öppen fungerar den som en egen hårddisk, med en egen enhetsbokstav i filhanteraren. Allt du sparar på den här disken krypteras.

Installationen för PC och Mac är ganska likartad, och vi kommer inte att separera dem. Skärmdumparna är från en PC-installation.

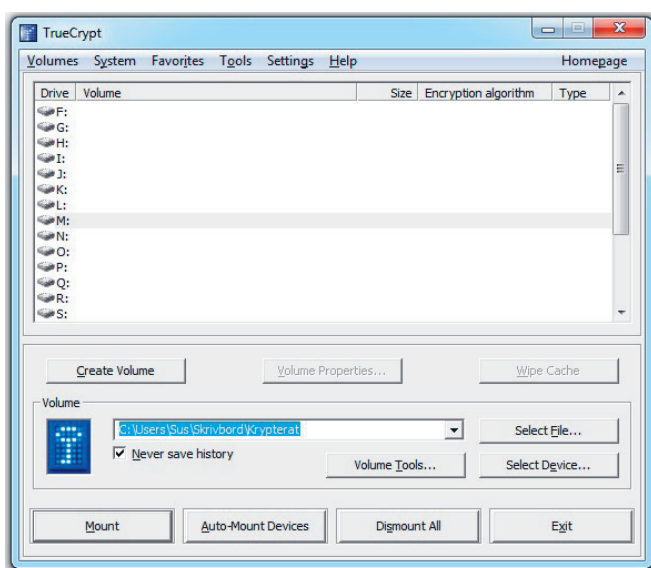
Så här gör du din första installation av TrueCrypt:

1. Gör en säkerhetskopia på din dator, om du inte redan gjort det. Tänk på att säkerhetskopian bör förvaras inlåst om den inte är krypterad.
2. Ladda hem programmet från <http://www.truecrypt.org/downloads>.
3. När du laddat hem programmet ska du helst inte köra det på en gång. Först bör du kontrollera att det är en korrekt version. Det gör du genom att verifiera den signatur som hör till programmet.
 - a. På PC: Högerklicka på filen. I listan som kommer upp väljer du "Egenskaper". Gå sedan in på fliken "Digitala signaturer". Dubbelklicka på raden där det står "TrueCrypt Foundation". I rutan du får upp ska det framgå att signaturen är OK.

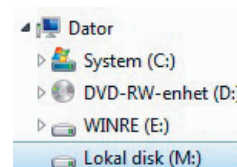


- b. På Mac måste du ha GnuPG installerat. Läs mer ovan om hur du gör det och hur du verifierar signaturer. Signaturen laddar du hem genom att klicka på "PGP Signature". TrueCrypts nyckel laddar du hem från <http://www.truecrypt.org/downloads2>. Länken finns under rubriken "Public Key".
4. Dubbelklicka på programfilen. Titta på licensavtalet och godkänn om du tycker att det är ok. Gå vidare.
5. I nästa ruta ska du välja var TrueCrypt ska installeras. Normalt är förslaget bra. På PC kan du avmarkera kryssrutan "Add TrueCrypt icon to desktop" om du vill hålla skrivbordet rent. Klicka på "Install".
6. Öppna programmet. I rutan som kommer upp väljer du "Create Volume".
7. Välj det förhandsinställda "Create an encrypted file container", om du vill börja med att bara kryptera en del av hårddisken.
8. I nästa steg väljer du om enheten ska vara dold eller synlig. Om du vill göra en osynlig enhet bör du läsa på i manualen. Här fortsätter vi med att skapa en standardvolym.
9. Nu ska du skapa din fil. Klicka på "Select File".
10. Välj i vilken mapp filen – som kommer att innehålla din krypterade enhet – ska ligga. Det kan vara var som helst på datorn. Hitta på ett namn och skriv i rutan "Filnamn". Du ska inte markera ett dokument som redan finns på din dator – det kommer i så fall att raderas. Du ska alltså *absolut inte* döpa den till samma namn som någon fil du vill kryptera! Vi kallar vår fil "Krypterat" och lägger den på skrivbordet. Klicka på "Spara" och sedan på "Next".
11. Nu ska du välja krypteringsmetod. Du kan låta förhandsalternativet stå.
12. I nästa steg ska du välja storlek på din krypterade enhet. Om du vill kunna spara filen till en cd kan den inte vara större än 700 MB, och för en dvd 4,5 GB. Tänker du spara på ett usb-minne kan du ha ännu större filer.
13. Sedan ska du ange ett lösenord. Tänk på att det ska vara ett starkt lösenord. Läs mer i guiden Digitalt källskydd. TrueCrypt accepterar lösenord på upp till 64 tecken. Men du kan inte använda å, ä och ö. Det går också att använda nyckelfiler – du kan exempelvis ha en viss mp3-fil på ett usb-minne som måste finnas tillgänglig för att låsa upp din krypterade enhet. Läs mer i manualen om hur du går till väga i så fall. I den här guiden låter vi kryssrutorna vara tomma och klickar på "Next".
14. När du ska ange format väljer du FAT, om du inte vet att du har andra behov.
15. Rör runt muspekaren i TrueCrypt-fönstret i cirka 30 sekunder. Programmet utnyttjar rörelserna som en slumpgenerator som används vid krypteringen. Ju mer du rör musen, desto bättre. När du inte ids hålla på längre klickar du på "Format".
16. Nu skapas din krypterade enhet. Klicka på "Exit" när den är klar.

17. När du vill använda din enhet ska den först monteras. Gå in i TrueCrypt. I dialogrutans nedre del kan du bläddra fram den enhet du just skapat. I rutans övre del väljer du vilken enhetsbokstav den ska få. Vi väljer M:, men vad du väljer är egal. På Mac väljer du istället en siffra. Tryck på "Mount".



18. När du angett ditt lösenord kan du använda disken precis som en vanlig, lös disk eller partition på datorn. I vårt fall finns den i filhanteraren på PC som M:. På Mac finns den i "Finder" under "Enheter" som "NO NAME". Du kan nu flytta filer som ska krypteras till den nya enheten.
19. När du är färdig öppnar du TrueCrypt och väljer "Dismount". Nu stängs enheten och krypteras. Det enda som syns är en fil på skrivbordet, som inte går att öppna. Den filen kan du nu flytta eller byta namn på som vilken annan fil som helst. Du kan även lägga den på en dvd eller ett usb-minne och radera den från datorn.



Om du vill spara TrueCrypt-filer på en cd eller usb-pinne kommer filerna i sig inte att kunna öppnas. Det kan vara en fördel om du bara sparar ner filerna på en cd, som du sedan kan förvara i bokhyllan – som om det vore en ljudbok eller film.

Men om du vill ha dokumenten med dig när du är på resande fot, och kunna öppna dem på en annan dator behöver du använda TrueCrypts "Portable Mode". Då sparas också en uppsättning av programfilerna till det minne där du sparat dina data.

Du kan också kryptera hela din dator, och kräva ett lösenord när den startas. Det här är det säkraste alternativet – men också det mest riskfyllda, eftersom du inte kommer åt någonting alls, ifall du skulle glömma ditt lösenord.

Bitlocker

BitLocker finns inbyggt i de dyrare versionerna av Windows, Ultimate och Enterprise. Du kan kryptera allt eller bara en del, en partition, som du i så fall måste skapa själv först.

För att kryptera externa hårddiskar eller usb-minnen finns BitLockerToGo.

Krypteringen på datorn hanteras via en krets som kallas TPM, Trusted Platform Module. Om du inte har en dator med Ultimate- eller Enterpriseversionerna från början, bör du kolla att din dator har en TPM-krets innan du uppgraderar.

Det finns kritiker som hävdar att lösningen med TPM-kretsen har brister. Men jämfört med att inte ha någon kryptering alls kan det vara en enkel metod att komma igång.

Du aktiverar BitLocker genom att öppna "Kontrollpanelen" och välja "Bitlocker-diskkryptering".

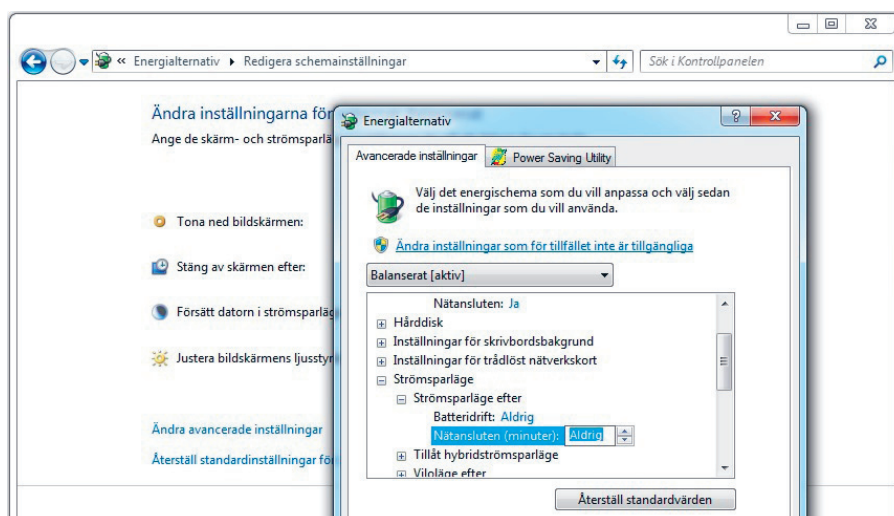
Om du bara har en enda disk på datorn kommer BitLocker att dela upp den i två delar, så kallade partitioner. På den ena finns systemprogrammen, som gör att datorn kan startas. På den andra kommer alla krypterade data att finnas.

Skapa ett starkt lösenord.

Du ska också skapa en återställningsnyckel. Om du glömmet ditt lösenord finns det möjlighet att återskapa din hårddisk om du gjort detta. Spara återställningsnyckeln genom att skriva ut den, eller på ett usb-minne som du förvarar på säker plats. Om du inte gör detta är datorn helt körd ifall du glömmet lösenordet.

När du startat om datorn fungerar allt i princip som vanligt. När datorn är upplåst är också alla filerna öppna.

Du bör ställa in att datorn inte tillåts att gå in i strömsparläge. Det är ett läge som "fryser" alla dina öppna program om du är inaktiv. Dessvärre finns möjlighet för angripare att komma åt ditt lösenord när den här proceduren används. Du ställer in vad datorn ska göra när du stänger av i "Kontrollpanelen", "Energialternativ", "Ändra inställningarna för strömsparläge" och därefter "Ändra avancerade inställningar". I listan väljer du "Strömsparläge" och väljer "Aldrig".



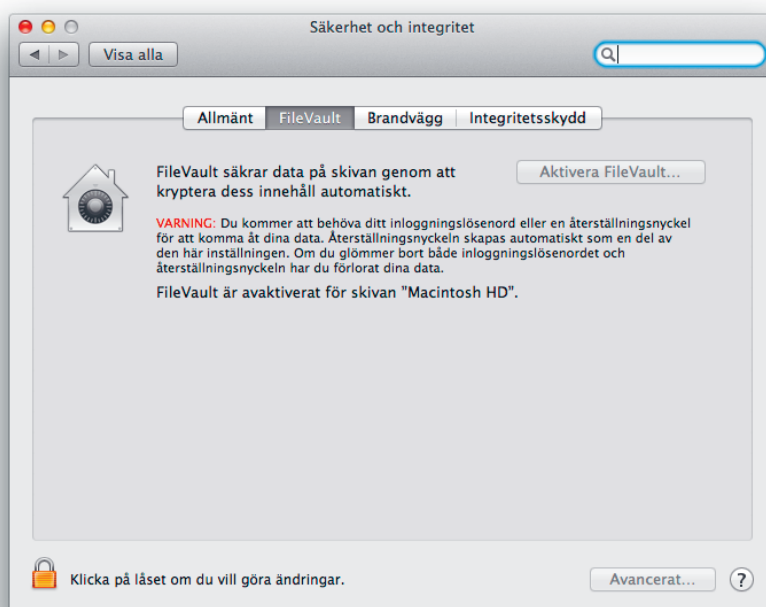
Filevault

Fulldiskkryptering via programmet FileVault finns inbyggt i moderna Macar. Precis som med BitLocker finns kritik mot svagheter, men om du tycker att det är krångligt att installera TrueCrypt är det bättre att du använder FileVault än att du inte har någon kryptering alls.

Aktivera krypteringen genom att gå in under "Systeminställningar" och väl "Säkerhet och integritet". Gå in under fliken "FileVault".

Klicka på låssymbolen för att kunna göra ändringar.

Klicka på "Aktivera FileVault".



Du får nu upp en ruta med en återställningsnyckel. Spara den på ett mycket säkert ställe. Nyckeln gör det möjligt att återställa datorn om du glömmet lösenordet. Men tappar du bort återställningsnyckeln är du helt körd.

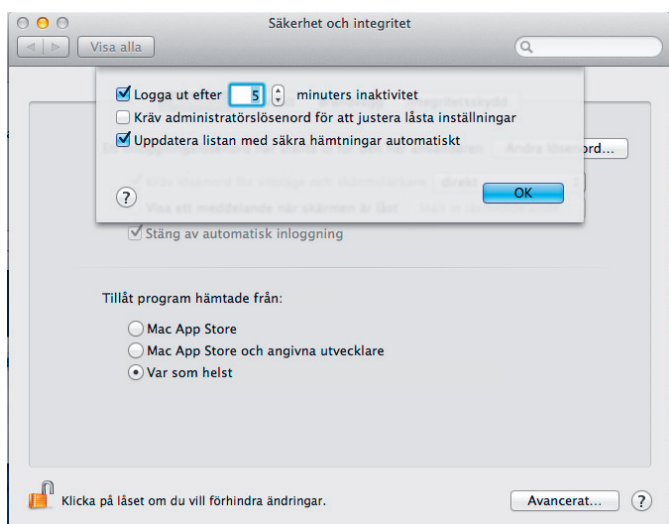
I nästa steg kan du välja att spara återställningsnyckeln hos Apple. Välj att inte göra det.

Om du inte redan tidigare angett ett lösenord kommer FileVault att tvinga dig att skapa ett. Lösenordet kommer att krävas varje gång du loggar in.

När alla data krypterats kommer du egentligen inte märka någonting, när du är inloggad kommer du åt alla dokument och program som vanligt.

Om du bara lämnar datorn kommer du dock inte bli utloggad, och om någon får tag i din dator har du ingen nytta av krypteringen. Du behöver därför också ställa in

att du ska bli utloggad när du lämnar datorn. Nere i högra hörnet klickar du på "Avancerat...". Ställ in en lämplig tid för att logga ut. Fem – tio minuter kan vara lagom.



Du kommer också åt denna inställning via "Systeminställningar", välj "Säkerhet och integritet" och fliken "Allmänt".

