Anders Thoresson

Kom igång med PGP!

Lär dig digitalt självförsvar!

Det här dokumentet om att komma igång med PGP är ett extramaterial som hör ihop med Internetguiden ”Digitalt självförsvar – en introduktion”. Det är en guide till ökad integritet och anonymisering på internet för privatpersoner. Innehållet kräver minimalt med förkunskaper. Hela boken, och mer extramaterial, finns att ladda ned kostnadsfritt här: www.iis.se/guider

Lär dig digitalt källskydd!

Det här dokumentet om att komma igång med PGP är ett extramaterial som hör ihop med Internetguiden ”Digitalt källskydd – en introduktion”. Det är en guide till ökat källskydd som riktar sig till journalister, arbetsledning och andra som arbetar redaktionellt. Innehållet är framtaget i samarbete med Svenska Journalistförbundet. Hela boken, och mer extramaterial, finns att ladda ned kostnadsfritt här: www.iis.se/guider

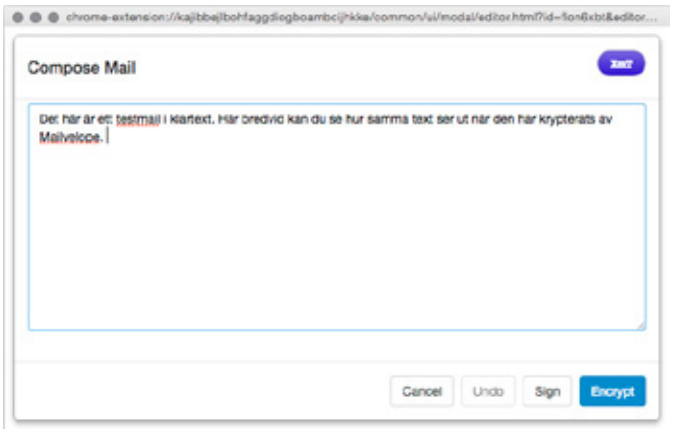
Det här lär du dig i XL-materialet

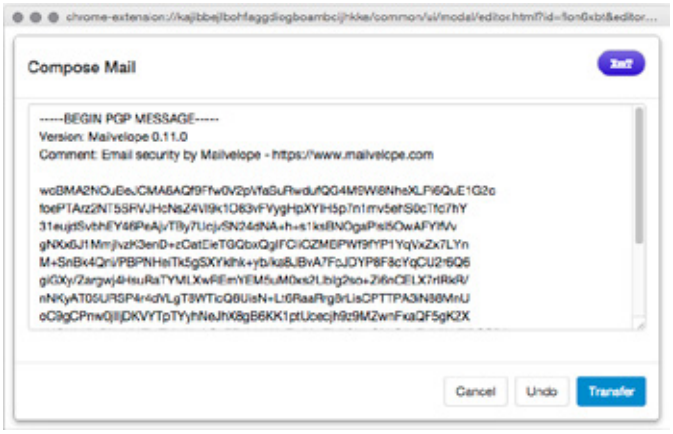
- Vad PGP är, hur det fungerar, varför det behövs och framför allt hur du kan använda tekniken för att kryptera e-post.
- Använda webbläsartillägget Mailvelope för att:
  - Skapa egna krypteringsnycklar
  - Skicka och ta emot krypterad e-post
  - Skicka ett första testmeddelande
- Hur du hittar krypteringsnycklar till personer du vill kommunicera med.
- Hur du hanterar dina egna nycklar på ett säkert sätt.
- Vett och etikett för krypterad e-post.

Problemet och lösningen

Kanske har du hört påståendet om att skicka e-post är som att skicka vykort? Precis så illa är det. Varför e-post kan läsas av många fler än sändare och mottagare går vi inte igenom här. Det här XL-materialet hoppar över bakgrunden och går direkt på lösningen: Kryptering.

Kryptering är ett sätt att skydda information från obehöriga. Genom kryptering görs innehållet i exempelvis e-post oläsligt. Istället för begripliga meningar återstår efter kryptering till synes slumpvis valda teckensekvenser som endast kan läsas av den som har tillgång till nyckeln.





Men det handlar givetvis inte om slumpen. För att skapa det krypterade innehållet i ett mejl förvrängs innehållet efter förutbestämda matematiska regler. Dessutom behövs det som kallas för *nyckel*. Varje person har sin egen uppsättning nycklar och det förvrängda resulatet är beroende *både* av de matematiska reglerna, den så kallade krypteringsalgoritmen, och nyckeln. Om samma mejl krypteras med två olika nycklar blir inte innehåller i den ”slumpvalda” teckensekvensen identisk.

En viktig grundprincip är att krypteringstekniken inte ska behöva vara hemlig för att skydda mot obehöriga ögon. Tvärtom. Den ska kunna vara offentlig och känd utan att det påverkar krypteringens säkerhet. Offentlig, öppen, teknik kan granskas och de med rätt kunskaper har därmed möjlighet att leta efter potentiella problem. Den personliga nyckeln, däremot, måste hållas hemlig.

För e-post är PGP ett av de mest spridda alternativen för kryptering, bland annat eftersom det uppfyller kravet på öppenhet. Det finns tusentals människor - experter och amatörer - som har och fortsätter granska koden som används i PGP-kryptering. Därmed vet vi att lösningen troligtvis inte innehåller några gömda dörrar genom vilka obehöriga kan ta sig in.

Det här är PGP

PGP har blivit den vanligaste lösningen för dem som vill skicka krypterad e-post. Hittills har vi pratat om att kryptering kräver en algoritm, det vill säga en matematisk regel för att förvränga texten, och en nyckel. Men i själva verket använder PGP två nycklar: Varje användare skapar en privat och en offentlig nyckel.

De två fungerar tillsammans och för att fortsätta på nyckelmetaforen går det att göra en liknelse med ett hänglås: Den offentliga nyckeln är då i själva verket hänglåset, medan den fysiska nyckel som låser upp låset motsvaras av användarens privata krypteringsnyckel. Du kan tänka på det som en nyckel som kan låsa, och en nyckel som kan öppna.

Finessen med den här lösningen är att den offentliga nyckeln inte behöver hållas hemlig. Om någon vill skicka dig ett hemligt meddelande i en fysisk låda kan du gå till järnhandeln och köpa ett nytt hänglås. Nycklarna behåller du själv, låset ger du till den person som vill kommunicera med dig. Hen skriver sitt meddelande, stoppar i lådan och låser den med hänglåset. Nu kan bara den som har nyckeln till låset – du – låsa upp den. När någon låser ett brev med just ditt hänglås är det bara du som kan öppna det. Inte ens den person som låst brevet kan öppna det igen.

Din offentliga PGP-nyckel kan du därmed sprida: Du kan publicera den på din webbplats, skicka den via e-post, ladda upp den till de sökbara databaser som kallas för nyckelservrar där det går att hitta offentliga nycklar till väldigt många av de internetanvändare som också utnyttjar PGP.

Din privata nyckel ska du däremot vårda riktigt ömt, precis som med nyckeln till det fysiska låset. Den som kommer över din privata nyckel kan nämligen med lite tur och skicklighet läsa e-post som det bara var tänkt att du skulle se. Din privata nyckel skyddas förvisso av ett lösenord, men den som kommer över din privata nyckel har all tid i världen på sig att försöka knäcka det.

Det innebär till exempel att du inte bör spara din privata nyckel i någon av nätets alla molntjänster. Du bör också skapa en säkerhetskopia av din privata nyckel. Skulle hårddisken i din dator krascha kan du annars aldrig mer läsa något av de mejl som är krypterat med din offentliga nyckel.

Kryptera med Mailvelope

Den som vill skicka krypterad e-post med PGP har flera olika programvaror att välja bland. För Windows är GPG4Win en av de mest använda, för Mac GPGTools. I båda fallen är det program som fungerar som komplement till ett befintligt e-postprogram, som Thunderbird eller Outlook.

I det är XL-materialet kommer vi använda Mailvelope, ett plugin till webbläsarna Chrome och Firefox. Den främsta anledningen är att det är snabbare att komma igång med och fungerar med de vanligaste nättjänsterna för e-post, som exempelvis Gmail och Outlook. Detta är tjänster som många använder eller där det är lätt att skapa ett nytt konto om man behöver skicka krypterad e-post från en annan adress än exempelvis jobbmejlen.

Mailvelope fick också höga betyg när den amerikanska medborgarrättsorganisationen EFF publicerade en säkerhetsgenomgång av tjänster som påstår sig erbjuda säker kommunikation[1].

Den stora nackdelen med Mailvelope är att det idagsläget inte går att kryptera bilagor utan bara innehållet i mejlet. Men om det är text du ska bifoga, exempelvis en Wordfil, kan du ju alltid kopiera texten från filen och inkludera det i mailet - istället för att bifoga filen.

Behöver du kunna skicka krypterade bilagor måste du därför installera antingen GPG4Mail[2], Enigmail[3] och Thunderbird[4] (om du kör Windows) eller GPGTools[5] (om du kör Mac).

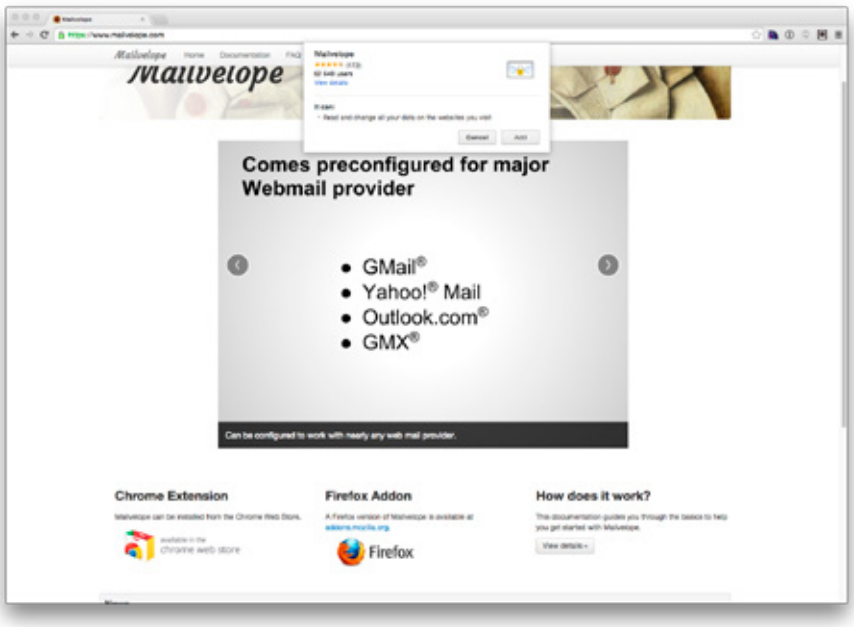
PGP för mer än e-post

Även om e-post är det vanligaste användningsområdet för PGP finns det inget som hindrar att du krypterar andra filer också. Källmaterial som du lägger på ett USB-minne kan exempelvis krypteras med din offentliga nyckel. På så vis är det bara du som kan låsa upp innehållet.

Vill du på detta sätt kryptera annat än e-post bör du installera ett PGP-program i din dator istället för att använda Mailvelope.

Om du inte redan har Chrome eller Firefox, installera någon av de två webbläsarna i din dator.

Installera sedan tillägget för Mailvelope, genom att klicka på antingen Chromes eller Firefox ikon på www.mailvelope.com.



Installera inte PGP på en dator du delar med andra

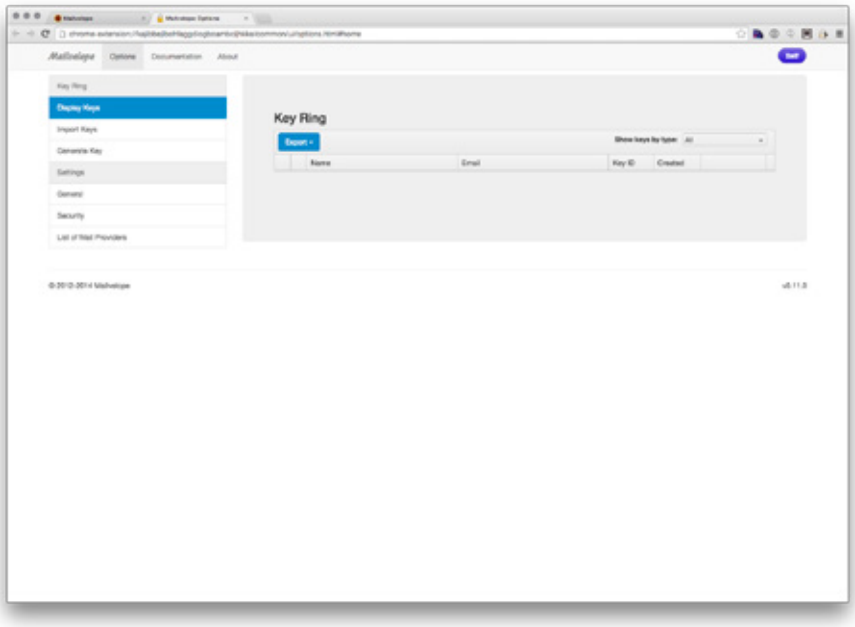
Eftersom din privata nyckel kommer att sparas på datorn där du installerar Mailvelope ska du helst inte göra det här på en dator som du delar med någon annan. Och absolut inte på en dator som står exempelvis på ditt bibliotek.

I webbläsarens verktygsfält dyker då en ny ikon upp, ett hänglås med en svart nyckel bredvid.

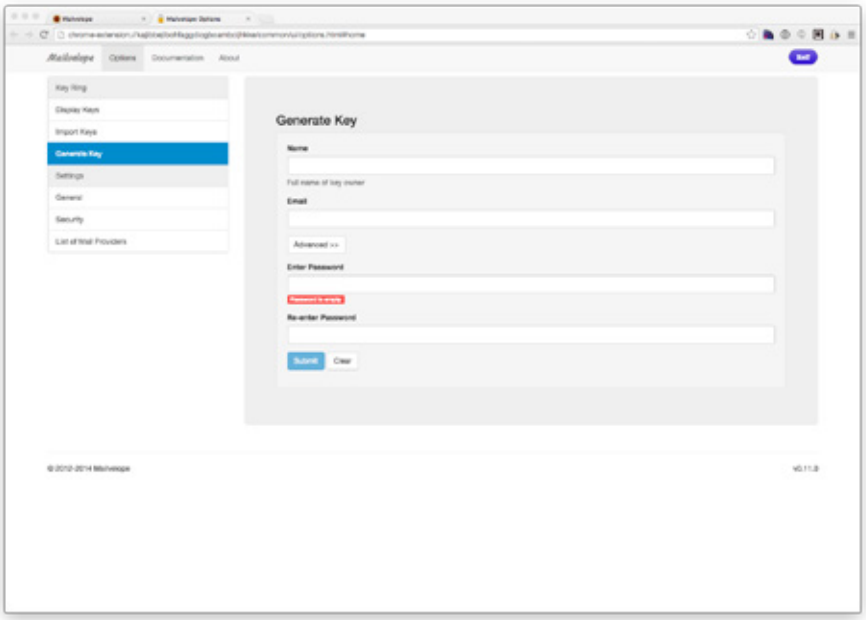
Skapa dina nycklar

När Mailvelope är installerat är det första du behöver göra att skapa ditt eget nyckelpar: En privat som du ska behålla för dig själv och en offentlig som andra använder för att skicka krypterade mejl till dig.

Klicka på Mailvelope-ikonen och välj *Options*. Du kommer då till inställningarna för Mailvelope.



I menyn till vänster väljer du *Generate key*.

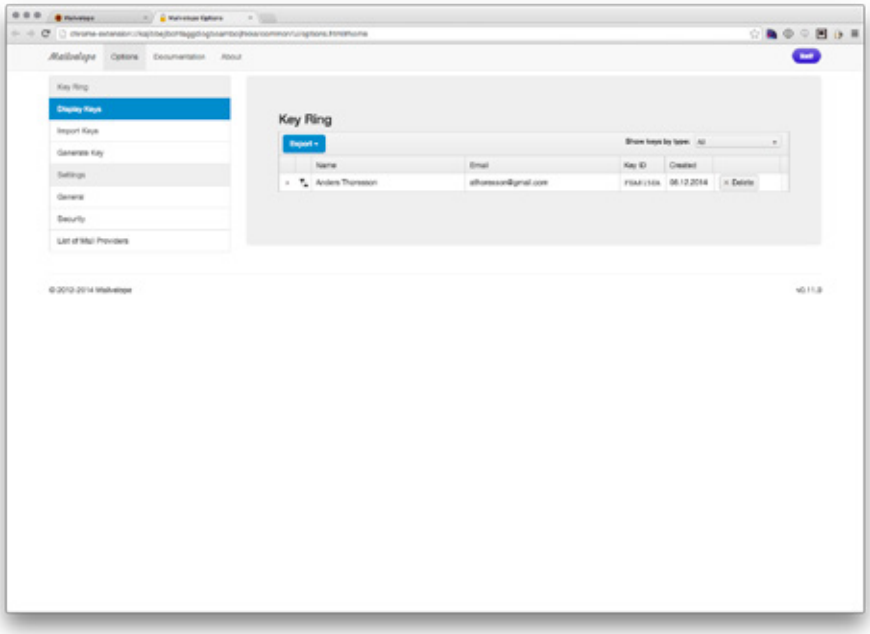


Här fyller du i ditt namn och din e-postadress. E-postadressen ska vara kopplad till någon av e-posttjänsterna som finns på nätet och som går att använda med Mailvelope, till exempel Gmail eller Yahoo Mail.

Du ska också mata in ett lösenord. Här är det viktigt att du väljer ett långt och svårt. Skulle någon komma över din privata nyckel och krypterade mejl som skickats till dig är det nämligen bara lösenordet som förhindrar den personen från att läsa e-post som bara var tänkt att du skulle se.

Under *Advanced* kan du välja vilken krypteringsalgoritm din nyckel ska använda, men standardinställningarna här duger bra.

Efter en stund ska du få ett meddelande om att nycklarna har skapats. Väljer du *Display keys* i menyn till vänster är din *key ring*, din samling med PGP-nycklar, inte längre tom: Där finns ditt alldeles färska nyckelpar.



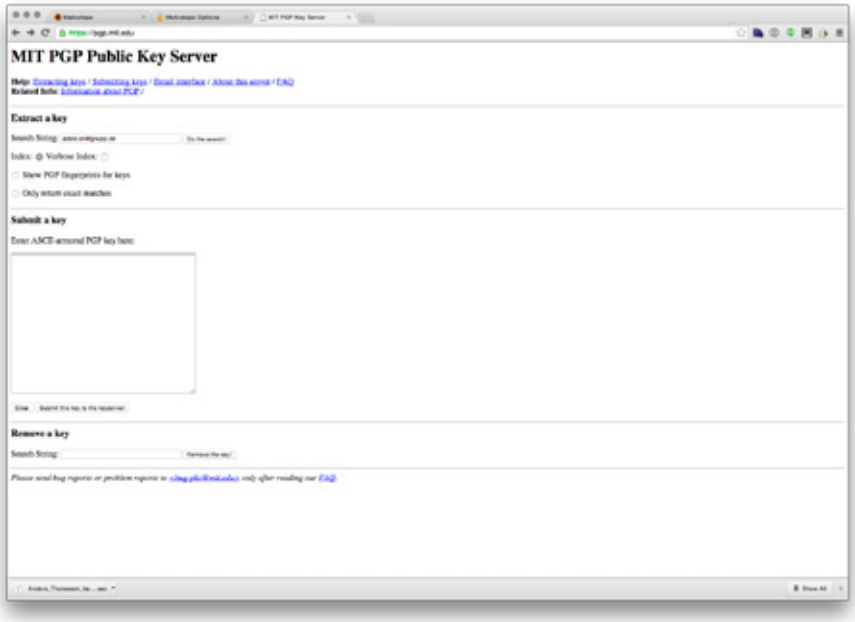
Nästa steg är att göra en kopia på dina nycklar. Om du hoppar över det här steget och du tappar bort din privata nyckel, till exempel på grund av att datorns hårddisk kraschar, kommer du inte längre kunna läsa krypterad e-post som skickas till dig.

Markera först ditt nyckelpar genom att klicka på det. Därefter väljer du Export, precis ovanför nyckeln och slutligen *Display key pair*. Upp dyker en ruta som innehåller en lång teckensekvens som inleds med texten -----*BEGIN PGP PUBLIC KEY BLOCK*-----. En bit ned ska det stå -----*BEGIN PGP PRIVATE KEY BLOCK*-----. Kopiera texten och klistra in i en textfil som du sedan sparar på ett säkert ställe, förslagsvis ett usb-minne som du sedan lägger på en plats där ingen kan hitta det.

Testa dina nycklar – skicka ditt första krypterade mejl

När du nu skapat och säkerhetskopierat ditt eget nyckelpar är du redo för att skicka och ta emot krypterad och signerad e-post. Ett första test kan du skicka till *adele-en@gnupp.de*. På den adressen finns ett datorprogram som skickar krypterade svar på test-mejl. För att kunna utföra testet behöver du först lägga till Adeles offentliga nyckel i din nyckelring.

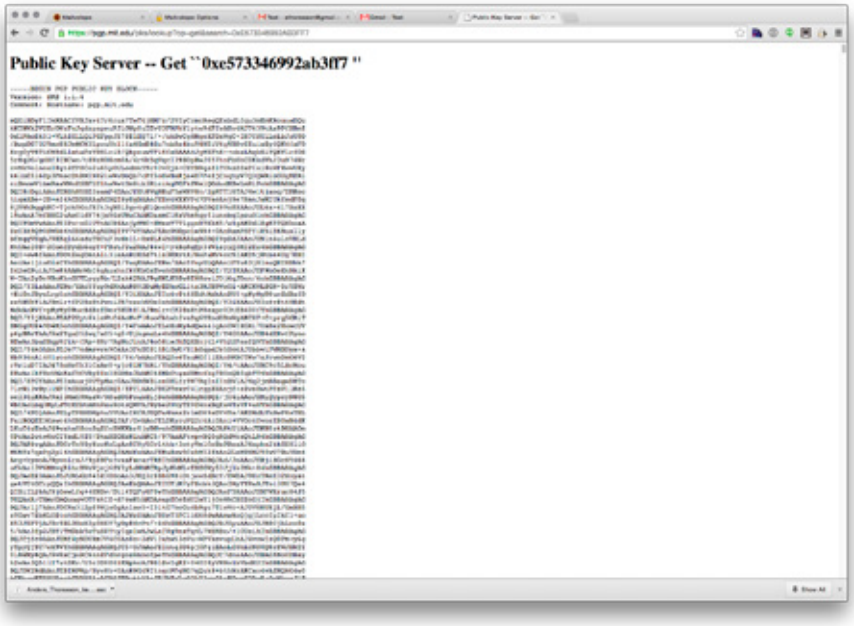
Öppna en ny flik i din webbläsare. Surfa till *pgp.mit.edu* som är en av de största så kallade nyckelservrarna, databaserna med offentliga PGP-nycklar, och skriv in *adele-en@gnupp.de* i sökfältet.



I träfflistan klickar du på nyckel-id:t för den nedersta träffen. Du ska då komma till en sida som påminner om din egen offentliga nyckel, en lång teckensekvens som inleds med texten -----*BEGIN PGP PUBLIC KEY BLOCK*-----.

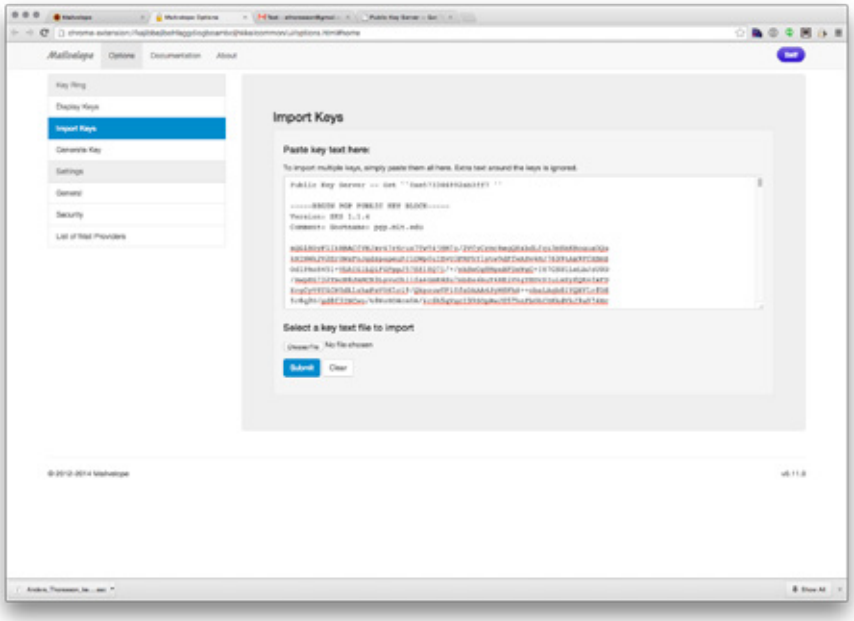
Globala nyckelservrar

Det finns flera nyckelservrar som du kan använda. De kopierar nycklar mellan varandra så att de alltid är uppdaterade. Exempel på andra ”adressregister” för publika PGP-nycklar är keyserver.pgp.com och keyserver.ubuntu.com



Kopiera texten från webbsidan och växla tillbaka till fliken med din nyckelring i din webbläsare.

Klicka på *Import keys* och klistra in Adeles offentliga nyckel i rutan. Därefter *Submit*.

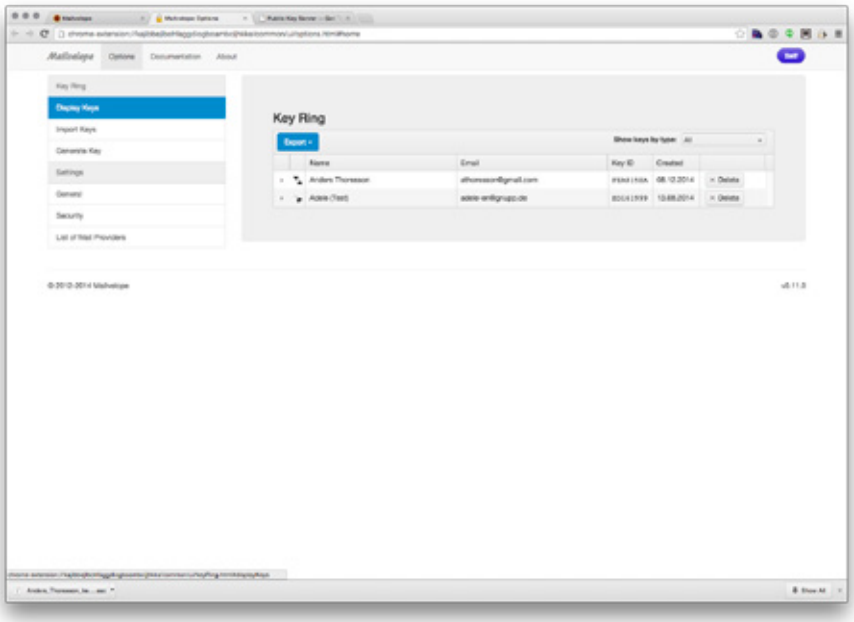


Om allt fungerade ska det dyka upp en grön ruta som bekräftar att Adeles offentliga nyckel nu är tillagd i din nyckelring.

Bra! Eftersom du nu har Adeles offentliga nyckel kan du skicka ett krypterat mejl som bara Adele kan läsa, eftersom det bara är hon som har den privata nyckel som behövs för att låsa upp det.

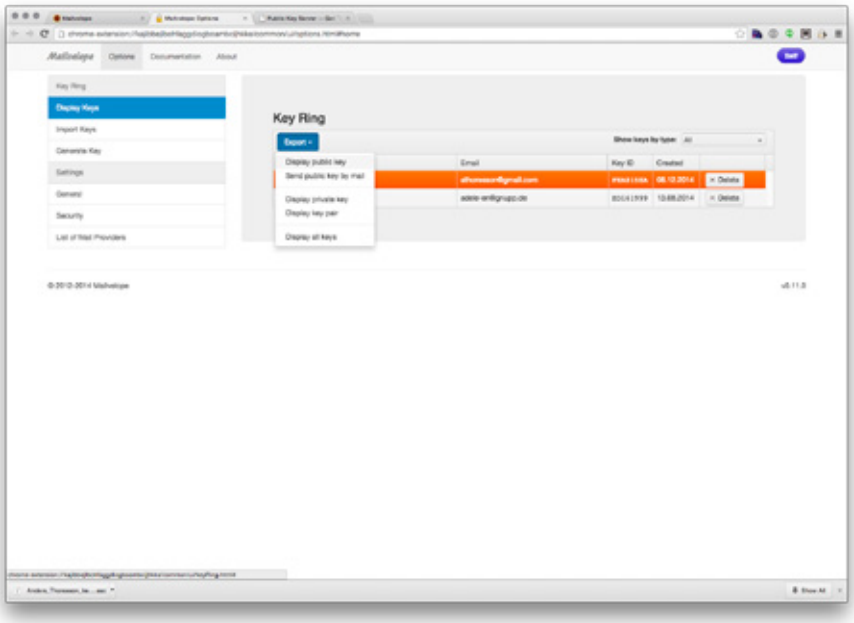
Men för att Adele ska kunna skicka ett krypterat svar tillbaka till dig måste hon få din offentliga nyckel. Eftersom du inte har publicerat den på någon nyckelserver än kan programmet inte på egen hand leta upp den. Däremot kan du själv skicka med din offentliga nyckel i testmejlet som du strax ska skicka. Detta bör du alltid göra då du skickar krypterade mejl, så att mottagaren enkelt kan svara dig krypterat.

Gå tillbaka till din nyckelring genom att klicka på *Display keys*. Tabellen ska nu innehålla två rader. En med ditt nyckelpar och en med Adeles offentliga nyckel.



Som du ser skiljer sig ikonerna i början på de två raderna åt. Ditt nyckelpar illustreras av två nycklar, Adeles offentliga av endast en nyckel.

Markera nu din nyckel, klicka på *Export* och välj *Display public key*.



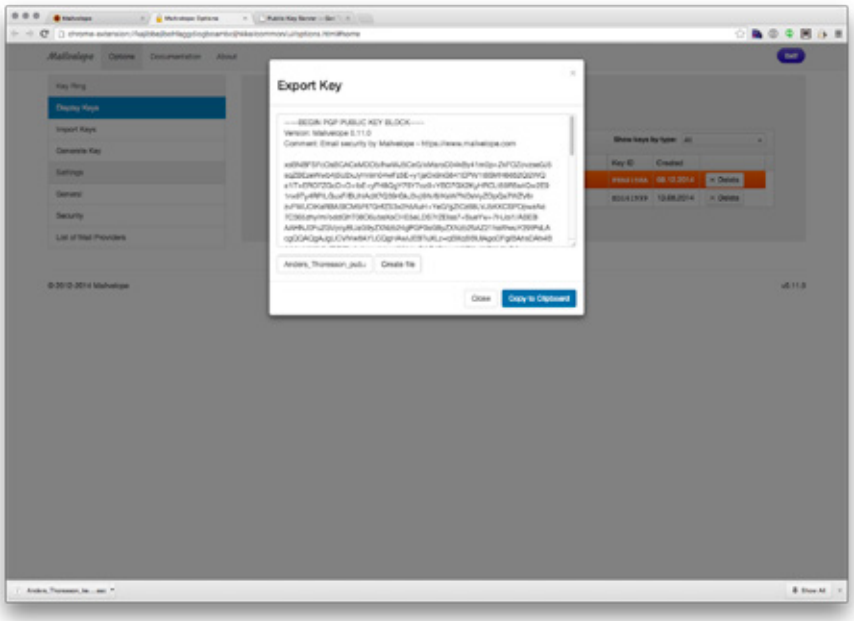
Observera att det här är ett kritiskt ögonblick! Välj inte *Display private key*! Din privata nyckel ska du aldrig skicka till någon annan. De som ska kommunicera med dig ska ha din offentliga nyckel, ingen annan.

Vi påminner en sista gång: Var noggrann och uppmärksam, skicka aldrig din privata nyckel!

Kom ihåg – din privata nyckel är privat!

Vi påminner en sista gång: Var noggrann och uppmärksam, skicka aldrig din privata nyckel!

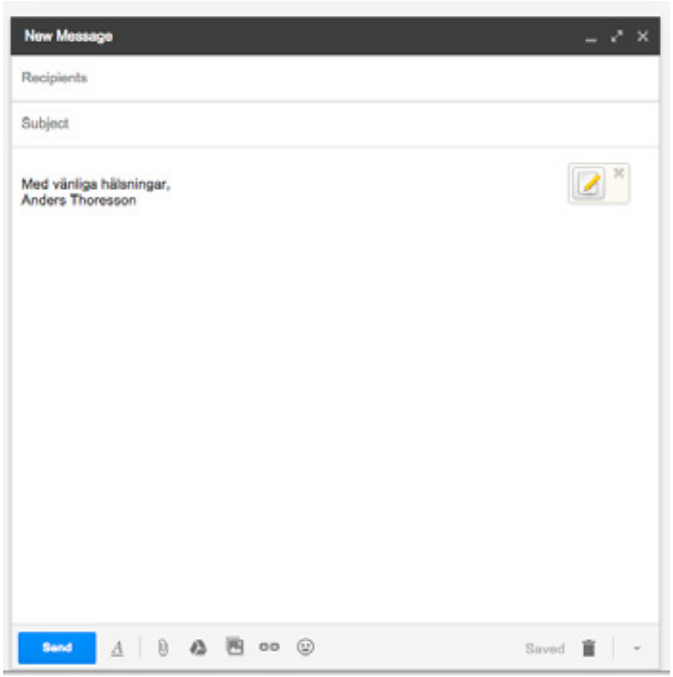
När du klickar på *Display public key* dyker en ny ruta upp.



Klicka på *Copy* to *Clipboard*.

Därefter öppnar du en ny flik i webbläsaren och loggar in på den e-posttjänst som du kopplat till din PGP-nyckel, det vill säga den adress som du angav när du skapade ditt nyckelpar.

Klicka på knappen för att skriva ett nytt mejl. I fönstret där du skriver ditt mejl ska en ny ikon nu finnas, ett papper med en penna.



Skriv först in *adele-en@gnupp.de* som mottagare och klicka sedan på den nya ikonen. Då öppnar sig ett nytt fönster där du skriver in texten som ska krypteras. Detta är återigen ett kritiskt ögonblick!

De flesta e-posttjänster har en funktion som automatiskt sparar utkast medan du skriver dina mejl. Detta är en funktion som finns till för att underlätta för dig som användare. Om du råkar stänga ner webbläsaren eller klicka på en knapp som tar dig till en annan webbsida kan du logga in igen och fortsätta skriva där du var. Alternativet hade varit att börja om från början.

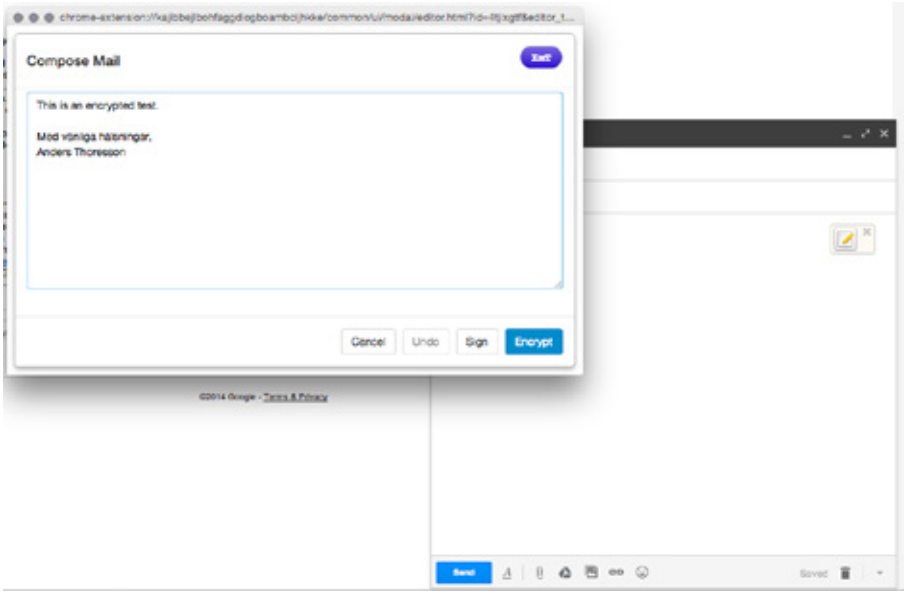
Men i just det här fallet är funktionen problematisk, eftersom utkasten sparas i klartext på mejltjänstens servrar. Ofta blir de dessutom kvar, även efter det att du skickat ditt mejl.

Av denna anledning har Mailvelope ett eget fönster där du skriver ditt mejl, och så länge du skriver där finns texten bara på din egen dator.

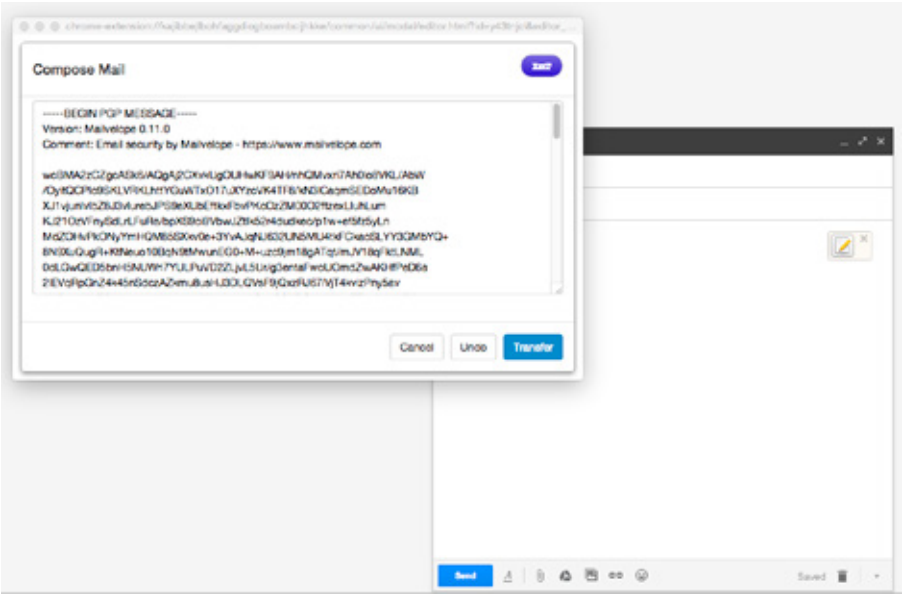
Skriv bara i Mailvelopes eget fönster

När du ska skriva ett mejl som ska krypteras, använd aldrig din e-posttjänsts eget fönster. Klicka istället alltid på ikonen som öppnar Mailvelopes fönster!

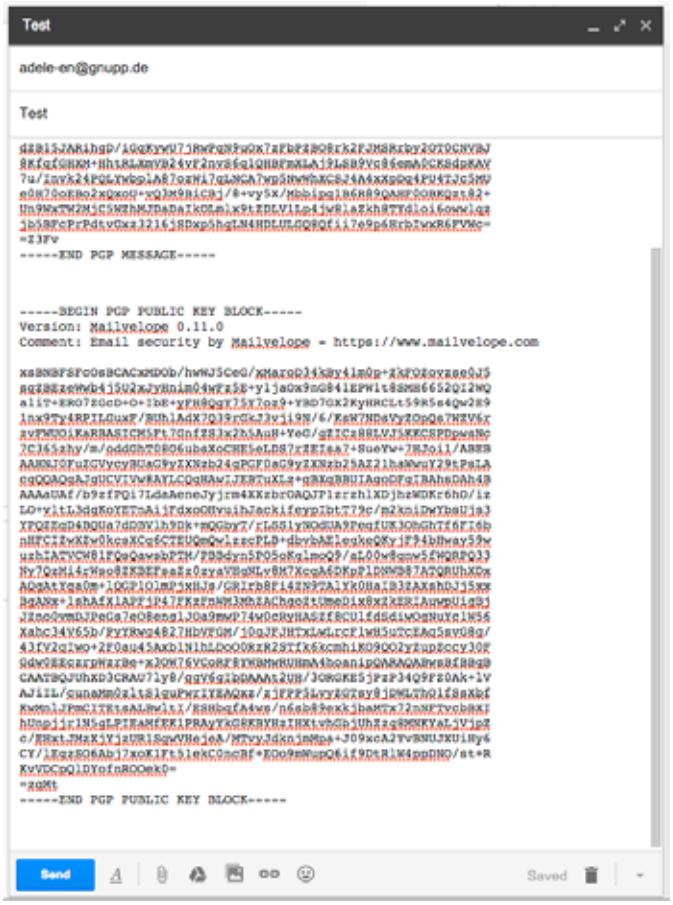
Eftersom det bara handlar om ett testmejl som ska besvaras av ett datorprogram spelar det ingen roll vad du skriver.



När du är klar klickar du på *Encrypt*. I den nya rutan som dyker upp väljer du *adele-en@gnupp.de* ur listan överst, klickar på *Add* och därefter på *Ok*. När rutan försvinner har innehållet i ditt mejl krypterats. Med ett klick på *Transfer* kopierar du det till e-posttjänstens fönster.

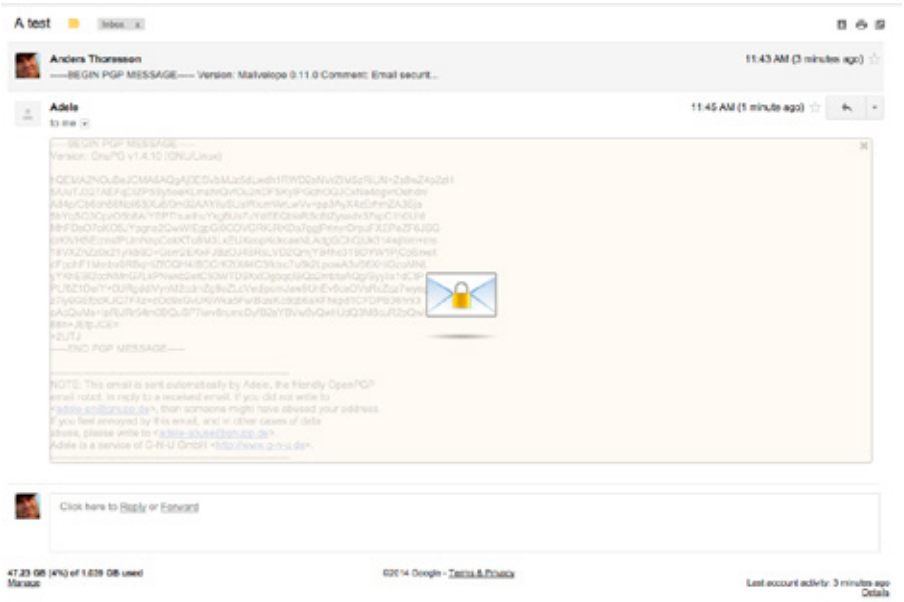


Nu kopieras ditt krypterade innehåll in i mejltjänstens ruta. Under det krypterade textblocket ska du placera muspekaren och klistra in din offentliga nyckel.

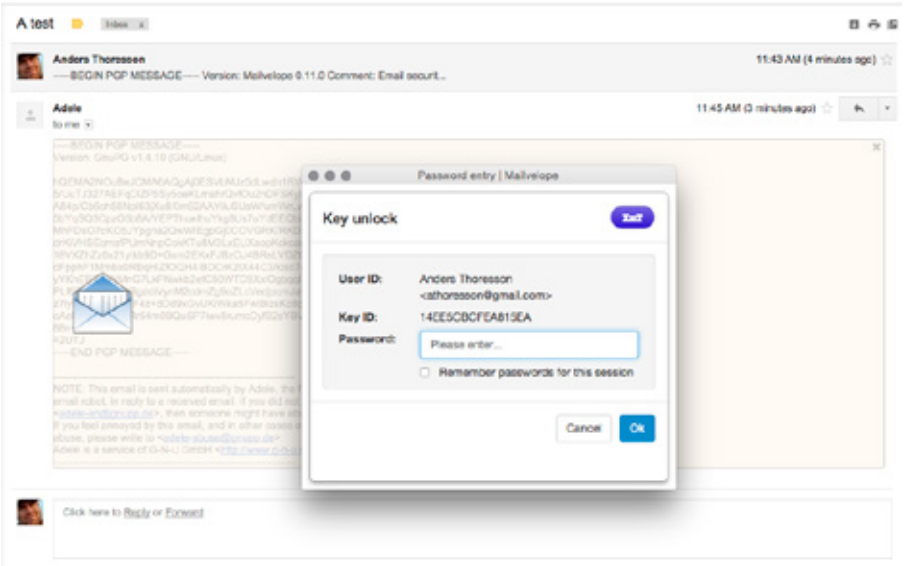


Med ett klick på *Send* skickar du sedan ditt krypterade meddelande och din offentliga nyckel till Adele. Efter en liten stunds väntan ska ett svar att dyka upp i din inkorg. Har du gjort rätt är det ett krypterat mejl från Adele, har du gjort fel innehåller det instruktioner om vad det var som gick galet.

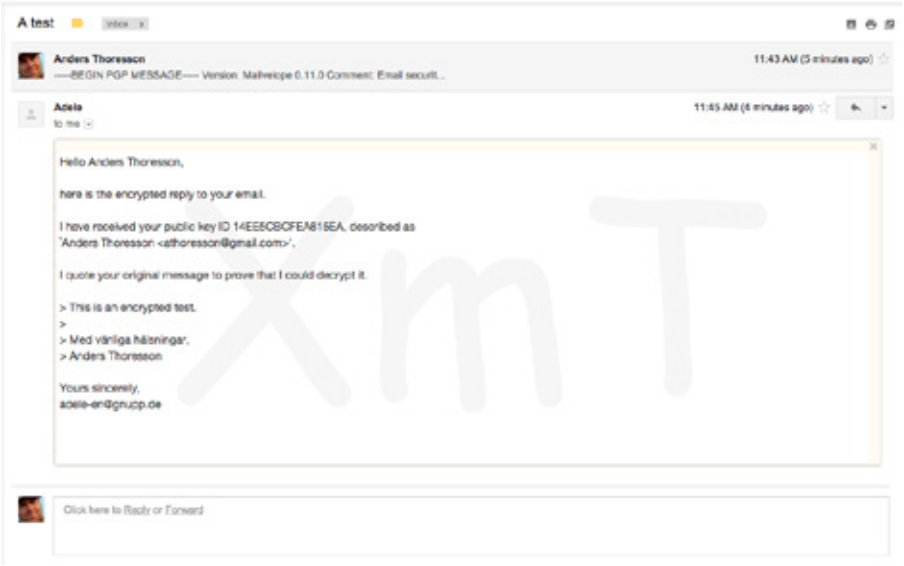
Mailvelope känner av att det rör sig om ett krypterat mejl och lägger en transparent platta med ett kuvert över innehållet.



Klicka på det låsta kuvertet och upp dyker en ruta där du ska mata in ditt lösenord för din privata nyckel.



Nu visas svaret från Adele i klartext.



Men bara så länge du inte gör något annat. Klickar du på en knapp eller stänger fliken för att sedan återvända till mejlet kommer du behöva låsa upp det med ditt lösenord igen. Och så ska det vara. Ett mejl som skickades krypterat bör aldrig sparas i klartext eftersom sändaren uppenbarligen gjort sitt yttersta för att bara du ska läsa det.

Bokstäverna i bakgrunden

I bakgrunden av klartextmeddelandet står det XmT. Det här är tre tecken som slumpas fram när du installerar Mailvelope. Därmed är sannolikheten stor att du har tre andra tecken.

De tre bokstäverna är en säkerhetsfunktion som Mailvelope visar på många av sina sidor i din webbläsare. Du kan gå till *Options* i Mailvelopes inställningar och där välja *Security* för att se vilka tre tecken och vilken ”säkerhetsfärg” som slumpades fram åt dig.

De övriga säkerhetsinställningarna kan du lämna som de är. Och valet *Where do you want to compose your mail?* bör du absolut inte ändra!

Publicera din offentliga nyckel

När du nu vet hur du ska göra för att skicka och ta emot krypterad e-post är det dags att publicera din offentliga nyckel. Hur du gör beror på hur du tänkt använda din nyckel. Om du bara ska kommunicera med en eller några utvalda personer kan du skicka den direkt till dem.

Om du vill att vem som helst ska kunna skicka krypterad e-post till dig kan du publicera din offentliga nyckel på din egen webbplats, om du har en, eller ladda upp den till nyckelservern där du hittade Adeles nyckel, https://pgp.mit.edu. Nyckelservern är som en adressbok för dig och alla andra PGP-användare. En bit ned på sidan finns en stor ruta med rubriken *Submit a key*. Här klistrar du in din *offentliga* (inte privata) nyckel och klickar på *Submit this key to the keyserver*.

Alla som söker efter det namn eller den e-postadress som du matat in när du skapade ditt nyckelpar kommer nu att hitta din offentliga nyckel.

Importera och verifiera andras nycklar

En viktig del i användningen av PGP är att verifiera att du verkligen använder en offentlig nyckel som hör till den personen som du kommunicerar med.

Om du ska skicka ett krypterat mejl till Alice måste du veta att det verkligen är hennes offentliga nyckel som du använder. Annars kommer du skicka ett krypterat mejl som inte hon men någon annan kan avkryptera.

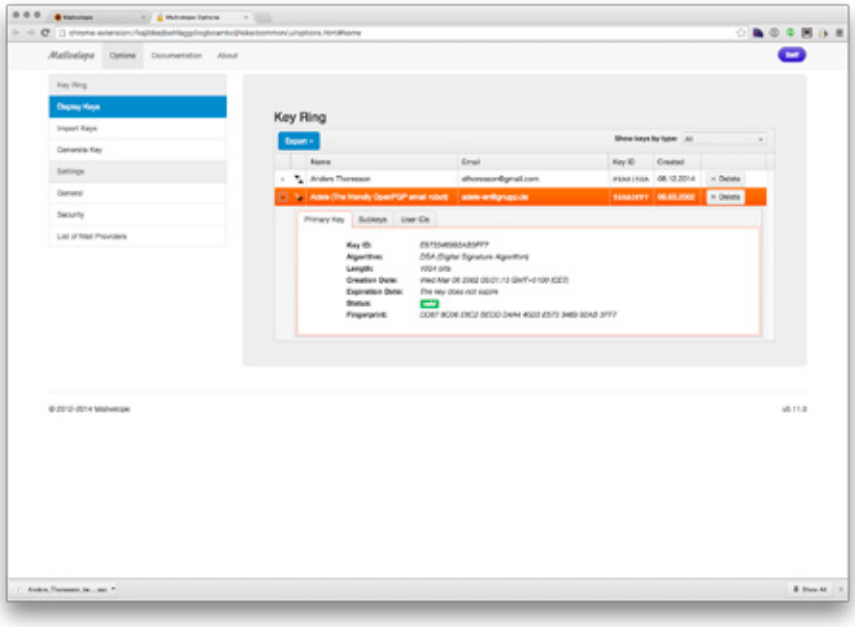
Innan du kan använda en annan persons offentliga nyckel måste du säkerställa att den verkligen hör till den personen som du tror. Vi kan återvända till liknelsen med det fysiska hänglåset för att förstå varför:

Alice skickar ett hänglås till Bob för att han ska kunna låsa in sitt hemliga brev i en låda och skicka till henne. Men på vägen sitter Charlie. Han byter ut hänglåset Alice köpte och skickar istället sitt eget lås till Bob. När Bob skrivit sitt brev och lagt i den låsta lådan snappar Charlie upp den, låser upp låset (som ju är det han köpte och som han därför har nyckeln till), läser brevet och låser sedan lådan igen, den här gången med det lås som Alice från början skickade till Bob.

Om Bob innan han låste in sitt brev hade ringt Alice och frågat om låset hon skickade var grönt hade han fått reda på att låset hon köpte i själva verket var rött. Charlies avlyssningsförsök hade därmed avslöjats.

För att kontrollera att vems en PGP-nyckel är finns något som kallas för fingeravtryck.

Öppna Mailvelopes *Options* igen och klicka på den lilla pilen framför Adeles offentliga nyckel. Då öppnas en ruta med detaljer om nyckeln.

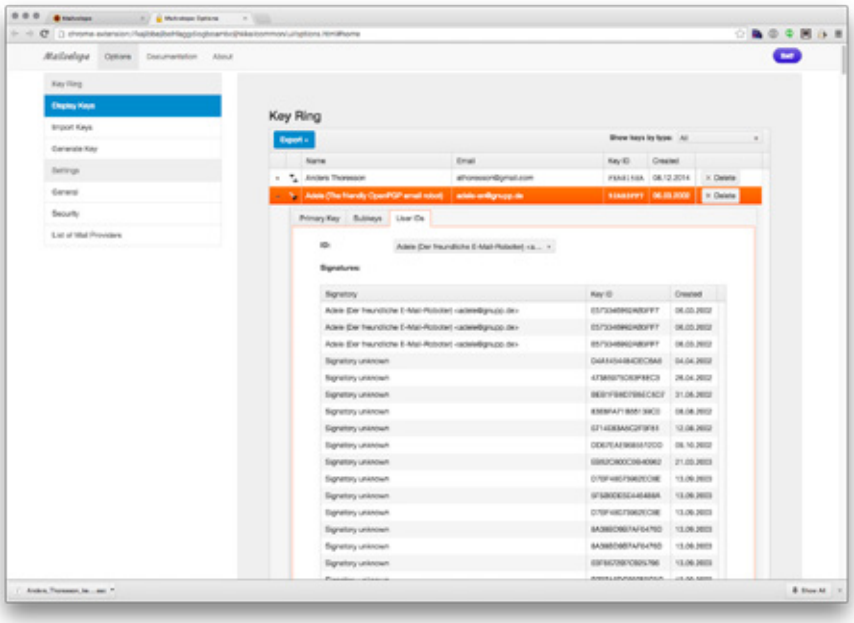


Längst ned finns Adeles fingeravtryck, en sekvens med 40 tecken uppdelade i grupper om fyra. Tanken är att det här fingeravtrycket kan användas för att verifiera att nyckeln hör till personen du vill kommunicera med. Hen kontrollerar fingeravtrycket för sin privata nyckel och skickar det till dig så att du kan jämföra med den offentliga nyckel du importerat till din nyckelring.

Den här kontrollen bör *inte* göras via e-post, eftersom en person som skapat en falsk nyckel i någon annans namn då kan skicka ett falskt fingeravtryck som matchar. Istället bör en annan kanal användas: Ett telefonsamtal, ett sms eller ett fysiskt brev, allt beroende på vilka omständigheter som passar bäst.

För att underlätta den här processen finns det även en möjlighet att signera andra användares nycklar, och låta tilltron på så viss sprida sig i systemet. Om du redan har bekräftat att du har Alice offentliga nyckel och sedan importerar en ny nyckel som Alice har signerat kan du sannolikt lita på att den stämmer. Förutsatt att du litar på Alice, vill säga.

Under fliken *User IDs* kan du se vem som signerat en nyckel.



Digitala signaturer

Lösningen med en offentlig och en privat nyckel innebär inte bara att det går att skicka krypterad e-post. Nyckelparet kan dessutom användas för att bekräfta vem avsändaren är. Genom att lägga till en *digital signatur* med hjälp av din privata nyckel kan alla som har din offentliga verifiera att det verkligen är du som har skrivit ett visst mejl.

Den digitala signaturen räknas fram utifrån krypteringsmetodens algoritmer, den privata nyckeln och innehållet i mejlet. Därmed innebär signaturen inte bara att det går att verifiera vem avsändaren är utan också att innehållet i mejlet inte manipulerats på vägen. Om texten ändrats kommer PGP varna för att signaturen inte är giltig.

Det går också att kombinera de två tillämpningarna. Du kan skicka ett mejl som är krypterat med hjälp av mottagarens offentliga nyckel samtidigt som du signerar det med hjälp av din egen privata nyckel.

Det här gör (inte) PGP

PGP krypterar innehållet i ett mejl och/eller verifierar vem det är som har skrivit det.

Däremot krypteras inte ärenderaden, eller vem som skickat mejlet och vilka som står som mottagare. PGP skyddar därmed bara *innehållet* i en kommunikation, men däremot döljs inte *vilka* som kommunicerar med varandra och inte heller om *vad* (om det står i ärenderaden). Detta är extremt viktigt att tänka på, då det ibland inte spelar roll vad som står i mejlet - det räcker med att veta att ett mejl har skickats.

PGP:s två nyckeltyper

PGP bygger på en krypteringsteknik som kallas för *public key cryptography*. Det innebär att varje användare skapar två nycklar, en privat och en offentlig.

- Med en annan användares offentliga nyckel kan du skicka krypterade meddelanden till hen eller verifiera att det verkligen är hen som skickat ett signerat mejl. Din offentliga nyckel kan du dela med dig av till andra.
- Med din privata nyckel kan du avkryptera mejl som någon skickar till dig eller signera e-post som du skickar. En privat nyckel måste hållas hemlig och skyddas av ett lösenord för att någon som ändå kommer över den inte ska kunna använda den.

Nycklarna i PGP är långa teckensekvenser som sparas som vanliga textfiler på datorns hårddisk. En offentlig PGP-nyckel inleds med texten BEGIN PGP PUBLIC KEY BLOCK medan en privat nyckel inleds med BEGIN PGP PRIVATE KEY BLOCK. Dessa två meningar är det enda som för ögat skiljer en privat nyckel från en offentlig. Var därför noga när du ska skicka någon din offentliga nyckel – välj inte fel bara för att du har bråttom eller slarvar!

PGP eller GPG

Förkortningen PGP står för *Pretty Good Privacy* och är namnet på det program som Phil Zimmermann utvecklade i början av 1990-talet. Idag är PGP ett varumärke som ägs av säkerhetsföretaget Symantec.

Det finns också en öppen standard med namnet OpenPGP som beskriver hur PGP fungerar. Symantecs produkter följer den standarden, men det gör även programmet GnuPG, som förkortas GPG. GPG finns till bland annat Windows, Mac och Linux.

God PGP-etik

När du börjar skicka krypterad e-post finns det lite etikettsregler att förhålla sig till:

- Om du fått ett krypterat mejl, svara inte utan att kryptera. Om personen som kontaktade dig bedömer att mejlet bör vara krypterat är du inte rätt person att göra en annan bedömning.
- Av samma anledning, spara aldrig ett krypterat mejl i klartext på din dator eller i din e-posttjänst.
- Tänk på att PGP bara krypterar innehållet i ett mejl. Fortfarande kan andra se vem som skickat mejl, vilka mottagarna är och vad som står i ärenderaden. Inte heller är det säkert att bifogade filer är krypterade.

Datorns säkerhet påverkar PGP

Att myndigheter och andra inte kan knäcka krypteringen i ett mejl som krypterats med PGP behöver tyvärr inte innebära att de inte kan läsa det. Genom att först rikta andra attacker mot en dator kan de exempelvis lyckas installera en tangentbordslogger som spelar in allt som skrivs på tangentbordet, inklusive lösenordet till den privata nyckeln. Och har någon väl kommit in i datorn kan de också komma över den privata nyckeln.

För säker kommunikation räcker det därför inte med PGP utan också att du gör ditt bästa för att hålla datorn så säker som möjligt.

Som när det gäller alla säkerhetsrelaterade frågor som rör din datoranvändning: Håll dig och dina program uppdaterade. I det här fallet, se till att du alltid använder den senaste versionen av Mailvelope och din webbläsare. Men också att du uppdaterar ditt operativsystem, kör ett antivirusprogram och så vidare. På så sätt minskar du risken för att drabbas av ett säkerhetshål i något av programmen.

Följ också Mailvelopes blogg på (https://www.mailvelope.com/blog) och twitterkonto @mailvelope för att hänga med i utvecklingen av programmet.

[1] Secure Messaging Scorecard – (https://www.eff.org/secure-messaging-scorecard)
[2] GPG4Win – (http://www.gpg4win.org)
[3] Enigmail – (https://www.enigmail.net)
[4] Thunderbird – (https://www.mozilla.org/thunderbird/)
[5] GPGTools – (https://gpgtools.org)

Kom igång med PGP!
Version 1.0 2015
Anders Thoresson

.SE klimatkompenserar för sina koldioxidutsläpp och stödjer klimatinitiativet ZeroMission. Se www.zeromission.se för mer information om ZeroMission.

Författare: Anders Thoresson
Redaktör: Hasse Nilsson
Projektledare: Jessica Bäck
Formgivning: Bedow
Första upplagan.

Alla .SE:s Internetguider
Du hittar alla .SE:s utgivna Internetguider och XL-material på www.iis.se/guider. Du kan beställa en prenumeration på nyutgivna guider genom att skicka namn och adress till publikationer@iis.se

Varje ny .se-adress bidrar till utvecklingen av internet
.SE (Stiftelsen för internetinfrastruktur) ansvarar för internets svenska toppdomän och administrerar registreringen av domännamn under .se. Överskottet från registreringsavgifterna för domännamn investeras i internetutveckling som gagnar alla internetanvändare, bland annat den här XL-materialet!

Organisationsnummer: 802405-0190
Besöksadress: Ringvägen 100 A, 9 tr, Stockholm
Brevledes på .SE Box 7399, 103 91 Stockholm
Telefon: +46 8 452 35 00. Fax: +46 8 452 35 02
E-post: info@iis.se www.iis.se