Instruktion för kryptering och signering av e-post

Innehållsförteckning

1. Inledning

För att skicka och ta emot säker epost gäller det att breven skyddas hela vägen från avsändare till mottagare. Kryptering kan användas för att skydda innehållet mot obehörig läsning. Meddelandet krypteras så att bara rätt mottagare kan avkryptera det och ta del av innehållet.
Kryptoteknik kan också användas för signering, så att mottagaren får en bekräftelse på att brevet kommer från rätt avsändare och inte har förvanskats på vägen. Kryptering och signering kan användas ihop.

Två olika standarder används i praktiken för epost-kryptering/signering:

- *S/MIME* bygger på en mera centraliserad säkerhetsmodell, där användarna förutsätt ha certifikat (liknande de som används för SSL/TLS) utfärdade av en betrodd instans.
- *OpenPGP* är från början tänkt för en distribuerad säkerhetsmodell, där användare A som känner användare B intygar att användare B är OK, osv. Man pratar om "web of trust", och så kallade nyckelservrar används för att ladda hem andras publika nycklar inklusive de signaturer de fått av de som litar på dem.

Vilken av dessa som ska väljas beror på situationen, inom en enhetlig organisation kan S/MIME vara det bästa valet, om man har många externa kontakter så kanske man väljer OpenPGP.

Den här instruktionen avser att på enkelt och lättfattligt sätt beskriva hur man som användare kan kryptera eller signera e-post.

2. Kryptering och signering av e-post med S/Mime

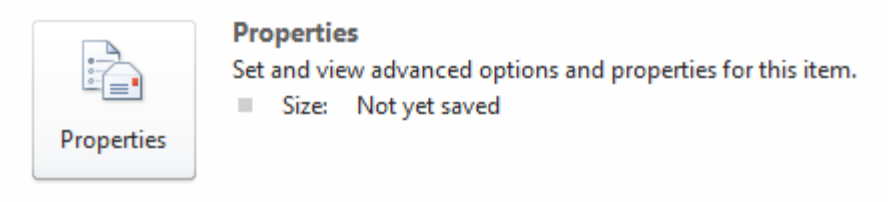
2.1 Certifikat

För att kunna kryptera och signera e-post med S/Mime behöver man först utfärda ett personligt certifikat. Information om hur detta görs från en windows-dator finns här:
https://mp.uu.se/web/info/stod/e-post/certifikat/windows

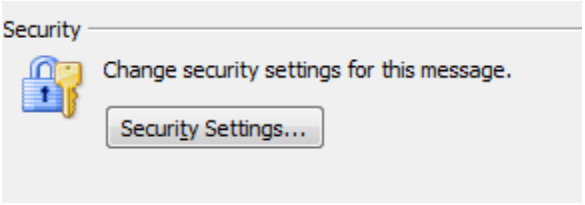
2.2 Kryptering av e-post i Outlook

1. Om mottagaren inte finns med bland dina Outlook-kontakter, följ instruktionen för att lägga till nya kontakter i steg 6 nedan.

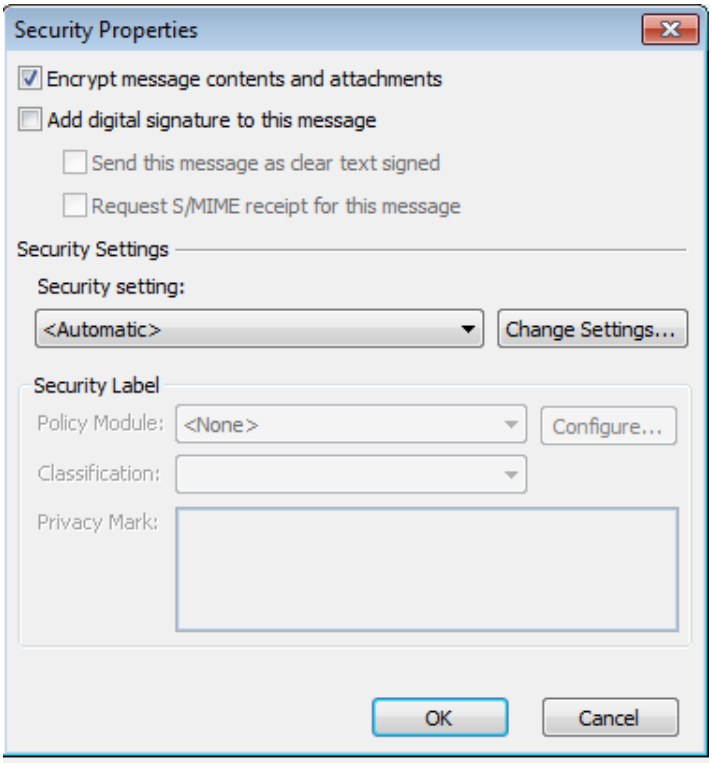
2. Öppna inställningarna för e-postmeddelandet



3. Öppna Security settings

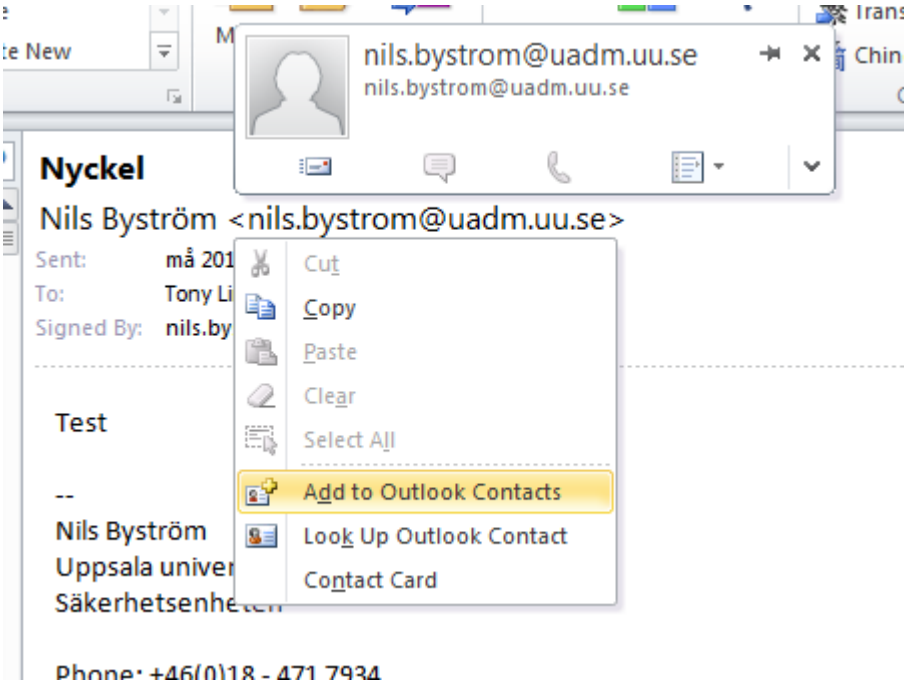


4. Markera Encrypt message contents and attachment.



5. Skriv och skicka brevet som vanligt.

6. I ett S/MIME-signerat mail från kontakten, klicka på avsändaren och välj ”Lägg till i kontakter/Add to Outlook Contacts”.

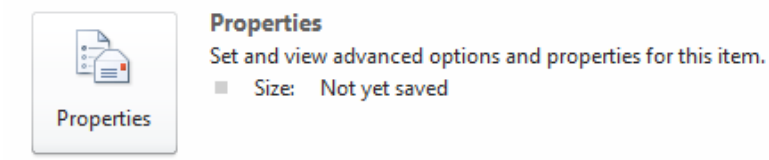


2.2.1 Snabbknappar

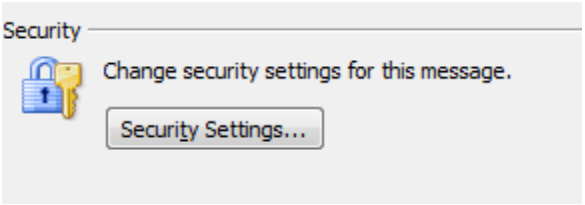
I Outlook finns snabbknappar för kryptering och signering men vissa tillägg avaktiverar dessa funktioner. Hör med ditt lokala IT-stöd om du är intresserad av att använda dessa knappar.

2.3 Signering av e-post i Outlook

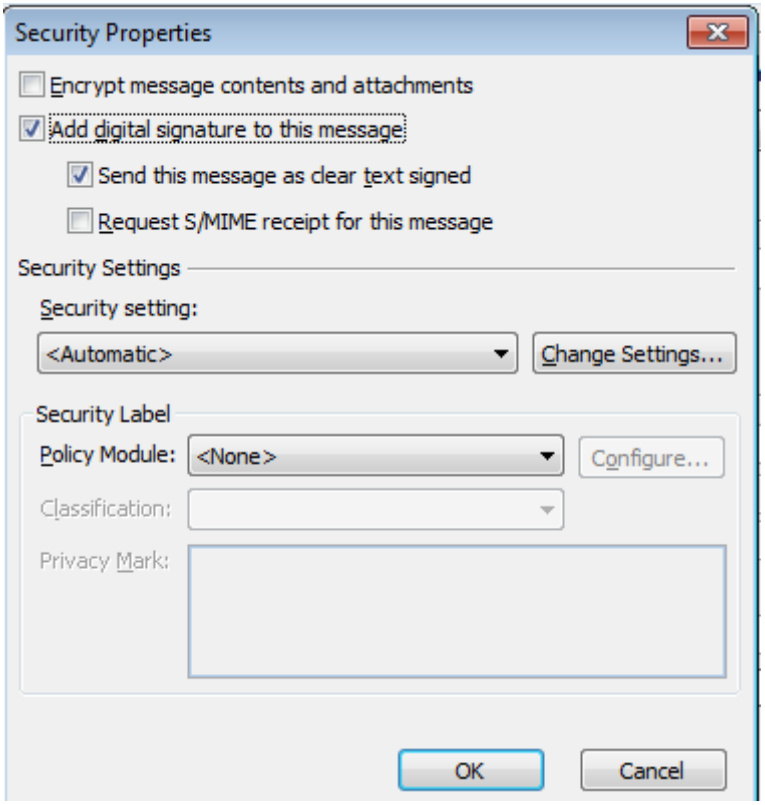
1. För att signera ett e-postmeddelande med ditt certifikat, börja med att öppna inställningarna för brevet.



2. Öppna Security settings



3. Markera Add signature to this message

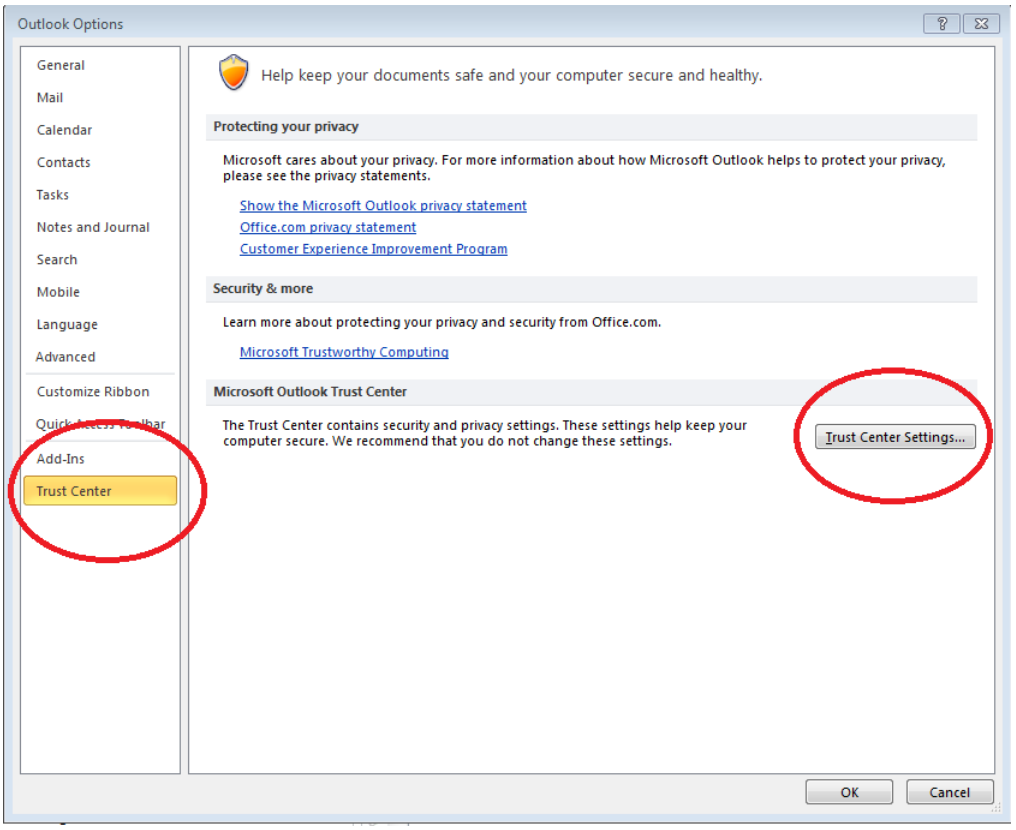


4. Skriv och skicka e-postmeddelandet som vanligt.

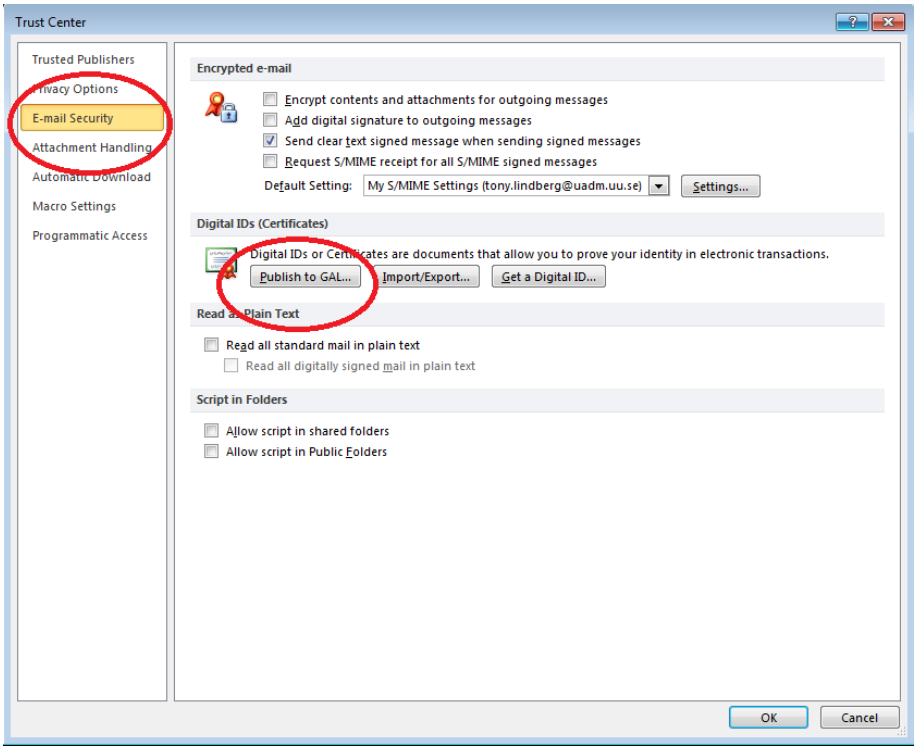
2.4 Kryptering och signering av e-post i Exchange webmail (OWA)

För att kunna signera och kryptera i OWA måste dels S/MIME kontrollen installeras i din webläsare och ditt certifikat måste laddas upp till den Globala adresslistan (GAL). När du tar emot ett S/MIME signerat brev så kommer du få frågan om du vill installera S/MIME kontrollen. Följ instruktionerna från OWA. Uppladdning av certifikatet till GAL görs via en Outlook-klient:

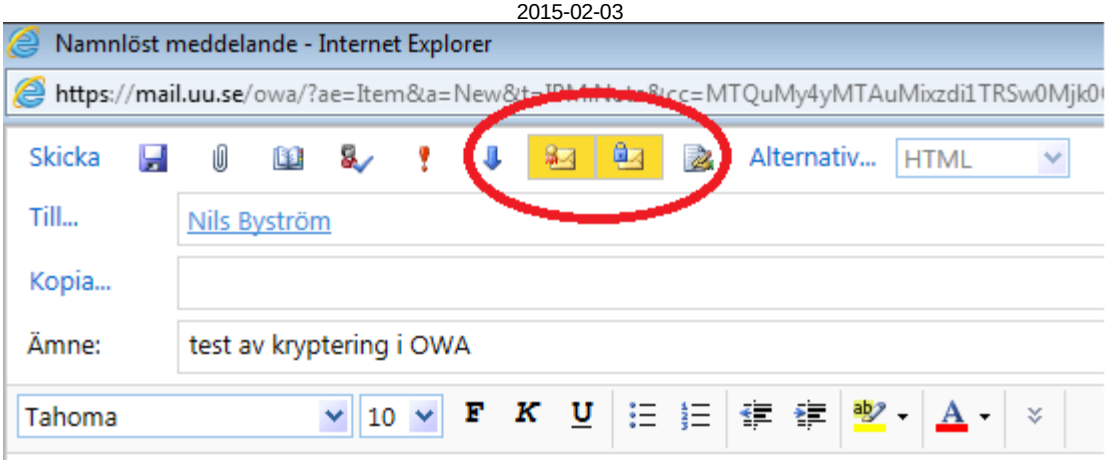
1. Öppna Trust Center Settings



2. Under E-mail security klicka på Publish to GAL…



3. När S/MIME kontrollen är installerad syns två nya knappar när man skriver ett brev i OWA, dessa används för att signera och kryptera brev. Knappen kryptering kräver att man har en kontakt skapad antingen via OWA eller via Outlook som innehåller mottagarens publika certifikat.



3. Kryptering och signering av e-post med OpenPGP

3.1 Inledning

OpenPGP är en öppen standard under IETF och använder inte proprietära algoritmer, således tillåtande interoperabilitet mellan olika produkter. *GnuPGP (Gnupg, Gpg)* är en vanligt förekommande fritt tillgänglig implementation OpenPGP.

Gnupg innehåller i sig inget fullskärmsstöd eller stöd för integrering i epostklienter. Ofta så kan man vilja installera något mer som hjälper till i integrationen. Några få exempel för:

- Windows: Gpg4win (http://www.gpg4win.org/) stöd för Outlook mm.
- Mac: Gpgtools (http://gpgtools.org/)
- Linux: Exempelvis Kmail, Mutt har openpgpstöd, Squirrelmail en plugin för detta.
- APG, Android Privacy Guard (http://apg.thialfihar.org/)

3.2 Nyckelhantering

OpenPGP bygger på s.k *web-of-trust* som innebär att någon annan, efter verifikation av nyckelns autenticitet, signerar ens publika nyckel utnyttjande sin egen. Antag att Anna ska skicka brev till Bertil och vill vara säker på att hon har rätt nyckel. Om Bertils nyckel är signerad av Caesar, vars nyckel Anna redan har eller kan verifiera så kan Anna, givet att hon litar på Caesar, anta att Bertils nyckeln är korrekt. I praktiken fungerat detta oftast bra, nästan oavsett vem man vill kommunicera med så har man någon gemensam bekant några steg bort i signaturträdet. I annat fall får man se till att meddela mottagaren den publika nyckeln via någon annan kanal, exempelvis ringa denne och meddela sin nyckels ”fingeravtryck”.

Ett nyckelpar består alltså av en privat nyckel som ägaren håller hemlig och en publik nyckel som sprids till de man kommunicera med. Text som ska skickas till nyckelinnehavaren *krypteras* utnyttjande den publika nyckeln och kan efter mottagandet *dekrypteras* utnyttjande den privata d:o. Likaså kan ett meddelande *signeras* med den privata nyckeln och *verifieras* med den publika.

Rekommendationer vid skapande av nycklar:

- Använd minst 2048 som nyckellängd
- Lägg in namn och epost på nyckeln så att andra kan hitta den på nyckelservern.
- Det kan vara bra att sätta en giltighetstid (t.ex. 2 år) så att gamla nycklar upphör automatiskt.
- Se till att sätta ett (för utomstående) svårgissat lösenord på nyckeln *ifall* del trots allt skulle komma på avvägar.
- Ta en kopia på den privata nyckeln och förvara säkert
- Ladda upp den publika på en s.k nyckelserver.

3.3 Kryptering av e-post i Outlook

För de som använder Windows och Outlook kan *Gpg4win* vara ett lämpligt val – det är fritt att använda och kan nyttjas både för fil- och epostkryptering.

Dokumentation
Det finns en utmärkt manual på www.gpg4win.org, studera denna.

Installation
Ladda ned installationsfilen från www.gpg4win.org. Efter nedladdningen så bör förstås autenticiteten verifieras – det finns en openpgp-signatur i en separat fil som kan användas för verifiering, men det förutsätter förstås att vi har någon fungerande openpgp-installation för att göra detta på. I övrigt beskrivs installationen utmärkt i gpg4win-manualen. Ett antal program installeras, GpgOL är det som innehåller outlook-stödet. *Kleopatra* är ett användargränssnitt för bland annat certifikathantering. Gpg4win stödjer både openpgp och s/mime. Outlook har redan stöd för s/mime så kan man vilja stänga av gpg4win:s motsvarande. När du efter installationen startar Outlook så finner du några val under Extras → Options, där kan du stänga av gpgOL:s s/mime-stöd. .Passa på att kontrollera att meddelandeformatet är satt till endast text.

Skapa ett OpenPGP-nyckelpar.
Detta gör du med programmet Kleopatra, se kapitel 7.1 i gpg4win-manualen. File → New Certificate. Fyll i namn och epost. Är det en test- eller lågsäkerhetsnyckelpar, skriv detta som kommentar. Det kan vara till fördel att sätta en begränsad livslängd på nyckeln, exempelvis två år, se avancerat-fliken. Kontrollera att nyckellängden är satt till minst 2048. Se till att nyttja ett bra lösenord (se diskussion ovan). Glöm inte att ta en backupp på din nyckel och förvara backuppen säkert.

Sprid din publika OpenPGP-nyckel.
Se 8.2 i gpg4win-manualen. Enklast är att ladda upp nyckeln till nyckelserver/rar (testnycklar ska du förstås inte ladda upp). Kleopatra: File → Export certificate to server.

Hämta dina kontakters OpenPGP-nycklar.
Se kap. 16 i gpg4win-manualen. I Kleopatra, klicka på 'Slå upp certifikat på server', sök efter exempelvis epostadress, markera i listan och importera nyckeln.
Men, som vi nämnt ovan, bara för att en nyckel finns på en nyckelserver så betyder inte det att det är korrekt.

- Antingen så verifierar du nyckeln genom att ta ”fingeravtrycket” för nyckeln vilket i du finner i nyckelinformationen (importerade nycklar → markera & klicka). Kontakta innehavaren på något alternativt sett, exempelvis per telefon, och försäkra dig om att fingeravtrycket stämmer. Utväxla gärna fingeravtryck så kan ni certifiera/signera varandras nycklar och ladda upp till nyckelservrar.
- Eller så kontrollerar du att nyckeln är certifierad/signerad med någon nyckel som (och vars innehavare) du litar på, samt markerar därefter 'Lita på certifieringar gjorda med det här certifikatet'.

. **Hur man skickar krypterade och/eller signerade brev via Outlook.**
- Skriv brevet som vanligt och ange mottagare etc.
- I övre vänstra delen på sidan finns det knappar för signering och/eller kryptering.
- Klicka på ”Sänd”.
- Om Kleopatra har problem att hitta korrekt nyckel för mottagaren så får du upp en dialogruta.

3.4 Läs mer

- http:www.openpgp.org
- http://www.gnupg.org/
- http://www.pgp.com/ (Kommersiell produkt från Symantec)