Kryptering af filer med personfølsomme oplysninger

Denne vejledning beskriver, hvordan én afsender kan kryptere en fil, som kun afsender selv eller én bestemt modtager kan dekryptere.

Som værktøj benyttes Cryptophane, der er en grafisk brugergrænseflade til GnuPG, som er en open source implementering af PGP. (Brug google / wikipedia, hvis du ønsker uddybende beskrivelser af disse systemer.)

Både afsender og modtager skal downloade og installere Cryptophane.
- Installationsproceduren er en simpel standard Windows-installer

Begge skal ligeledes oprette en privat nøgle:
- I Cryptophane vælges Keys, Generate Secret Key
- Afsender og modtager indtaster deres navne og emailadresser.
- Ligeledes indtastes en passphrase, som er en lang og kompleks adgangskode, der naturligvis ikke bruges andre steder.

Modtager skal nu sende sin offentlige nøgle til afsender:
- I Cryptophane vælger modtager File, Export Public Keys
- Den private nøgle markeres og der klikkes OK
- Filen gemmes med et sigende navn; f.eks. modtagerens navn + offentlig
- Den gemte nøglefil sendes vedhæftet til en email til afsender

Afsender skal nu importere og signere den modtagne nøglefil:
- I Cryptophane vælger afsender File, Import Keys
- Den tilsendte nøglefil vælges og importeres
- Den inporterede offentlige nøgle skal nu signeres som pålidelig
  Under processen bør modtager kontaktes telefonisk for sammenligning af Fingerprint
  Modtager ser Fingerprint for sin private nøgle med Keys, Properties of Selected Key
- Afsender markerer den importerede nøgle og vælger Keys, Sign Selected Key
- Der sættes flueben i "I have checked the above fingerprint with the key owner and they match."
- Der klikkes på [I am POSITIVE that this key belongs to its indicated owner]
- Nøglen signeres med afsenders Passphrase

Både afsender og modtager er nu klar til henholdsvis at kryptere og dekryptere filer.
- De kan begge afslutte Cryptophane.

Afsender krypterer filen:
- Filen findes med Windows Stifinder
- Der højreklikkes på filen og vælges "Encrypt and/or Sign"
- Sørg for, at der er flueben i "Encrypt with public key"
- Sæt flueben ved modtagerens offentlige nøgle
- Klik på [Process]
- Signer med passphrase
- Der oprettes en krypteret fil med filtypenavnet gpg i samme mappe som originalfilen
- Afsender kan nu trygt sende den krypterede fil vedhæftet en email til modtager

Modtager dekrypterer filen:
- Filen gemmes
- Der højreklikkes på filen og vælges Decrypt
- Passphrase indtastes

Modtager skal huske, at opbevare filen forsvarligt eller slette den med Shift + Slet.

Offentlige nøgler kan genbruges og kan med fordel stilles til rådighed f.eks. på en hjemmeside.

Uddybet, illustreret, engelsksproget vejledning

Udarbejdet af datakonsulent Bo Christensen