////Denne delen bør starte med en kortfattet redegjørelse for hvordan Public Key kryptografi fungerer (Teori).

Der etter en forklaring av hvordan elektronisk signering skal fungere.////

Kryptografi tillater to parter å skjule informasjonen de sender til hverandre. Senderen forandrer meldingen slik at bare mottaker har mulighet

til å bruke den, altså under transit er meldingen uforståelig for en inntrenger.

Public Key kryptografi er et kryptografisk system som trenger to unike nøkler; en nøkkel til å kryptere, en nøkkel til å dekryptere. ingen av

nøklene kan gjøre begge deler. Den ene nøkkelen blir utgitt offentlig og brukes til å kryptere, mens den andre er privat og brukes til å dekryptere.

Siden alle har tilgang til den offentlige nøkkelen betyr det at alle kan kryptere en melding med den, men bare du som har den private nøkkelen

kan dekryptere meldingene. På samme måte kan du kryptere meldinger hvis du har en offentlig nøkkel, men ingen andre enn personen med den tilsvarende

private nøkkelen kan dekryptere.

En annen måte man kan bruke offentlige og private nøkler sammen er i digital signering av informasjon, eller sertifisering.

Dette gjøres omvendt fra public key kryptografien som er beskrevet ovenfor; signaturen krypteres av en private key, og blir dekryptert av public keyen.

Sertifisering er nyttig, ettersom at ennhver datamaskin kan verifisere signaturen, men bare den originale kilden kan skape den. Altså betyr dette at man kan være sikker på at signert informasjon kommer fra kilden signaturen tilhører

OS liste

Andreas - Laptop: Windows 7 home premium

Stasjonær: Windows 7 professional

Nico - Laptop: Windows 7 Home Premium

Stasjonær: Windows 7 (...)

magnus: Laptop: Windows 7 home

Stasjonær: Windows 7

Per Jarle: Laptop: Windows 7

Stasjonær: XP