



Sikker dokumentafl levering?

Robin Sharp

Informatik og Matematisk Modellering

B.321, DTU.

Phone: (+45) 4525 3749

e-mail: robin@imm.dtu.dk

Februar 2005

Krav til sikker dokumentaflevering



Typiske krav anno 2005:



- **Forfatteren** skal kunne **identificeres**.
- Dokumenter skal **ikke kunne gå tabt**.
- **Umuligt at ændre** i dokumentet uden at det kan opdages.
- Måske behov for **kvittering** for modtagelse.
- Måske behov for **fortrolighed** (personlige data mv.).
- Måske behov for kontrol af **afleveringsfrister**.

John Lennon

Let at imødekomme med personlig aflevering af papirer!

Hvem er forfatteren?



- Forfatteren identificeres ved sin **signatur**.
- Til elektroniske dokumenter bruges en **e-signatur**, for eksempel dannet ved brug af et **certifikat**.
- Signerede dokumenter kan **ikke ændres** uopdaget.
- **Veludviklet teknologi**, kan let indbygges i programmer til håndtering af e-mail, web mv.
- E-signaturen kan indkorporere **dato, tid** mv.
- Information i certifikat kan bruges til **kryptering** af dokument for at sikre fortrolighed.
- Relativt let at indbygge faciliteter, der kan håndtere **multiple signaturer**, fx. ved flere forfattere.

Spørgsmål omkring certifikater



- **Certifikatudstederen (CA) skal anerkendes** af alle modtagere af dokumentet. Hvordan sikres dette:
 - CA er **monopol**, alle personer registreres centralt?
 - **Indbyrdes anerkendelse** af CA'er?
- Kan/skal **samme certifikat bruges til alting**, fx. skole, universitet, skattekontor, SU, e-handel, job, ... ?
- Certifikater kan **tilbagekaldes**. På hvis anledning kan dette ske? Af hvilke grunde?
- Hvis ansvar er det at checke, at certifikat er **gyldigt**?
- Hvordan **opbevares** certifikatet sikkert?
- Hvad er den juridiske situation, hvis certifikat **stjæles**?

Spørgsmål omkring øvrige sikkerhed



- Kan vi stole på **tidsangivelser**, fx. ift. tidsfrister?
- Kan vi stole på, at et dokument kun afsendes hvis der er en person, der **med vilje sender** det afsted?
- Hvilke krav stilles til **opbevaring** af modtagne dokumenter?
- Kan vi vide, at “**forfatteren**” virkelig er **ophavsmand**?
 - a) Ved aflevering af rapport/fristil e.l.?
 - b) Ved on-line besvarelse af eksamensspørgsmål i et eksamenslokale?

Disse er vanskelige spørgsmål, der bør tiltrække sig opmærksomhed!