

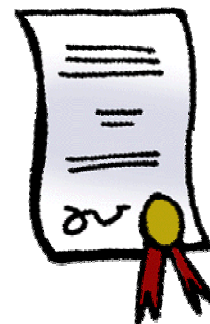


Digital Signatur

Mobilitet

15. februar 2005

Lars Møller Kristensen



Fordele og ulemper

- Erfaring fra pilotprojekter sidst i 90'erne
- Kvalificerede certifikater
 - kræver bl.a. udstedelse på hardware
- OCES også som software certifikater
 - Nøgler genereres direkte på brugerens computer
- Men hvad så med mobiliteten ?



- OCES installeret i en browser
 - Microsoft (MS Crypto API)
 - Java (PKCS#12)
- Password beskyttet sikkerhedskopi
 - Eksport - Import (nøglefil)
 - ~ som nøglen til netbank



- OCES installeret direkte på hardware
 - USB tokens
 - Smartcards
- To faktor autentificering
 - Noget man ved (kode)
 - Noget man har (hw)
- Kræver driver på pc'ere
 - Smartcard kræver smartcard læser



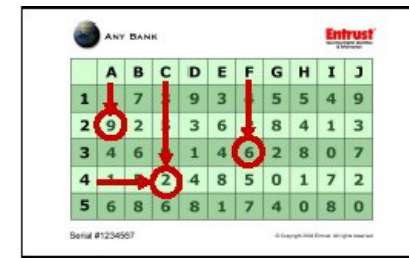
Mobilitet i dag - cd-rom kort

- OCES installeret på cd-rom kort
 - Nøgler genereret centralt hos CA
 - Adgang via 4 cifret pin-kode (begrænset antal forsøg - brute force)



- Kræver tilpasset signerings applet
 - Opensign som framework
- Evt. kombineres med studiekort

- Central Roaming løsning
- OCES certifikat genereret på krypto hardware hos CA / hostingselskab
- Privat nøgle tilgås via bruger autentifikation
 - Brugernavn + kodeord
 - Engangskode for at opnå ægte 2 faktor autentifikation, eks. via mobiltelefon eller kodeark
 - Kan evt. kombineres med studiekort

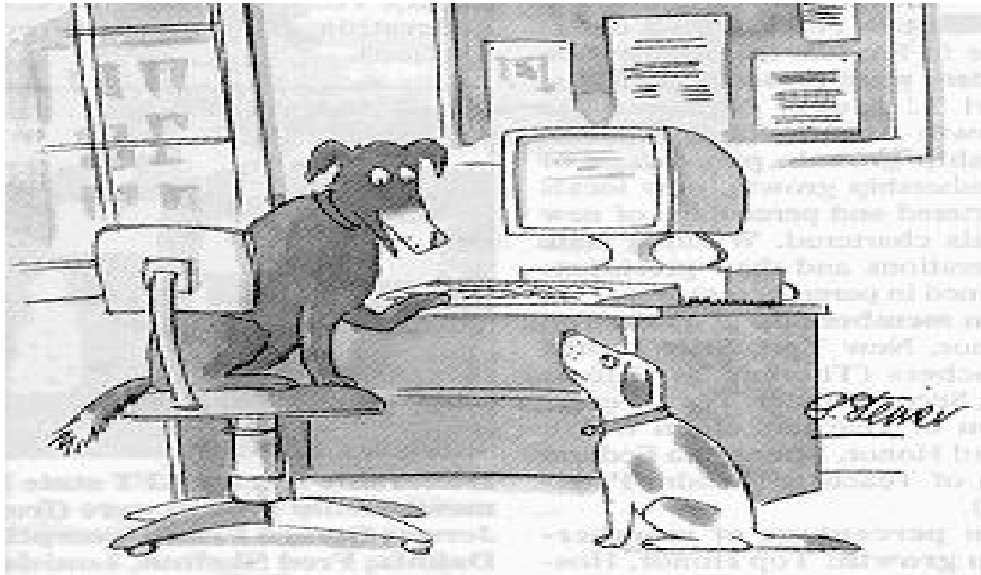


117.600 3 kodesæt
5.5 mio. 4 kodesæt

- Kræver klient applikation

	SW	HW	Tilgængelig	
Browser cert.	X		✓	Export / Import
USB Tokens		X	✓	2-faktor
Smartcards		X	✓	2-faktor
CD-Rom kort		X	✓	Opensign framework 2-faktor
Smartcard Server	(X)			Klient app. + en gangskode

Spørgsmål ?



On the Internet, nobody knows you're a dog!
(The New Yorker 1993)