Elektronisk signatur, sertifikater og tilhørende tjenester – begrepsavklaringer mv

Advokat dr. juris Rolf Riisnæs
WIKBORG REIN
rri@wr.no

Arbeidsgruppen for revisjon av tinglysingsloven
20. november 2009

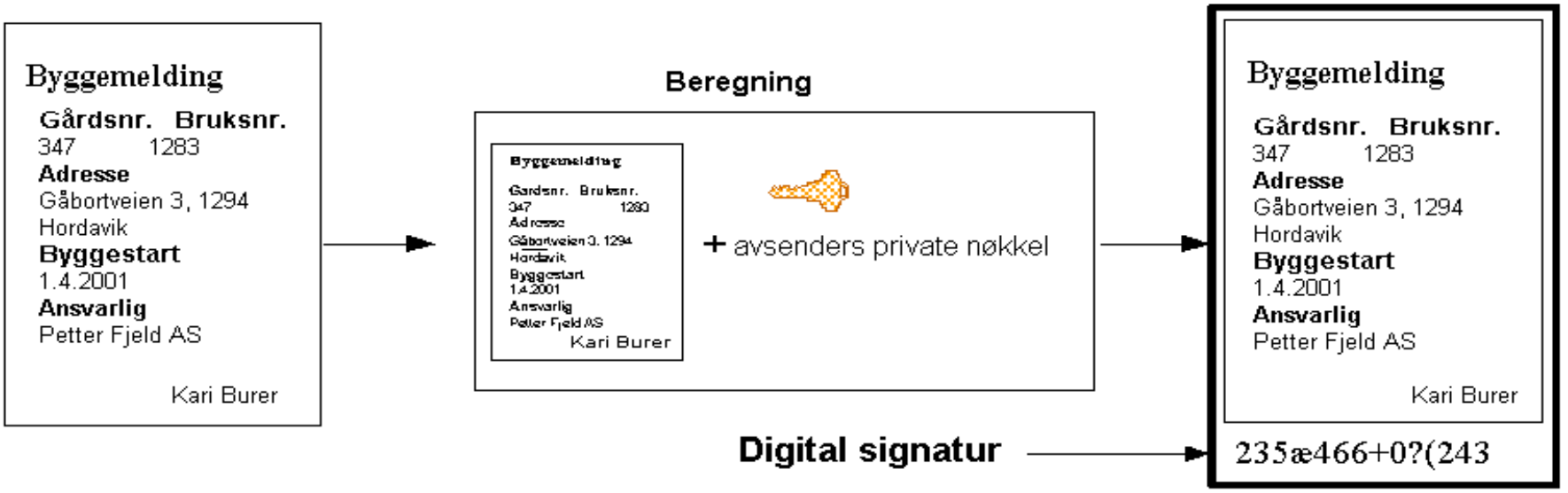
Hvorfor elektroniske signaturer mv?

- Forutberegnelighet med hensyn til rettsvirkninger
  - Form- og prosedyrekrav, evt. indirekte krav
  - Gyldighetsbetingelse, ordensregel eller vilkår for sekundærvirkninger
- Sikkerhet med hensyn til faktum
  - Bevis- og dokumentasjonsbehov
- Tillit
  - Hva som skal til for at partene har den tillit til systemet og til hverandre at de ønsker å gjennomføre transaksjonen

Signaturen kan ha ulike funksjoner

- Underskrifter og autografer
- Elektronisk signatur og digital signatur
- Digital signatur for enhetsautentisering
- Digital signatur opphavsautentisering
- Digital signatur som uttrykk for kunnskap om innhold
- Digital signatur som uttrykk for vilje (kunnskap om innhold *og* kontekst)
- Noen ord om begrepet ”ikke-benekting”

Digital signatur

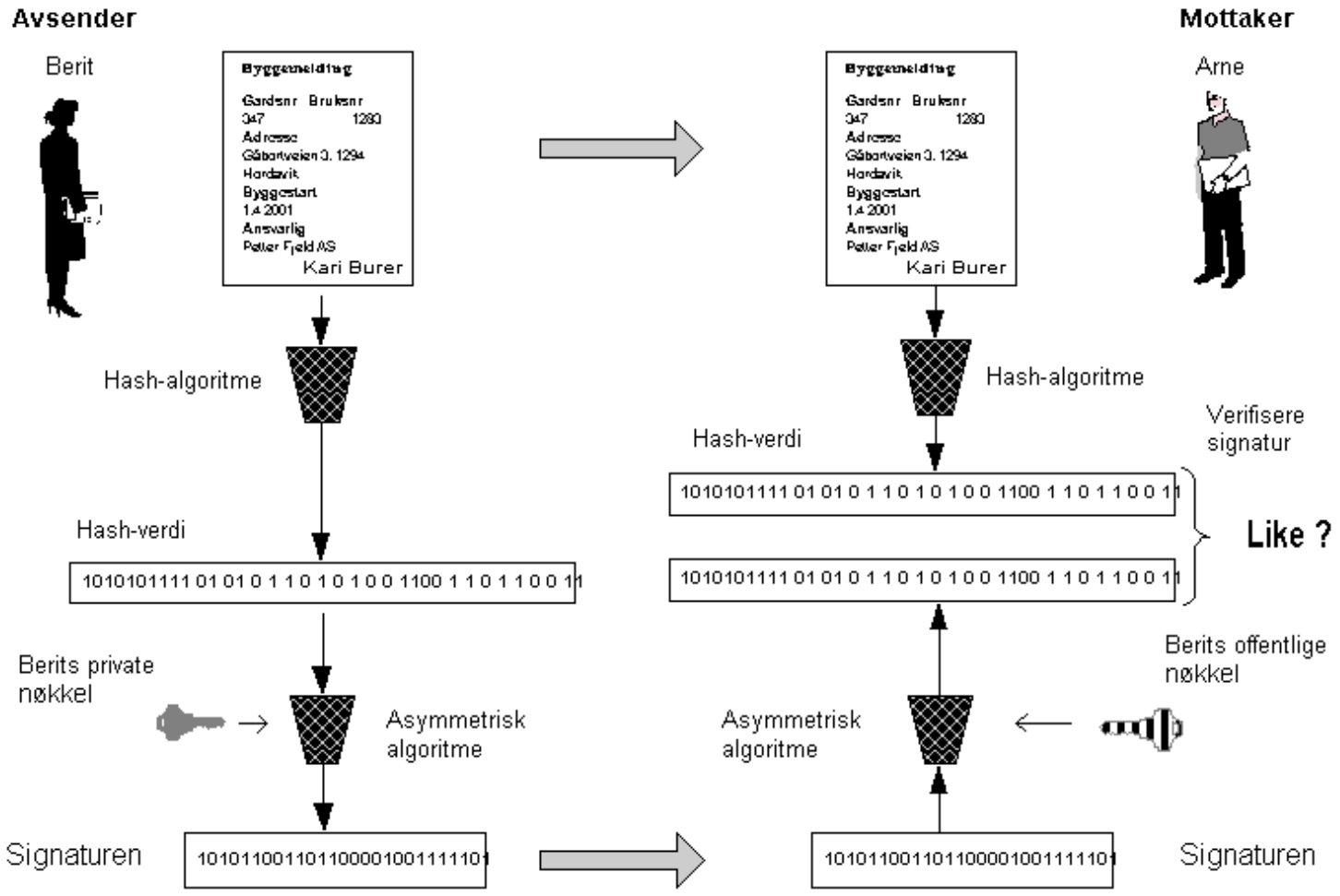


Digital signatur "forsegler "dokumentet

Endringer vil bli oppdaget

Hentet fra NOU 2001:10 fig 3.1

Digital signatur - forts.



Hentet fra NOU 2001:10 fig 3.2

Digitale sertifikater

- Formål: Å kunne kople en person, organisasjon eller rolle til en handling, melding, eller et nettsted
- Sertifikat (trad.): En elektronisk melding som kopler en offentlig nøkkel til et navn, en rolle eller et pseudonym (sertifikatinnehaveren)
- Konstaterende erklæring om faktiske forhold
- Pålitelighet og anvendelighet kan variere – en utfordring for den som vurderer å stole på sertifikatet (sertifikatmottakeren)

eSignaturlovens definisjoner

- *§ 3 nr. 1 Elektronisk signatur*: data i elektronisk form som er knyttet til andre elektroniske data og som brukes som autentiseringsmetode.
- *§ 3 nr. 2 Avansert elektronisk signatur*: en elektronisk signatur som
  a) er entydig knyttet til undertegneren,
  b) kan identifisere undertegneren,
  c) er laget ved hjelp av midler som bare undertegneren har kontroll over, og
  d) er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering.

eSignaturlovens definisjoner forts.

- *§ 3 nr. 4 Undertegner:* den som disponerer et signaturfremstillingssystem og som handler på vegne av seg selv eller på vegne av en annen fysisk eller juridisk person.
- *§ 3 nr. 9 Sertifikat:* en kopling mellom signaturverifikasjonsdata og undertegner som bekrefter undertegners identitet og er signert av sertifikatutsteder.
- *§ 4 Kvalifisert sertifikat:* Betegnelsen kvalifisert sertifikat skal kun brukes om sertifikater som oppfyller kravene i denne paragrafen og utstedes for en begrenset periode av en sertifikatutsteder som oppfyller kravene i §§ 10-15.

...

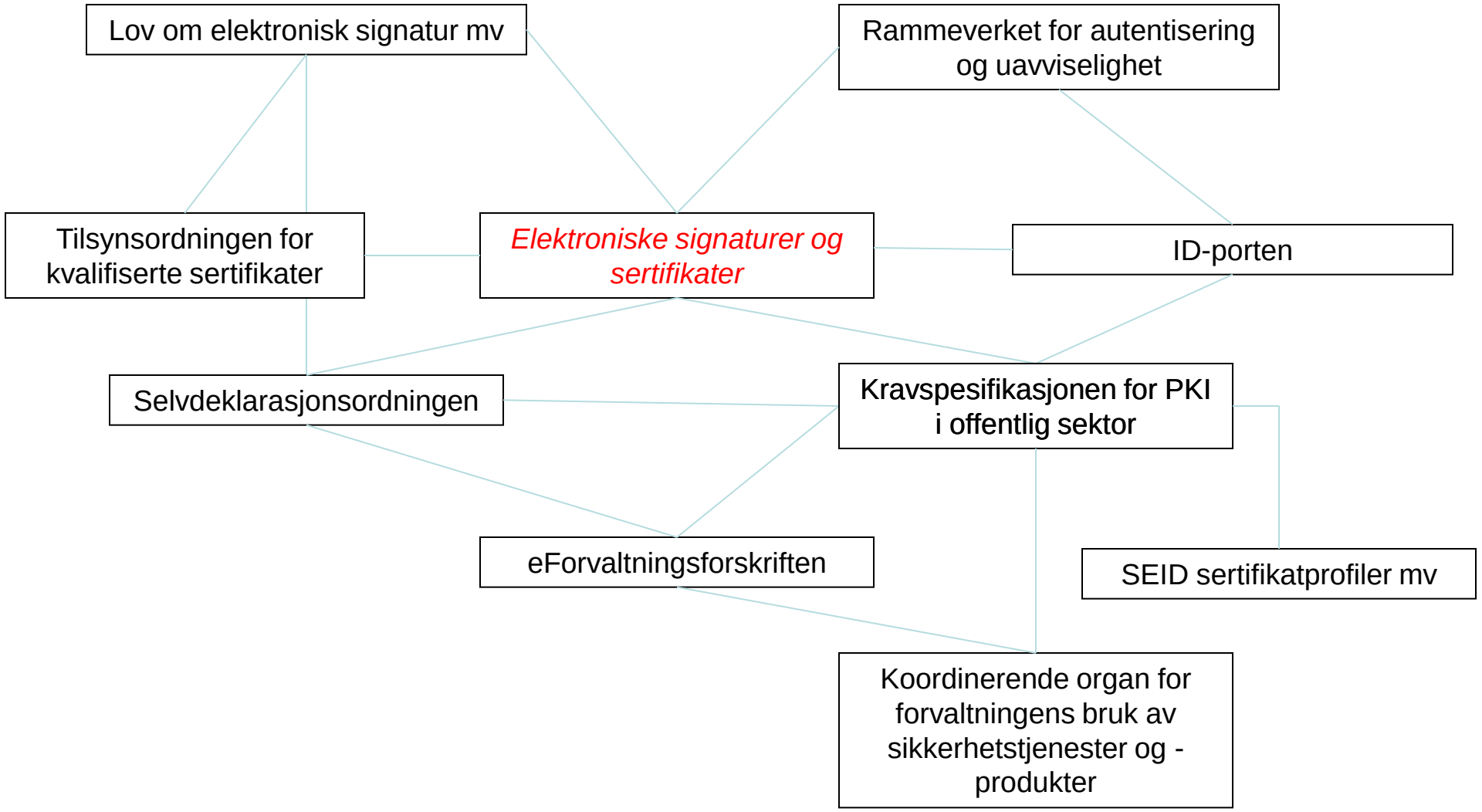
eSignaturlovens definisjoner forts.

- *§ 3 nr. 3 Kvalifisert elektronisk signatur :* en avansert elektronisk signatur [jf. § 3 nr 2] som er basert på et kvalifisert sertifikat [jf. § 4 og kap III] og fremstilt av et godkjent sikkert signaturfremstillingssystem [jf. kap II].

- *§ 6 Rettsvirkninger av elektronisk signatur :*
  Dersom det i lov, forskrift eller på annen måte er oppstilt krav om underskrift for å få en bestemt rettsvirkning og disposisjonen kan gjennomføres elektronisk, oppfyller en kvalifisert elektronisk signatur alltid et slikt krav.
  En elektronisk signatur som ikke er kvalifisert, kan oppfylle et slikt krav.

Myndighetsinitiativ mv

- Tilsynsordningen for kvalifiserte sertifikater
- Selvdeklarasjonsordningen, jf esignl § 16a og eForvaltningsforskriften § 27
- Kravspesifikasjon for PKI i offentlig sektor
  - Person Høyt
  - Person Standard
  - Virksomhet Høyt/Standard
- Rammeverket for autentisering og uavviselighet
  - Sikkerhetsnivå 1-4


Lov om elektronisk signatur mv
Rammeverket for autentisering og uavviselighet
Tilsynsordningen for kvalifiserte sertifikater
Elektroniske signaturer og sertifikater
ID-porten
Selvdeklarasjonsordningen
Kravspesifikasjonen for PKI i offentlig sektor
eForvaltningsforskriften
SEID sertifikatprofiler mv
Koordinerende organ for forvaltningens bruk av sikkerhetstjenester og -produkter

Utfordringer med elektronisk signatur

- Hva som skal dokumenteres (bevises)
  - Oppfyllelse av formkrav
  - Innholdet i et dokument som ”står på egne ben”
  - Resultatet av en elektronisk dialog eller arbeidsflyt
- Den rettslig relevante disposisjonen
- Kontroll med arbeidsflyt- og signaturmiljøet
- Koblingen mellom brukeropplevelsen og det signerte materiale
- Kontroll med og tilgang til sertifikater, signaturattributter mv som er nødvendig for å tolke og validere signaturen
- Hvordan beviset skal føres

Oppsummering – praktisk tilnærming

- Elektronisk signatur – upresist fellesbegrep for ulike løsninger der autentisering av avsender er i fokus
- Digital signatur – vanlig begrep for elektronisk signatur basert på PKI (sertifikatbasert)
- Avansert elektronisk signatur – per i dag i praksis en digital signatur
- Kvalifisert elektronisk signatur – elektronisk signatur som er underlagt særlige krav og tillagt visse rettsvirkninger iht esignaturloven § 6

Oppsummering – praktisk tilnærming (forts.)

- Sertifikat – en elektronisk melding som kopler en offentlig nøkkel til et navn, en rolle eller et pseudonym
- Kvalifisert sertifikat – et sertifikat som er utstedt iht kravene i esignaturloven
- Person Høyt sertifikat – basert på kravene til et kvalifisert sertifikat og oppfyller kravene i Kravspesifikasjon for PKI i offentlig sektor (kan benyttes for flere formål)
- Elektronisk signatur på nivå 4 – avansert elektronisk signatur basert på et Person Høyt (kvalifisert) sertifikat som oppfyller kravene i Kravspesifikasjonen for PKI og Rammeverket for autentisering og uavviselighet