Tekniske og juridiske krav til sikkerhet i systemer for eID og elektroniske signaturer

Særlig om kravet til brukerens enekontroll («sole control»)

Kristian Gjøsteen[1] Marte Eidsand Kjørven[2]

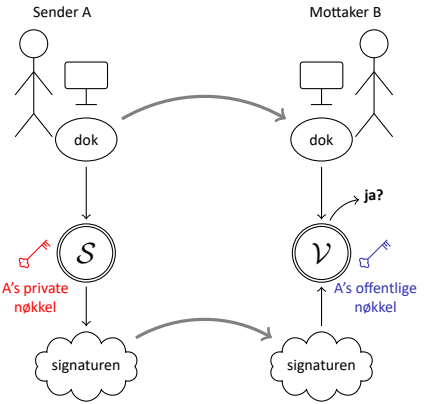
[1]Institutt for matematiske fag, NTNU

[2]Institutt for privatrett, UiO

IDentitet 2023

Rettslige problemstillinger knyttet til A's private nøkkel

- Hvilke krav til sikkerhet påhviler utstederen/systemeieren?
  - Kan systemet legge opp til at andre enn A har tilgang til hele eller deler av nøkkelen?
  - Andre sikkerhetskrav til selve nøkkelen?
- Hvilke krav påhviler A/brukeren?
- Er det forbudt å bruke en annens private nøkkel?



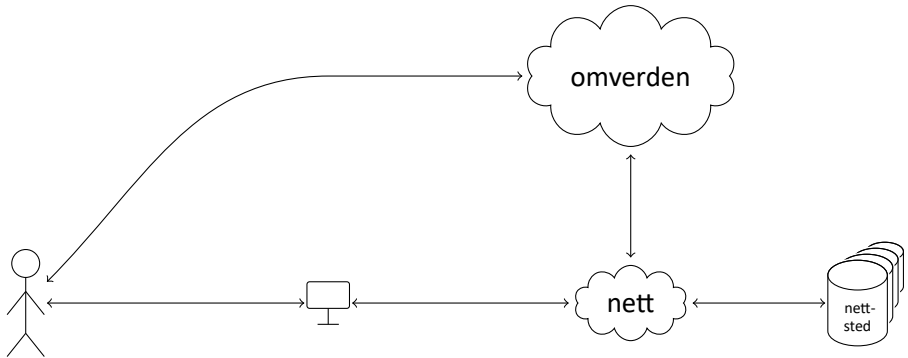
Rettslige utgangspunkter

- Tekniske krav til systemer for eID følger av vedlegg til gjennomføringsforordning (EU) 2015/1502, gjennomført i selvdeklarasjonsforskriften:
  - Nivå betydelig:
    - «Det elektroniske identifikasjonsmiddelet er utformet slik at det kan antas det bare brukes dersom eieren har kontroll over eller er i besittelse av det.»
- Tekniske krav til systemer for elektroniske signaturer følger av eIDAS:
  - Avanserte elektroniske signaturer, jf. art. 26:
    - «den er framstilt ved hjelp av elektroniske signaturframstillingsdata som underskriveren, med en høy grad av pålitelighet, har enekontroll over bruken av»
  - Kvalifiserte elektroniske signaturer, jf. art. 28:
    - Samme som for avanserte + krav i vedlegg II, herunder krav om at «den rettmessige underskriveren på en pålitelig måte kan hindre andre i å bruke de elektroniske signaturframstillingsdataene som brukes til framstilling av elektroniske signaturer»

Hva er en elektronisk signatur?

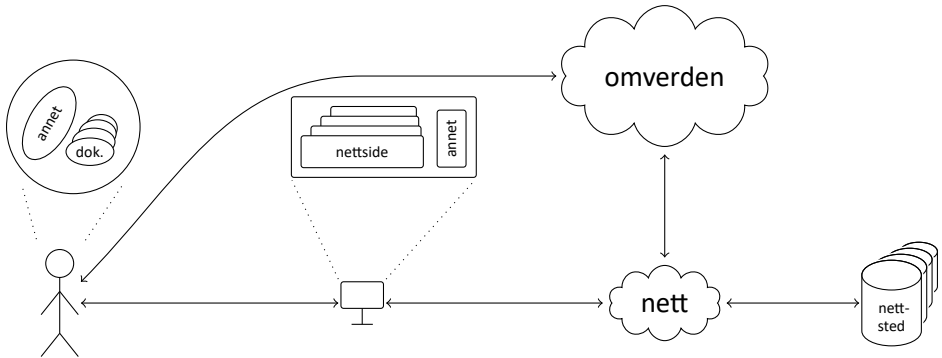
En bruker og en datamaskin lager *signaturer* på *dokumenter*.

Hva er en elektronisk signatur?



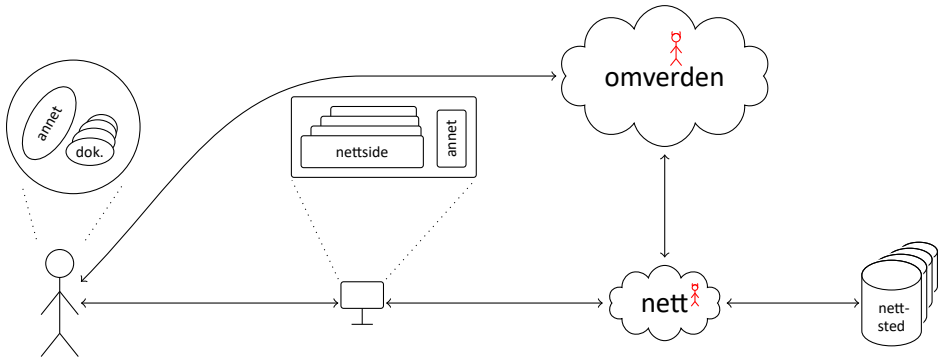
En bruker og en datamaskin lager *signaturer* på *dokumenter*.

Hva er en elektronisk signatur?



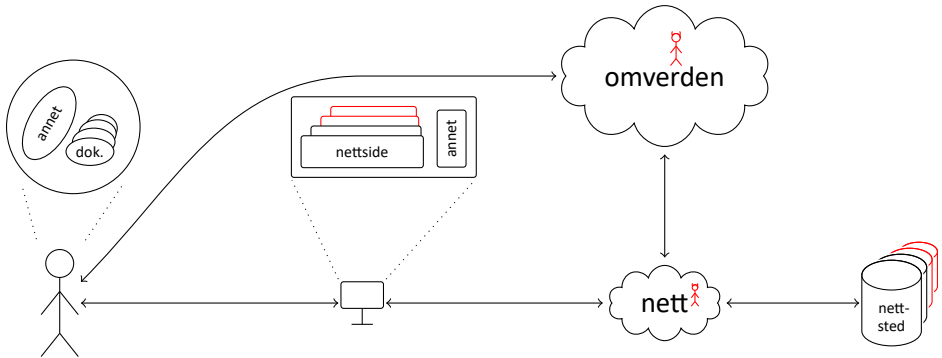
En bruker og en datamaskin lager *signaturer* på *dokumenter*.

Hva er en elektronisk signatur?



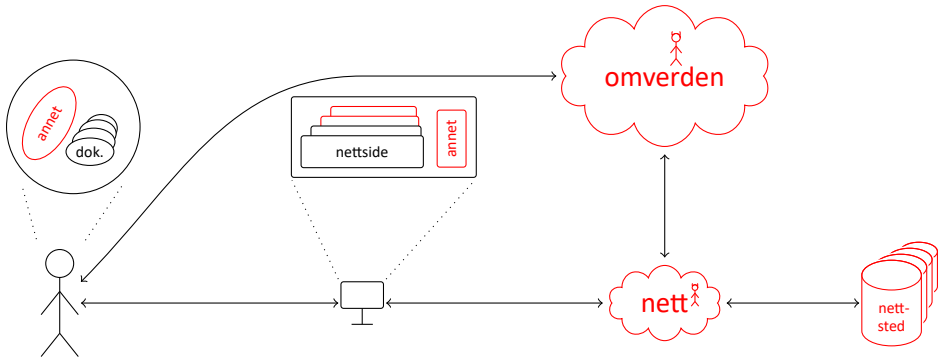
En bruker og en datamaskin lager *signaturer* på *dokumenter*.

Hva er en elektronisk signatur?



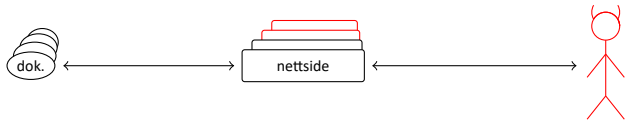
En bruker og en datamaskin lager *signaturer* på *dokumenter*.

Hva er en elektronisk signatur?



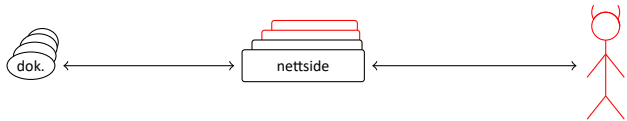
En bruker og en datamaskin lager *signaturer* på *dokumenter*.

Hva er en elektronisk signatur?



En bruker og en datamaskin lager *signaturer* på *dokumenter*.

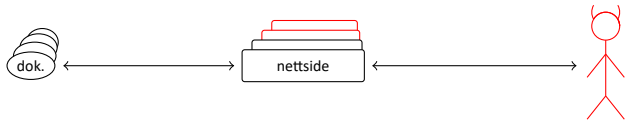
Hva er en elektronisk signatur?



En bruker og en datamaskin lager *signaturer* på *dokumenter*.

- Sikkerhet: Hver signatur kommer fra en villet signering.

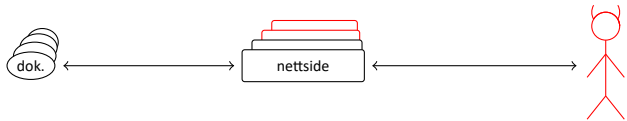
Hva er en elektronisk signatur?



En bruker og en datamaskin lager *signaturer* på *dokumenter*.

- Sikkerhet: Hver signatur kommer fra en villet signering.
- Betydningen av *enekontroll* må ligge i nødvendige antagelser for sikkerhet.

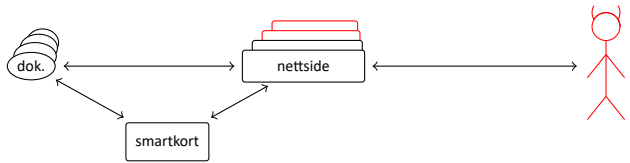
Hva er en elektronisk signatur?



En bruker og en datamaskin lager *signaturer* på *dokumenter*.

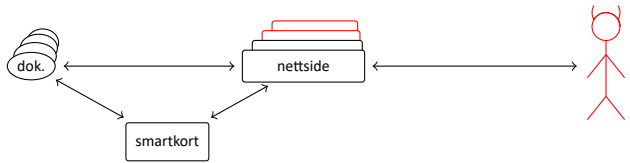
- Sikkerhet: Hver signatur kommer fra en villet signering.
- Betydningen av *enekontroll* må ligge i nødvendige antagelser for sikkerhet.
- En bruker må kunne, i prinsippet, sørge for at antagelsene er oppfylt.

Eksempel: Smartkort-løsning



På en ærlig datamaskin vil nettsiden (ærlig *eller* uærlig) vise dokumentet til brukeren og be smartkortet signere. Brukeren lar smartkortet signere.

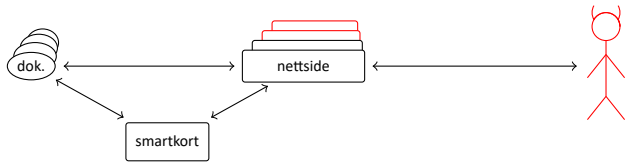
Eksempel: Smartkort-løsning



På en ærlig datamaskin vil nettsiden (ærlig *eller* uærlig) vise dokumentet til brukeren og be smartkortet signere. Brukeren lar smartkortet signere. Sikkerhet?

Argumentet går som følger: Vi har en signatur på et dokument.

Eksempel: Smartkort-løsning

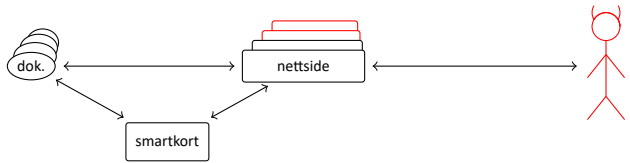


På en ærlig datamaskin vil nettsiden (ærlig *eller* uærlig) vise dokumentet til brukeren og be smartkortet signere. Brukeren lar smartkortet signere. Sikkerhet?

Argumentet går som følger: Vi har en signatur på et dokument.

- Kryptografien sier at smartkortet laget signaturen.

Eksempel: Smartkort-løsning

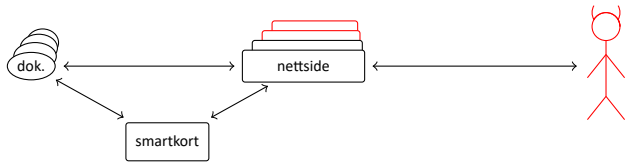


På en ærlig datamaskin vil nettsiden (ærlig *eller* uærlig) vise dokumentet til brukeren og be smartkortet signere. Brukeren lar smartkortet signere. Sikkerhet?

Argumentet går som følger: Vi har en signatur på et dokument.

- Kryptografien sier at smartkortet laget signaturen.
- Hadde brukeren fysisk kontroll på smartkortet, da lot brukeren smartkortet signere.

Eksempel: Smartkort-løsning

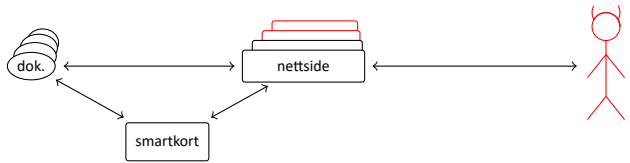


På en ærlig datamaskin vil nettsiden (ærlig *eller* uærlig) vise dokumentet til brukeren og be smartkortet signere. Brukeren lar smartkortet signere. Sikkerhet?

Argumentet går som følger: Vi har en signatur på et dokument.

- Kryptografien sier at smartkortet laget signaturen.
- Hadde brukeren fysisk kontroll på smartkortet, da lot brukeren smartkortet signere.
- Var datamaskinen ærlig, da viste nettsiden dokumentet til brukeren før signering.

Eksempel: Smartkort-løsning

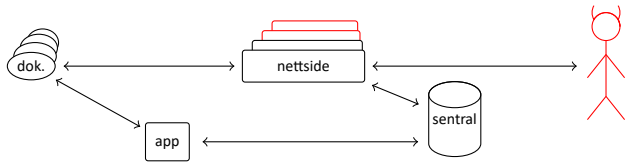


På en ærlig datamaskin vil nettsiden (ærlig *eller* uærlig) vise dokumentet til brukeren og be smartkortet signere. Brukeren lar smartkortet signere. Sikkerhet?

Konklusjon: Enten

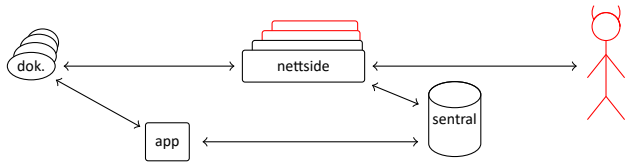
- mente brukeren å lage signaturen; eller så
- har brukeren gjort en feil; eller så
- har brukeren ikke fysisk kontroll på smartkortet; eller så
- har brukeren brukt en uærlig datamaskin.

Eksempel: En mulig app-løsning



På en ærlig datamaskin vil en ærlig nettside vise dokumentet til brukeren. Deretter lar brukeren app-en la sentralen signere.

Eksempel: En mulig app-løsning

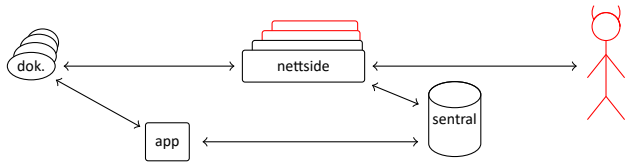


På en ærlig datamaskin vil en ærlig nettside vise dokumentet til brukeren. Deretter lar brukeren app-en la sentralen signere. Sikkerhet?

Argumentet går som følger: Vi har en signatur på et dokument.

- Kryptografien sier at sentralen laget signaturen.
- Var sentralen ærlig og laget signaturen, da lot app-en sentralen signere.
- Hadde brukeren fysisk kontroll på app-en, da lot brukeren app-en la sentralen signere.
- Var nettsiden ærlig viste den dokumentet til brukeren.

Eksempel: En mulig app-løsning



På en ærlig datamaskin vil en ærlig nettside vise dokumentet til brukeren. Deretter lar brukeren app-en la sentralen signere. Sikkerhet?

Konklusjon: Enten

- mente brukeren å lage signaturen; eller så
- har brukeren gjort én eller flere feil; eller så
- har brukeren gått til et uærlig nettsted, eller så
- har brukeren brukt en uærlig datamaskin; eller så
- har sentralen vært uærlig.

App-løsning og enekontroll

- Uttalelse fra FESA ifbm. revisjon av forgjengeren til eIDAS:
  - "The market develops forms of "delegated signing" where thin end-user devices (such as mobile phones) perform the signing by relying on the signature process being carried out by a third party that also manages the keys of the end-user associated with the device. This technology opens interesting possibilities, but it also shows inconsistencies between the requirements of the definition of advanced electronic signatures, the requirements for SSCDs in Annex III, and the requirements of Annex II. It seems that the requirements of Annex III would be no problem in this case, but it is **questionable whether such a scheme would meet the "sole control" requirement of the definition of advanced electronic signatures**, and it is also inconsistent with the requirement in Annex II, point (j), that forbids the certificationservice-provider to store the private keys."

App-løsning og enekontroll

- eIDAS fortalen pkt. 52
  - Genereringen af elektroniske signaturer på afstand, hvor miljøet til elektronisk signaturgenerering forvaltes af en tillidstjenesteudbyder på vegne af underskriveren, forventes at udvikle sig på grund af de mange økonomiske fordele forbundet hermed. Med henblik på at sikre, at sådanne elektroniske signaturer opnår samme juridiske anerkendelse som elektroniske signaturer, der genereres ved hjælp af et miljø, der fuldt ud forvaltes af brugeren, skal de udbydere, der udbyder elektroniske signaturtjenester på afstand, dog anvende specifikke ledelsesmæssige og administrative sikkerhedsprocedurer og benytte pålidelige systemer og produkter, herunder sikre elektroniske kommunikationskanaler, med henblik på at sikre, at miljøet for elektronisk signaturgenerering er pålideligt, og at det udelukkende anvendes under underskriverens enekontrol.

Oppfyller BankID-systemet tekniske krav til sikkerhet?

- Opinion No. 3/2022 of the Cooperation Network on the Norwegian eID schemes «Buypass ID» and «BankID»
- BankID godkjennes som eID på sikkerhetsnivå høyt når følgende tiltak er iverksatt:
  - Removing the use of 'scratch cards'
  - Strengthening the policy for use of Apps as possession-based authentication factor to always require the use of secure hardware elements for protection of secrets
  - Implementing a control to prevent the use of weak passwords
  - Strengthening the delivery process by providing at least one authentication element through a secure channel
  - Further strengthening the reactivation procedures, to ensure a suspended eID means can only be reactivated by its rightful holder

Hvilke krav stilles til **brukeren** mtp. å beholde enekontroll?

- Ikke regulert i eIDAS
- Finansavtaleloven § 3-19 og BankID-avtalen
- Gir brudd på kundens plikt til å beskytte personlig sikkerhetsinformasjon en rett for tjenesteyter til å si opp avtalen/sperre BankID?
  - Kanskje, men det følger ikke av EU-retten
  - Må ses i sammenheng med krav til systemene, herunder krav til universell utforming og CRPD, jf. eIDAS artikkel 15 og fortalen pkt. 29
  - Sml. Passloven § 5 (2) a.

Er det ulovlig å hjelpe andre ved bruk av deres eID?

- Straffeloven § 202 om identitetskrenkelse
  - Forbudt å opptre med en annens identitet med forsett om å oppnå en uberettiget vinning eller påføre en annen tap eller ulempe
- Straffeloven § 366 om misbruk av identitetsbevis
  - Forbudt å bruke en annens identitetsbevis «med forsett om å oppnå en fordel for seg eller andre»
  - Forbudt å overlate et identitetsbevis til en annen, dersom «han eller hun vet eller bør forstå at det vil bli brukt ulovlig»