UKE 12
Krav om informasjonssikkerhet

IN1030 - Gruppe 1 & 3D

Plan for i dag

- **Repetisjon UML modellering**
- **Introduksjon til informasjonsikkerhet**
- **K.I.T.**
- **Tiltak**
- **Risiko og trusler**
- **Ukeoppgaver**

Hva er forskjellen på aktører og interessenter?

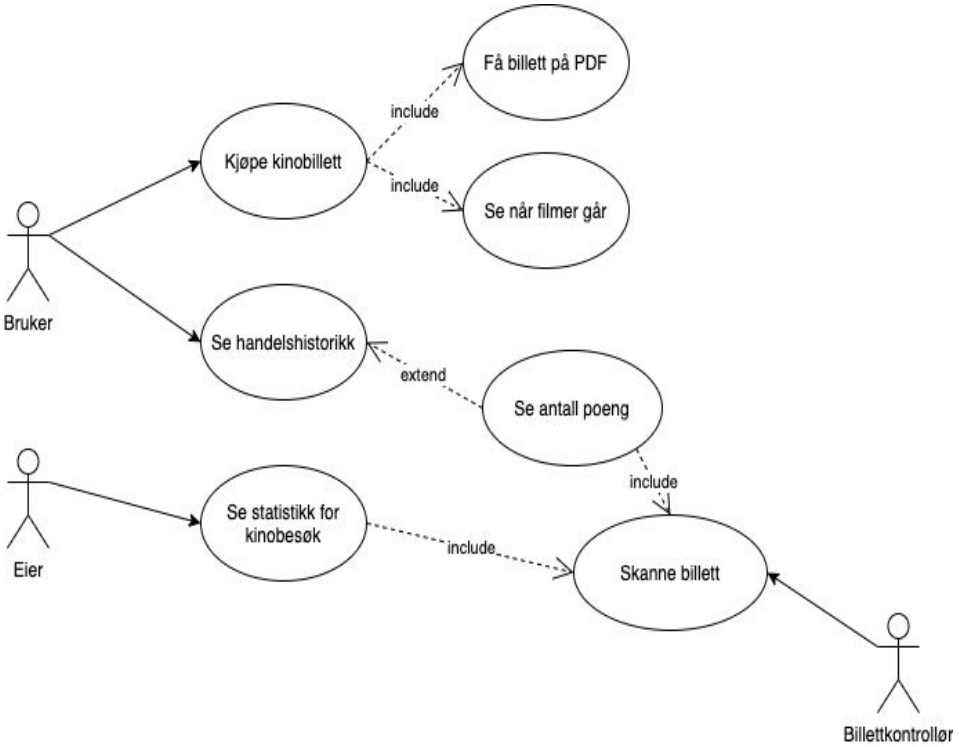
- **Aktører**: de som bruker/brukes av systemet. aktiv rolle, kommuniserer med systemet.
    - individer
    - systemer

  Primæraktør: eget **mål** i kommunikasjonen med systemet.

  Sekundæraktør: trengs for at primær aktøren skal nå målet, kommuniserer også aktivt med systemet.

- **Interessenter**:
    - de som påvirker/påvirkes av systemet. kommuniserer ikke nødvendigvis med systemet.
        - individer
        - grupper
        - organisasjoner
        - institusjoner

IN1030 Oblig4 - Use Case eksempel



- Handler om å identifisere aktørens mål → et use case

To relasjoner i et use case diagram:

Include-relasjonen

- Et use case kan være en del av ett eller flere andre use case
- Indikerer at et (sub) use case inneholder nødvendig funksjonalitet for gjennomførelsen av et annet basiscase

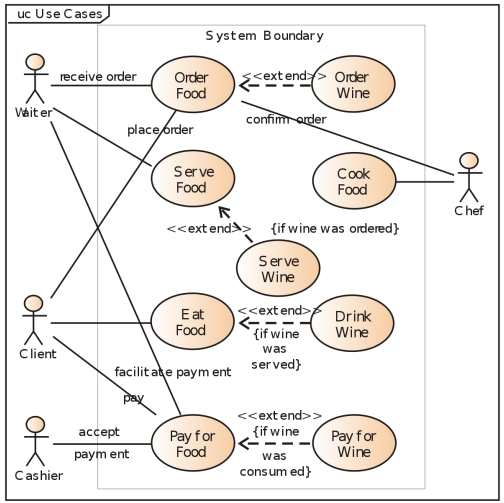
Extend-relasjonen

- Et use case som beskriver tilleggsoppførsel som utføres under gitte omstendigheter
- Utvider oppførselen/funksjonalitet til et basiscase, som utføres under spesielle omstendigheter

Diagrammer for dette emnet

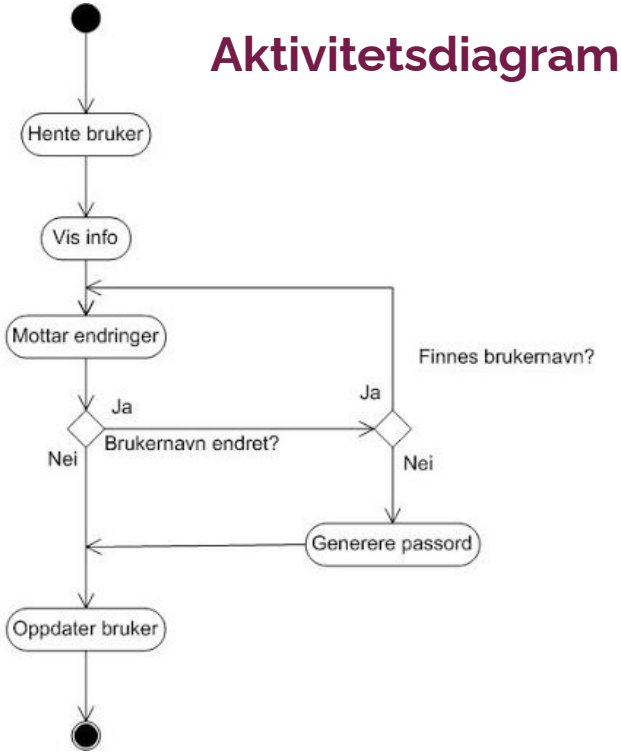
Use Case-diagram:

1.



Aktivitetsdiagram:

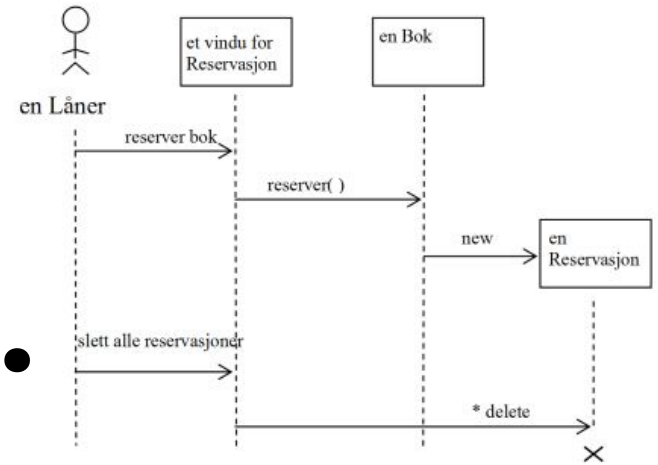
2.



Diagrammer for dette emnet

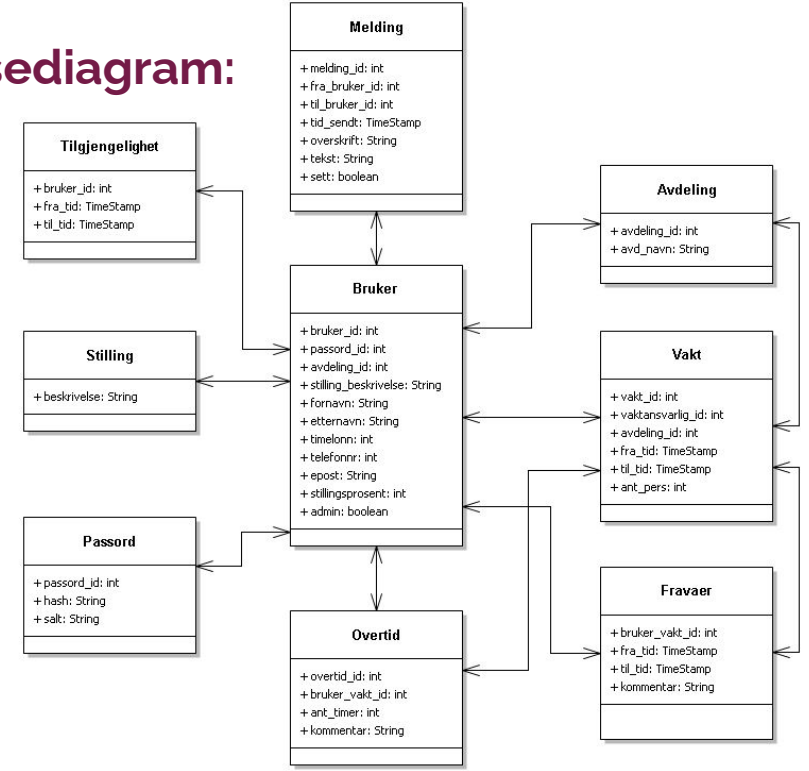
Sekvensdiagram:

3.

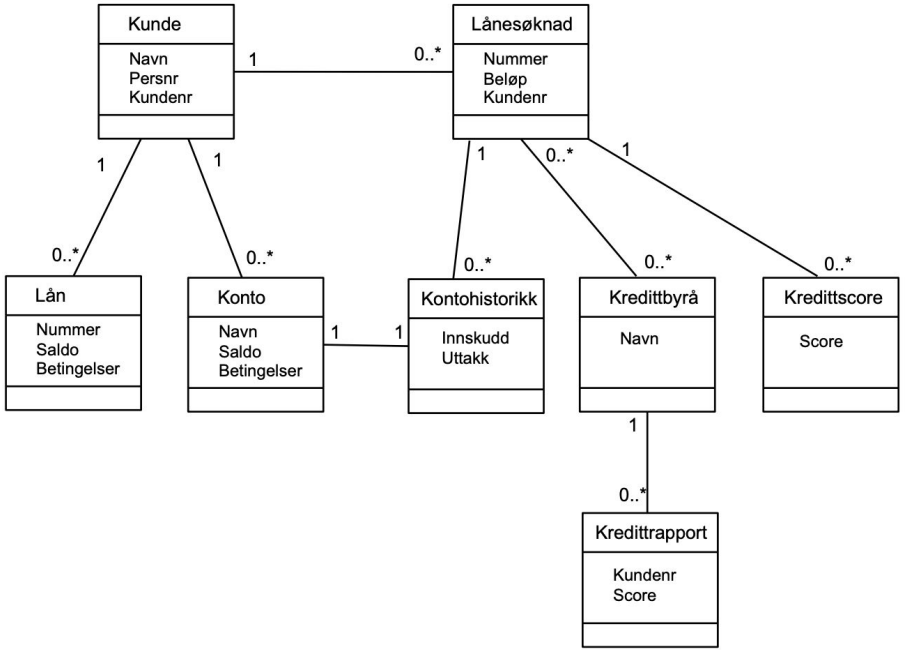


Klassediagram:

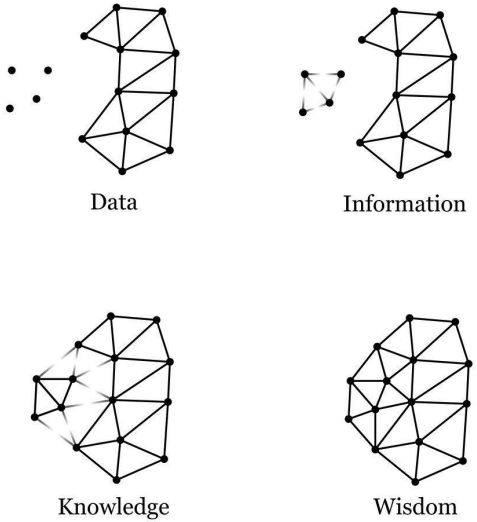
4.



Domenemodell - klassediagram uten metoder



Informasjonssikkerhet



Verdier, trusler, sårbarheter og tiltak

- **Verdier**
  - Informasjon av verdi
  - Personopplysningsvern for de registrerte (privatpersoner)
- **Trussel**
  - Et potensielt angrepsscenario som styres eller trigges av en trusselaktør, og som kan ha negative konsekvenser for verdier (brudd på sikkerhet/personvern).
- **Sårbarhet**
  - Fravær av sikkerhetstiltak mot trusler
- **Sikkerhetstiltak**
  - Metode for å forhindre trusler eller redusere konsekvenser

Informasjonssikkerhet

Beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet. I tillegg kan andre egenskaper, f.eks. autensitet, sporbarhet, uavviselighet og pålitelighet omfattes (ISO 27000:2016)

Informasjonssikkerhet

- Informasjonssikkerhet = beskytte **informasjonsressurser** mot skade.

- Eksempel på informasjonsressurser som skal beskyttes:
  - Data, programvare, konfigureringer, utstyr og infrastruktur

- Dekker tilsiktet og utilstiktet skade
  - Trusselagenter → mennesker eller naturlige hendelser
  - Mennesker kan gjøre skade tilsiktet/utilsiktet

Sikkerhetsmål K.I.T.

SIKKERHETSMÅL OG SIKKERHETSTILTAK

- ***Sikkerhetsmål***
  - En egenskap man kan ønske å oppnå eller tilby
  - Kan oppnås og ivaretas med ulike sikkerhetstiltak
  - Uavhengig av spesifikk implementering
- ***Sikkerhetstiltak***
  - Tiltak for å oppnå/ivareta sikkerhetsmål
  - Basert på spesifikk implementering
  - Benyttes for å forebygge, oppdage eller gjenopprette

Konfidensialitet

● At informasjon ikke blir gjort tilgjengelig eller vist til uautoriserte individer, entiteter eller prosesser.

● **Trusler:**
  ○ Datatyveri
  ○ Datalekkasje
  ○ Angrep: Session hijacking attacks (impersonating)
  ○ Have I been pwnd ?

Eksempler på sikkerhetstiltak:

- Kryptering
- Autentisering og tilgangskontroll
- Anonymisering
- Skallsikring
- Bevissthet

Integritet

- **Dataintegritet**: å sikre at data ikke blir endret/slettet på en uautorisert måte
- **Systemintegritet**: å opprettholde korrekthet og kompletthet av dataressurser
- **Trusler:**
  - Ødelagte data og miskonfigurerte systemer
  - Virus, Spam
  - System er ikke lenger til å stole på
  - Angrep: SQL poisoning, cross-site scripting attacks
  - Hydro & Løsepengeviruset
- **Eksempler på sikkerhetstiltak:**
  - Kryptografisk integritetssjekk
  - Konfigurasjonsstyring
  - Endringsledelse
  - Tilgangskontroll
  - Skallsikring
  - Sertifisert programvare
  - Bevissthet

Tilgjengelighet

- Å sikre at data og tjenester er tilgjengelige og anvendbare ved forespørsel fra en autorisert entitet

- **Trusler**:
  - Løsepengevirus
  - Tjenestenekt (DoS / DDoS)
  - Hindring av autorisert tilgang til ressurser
  - Forsinkelse av tidskritiske funksjoner

Eksempler på sikkerhetstiltak:

- Redundans av ressurser
- Backup
- Hendelsesrespons og beredskap
- Failover-konfigurasjon

Sikkerhetsmål - opprettholde:

Konfidensialitet: jeg skal **ikke se** data jeg ikke skal kunne se.

Integritet: jeg skal **ikke endre** data jeg ikke skal kunne endre.

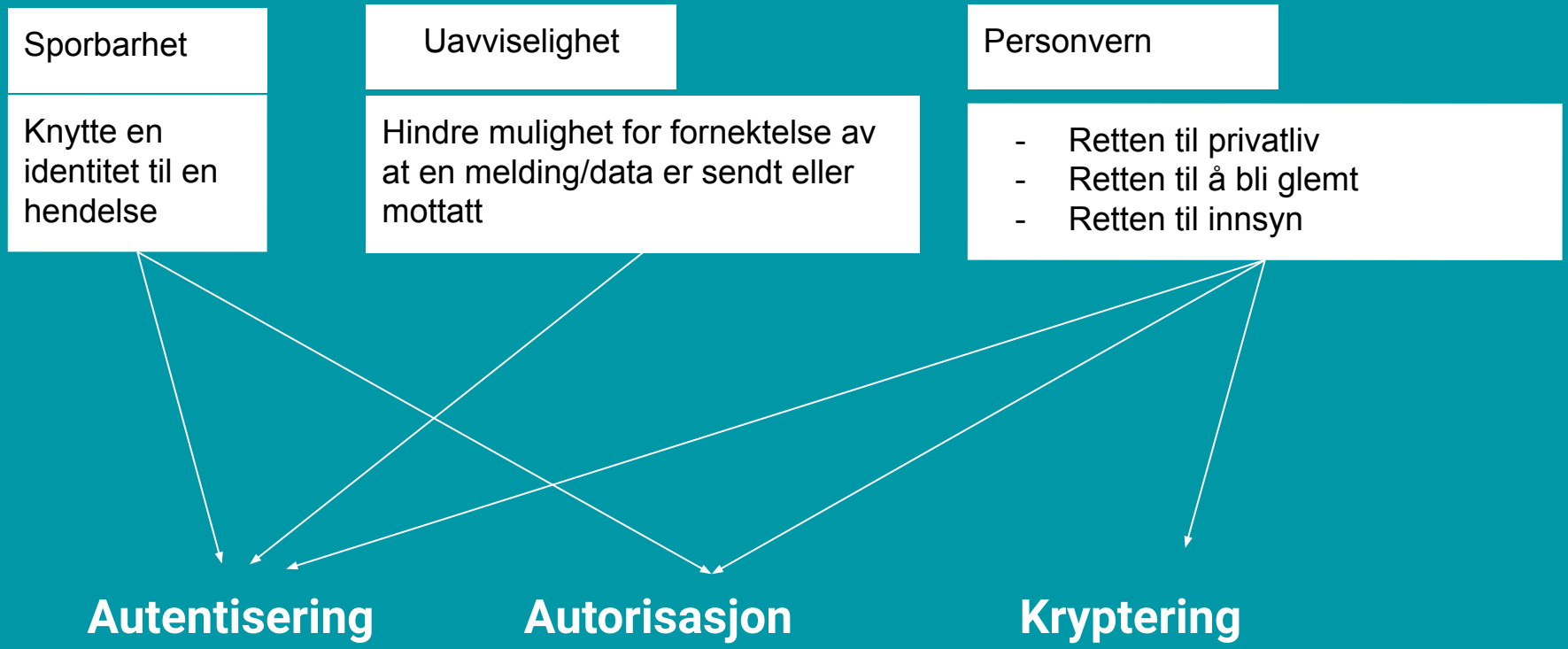
Tilgjengelighet: jeg **skal kunne gjøre det jeg vil** med data jeg skal kunne gjøre det jeg vil med.

Sikkerhetstiltak

Hva gjør vi da?

Konfidensialitet	Integritet	Tilgjengelighet
Tilgangskontroll Skallsikring Kryptering	Tilgangskontroll Endringskontroll Kryptografiske algoritmer Skallsikring	Sikkerhetskopier Redundante system (flere enheter) Gode rutiner for hendelseshåndtering og gjenoppretting

Flere begrep og hvordan vi kan sikre det



Hva gjør vi da?

Autentiserer: er bruker bruker?

Autoriserer: utdeling av rettigheter

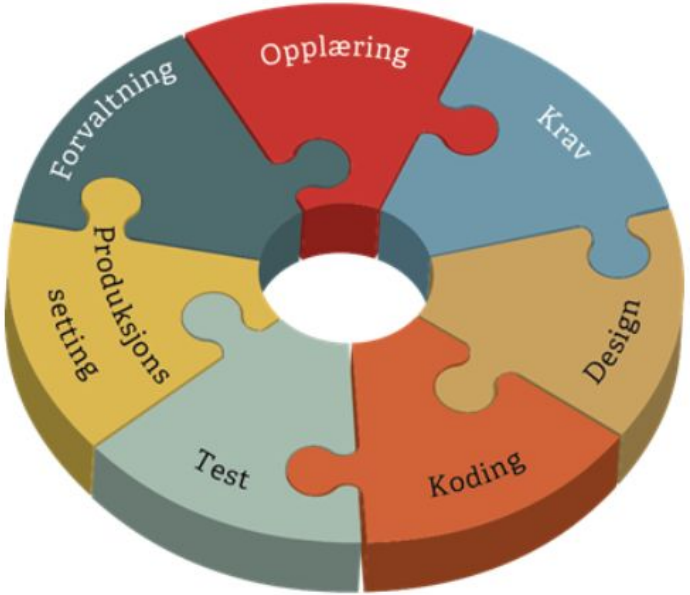
Krypterer: hold data hemmelig

Tiltakskategorier

Fysiske tiltak	Tekniske tiltak	Administrative tiltak
Låse inn Overvåke Adgangskontroll Strømførsel	Autentisering Kryptering Autorisering	Opplæring Bakgrunnssjekk Internkontroll

PREVENTIVE	DETEKTIVE	KORRIGERENDE

Innebygd personvern og informasjonssikkerhet:



Information Security Management

Hvordan og hvem finner og håndterer farene?

Globalt:
ISO: International Organisation for Standardization -- ISO27001-standarden
OWASP: Open Web Application Security Project

Organisasjon (lokalt):
Ledelsen: hvilke mål og prioriteter bedriften skal sette.
Internkontroll: ansvar for å **sette i livet** de mål og prioriteringer bedriftens styre har definert.
Drift: ansvar for å **drifte** de mål og prioriteringer bedriftens styre har definert.

Ukesoppgaver

Trussel
Trusselaktør
Sårbarhet

Trusselscenario
Trusselmodellering

Sporbarhet
Uavviselighet
Internkontroll
Styring

Risikovurdering
Risiko
Verdi
Konsekvens

Personvern

Konfidensialitet
Integritet
Tilgjengelighet

Fysiske tiltak
Administrative tiltak
Tekniske tiltak
Preventive tiltak
Detektive tiltak
Korrigerende tiltak

Autentisering
Autorisering
Kryptering
Skallsikring
Tilgangskontroll
Sikkerhetskopier

Official website of the Department of Homeland Security

jehank@uio.no