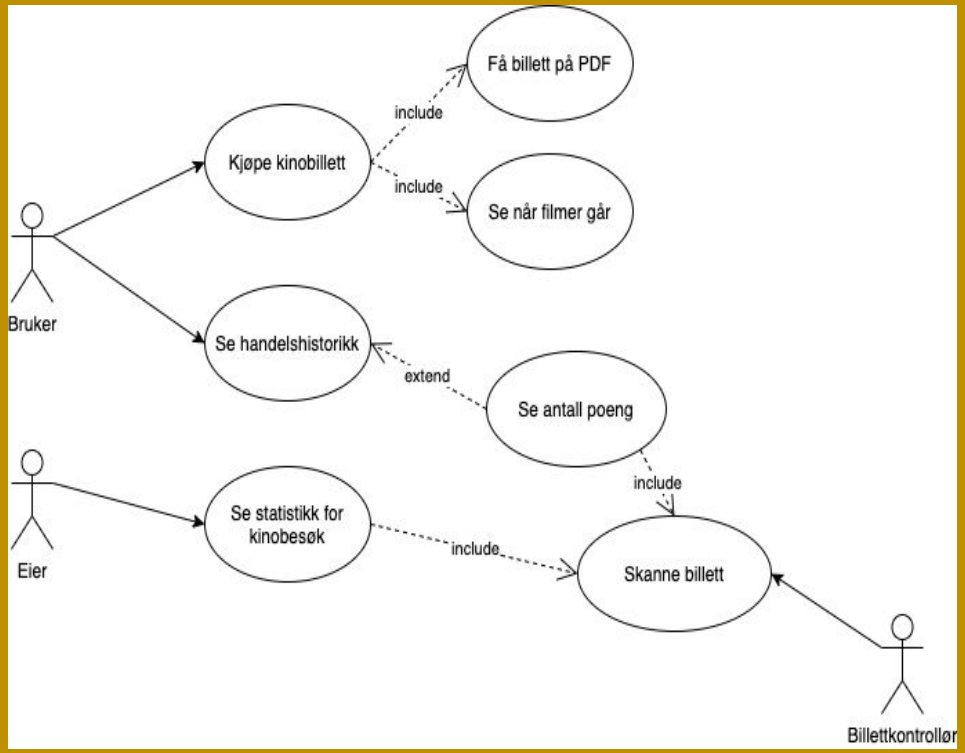
Krav om informasjonssikkerhet

IN1030 - Gruppe 4

Dagens plan

- Gjennomgang av oblig 5
- Repetisjon UML modellering
- Kjapp gjennomgang av informasjonssikkerhet (en del repetisjon fra IN1020)
- Ukesoppgaver + obligjobbing

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

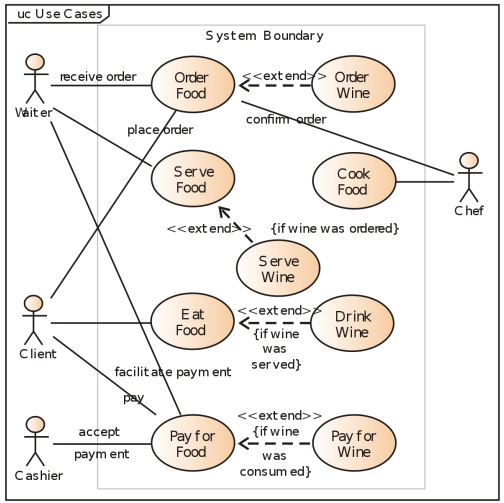
Extend-relasjonen

- 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

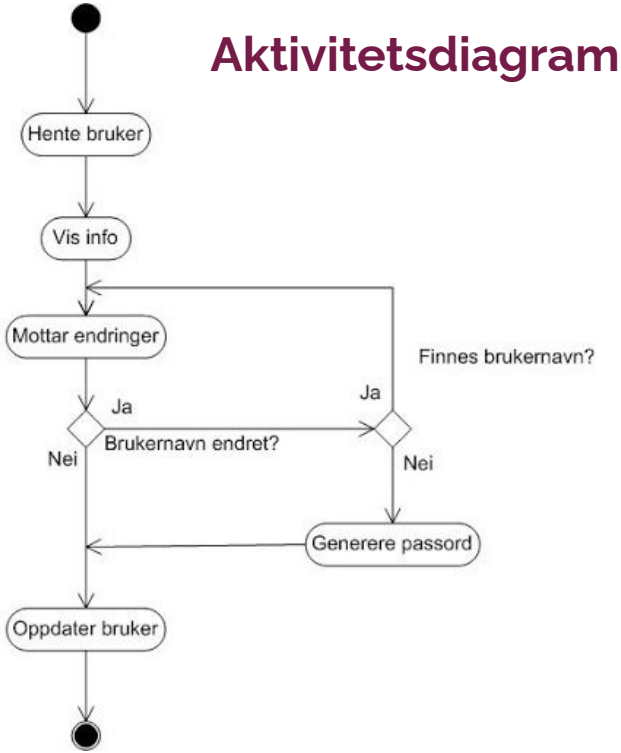
Use Case-diagram:

1.



Aktivitetsdiagram:

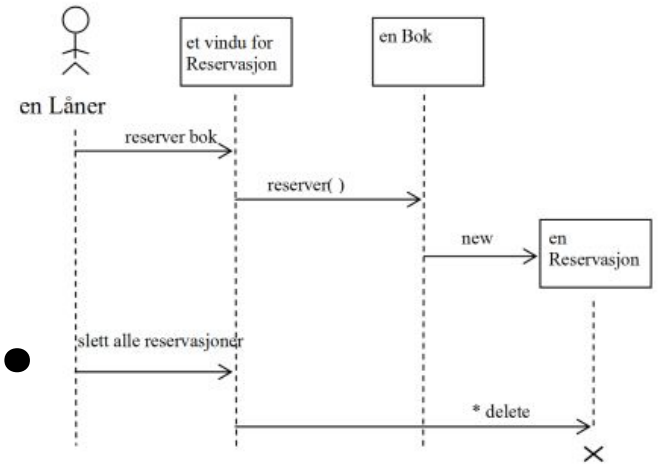
2.



Diagrammer for dette emnet

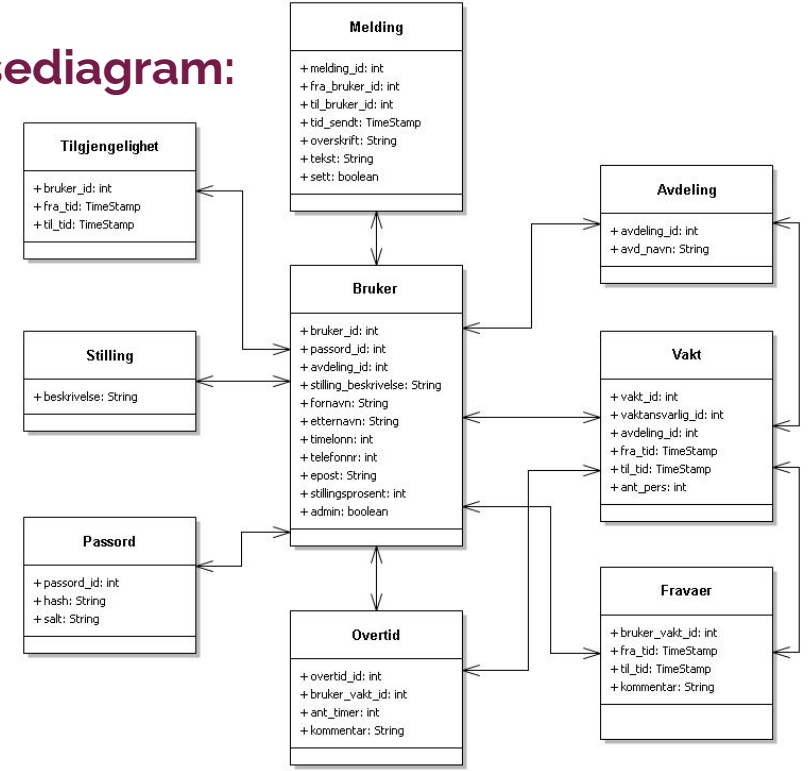
Sekvensdiagram:

3.

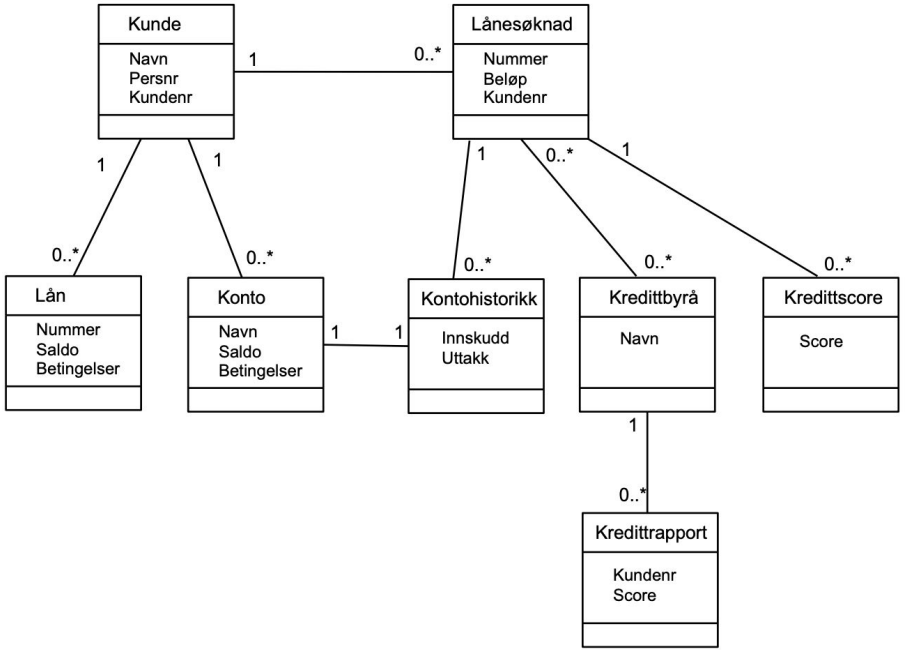


Klassediagram:

4.



Domenemodell - klassediagram uten metoder



IN1020 - Oblig1

VERDIER → TRUSSELAKTØRER

Sikkerhetstiltak → K.I.T (konfidensialitet, integritet, tilgjengelighet)

Sporbarhet og autentisering

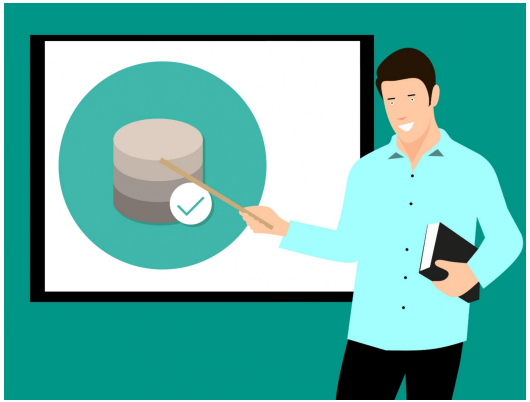
Private policy - policy for autorisasjon (tilgang)

Sikkerhetsmål: K. I. T.

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 er skal kunne gjøre det jeg vil med.



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

Sikkerhetsmål K.I.T.

Konfidensialitet

- At informasjon ikke blir gjort tilgjengelig eller vist til uautoriserte individer, entiteter eller prosesser.
- Trusler:
    - Datatyveri
    - Datalekkasje

- 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
- 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:
    - Tjenestenekt
    - Hindring av autorisert tilgang til ressurser
    - Forsinkelse av tidskritiske funksjoner
- Eksempler på sikkerhetstiltak:
    - Redundans av ressurser
    - Backup
    - Hendelsesrespons og beredskap
    - Failover-konfigurasjon

Tiltakskategorier

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

Tiltak kan gjøres i ulike faser:

PREVENTIVE	DETEKTIVE	KORRIGERENDE

Hva gjør vi da?

Autentiserer

Autoriserer

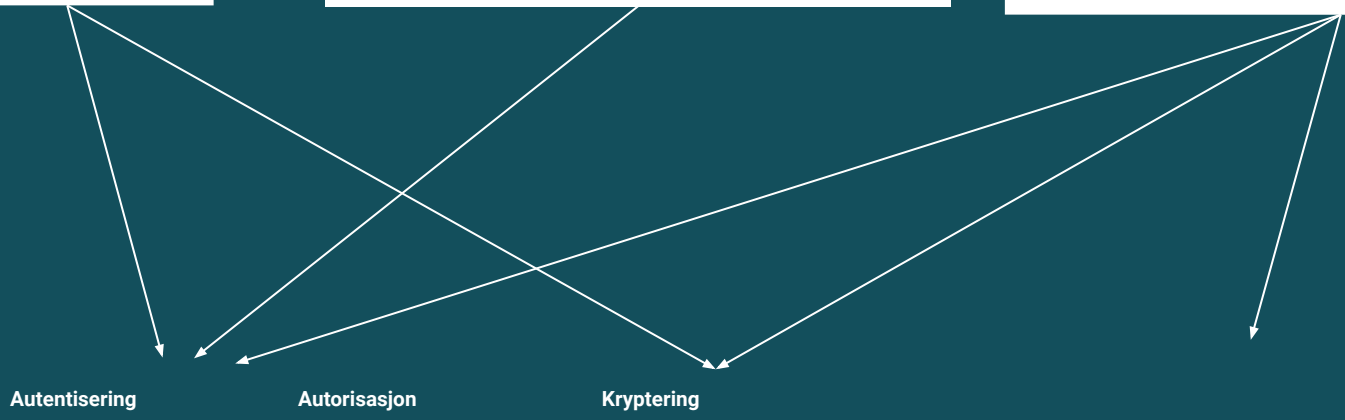
Krypterer

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

Sporbarhet	Uavviselighet	Personvern
Knytte en identitet til en hendelse	Hindre mulighet for fornektelse av at en melding/data er sendt eller mottatt	- Retten til privatliv - Retten til å bli glemt - Retten til innsyn



Verdier, trusler, sårbarheter og tiltak

- Verdier
  - Informasjon av verdi
  - Konfidensialitet, integritet og tilgjengelighet for data og systemressurser tilhørende organisasjoner
  - 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

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