

IN2120 – Informasjonssikkerhet

Del 1b: Begreper om informasjonssikkerhet

Audun Jøsang

Gudmund Grov

Nils Petter Wien



Høst 2023

Universitetet i Oslo

Betydninger og oversettelse av begrepet “sikkerhet”

Engelsk

- Security →
- Safety →
- Certainty →

Norsk

- Sikkerhet
- Trygghet
- Visshet



Presis oversettelse

- Security
 - Safety
 - Certainty
- } →

- Sikkerhet



Upresis oversettelse


Presis eller tvetydig oversettelse av begrepet “ansvar”

Engelsk

Norsk

- Responsibility → • Ansvar (for mellomledere og medarbeidere)
(operativt ansvar, å ha som oppgave)
- Accountability → • Regnskapelighet (for toppledere og eiere)
(overordnet ansvar, å stå til regnskap)



- Responsibility }
• Accountability } • Ansvar  *Tvetydig*

Hva er sikkerhet ?

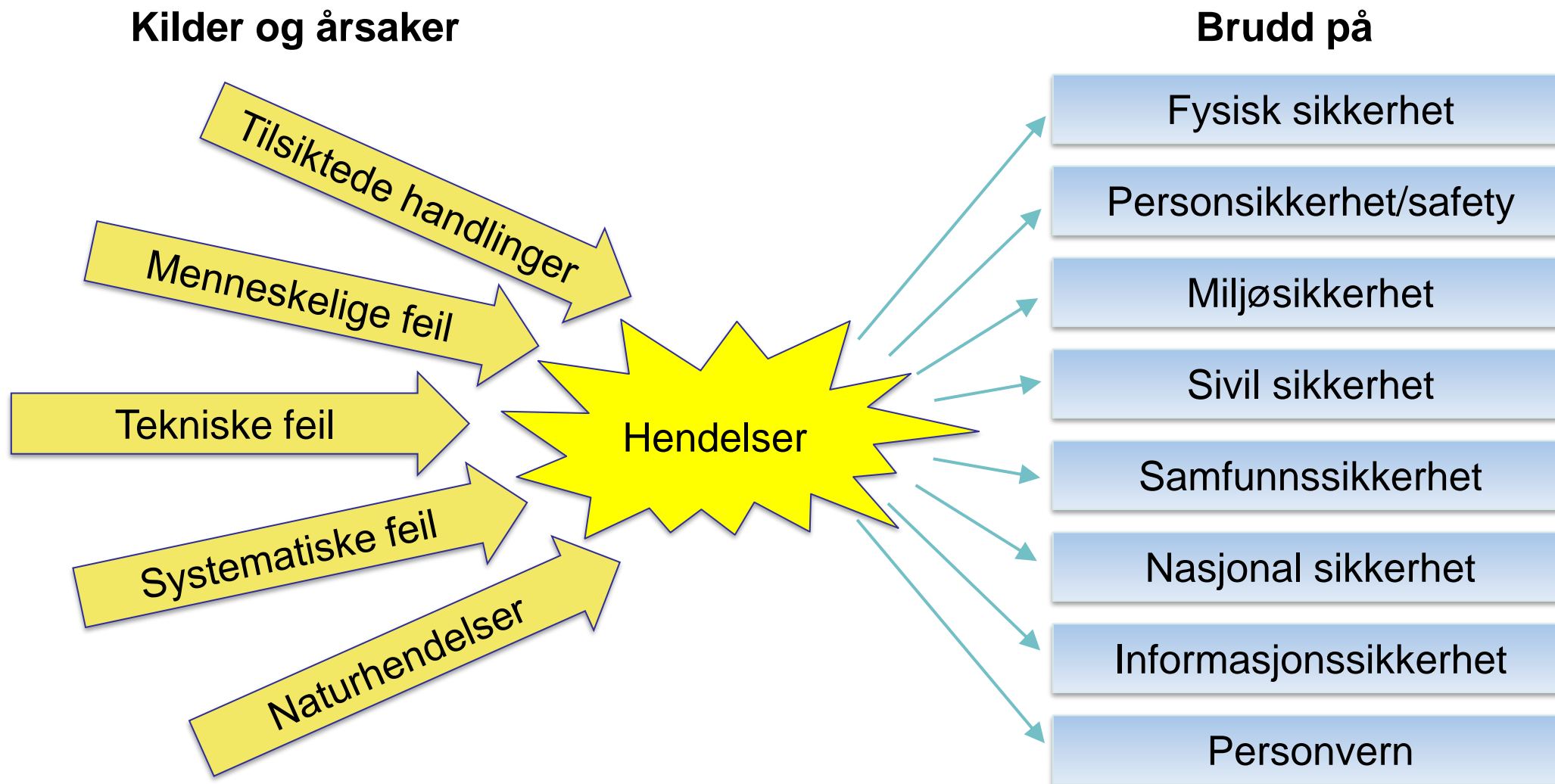
Sikkerhet er beskyttelse av verdier mot skade

eiendom, infrastruktur, demokrati, lov og orden, liv og helse, miljø, informasjon, persondata



- **Fysisk sikkerhet:** hindre innbrudd, tyveri og tukling med utstyr
- **Samfunnssikkerhet:** opprettholde funksjonalitet i kritiske infrastrukturer
- **Nasjonal sikkerhet:** demokrati, politisk stabilitet, territorial integritet
- **Sivil sikkerhet og rettssikkerhet:** opprettholdelse av lov og orden
- **Personsikkerhet / trygghet / safety:** beskyttelse av liv og helse
- **Miljø sikkerhet:** hindre forurensing og fremmede arter
- **Informasjonssikkerhet:** beskyttelse av informasjonsverdier
- **Personvern:** følge prinsipper for innhenting, lagring, behandling og deling av personopplysninger

Ulike kilder til brudd på sikkerhet



Hva er informasjonssikkerhet ?



- *Informasjonssikkerhet* er å beskytte *informasjonsverdier* mot skade.
- Hvilke informasjonsverdier skal beskyttes?
 - Eksempel: data, programvare, konfigureringer, utstyr og infrastruktur
- Hvordan kan informasjonsverdier skades?
 - Brudd på et eller flere av sikkerhetsmålene Konfidensialitet, Integritet og Tilgjengelighet (KIT)
- Dekker både tilsiktet og utilsiktet skade
 - Trusselaktører kan være mennesker eller naturlige hendelser
 - Mennesker kan gjøre skade både tilsiktet og utilsiktet
- Definisjon av informasjonssikkerhet:
 - ***Beskyttelse av informasjonens Konfidensialitet, Integritet og Tilgjengelighet.***
 - I tillegg kan andre egenskaper, f.eks. autentisitet, sporbarhet, ubenektelighet og pålitelighet omfattes. (ISO/IEC 27000:2018)*

Kjært barn har mange navn



- **Informasjonssikkerhet:** generelt begrep, dekker f.eks. også beskyttelse av informasjon på papir, populært fra 1970-tallet.
- **Datasikkerhet:** kan tolkes som beskyttelse av data, men også systemer, populært fra 1980-tallet.
- **IT-sikkerhet:** tolkes som sikkerhet i IT-systemer, populært fra 1990-tallet.
- **Cybersikkerhet:** tolkes ofte som sikkerhet for alt som har å gjøre med Internett og som er koblet til Internett, populært fra 2010-tallet.
- **Digital sikkerhet:** skapt av norske myndigheter i 2019, med hensikt å være et samlebegrep for alle begrepene ovenfor, rimer godt med «digitalisering» og ser ut til å bli populært fremover.
- I praksis betyr alle begrepene det samme, men deres popularitet har endret seg.
- «Informasjonssikkerhet» er brukt jevnlig gjennom hele denne perioden. Dessuten er «informasjonssikkerhet» en direkte oversettelse av det engelske «information security» som samtidig er nedfelt i en rekke internasjonale standarder og rammeverk.

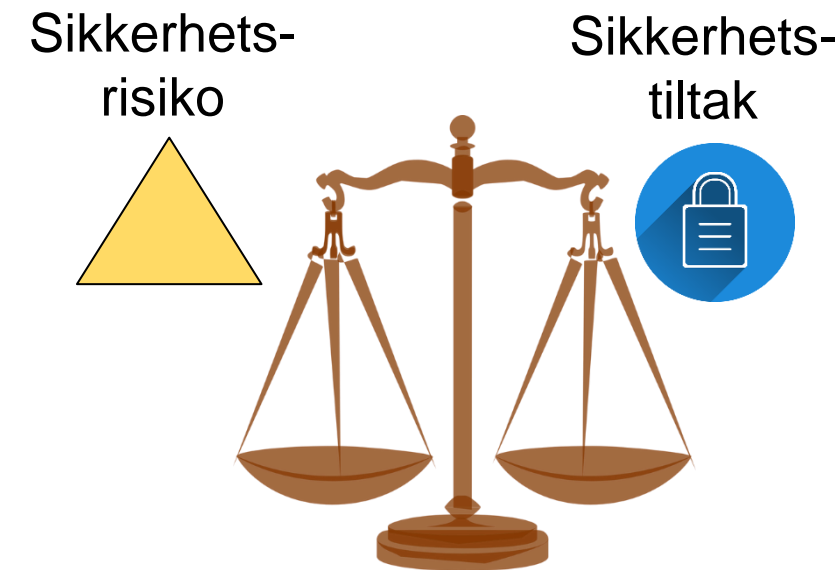
Kilder til krav om informasjonssikkerhet

- **Vanlig god praksis:** Krav om adekvat sikkerhet i forretningsprosesser i henhold til vanlig god praksis og forvaltning.
 - Vanlig god praksis setter f.eks. krav om brukerautentisering og tilgangskontroll.
- **Risikovurdering:** Krav om å begrense sikkerhetsrisiko til et akseptabelt nivå. Tiltak identifiseres gjennom risikovurdering og risikohåndtering.
 - Risikovurdering kan f.eks. sette krav om 2-faktorautentisering
- **Regelverk:** Juridiske, lovbestemte, regulatoriske og kontraktmessige krav til informasjonssikkerhet, f.eks.:
 - Sikkerhetsloven setter en rekke krav om sikkerhetstiltak for virksomheter som er underlagt loven.
 - GDPR setter krav om beskyttelse av persondata.
 - Juridiske krav om informasjonssikkerhet henviser ofte til at innføring av tiltak for informasjonssikkerhet må baseres på risikovurdering

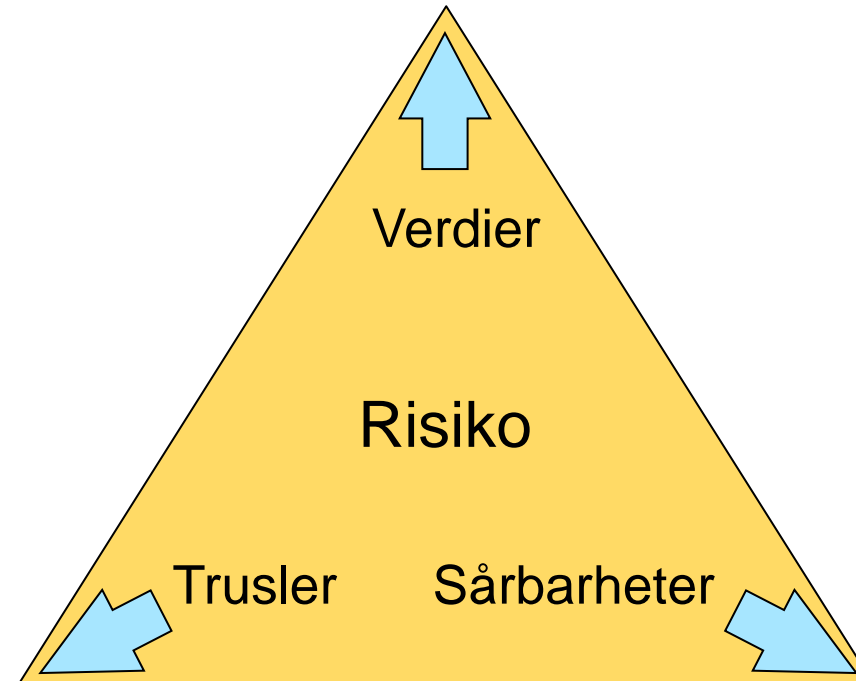


Målsetting for styring av informasjonssikkerhet

- Ville det være mulig å løse alle sikkerhetsproblemer?
- Nei, fordi:
 - Det oppdages stadig nye sårbarheter i gamle systemer
 - Nye digitale tjenester, ofte med sårbarheter, eksponeres online
 - Trusselaktører er flinke til å finne sårbarheter som kan utnyttes
 - Det utvikles stadig mer effektive angrepsverktøy
 - Økende antall og alvorlighet av trusler
- Konklusjon: Informasjonssikkerhet er en kontinuerlig prosess for å stoppe trusler og fjerne sårbarheter
- Målsetting for styring av informasjonssikkerhet er å oppnå god balanse mellom sikkerhetsrisiko og sikkerhetstiltak.



Generell risikomodel for IT-sikkerhet

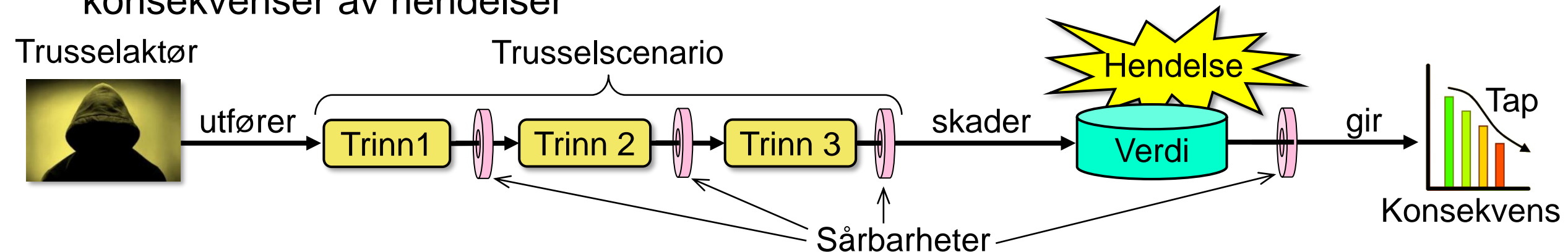


- **Generell modell for risiko**

- Jo større og flere verdier du har, jo større og flere trusler du er utsatt for, og jo mere sårbar du er, desto større risikoeksponering har du.

Verdier, Trusler, Sårbarheter og Tiltak

- **Verdier:** (Informasjons)ressurser som er av verdi for organisasjonen.
 - Data, systemer, applikasjoner, nettverk, enheter, tjenester, mennesker
 - Mål for informasjonssikkerhet er å beskytte verdienes KIT, avhengig av behov.
 - Person(opplysnings)vern
- **Trussel:** Et potensielt angrepsscenario som kontrolleres av en trusselaktør, som kan skade organisasjonens verdier
- **Sårbarhet:** Manglende sikkerhetstiltak mot trusler og evne til å håndtere hendelser.
- **Sikkerhetstiltak (Security Control):** Metode for å forhindre trusler eller redusere konsekvenser av hendelser



Tiltak/virkemidler/controller for sikkerhet



Sikkerhetstiltak – ulike faser

- **Preventive tiltak:**
 - Forhindre og avskrekke angrepsforsøk
 - Eksempel: kryptering av filer for konfidensialitet
- **Oppdagende/detektive tiltak:**
 - Varsle angrep som forsøkes eller som allerede er skjedd.
Eksempel: Inntrengingsdeteksjon (IDS)
- **Korrigerende tiltak:**
 - Gjenopprette skade på dataressurser etter angrep.
 - Eksempel: Hente backup av programmer og data ved tap/kompromittering av ressurser
- Det er alltid nødvendig å benytte en kombinasjon av tiltak fra alle tre faser for å opprettholde dekkende beskyttelse.

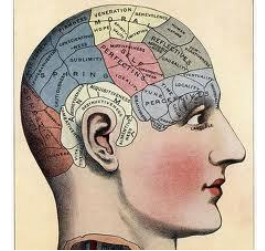


Sikkerhetstiltak for ulike datatilstander

- Informasjon/data kan befinne seg i ulike tilstander.
- Ulike tilstander krever ulike sikkerhetstiltak:

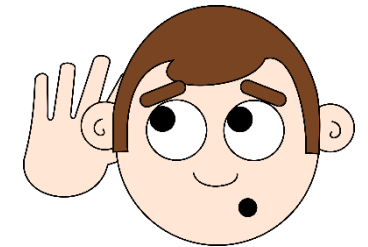
- Under lagring

- Fysiske media for lagring av informasjon
- Fysiske, digitale, eller mentale metoder for sikkerhet
- Eksempel tiltak: adgangs/tilgangskontroll, kryptering, holde på hemmeligheter, fysisk skjerming



- Under overføring

- Kabler (glassfiber eller kobber) radiobølger eller lyd
- Fysisk eller digitale metoder for sikkerhet
- Eksempel tiltak: kryptering eller fysisk skjerming



- Under prosessering (bruk)

- Operativsystemer og programmer som kjører på mikroprosessor
- Fysisk eller digitale metoder for sikkerhet
- Eksempel tiltak: OS-sikkerhet, tilrodd beregning, eller fysisk skjerming

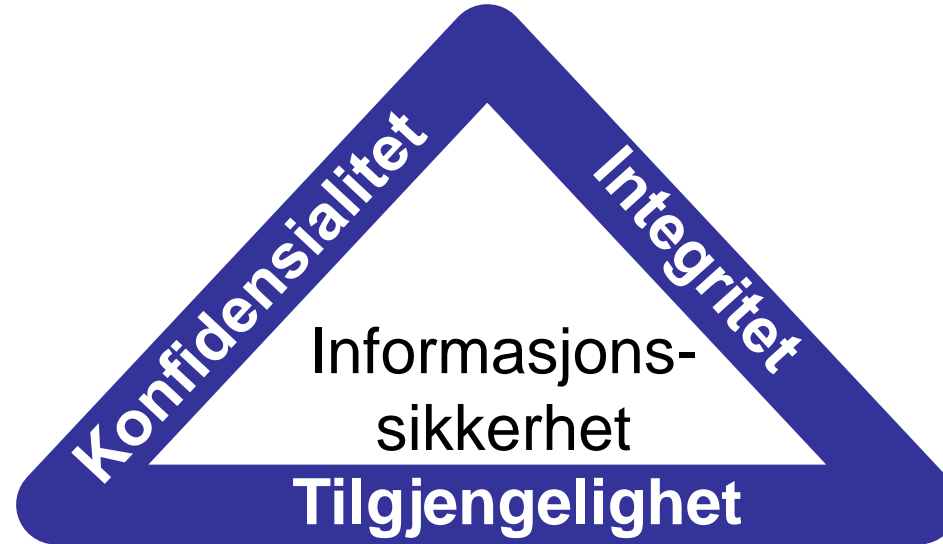


- Data / informasjon må beskyttes i alle tilstander

Generelle sikkerhetsmål: KIT+P

- Informasjonssikkerhet er tradisjonelt definert som opprettholdelse av KIT:

- Engelsk: CIA
 - Confidentiality
 - Integrity
 - Availability:



- Person(opplysnings)vern (data protection) er et tilleggsmål som bl.a. forutsetter KIT. GDPR (General Data Protection Regulation) definerer krav til personvern.

Personvern

Sikkerhetsmål og tiltak/controller

- Sikkerhetsmål
 - Uavhengig av spesifikk implementering
 - Kan implementers med ulike tiltak/controller
- Sikkerhetstiltak / controller / mekanismer
 - Basert på spesifikk implementering, ofte bundet til spesifikke produkter

Sikkerhetsmål:

Konfidensialitet – Integritet – Tilgjengelighet

støtter

Sikkerhetstiltak:

f.eks. låser – kryptering – autentisering - sikkerhetskultur



Analogi for sivil sikkerhet

Konfidensialitet

- Egenskapen av at informasjon ikke blir gjort tilgjengelig eller vist til uautoriserte individer, entiteter eller prosesser.
(ISO/IEC 27000)
- Trusler:
 - Datatyveri (ekstern trussel)
 - Datalekkasje (intern trussel).
- Sikkerhetstiltak eksempler:
 - Kryptering,
 - Kryptografiske kommunikasjonsprotokoller, f.eks. TLS
 - Autentisering og tilgangskontroll,
 - Anonymisering, f.eks. gjennom pseudonym eller VPN
 - Skallsikring
 - Sikkerhetskultur, bevissthet
 - ...



Integritet

- **Dataintegritet:** Egenskapen av at data ikke har blitt endret eller slettet på en uautorisert måte. (X.800)
- **Systemintegritet:** Egenskapen av å opprettholde korrekthet og komplettethet av dataressurser (ISO/IEC 27000)
- Trusler: Ødelagte data og mis konfigurerte systemer
- Sikkerhetstiltak eksempler:
 - Hashing, MAC, kryptering
 - Konfigurasjonsstyring
 - Endringsledelse
 - Autentisering
 - Tilgangskontroll
 - Sertifisert programvare
 - Sikkerhetskultur, bevissthet
 - ...

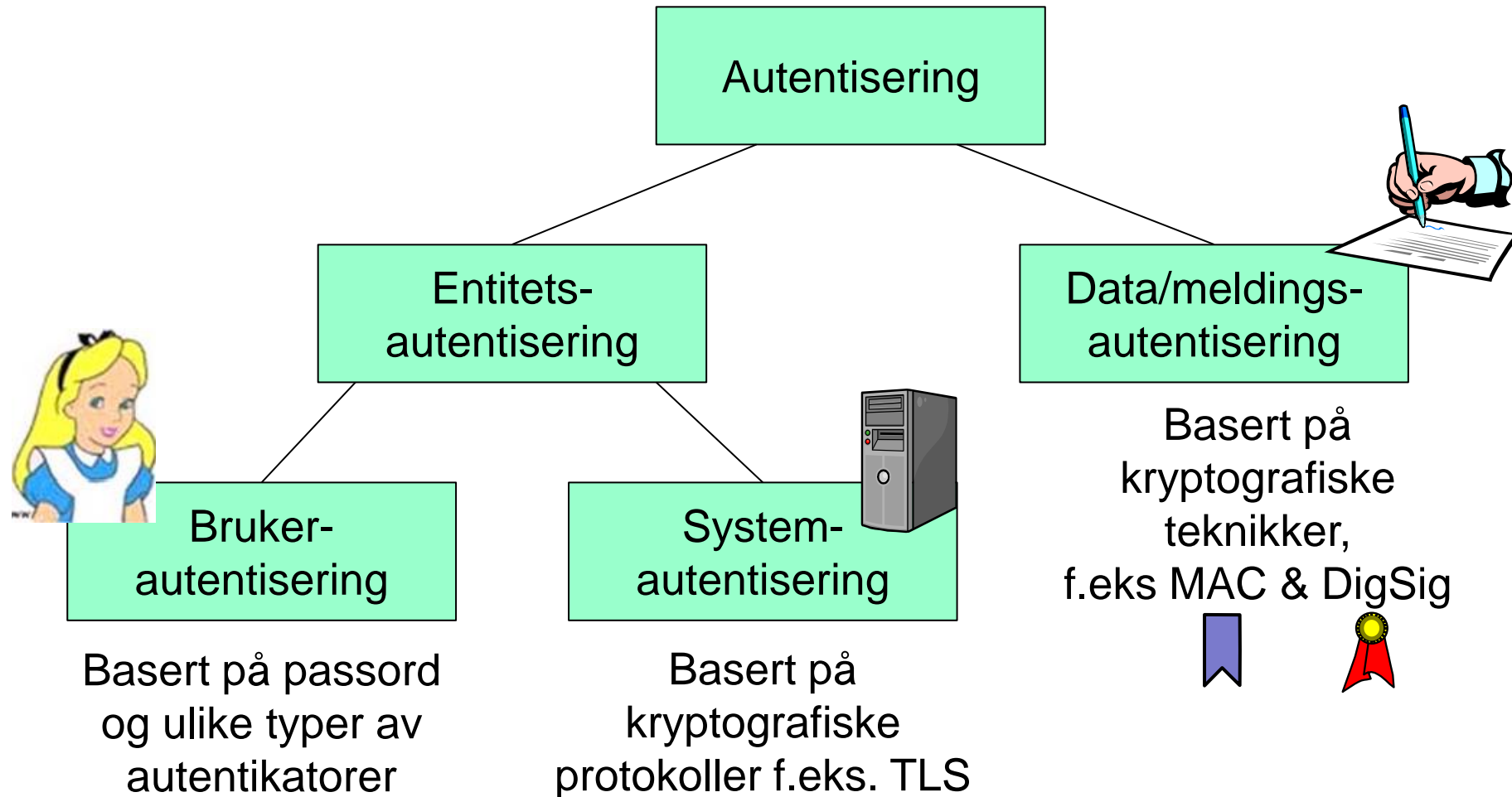


Tilgjengelighet

- Egenskapen av at data og tjenester er tilgjengelige og anvendbare ved forespørsel fra en autorisert entitet. (ISO/IEC 27000)
- Trusler:
 - Tjenestenekt, overlastangrep (DoS / DDoS)
 - Løsepengevirus
 - Forsinkelse av tidskritiske funksjoner.
- Sikkerhetstiltak eksempler:
 - Redundans av ressurser,
 - Failover-konfigurasjon
 - Brannmur
 - Sikkerhetskopiering (backup)
 - Hendelsesrespons og beredskap,



Typer av autentisering

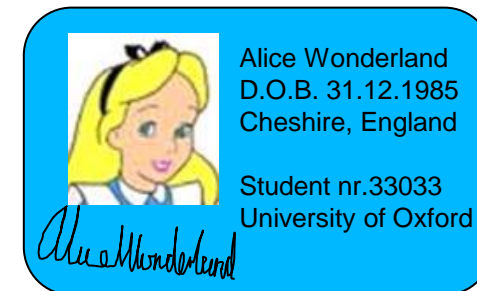


Brukerautentisering

- Oppgi bruker-ID (selv-identifisering)
 - Bruker oppgir (påstår å ha) en bestemt identitet
- Autentisering med autentikator(er)
 - Bevis at du har identiteten du påstår å ha
- Trussel: Identitetstyveri, falsk innlogging
- Sikkerhetstiltak: Autentikatorer, f.eks.:
 - Passord,
 - Personlig kryptografisk brikke,
 - BankID, OTP-generator
 - ID-kort
 - Biometri
 - Sekundære kanaler
 - 2FA, multifaktorautentisering

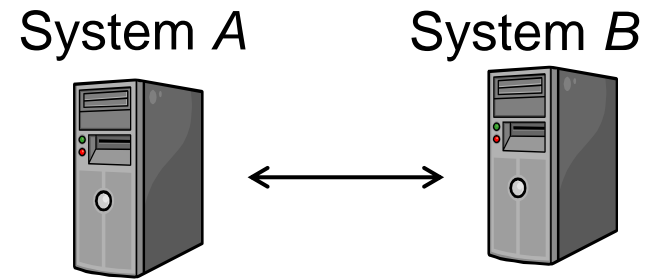


Oppgi bruker-ID



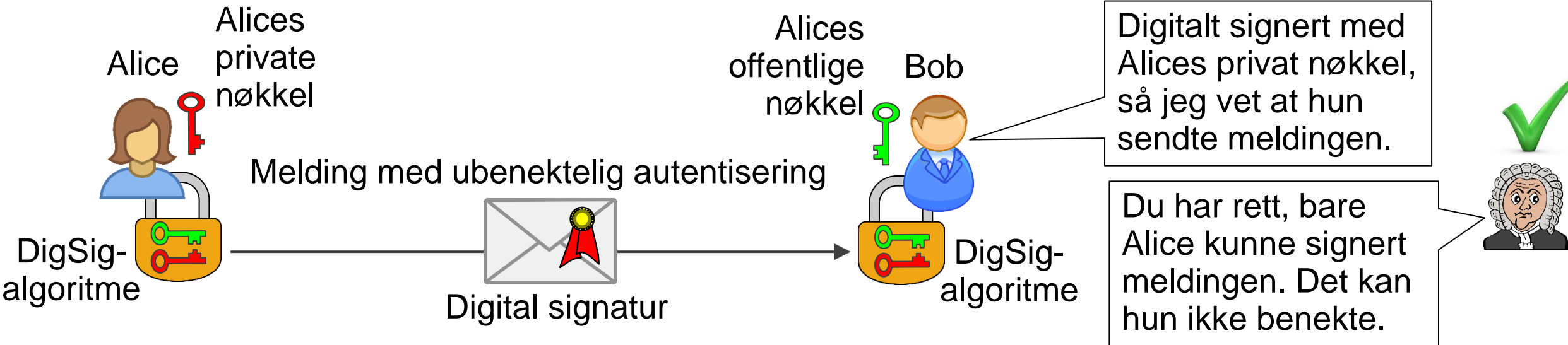
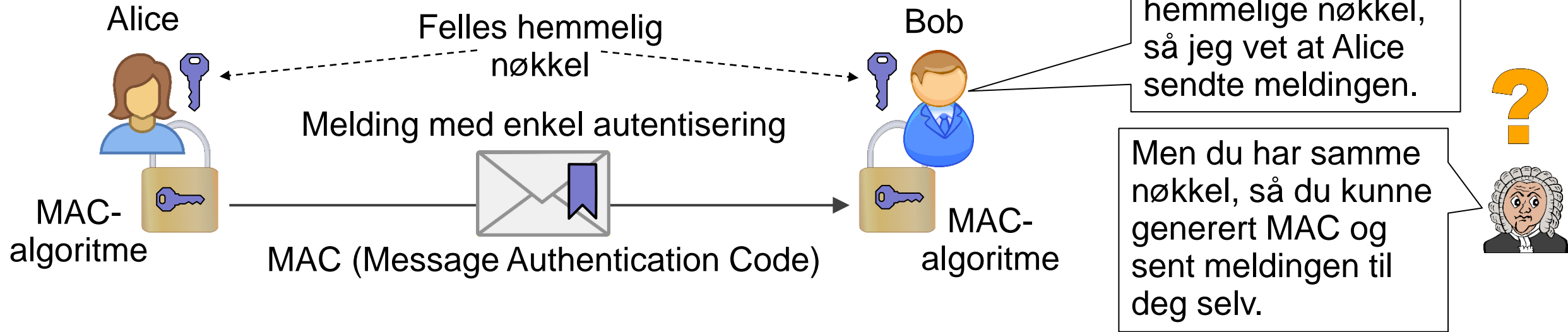
Autentikator for
autentisering

Systemautentisering



- **Formål**
 - Korrekt identifisering av systemer gjennom nettverk
- **Trusler:**
 - Falske systemer
 - Falske transaksjoner
 - Man-in-the-middle angrep
 - Nettverksinnbrudd
- **Sikkerhetstiltak:**
 - Kryptografiske protokoller for autentisering og integritet
 - For eksempel: TLS, IPSEC

Enkel eller ubenektelig meldingsautentisering



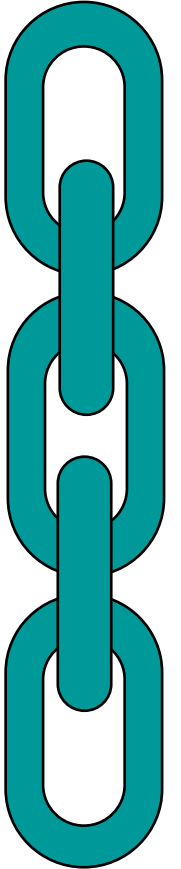
Sporbarhet (Accountability)

- Formål: Å kunne spore hendelser og handlinger til bestemte brukere og entiteter, slik at de må stå til regnskap for sine handlinger (to be accountable)
 - *Logger må oppbevares og beskyttes, slik at handlinger som påvirker sikkerheten kan spores til rette vedkommende.* (TCSEC/Orange Book)
- Trusler:
 - Å ikke være i stand til å identifisere hvem som stod bak en handling
 - Å mangle tilstrekkelig bevis for å kunne gjøre anmeldelse
- Sikkerhetstiltak:
 - Autentisering av alle brukere
 - Logging av systemhendelser
 - Elektroniske bevis
 - Ubenektelighet med digital signatur
 - Digital etterforskning



Pålitelighet

- Egenskapen at systemer ikke inneholder (mange) feil eller svakheter. Hvis feil likevel forekommer, betyr pålitelighet også at systemene kan tolerere visse feil uten at (all) funksjonalitet faller ut.
- Fokuserer mest på å forhindre ikke-tilsiktete hendelser, men er også viktig for å forhindre eller redusere konsekvens av tilsiktete hendelser.
- Trusler:
 - Lav kvalitet i utvikling, konfigurering, feilretting og drift av systemer samt spesielt manglende oppmerksomhet på sikker systemutvikling.
- Tiltak:
 - God (eller beste) praksis for sikker utvikling og drift av systemer, som også kalles «innebygd informasjonssikkerhet»



Tilgangsautorisering



- Tilgangsautorisering er å spesifisere tilgangsrettigheter for entiteter, dvs. for brukere, roller og prosesser
 - Spesifiserer hvem som skal ha tilgang til hva
 - Autoriseringspolicyen er vanligvis definert av mennesker
 - Autoriseringspolicyen blir formalisert som regler og konfigureringer for tilgangskontroll i systemer.
- Autorisering kan bli delegert
 - Leder → Sys.Admin → Bruker
- Vær oppmerksom på forvirring i andre lærebøker og kilder:
 - Noen steder defineres tilgangsautorisering som ekvivalent med tilgangskontroll. Dette er fullstendig feil, fordi den gjør definisjonen på konfidensialitet meningsløs, på den måten at det ikke ville være et brudd på konfidensialitet hvis en hacker får tilgang til en konto med et cracket passord og stjeler data.

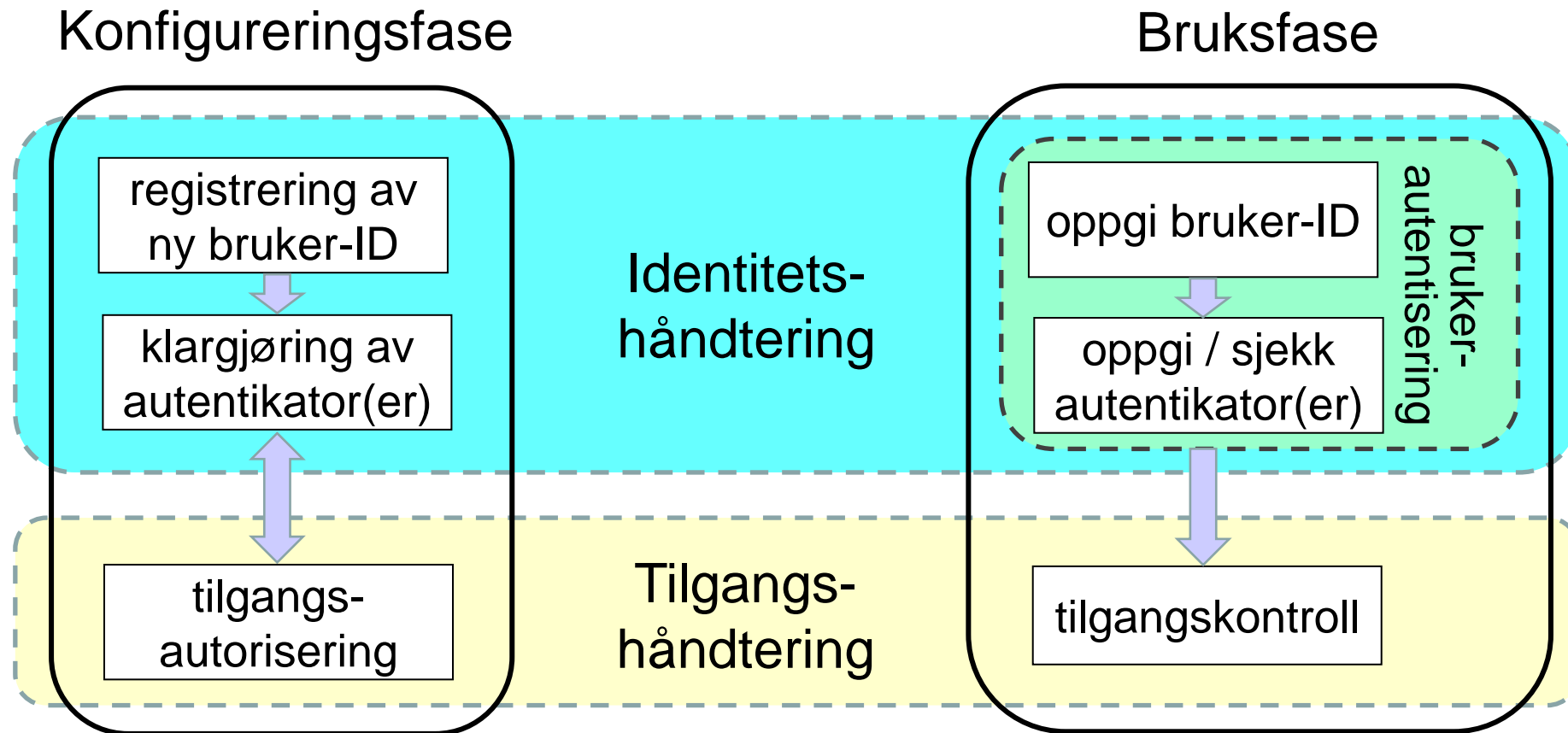
Tilgangskontroll



- Tilgangskontroll foregår etter at brukeren er autentisert.
- Brukeren/entiteten må være autentisert for at systemet skal vite hvem som prøver å utføre en handling eller forespør tilgang.
- Tilgangskontroll benytter autoriseringspolicy/regler for å avgjøre om brukeren er autorisert for tilgang til ressurser.
- Policy/regler for tilgangsautorisering defineres under konfigureringsfasen slik at tilgangskontroll kan utføres under bruksfasen.
- Mange ulike måter å definere regler for tilgangskontroll, f.eks.
 - Identitetsbasert (DAC)
 - Merkebasert (MAC)
 - Rollebasert (RBAC)
 - Attributtbasert (ABAC) (generalisering av alle måtene ovenfor)

Identitets- og tilgangshåndtering IAM

Identity and Access Management



Slutt på presentasjonen

