

UiO : Institutt for informatikk

Hvem er hvem på internett?

Hvordan kunne stole på digitale aktører.

IN1020 – Introduksjon til datateknologi

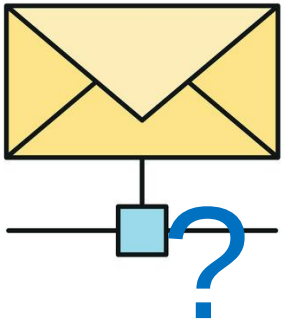
27.08.2025

Kristin Skar
kritisk@ifi.uio.no

Problemstilling







Skatteetaten

I dag: Hvem er hvem på internett?

Hvordan kunne stole på digitale aktører

Ressurser:

- Forelesning 27.08.25
- Notat om sikkerhet uke 2
- Ukeoppgaver og pensumlitteratur
  (Heide/Nätt: Kap 4, 5 (123-128) og 6 (145-157))

Nøkkelord:

- Autentisitet
- Autentisering
- Tilgangskontroll

Entiteter og identiteter

- Entitet?
  - Noe som har fysisk, juridisk eller prosessuell eksistens
  - Entiteter kan gis en *identitet*, som gjør det mulig å referere til entiteten
- Identitet?
  - Representasjon av entiteten, gjennom et sett med attributter som er tilordnet entiteten
  - *Kan kjenne igjen entiteter basert på identiteten*
  - Som regel har man *identifikator*
- Digital identitet?
  - Digital representasjon av en *entitet*, gjennom bruk av digitale, maskinlesbare data (*attributter*)

Autentisitet

- Hvordan muliggjøre tillitt til at *identiteter (entiteter)* er autentiske:
  - Autentisk *individ (bruker, person)*?
  - Autentisk *organisasjon*?
  - Autentisk *(data)system*?

- I tillegg ønske om
  - Autentisk *opprinnelsen til data* (ofte kalt *en melding*)?

Sikkerhetsmål

- Konfidensialitet
- Integritet
- Tilgjengelighet
- Autentisitet
- Uavviselighet
- Sporbarhet
- Personvern



- Brukerautentisitet
- Organisasjonsautentisitet
- Systemautentisitet
- Dataautentisitet

Identitetshåndtering

- Identitetshåndtering er *prosessen med å registrere og autentisere identiteter*

Autentisering

- Autentisering er mekanismen for å bekrefte en hevdet identitet:
  - *brukerautentisering*
  - *organisasjonsautentisering*
  - *systemautentisering*
  - *dataautentisering*

Brukerautentisering

Å verifiserer en hevdet identitet for en bruker.

- Hvordan oppnå *brukerautentisitet* (også kalt *personautentisitet*)?
  Svar: Bruk av *autentiseringsfaktorer*



Brukerautentisering

Autentiseringsfaktor

- Tre hovedkategorier *bevismateriale* (autentiseringsfaktor) for identitet: Noe du vet, noe du har og/eller noe du er
- I tillegg:
  - Andre mekanismer, som SMS eller e-post til *en kanal du har kontroll* over
  - Kombinasjon av flere

"Always remember the three main authentication factors: What can be easily guessed, what can be left in a cab, and what can be chopped off"

Autentiseringsfaktor: Noe du vet

Eksempler:

- Passord til IT-system
- Kode til elektronisk dørlås
- Mønster du husker

Fordel?

- Du har det alltid med deg

Ulempe?

- Lett å glemme
- Lett å gjette for uvedkommende
- Lagres på datamaskin? Nedskrevet?
- Lagres hos tjenesteleverandør
- Ikke veldig sikkert

Autentiseringsfaktor: Noe du har

Eksempler:

- Nøkkel til lås
- Engangspassord fra *kodegenerator*
- SIM-kort
- Kontaktløse brikker (RFID-kort)
- *FIDO*-enhet

Fordel?

- Du slipper å huske

Ulempe?

- Lett å miste
- Kan stjeles/«lånes»
- Glemmes hjemme?

Autentiseringsfaktor: Noe du er - *biometri*

Eksempler:

- Ansiktsgjenkjenning
- Fingeravtrykk
- Scanning av øyet
- Signatur
- Ganglag

Fordel?

- Du slipper å huske
- Du har det alltid med deg

Ulempe?

- Unikt nok?
- Permanent nok?
- Sikkert nok?
- Krever ekstrautstyr (sensorer, lesere, ol)
- Ressurskrevende å sammenligne

123456	1234567	abc123
password	football	starwars
12345678	iloveyou	123123
qwerty	Admin	dragon
12345	monkey	passw0rd
123456789	welcome	Master
letmein	login	superman

Kan koder/passord knekkes?

- Passord lagres kryptert
- Likevel kan de «knekkes»:
  - Intelligent søk. Kunnskap om deg?
  - Systematisk gjetting *(brute-force)* og «ordlisteangrep»
  - Utnytte svakheter i datasystemene

- https://haveibeenpwned.com/

Flerfaktor-autentisering

Utfordring: Passord kan gjettes, objekter kan mistes/stjeles

Løsning: Autentisering med kombinasjon av flere faktorer

- Kombinasjon av to eller flere ulike faktorer
- Øker sikkerheten betydelig, men autentisering blir mer tungvint for den som skal autentisere seg.
- Økende antall tjenester tilbyr flerfaktor- eller tofaktor-autentisering (2FA)

Autentiseringsløsning som tjeneste

Aktører tilbyr elektronisk identitet og autentisering som en tjeneste.

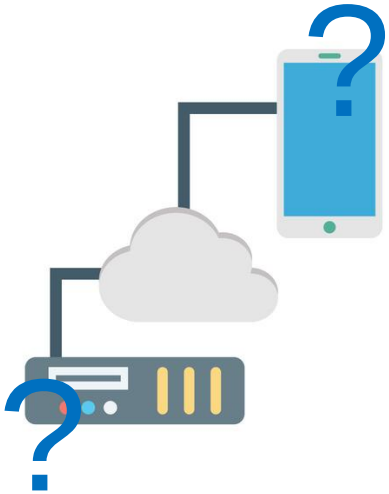
- **Eksempler**: BankID, Feide, Google, Facebook, etc.
- **Fordeler**?
  - God kompetanse, ekspertise og dermed økt sikkerhet i tjenesten som tilbys
  - Brukerne må forholde seg til færre brukeridentiteter/passord
- **Ulemper**?
  - Knekkes autentiseringsfaktoren(e) vil hackere ha tilgang til flere tjenester som deg.
  - Vane å logge inn gjør oss til et enkelt mål for svindel.

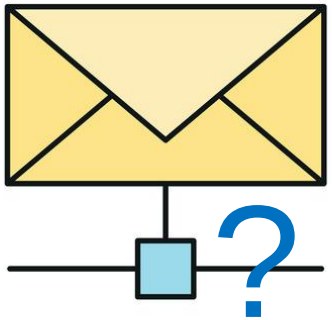
Elektronisk identitet - eID

«E-postkontoen er navet i ditt digitale liv»

Autentisering av organisasjon, system og data?







Organisasjonsautentisering

Å verifisere at en *virksomhet/organisasjon* er ekte, altså den den utgir seg for å være, i en online interaksjon.

- Hvordan oppnås *organisasjonsautentisitet*?
  Svar: Bruk av *kryptografi*



Systemautentisering

Å verifisere korrektheten av et systems identitet.

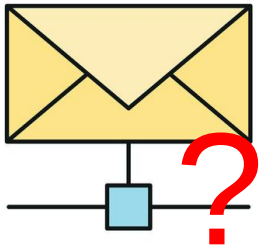
- Hvordan oppnås *systemautentisitet*?
  Svar: Bruk av *kryptografi*



Autentisering av dataopprinnelse

Å verifisere opphav til/avsender av data/melding.

- Hvordan oppnå *dataautentisitet*?
  Svar: Bruk av *kryptografi*



Oppgave 1

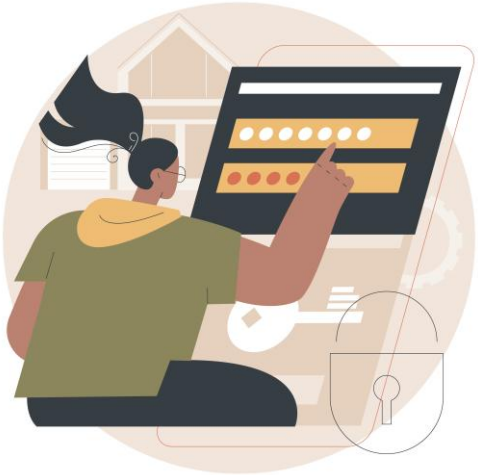
Sikkerhetsmål

Sikkerhetsmål er et sentralt begrep innen informasjonssikkerhet. Hvilke av følgende definerer vi som sikkerhetsmål i IN1020:

Velg ett eller flere alternativer

- ❑ Integritet
- ❑ Dataautentisitet
- ❑ Dataorm
- ❑ Autorisering
- ❑ Brannmur

Tilgang?



- Nødvendig å kunne styre *tilgang* til *ressurser*.
- Hvem *beslutter* hvem som skal ha tilgang til hva?

Tilgangskontroll

Tilgangskontroll er sikkerhetsmekanismen som bidrar til at bruker/enheter kun får tilgang til ressurser de er skal ha tilgang til:

Tilgangskontroll = autentisering + autorisasjon

Autorisering

«Å autorisere er å godkjenne eller gi løyve»

snl.no

- Tilgangsautorisering er å *spesifisere* tilgangsrettigheter for brukere/enheter.
- Autorisering er altså **ikke** teknologi, men policy.
- Eksempel på en slik policy:
  «En ansatt i lønnsavdelingen skal ha tilgang til lønnssystemet.»

Tilgangskontroll

Tilgangskontroll benytter seg av forhånds-spesifiserte tilgangsrettigheter for å beslutte om tilgang til ressurser skal gis eller ikke når en autentisert bruker/enhet gjør en forespørsel om tilgang.

Eksempler på forespørsler fra *subjekter* for *objekter*:

- Anne vil lese innholdet i en fil
- Per vil oppdatere kontobalansen på en bankkonto
- Kirurgen vil oppdatere en pasientjournal etter operasjon
- En applikasjon vil opprette en nettverksforbindelse mot en annen maskin

Hvem styrer tilgang?

Ethvert datasystem må ha en funksjon, hvis oppgave er å håndtere tilgangsforespørsler fra subjekter på objekter:

1. Kontrollere forespørsel mot gjeldende policy
2. Innvilge eller avvise tilgang
3. Logge hendelsen til hendelseslogg (ivaretar sporbarhet)



Refleksjon:

Betyr det at du *har tilgang til en ressurs* at du også er *autorisert* til ressursen?

Tilgang, logging og sporbarhet

- ✓ *Loggføring* av hendelser er bidrag til sikkerhetsmålet *sporbarhet*.
- ✓ Kan loggføring av hendelser ha flere funksjoner?
- ✓ Kan vi stole på hendelsesloggene?
- ✓ Hvor lenge kan logger lagres?





Refleksjon:

Har all informasjon samme beskyttelsesbehov?

Oppgave 2

Konfidensialitet

Konfidensialitet for persondata er et sentralt krav i norsk personvernlovgivning. Hvilke av følgende sikkerhetstiltak kan bidra til konfidensialitet for persondata i et IT-system:

Velg ett eller flere alternativer

- ❑ Kryptere alle data som lagres
- ❑ Identifisere alle brukere av IT-systemet
- ❑ Sikkerhetskopiere alle data
- ❑ Innføre tilgangskontroll til IT-systemet
- ❑ Ha gode rutiner for gjenoppretting av data

Øktas læringsmål

- Forstå sikkerhetsmålet *autentisitet*, kjenne til de ulike formene for *autentisering*, samt styrker og svakheter ved ulike *autentiseringsfaktorer.*
- *Tilgangskontroll*: Forstå hvordan tilgangskontroll fungerer, og hva som oppnås.

Ikke pensum

Alt kan hackes, anbefalt TED-talk:
https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked



Takk for i dag!

mn.uio.no/ifi

