# IN1020: Notat sikkerhet uke 2

Om autentisitet og tilgangskontroll

## 1 Autentisitet

Tillit er et av grunnfundamentene i digital samhandling og det som gjør at digitalisering av en rekke tjenester faktisk kan fungere, også de mer samfunnskritiske tjenestene. *Å ha tillit til* at noe er autentisk – det vil si ikke falskt/forfalsket - er tradisjonelt knyttet til f.eks. merkevarer, kunstverk, dokumenter eller annet. Pengesedler har f.eks. kjennetegn som vannmerker og sikkerhetstråder for å gjøre dem vanskelig å forfalske. I digitale omgivelser vil de tekniske tiltakene identifisering og autentisering bidra til nødvendig *tillit* til autentisiteten til noe/noen.

Autentisitet er et gradsbegrep; *Hvor stor* er tilliten til at en entitet faktisk har en hevdet identitet. Men merk at selv om man har tillit til at en gitt identitet er ekte, betyr det ikke nødvendigvis at man skal stole på vedkommende eller det som står bak identiteten. Dessverre viser det seg at mange blir relativt naive når de beveger seg fra en fysisk til en digital verden, og er raske til å stole blindt på informasjon som tilsynelatende ser ekte ut. Man lar seg lure og risikerer å bli svindlet.

Innen digitale tjenester er det nødvendig å kunne ha tillitt til ulike typer entiteter. Hvor stor tillit har du til at

- en *bruker* (person) er autentisk?
- en *organisasjon* er autentisk?
- et *(data)system* er autentisk?
- *opprinnelsen til data* (ofte kalt en melding) er autentisk?

### 1.1 Identitet og identifikator

En identitet er rett og slett akkurat den eller det noen eller noe er. Dette gjelder for personer, mobiltelefoner, datamaskiner eller kanskje en *prosess* som kjører på en datamaskin. For å identifisere en identitet brukes en identifikator. Eksempler er personnummer for en norsk person, IMEI-nummeret for en mobiltelefon, eller et brukernavn i et datasystem. I datasystemer vil man stort sett alltid ønske entydige eller unike identifikatorer.

### 1.2 Identifisering og autentisering

**Identifisering:** Når en bruker oppgir brukernavnet sitt (identifikatoren) til et datasystem ved innlogging, sier man at man gir seg til kjenne – man *identifiserer seg*. Fordi en identifikator som regel er kjent av andre, kan jo hvem som helst oppgi akkurat din identifikator (f.eks. brukernavn), noe som vil være et forsøk på ID-tyveri.

**Autentisering:** For å vanskeliggjøre ID-tyverier eller andre former på forfalskninger trenger vi måter å bekrefte at identifikatoren som oppgis faktisk tilhører den eller det som oppgir den. Prosessen med å bekrefte en identifikator kaller vi *autentisering*. Når du taster passordet ditt

og det sjekkes om det stemmer med det som er knyttet til brukernavnet, *autentiseres* du til systemet.

Men hvordan kan så organisasjoner, systemer eller dataopphav autentiseres?

### 1.3 Flere former for autentisering

Ikke uventet sammenfaller autentiseringsformene med målene for autentisitet:

- Brukerautentisering: Er å verifisere en påstått identitet til en bruker som vil logge seg inn i et datasystem. Dette krever som regel en aktiv handling fra oss. For å oppnå brukerautentisering benytter man det man kaller autentiseringsfaktorer. En autentiseringsfaktor er noe som på et tidspunkt er blitt knyttet til brukeren, noe som brukeren innehar eller har kontroll over, og som kan bekrefte identiteten. Eksempler er et passord, en kode eller et fingeravtrykk. Tjenester med behov for sterk grad av sikkerhet kan kreve at en bruker autentiserer seg med en kombinasjon av flere autentiseringsfaktorer (multifaktor autentisering).
- Organisasjonsautentisering: Er å verifisere at en virksomhet eller organisasjon er ekte, altså den den utgir seg for å være i en online interaksjon.
- Systemautentisering: Datamaskiner og datasystemer kommuniserer seg imellom, og systemautentisering er prosessen for å sikre tillit mellom slike. Dette gjøres svært ofte med egne programmer, kalt protokoller, som sørger for autentisert kommunikasjon mellom datasystemer.
- Dataautentisering: Det er nødvendig med tillit også til at meldinger sendt digitalt er autentiske, det vil si at de kommer fra mottakeren man antar de kommer fra. Dataautentisering er mekanismen som kan bidra til dette.

Å autentisere organisasjoner, systemer eller data krever andre autentiseringsfaktorer enn de som vanligvis benyttes for brukerautentisering (passord, koder, biometri), og her skal vi etterhvert se at *kryptografi* egner seg ypperlig for dette formålet. I digitalisering av tjenester vil bruk av kryptografiske algoritmer faktisk kunne gi oss høy grad av autentisitet også for organisasjoner, systemer og data.

## 2 Tilgangskontroll

Tilgangskontroll, også kalt aksesskontroll, er sikkerhetstiltaket eller mekanismen for å styre hvem som har anledning til å utføre handlinger med eller på ressurser i datasystemer.

Vi mennesker har eierskap til ting, og vi har en rekke skrevne og uskrevne regler for hvem som skal ha anledning til å utføre handlinger med eller på disse tingene. Disse reglene for tilgang må også gjenspeiles i datasystemene. Eksempel: Når du logger inn på nettsiden til Skatteetaten skal du ha som privatperson ha tilgang til data om deg selv og ingen andre, mens en ansatt i Skatteetaten muligens innehar en rolle som gjør at vedkommende kan trenge og få tilgang til data om langt flere personer.

### 2.1 Autorisering og tilgangskontroll

**Autorisering:** Handler om å definere prinsipper for tilgang, altså å spesifisere tilgangsrettigheter til ressurser. Dette har ingenting med teknologi å gjøre, men er administrative avgjørelser som stort sett vil være satt av noen med myndighet i en virksomhet. Et konkret eksempel på en slik policy er at en ansatt i lønnsavdelingen i en virksomhet skal ha tilgang til lønnssystemet.

**Tilgangskontroll:** Er mekanismen som styrer tilgang til ressurser. Det er helt opplagt at man heller ikke i et datasystem vil tillate at alle har tilgang til alt. Tilgangskontroll er å håndheve eller overholde autorisasjonspolicyene i et datasystem, og er således et teknisk tiltak.

For å forstå tilgangskontroll må vi også kjenne begrepene subjekt og objekt, slik de brukes i denne konteksten:

**Subjekt:** Den som ønsker å utføre en handling. Dette kan på et abstrakt nivå dreie seg om brukere som ønsker tilgang til en eller annen ressurs, mens det på et lavere nivå kan dreie seg om for eksempel en applikasjon eller et dataprogram som ber om tilgang til å opprette en nettverksforbindelse til en annen maskin.

**Objekt:** Ressursen man ønsker å utføre handlingen på, f.eks. lese en bestemt fil/dokument.

## 2.2 Stegene i tilgangskontroll

Tilgangskontroll består av to steg som utføres i rekkefølge:

1. Autentisering: Dette er å bekrefte identiteten til subjektet. Før du kan få tilgang, må systemet vite hvem du er (bruker, datamaskin, prosess, el).

2. Kontrollere autorisasjon: Dette innebærer å sjekke at det autentiserte subjektet har tilgang til å utføre den ønskede handlingen på objektet etter de forhåndsdefinerte reglene (policyen).

## 2.3 Håndtering av tilgang i datasystemer

I et datasystem er det datasystemet selv som håndterer tilgang og tilgangskontroll. Ethvert datasystem må derfor ha en funksjon hvis oppgave er å løpende håndtere tilgangsforespørsler fra subjekter på objekter. Denne funksjonen må bestå av følgende oppgaver:

- Kontrollere forespørsel mot gjeldende policy.
- Innvilge eller avvise den forespurte tilgangen.
- *Loggføre* hendelsen til en hendelseslogg (ivaretar sporbarhet), både avviste og innvilgede forespørsler.