Digdir-rapport ISSN <nr>

2020:12

Innsiktsrapport - Utfordringer med virksomhetssertifikater

www.digdir.no

Digitaliseringsdirektoratet
postmottak@digdir.no
22 45 10 00
Postboks 1382 Vika, 0114

Besøksadresser:
Industriveien 1, 8900 Brønnøysund
Skrivarvegen 2, 6863 Leikanger
Grev Wedels Plass 9, 0151 Oslo

Innhold

1 Problemstillingen

Deling av opplysninger skal være i samsvar med loven. Sentrale lover som forvaltningsloven, personopplysningsloven og særlovgivning på det enkelte området stiller krav til de forskjellige aktørene involvert i delingen.

For å kunne ivareta tilstrekkelige informasjonssikkerhetstiltak for å sikre personopplysningers integritet, tilgjengelighet og konfidensialitet ved deling, er det normalt behov for å identifisere og autentisere aktørene som deltar i samhandlingen. På nasjonalt / tverr-sektorielt nivå er det fram til i dag "virksomhetssertifikater" som er lovregulert som en slik autentiseringsmekanisme.

Det er identifisert flere utfordringer ved dagens bruk av virksomhetssertifikat, blant annet at sertifikatene potensielt gir vide tilganger og fremstår som for kraftfulle eller upresise, som gir sikkerhets- og tillitsmessige utfordringer.

Denne rapporten belyser slike utfordringer gjennom konkrete eksempler samt generelle problemstillinger som prosjektdeltakerne kjenner godt fra operativt daglig arbeid med våre respektive fellesløsninger. Basert på en analyse av dette underlagsmaterialet presenterer vi så en rekke behov som vil danne grunnlag for å senere utrede om det trengs etableres nye løsninger eller prosesser for å forbedringer.

1.1 Hva er et virksomhetssertifikat

En god forklaring finnes hos Buypass:
https://www.buypass.no/produkter/virksomhetssertifikat-esegl

1.2 Identitetslandskap

I denne rapporten beskriver vi i hovedsak behov og løsninger knyttet til identitet og autentisering av enheter.

- Med "enhet" eller "underenhet" mener vi i denne rapporten er en organisatorisk enhet, men ikke nødvendigvis
  - fysisk enhet som en maskin, et system eller en sensor
  - En fysisk person er også en entitet, men ligger utenfor beskrivelsen av en enhet vi bruker i denne rapporten
- En enhet kan ha en flere identiteter knyttet til seg. Til identiteten knyttes gjerne en identifikator.
- En identitet kan flere attributter eller data knyttet til seg.
- En eller flere delte hemmeligheter kan knytte enheten til den påståtte identiteten. Kontroll av hemmelighetene kalles autentisering

Tilgangsstyring eller autorisasjon er en annen prosess enn identifikasjon og autentisering. Hensikten med autorisasjon er å avgjøre om en kjent enhet skal ha tilgang til en ressurs eller tjeneste.

Data knyttet til en identitet kan benyttes for autorisasjon, men i de fleste tilfeller er data fra andre datakilder nødvendig for tilgangsstyring.

Utfordringer knyttet til autorisasjon ligger i hovedsak utenfor omfanget av denne innsiktsrapporten.

2 Juridiske rammer

2.1 Kort om den juridiske vurderingen

I dette punktet skal det vurderes hvilke krav regelverket stiller til presisjon ved autentisering. Dette innebærer at en først må se på utgangspunktene for ansvarfordeling i en delingssituasjon. Deretter må en se om det er noe som setter mer spesifikke krav enn det som følger av utgangspunktene.

2.2 Kort om pliktsubjektene og rettslig grunnlag

2.2.1 Personvernregelverket

Når en skal dele data, er det viktig å være bevisst hvem som har ansvaret for hva. I personvernforordningen (pvf.) er den behandlingsansvarlige det primære pliktsubjektet. Det kommer blant annet til uttrykk ved at den behandlingsansvarlige har ansvaret for å "påvise" av personvernprinsippene i pvf. artikkel 5 nr. 1 overholdes, jf. artikkel 5 nr. 2.

En behandlingsansvarlig er etter pvf. artikkel 4 nr. 7 "en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes"

Databehandlere behandler personopplysninger på vegne av den behandlingsansvarlige og er i pvf. artikkel 4. nr. 8 definert som "en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige".

Når data skal deles mellom to selvstendige behandlingsansvarlige, vil de behandlingsansvarlige måtte sørge for å ha tilstrekkelig behandlingsgrunnlag for sin behandling av personopplysningene. Dette gjelder også om opplysningene deles gjennom databehandlere. I tillegg kreves det et behandlingsgrunnlag for den handlingen det ligger i å dele personopplysningene. Dette kan enten inngå som en del av en del av de andre behandlingsgrunnlagene, eller være et selvstendig behandlingsgrunnlag. I en delingssituasjon overtar mottaker behandlingsansvaret med de plikter personvernregelverket oppstiller i det opplysningene er overgitt fra tilbyder.

2.2.2 Taushetspliktregelverk

Visse typer opplysninger er underlagt taushetsplikt, jf. blant annet gjennom forvaltningslovens (fvl.) § 13. Det finnes flere unntak fra taushetsplikten der hvor formålet er deling av opplysninger mellom offentlige aktører. Bestemmelsen(e) som fastsetter unntaket vil være det rettslige grunnlaget for delingen av de taushetsbelagte opplysningene, og normalt vil det fremgå av dette grunnlaget hvem som skal være mottaker av opplysningene.

Pliktsubjektet etter taushetspliktbestemmelsene i forvaltningsloven er “Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan”, jf. § 13.

2.3 Utgangspunktet: hvem kan opplysningene deles med

Utgangspunktet er at det følger av det rettslige grunnlaget for delingen hvem opplysningene kan deles med. Det rettslige grunnlaget for delingen er altså behandlingsgrunnlaget i personvernforordningen og unntaksbestemmelsen(e) for taushetspliktregelverket.

Dersom det rettslige grunnlaget ikke presist angir hvem som skal være mottaker av opplysningene, men angir en aktør, må utgangspunktet være at den som utleverer opplysningene har ansvaret frem til denne aktøren har mottatt dem. Dette må kunne sies å følge av systematikken i regelverket. Det er altså to risikosfærer og hver aktør har ansvaret i sin egen risikosfære. Nøyaktig når ansvarsovergangen skjer, behandles ikke videre her.

Aktøren som mottar opplysningene vil være konsumenten. Når konsumenten har mottatt opplysningene er det opp til konsumenten selv å sørge for at opplysningene behandles i tråd med det rettslige grunnlaget og i tråd med regelverket. Blant annet må konsumenten sørge for at opplysningene underlegges egnede og adekvate sikkerhetstiltak. Dette kan f. eks innebære at konsumenten må sørge for et system med tilgangskontroll slik at kun de som skal ha disse opplysningen har tilgang til disse.

2.4 Finnes det noen nærmere krav til autentisering av mottaker?

Selv om utgangspunktet er at hver aktør har ansvar innenfor sin risikosfære og at det følger av det rettslige grunnlaget for delingen hvem som kan være mottaker, kan det spørres om det finnes noen rettsregler som setter nærmere krav til autentisering.

2.4.1 Personvernregelverket

I personvernregelverket er det på et overordnet nivå naturlig å ta utgangspunkt i artikkel 5. Etter artikkel 5, kan både nummer 1 bokstav a og særlig nummer 1 bokstav f gi utgangspunkt for en slike rettsregler. Bestemmelsene angir imidlertid bare overordnede prinsipper, og etter sin ordlyd er bestemmelsene for vide til å innfortolke spesifikke krav til autentisering.

Personvernforordningens artikkel 32 gjelder krav til sikkerhet ved behandlingen. Denne bestemmelsen sier at behandlingsansvarlige og databehandleren skal “gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen”. Deretter gir bestemmelsen fire bokstaver med typer mulige sikkerhetstiltak. Bestemmelsen gir også i nummer 2 og nummer 4 noe videre anvisning på egnede tiltak.

Artikkel 32 er mer presis enn artikkel 5 når det gjelder sikkerhetstiltak. Den legger imidlertid også opp til en nokså bred vurdering. Det er tilsynelatende få kilder med rettskildemessig vekt, som stiller nærmere krav til autentiseringspresisjon. Datatilsynet viser på sine nettsider til NSM sine Grunnprinsipper for IKT-sikkerhet 2.0. I disse prinsippene punkt 2.6.6 bokstav a følger det “Styr tilganger til enheter. a) Identifiser enheter sikkert og unikt med f.eks.

sertifikater. Dette er ikke minst viktig for de ansattes klienter". Selv om dette gir noe nærmere anvisning, gir heller ikke dette grunnlaget for en tydelig rettsregel. Prinsippene har trolig heller ikke stor rettskildemessig vekt. I vurderingen av hva som er egnede sikkerhetstiltak, vil også andre hensyn enn optimalt sikkerhetsnivå kunne komme inn. Eksempelvis effektivitetshensyn.

Samlet sett gir tilsynelatende rettskildematerialet få spesifikke føringer. Slike føringer er trolig ikke nødvendig, dersom det skal innføres sikkerhetstiltak som bare øker sikkerheten ved behandlingen av personopplysningene. Det er grunn til å tro at dette bare er positivt. Dersom foreslåtte sikkerhetstiltak for autentisering også medfører ulemper, kan det være grunnlag for å gjøre en nærmere vurdering av om dette er et egnet sikkerhetstiltak etter artikkel 32.

2.4.2 Taushetsplikt- og forvaltningsregelverket

Tilsynelatende fastsetter heller ikke eForvaltningsforskriften og lov om elektroniske tillitstjenester så spesifikke krav til autentisering som behovene i denne rapporten peker på, jf. eksempelvis eForvaltningsforskriftens § 16. Dermed gjelder det samme her som for personvernregelverket, nemlig at autentiseringsløsninger som øker sikkerheten er ubetinget positivt. Dersom det innføres autentiseringsløsninger som medfører ulemper, må disse løsningene vurderes også mot dette regelverket.

3 Dagens utfordringer

3.1 Konkrete eksempler på utfordringer

Dette kapittelet inneholder noen konkrete eksempler der dagens virksomhetssertifikater byr på problemer. For hvert eksempel lister vi avslutningsvis opp de generiske behovene som prosjektgruppa mener eksempelet belyser.

3.1.1 eResept: forskrivning av medisin for smertebehandling

En enhet for smertebehandling (normalt en klinikk eller avdeling) er vanligvis en avgrenset funksjon ved et sykehus eller et sykehjem. Ettersom slike enheter ikke er hovedenheter kan de ikke få utstedt virksomhetssertifikat.

Medisinen som enhetene foreskriver er ofte forbundet med høy risiko (liv og død), og er derfor underlagt et eget regelverk. Dette medfører at enheter som driver med smertebehandling har egne grenser for hvor store mengder smertelindrende medisin de har lov til å forskrive. F.eks. har en avdeling for dokumentasjon og arkivtjenester andre grenser for forskrivning av morfinpreparater enn en kirurgisk avdeling. Ved bruk av virksomhetssertifikater knyttet til juridisk person klarer man ikke skille disse enhetene.

Det er nødvendig å ha tilstrekkelig god oversikt og kontroll over systemet som brukes til

forskrivning av denne typen legemidler og konteksten for bruk. Relevante krav i denne sammenhengen er at helsepersonellet har riktige autorisasjoner, og at forskrivningen skjer i forbindelse med behandling av en pasient i en avdeling som driver med smertebehandling. Dette gjelder både synkront ved API-bruk og asynkront i meldingsutveksling.

Generiske behov:

- *Ivareta informasjonssikkerhet (kontroll og oversikt) ved å identifisere underenheter*
- *Hindre for vide tilganger*
- *Adressering i meldingsutveksling av enhet med behandlingsgrunnlag*
- *Verifisering/autentisering/identifisering av enhet hvor et system blir brukt*
- *Tilgangskontroll basert på kobling person + enhet + system*

3.1.2 eResept: bandasjister

Det er mange aktører i eResept som mottar og sender meldinger, feks. kjernejournal, HELFO som skal betale, apotekene som skal levere ut medisin, samt en gruppe som heter "bandasjister", som blant annet selger sårmateriell. Slike produsenter tilhører virksomheter som også selger/produserer helt andre produkter. Den overordna juridisk enheten (virksomheten) har en næringskode som tilsier at den ikke har noe med helsesektoren å gjøre, og skal derfor ikke få tilgang til eResept.

Av praktiske årsaker er det etablert en praksis hvor en likevel aksepterer slike toppnivå-sertifikater selv om man mangler mekanismer for å hindre tilgang fra andre enheter enn bare bandasjisten i virksomheten.

- *Behandlingsansvar ikke gitt av næringskode*
- *Ivareta informasjonssikkerhet (kontroll og oversikt) ved å identifisere underenheter*
- *Hindre for vide tilganger*
- *Adressering i meldingsutveksling av enhet med behandlingsgrunnlag*
- *Verifisering/autentisering/identifisering av enhet hvor et system blir brukt*
- *Autentisering av system tilknyttet enhet som ikke er virksomhet*

3.1.3 Student- og elevbevis

Apper for student- og elevbevis leveres av tredjeparter. I høyere utdanning leveres det av en fellestjeneste i sektoren, mens i lavere utdanning leveres tjenesten av kommersielle leverandører. Organisasjonen som dataansvarlig må godkjenne at API-backender skal ha tilgang til dataene om sine studenter eller elever, samt at appene skal kunne gjøre oppslag mot APIene. Disse godkjenningene og autentiseringene av backend dataflyt gjøres i dag manuelt. Autentiseringen på brukernivå mellom app og API håndteres av Feide.

- *Tilgangskontroll basert på kobling mellom person, system og enhet.*

- *Dataminimering der klient bare får tilgang til innlogget brukers informasjon ved enhet, selv ved system-til-systemintegrasjon*
- *Bruk av virksomhetssertifikat e.l. hos en tredjepartsleverandør / underleverandør*

3.1.4 Helsepersonell med arbeid for flere behandlingssteder

Et kommunalt ansatt helsepersonell kan i noen tilfeller reise rundt mellom ulike behandlingssteder, mens andre kan gjøre hjemmebesøk hos pasientene i løpet av en dag. Et behandlingssted i helsesektoren er en underenhet av en juridisk hovedenhet hvor det ytes helsehjelp, og kan tilhøre både en kommune eller et privat selskap med kontrakt med kommunen. Etter § 19 i pasientjournalloven, så kan en dataansvarlig kun dele helseopplysninger dersom det eksterne helsepersonellet har et tjenstlig behov for informasjonen som deles gjennom et datadelingsgrensesnitt. Ved tilgangskontroll i datadelingsgrensesnitt er det derfor behov for å sannsynliggjøre helsepersonellets rett til tilgang. Eksempler på informasjon som bidrar til sannsynliggjøring, kan være identiteten til virksomheten hvor helsepersonellet er ansatt, behandlingsstedet hvor helsepersonellet yter helsehjelp og systemet som helsepersonellet benytter.

Helsepersonellets tjenstlige behov oppstår når et helsepersonell yter helsehjelp eller i forbindelse med administrasjon av helsehjelpen til den enkelte. I forbindelse med datadeling er det ofte bare fagsystemet og helsepersonellet selv som kan avgjøre hvorvidt det foreligger et tjenstlig behov.

Behandlingsstedet i kommunal sektor er som regel ikke en hovedenhet og kan derfor ikke få virksomhetssertifikat, se diskusjon rundt avdelinger ved et sykehus ovenfor. Men dette eksempelet belyser en annen dimensjon, nemlig at rett på tilgang er flyktig og det varierer gjennom dagen for samme innloggede bruker.

I tillegg til behovene som er skissert opp i eResept-eksemplene får vi her behovene:

- *Tilgangskontroll basert på kobling person + enhet + system*
- *Støtte flyktige strukturer*

3.1.5 eResept: store apotekkjeder

I henhold til standarden kan virksomhetssertifikater bare utstedes til hovedenheter i Brreg. Men i noen tilfeller har vi også behov for å identifisere og autentisere underenheter. Apotekkjedene er et eksempel på dette. For å skille mellom hovedenhet og underenhet i apotekkjedene legges hovedenhet (juridisk person) sitt org.nr. i *Subject Serial,* mens underenheters org.nr. ligger i *Subject Ou*. Denne praksisen fungerer for organisasjoner med to ledd, men ikke flere. Dersom man har mange underenheter kan det også medføre en potensielt stor kostnad.

- *Ivareta informasjonssikkerhet ved å identifisere underenheter*
- *Adressering i meldingsutveksling av enhet som ikke er virksomhet*
- *Autentisering av system tilknyttet enhet som ikke er virksomhet*

3.1.6 Delegert systemeierskap til underenheter i utdanningssektoren

I større organisasjoner som universiteter er systemeierskap delegert nedover i organisasjonen til enheter som fakulteter, institutter, forskningsprosjekter og lignende. Det samme gjelder kommuner og privatskoler der skoler kan ha egne fagsystemer med eget eierskap. Disse fagsystemene integreres med andre fagsystemer internt i organisasjonen og eksternt med andre enheter.

Mange av disse enhetene finnes ikke i enhetsregisteret hverken som organisasjoner eller virksomheter. Noen er i sektorspesifikke register, som f.eks. fakulteter, institutter og utenlandsskoler, mens andre bare er registrert lokalt i organisasjonen. Levetiden for enheter varierer, men omorganiseringer gjøres ofte og forskningsprosjekter opprettes og avsluttes hele tiden.

På avsendersiden må behandlingsansvarlig ha kontroll på datautvekslingen ut av den juridiske enheten som helhet, og hvilke enheter og fagsystemer som deler data. Utstedelse av underenhet-identiteter og tilliten til denne blir viktig for kunne delegere ansvar til underenheter og hindre flaskehalser oppover i systemet som unødig hindrer legitim dataflyt.

På avsender- og mottakersiden vil det noen ganger være nødvendig å identifisere enhet og fagsystem som utveksler data på et mer detaljert nivå enn organisasjonen. Eksempler kan være forskningsprosjekter som bare skal utveksle data med gitte institutter/organisasjonsenheter i andre organisasjoner.

I særskilte situasjoner, spesielt rundt forskningsprosjekter og tungregning, blir identifiseringen av person i kombinasjon data fra et fagsystem/enhet kritisk. Gitte kriterier til fagsystemets/enhetens data gjør at enkelte klasser av personer, f.eks. basert på nasjonalitet, ikke skal gis tilgang (enten de er tilknyttet avsenderorganisasjonen eller en mottakerorganisasjon), selv om de kan ha tilgang til andre data fra samme organisasjon.

- *Delegering av ansvar og kontroll nedover i underenheter er nødvendig i større organisasjoner for å unngå trange flaskehalser*
- *Virksomhetssertifikater er for "sterke" og grovkornede og kan gi for store tilganger der det er behov for sterkere kontroll*
- *Enhetene og strukturen på disse varierer mellom sektorer også innenfor en sektor. Det finnes ikke dekkende registre over strukturene og endringene i disse. Utstedelse av identiteter og tillitskjeder for disse må kunne gjøres også på sektornivå og organisasjonsnivå. Kanskje også på enhetsnivå for underenheter og fagsystemer.*
- *Tilgangskontroll basert på kobling mellom person, system og enhet*
    - *få identifisert fagsystemet som en tilleggsikkerhet (implisitt enheten)*

3.1.7 Store plattformer og skytjenester

I både utdannings- og helsesektoren har vi en utfordring i forbindelse med "multi-tenant" system og felles plattformer. Det finnes flere slike system, for eksempel Helseplattformen i Trøndelag.

Helseplattformen er et samarbeid om et felles pasientjournalsystem i Helse Midt-Norge som vil dekke opp mot 1000 virksomheter. Disse virksomhetene har i dag et selvstendig behandlingsansvar.

En av utfordringene ved autentisering i slike plattformer er å ha tillit til hvordan identitetene og autentiseringsmidlene håndteres internt i plattformen.
Hvis Helseplattformen må verifisere alle behandlingssteder i tillegg til virksomhetene som er medlemmer får de et forvaltningsansvar for alle koblinger mellom identifikatorer, nøkler og hemmeligheter. Å sjonglere mange tusen sertifikater i kjøretid vil medføre en risiko for feilhåndtering.

Ved å følge mønsteret i eOppslag kan Helseplattformen tilfredsstille krav til virksomhetsidentifisering som datadelingstjenester stiller i sin tilgangskontroll, ved at behandlingsansvarlig delegerer en rettighet som lar Helseplattformen opptre på sine vegne. En mangel ved dette mønsteret er at delegeringen skjer for hovedenhet, og dekker ikke behandlingssted.

- *Delegering av ansvar og kontroll nedover i underenheter*

3.2 Generelle utfordringer

I dette del-kapittelet belyser vi noen generelle utfordringer som er kjent for prosjektgruppa, uten å gå detaljert inn på konkrete navngitte eksempler.

3.2.1 «Universalnøkkel»

Virksomhetssertifikat brukes i økende grad for å identifisere og ha tillit til aktørene i forbindelse med samhandling, i flere forskjellige infrastrukturer. Siden det ikke eksisterer noen standardiserte mekanismer (som er tatt i praktisk bruk) for å begrense konteksten/bruksområdet for sertifikatet, medfører dette at et virksomhetssertifikat anskaffet til ett formål, kan gjenbrukes mot alle andre systemer som baserer seg på virksomhetssertifikat. Man har altså fått en "universalnøkkel"-utfordring.

Anskaffelsesprosessen av virksomhetssertifikatet blir oppfattet som komplisert og/eller tidkrevende, samt for mindre aktører så er høy kostnad (spesielt på kvalifiserte segl) drivere som fører til gjenbruk av samme sertifikat i mange systemer.

Når et virksomhetssertifikat benyttes til mange ulike formål må privat nøkkel gjøres tilgjengelig for mange systemer og personer, og dette fører til at tilliten til virksomhetssertifikater som konsept blir svekket.

Samtidig er det udiskutabelt at virksomhetssertifikatet løser et reelt problem, siden de har hatt så stor suksess og fått så stor utbredelse. Denne utbredelsen har så brakt fram konsekvenser man kanskje ikke så for seg når konseptet med virksomhetssertifiktater ble formalisert.

- *Unngå gjenbruk av autentiseringsmekanismer*
- *Støtte delegering av tilgang bruk av virksomhetssertifikat e.l. hos en tredjepartsleverandør / underleverandør*

3.2.2 Offentlige utvalg, forskningsprosjekter, etc

Offentlige utvalg har ikke org.nummer, men har stort samhandlingsbehov med andre både offentlige og private enheter.

Tilsvarende er det mange flerårige prosjekter med deltagere fra flere organisasjoner, samt senter i høyere utdanning som ikke er egne enheter med organisasjonsnummer.

Slike enheter har fagsystemer som trenger kontrollert samhandling med andre enheter.

- *Adressering i meldingsutveksling av enhet som ikke er virksomhet*
- *Autentisering av system tilknyttet enhet som ikke er virksomhet*

3.2.3 Tidkrevende å få tak i virksomhetssertifikat

Det kan ofte være svært tidkrevende å få den som er registrert som nøkkelrolleinnehaver i Enhetsregisteret til å bestille sertifikat. Man må gå «til topps» i organisasjonen, og i store organisasjoner som t.d. Oslo Kommune og universiteter medfører dette at utviklings-team må vente lenge før de kommer i gang med prosjekter som krever integrasjon mot infrastrukturer som baserer seg på virksomhetssertifikat.

Digitaliseringsdirektoratet kjenner også eksempler på innovasjonsprosjekter/piloter som ikke har blitt igangsatt siden prosessen med å få tilgang til organisasjonens virksomhetssertifikat i produksjon er såpass krevende, samt setter store føringer til driftsmiljøet til piloten.

- *Tidkrevende å få tilgang til virksomhetssertifikat*

3.2.4 Parallelle løsninger for adressering

Fravær av bruksområdebegrensninger for virksomhetssertifikater medfører at det er bygd opp flere parallelle register/systemer som for alle praktiske formål gjør det samme: gir en avsender mulighet til å finne hvilket spesifikt virksomhetssertifikat som en mottaker ønsker å bruke for å samhandle innen et spesifikt bruksområde. Dette er primært synlig innen asynkron meldingsutveksling der det skal sendes en kryptert melding til en mottaker som ikke nødvendigvis er tilstede på samme tid.

Eksempler på slik er : BCP/BCL, adresseregisteret til KS sitt SvarInn/SvarUT / Fiks-io. RESH til Helse, etc.

Hver adresseringsløsning har sin eget forvaltningsregiemene og regler for hvordan man blir "medlem" av registeret, og hvem som får lov til å vedlikeholde informasjonen i registeret.

At hver samhandlings-infrastruktur har sitt eget register, er trolig ikke et ressursproblem i seg selv, men vi tror det vil være effektivitetsgevinster dersom det eksisterte en enhetlig måte å identifisere underenheter og bruksområder på.

3.2.5 Adressere sensitivt innhold til riktig "gruppe av personer" i meldingsutveksling

Tilgangsstyring i Altinn er utformet med utgangspunkt i ledende roller registrert for enheten i Enhetsregisteret. Disse rollene anses å ha fullmakt til å opptre på vegne av enheten på generelt grunnlag. Dette gjelder alle virksomheter – både private og offentlige.
Disse nøkkelrollene har tilgang til alle elementer i virksomhetens innboks, og styring av hvem som skal kunne gi tilgang til elementene i innboks.
Dette gjør at innhold som skal skjermes fra "administrasjonen", særlig taushetsbelagte personsensitive opplysninger, ikke får tilstrekkelig sikring, da de følger "en administrativ tillits-akse" som ikke nødvendigvis er relevant, for eksempel opplysninger underkastet lovgivning for helseopplysninger.

KS "SvarUt" og Digdirs DPV
KS tjeneste for sending av opplysninger (SvarUt) og Digitaliseringsdirektoratets post til virksomheter (DPV) anvendes for å sende (taushetsbelagte) helseopplysninger fra fastleger til kommunens helsetjeneste, omsorgstjeneste og utdanning. Fastlegen sender opplysningene til "kommunen" og ikke "kommunehelsetjenesten" fordi de ikke har oversikt over mottakerne som trenger opplysningene.

En konsekvens for individene helseopplysningene er koblet til, er at posten kan leses av uvedkommende, eksempelvis de som administrerer tilgangene i den enkelte kommune.

Et resultat av dette er at personsensitiv post blir ligget i Altinns postboks. Trolig både fordi mottaker ikke alltid er kjent, og man kan spekulere i om ikke alle som trenger å lese posten er kjent, og at postboksen anvendes som (mer langsiktig) lagring av opplysningene, og man ikke anvender andre mekanismer for kommunens interne behov for deling.

Drøfting (KS "SvarUt" og Digdirs DPV)
Det er ikke mulig å anvende (kommunens) mottakers fødselsnummer, da mottaker kan variere ut ifra hvem som bekler rollene. Helsebehandlingsansvarlig beveger seg eksempelvis mellom kommuner.

For kombinasjonen av "Altinn meldingsboks med anvendelse av eMelding til å levere meldingene" har man en "kompenserende løsning" med tagging "Tausbelagt post" for hhv. helse, sosial og omsorg, oppvekst og utdanning, samt administrasjon. En utfordring med dette er at hovedadministrator for kommunen (typisk rådmann, eller delegert) er en som bestemmer hvem som kan gi tilgang til helseopplysningene, en rolle som ikke er en naturlig del av tillitskjede knyttet til personsensitive data. Dette har man ikke hvis man anvender KS "SvarUt".

3.2.6 Forskjellige hierarki i samme sektor :

Helseinstitusjoner kan være organisert under forskjellige organisasjonsledd i enhetsregisteret. Noen institusjoner er direkte underenheter til juridisk person, mens andre "henger" på et organisasjonsledd. Dette er typisk for helsetjenestene i kommunene. Dette betyr at selv en sektor-løsning for et avgrenset bruksområde, må måtte forholde seg til ulike hierarki-strukturer for å adressere, identifisere og autentisere.

- *Støtte flyktige strukturer*

3.3 Innspill frå referansegruppa

Prosjektet har gjennomført en spørreundersøkelse der vi ba virksomhetene i referansegruppen om å belyse problemer og utfordringer som de ser med virksomhetssertifikater.

Svarene på spørreundersøkelsen bekrefter i stor grad de utfordringene som er nevnt i forrige kapittel, og ligger som vedlegg til denne rapporten.

4 Behov

Dette kapittelet inneholder en drøfting og generalisering av de funnene som er presentert i forrige kapittel. Behovene som listes opp her, vil forme evalueringskriterier som potensielle nye løsninger må vurderes opp mot.

Behovsanalysen peker primært på at for at behandlingsansvarlige skal ha nødvendig kontroll og oversikt med deling av data, er det i mange tilfeller påkrevd at samhandling kan avgrenses til å skje direkte mellom under-enheter. Virksomhetssertifikats mangel på granulær identifikasjon gjør at vi mangler en mekanisme som kan brukes for å håndheve dette behovet.

4.1.1 Ivareta informasjonssikkerhet ved å identifisere underenhet

Selv om overordnet lovverk som Personvernforordningen (art 4, nr7) som hovedregel plasserer behandlingsansvaret på virksomheten:

> behandlingsansvarlig»: en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes

så skal den behandlingsansvarlige (art 32) også:

> ...gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen

Det er behandlingsansvarlig som har eierskapet/ansvar for data, og er den som er pålagt å ha oversikt og kontroll over "hvor data går hen" og forvalte og håndheve tilganger til data. I praksis har datatilbyder ofte et behov for å vite noe om kontekst som ligger til grunn for en forespørsel om tilgang til data. Kontekst kan beskrive det tjenstlige behovet og si noe om hva som er relevant og nødvendig informasjon for å kunne begrense informasjonsmengden som deles. Behovet for presis identifisering gjelder ikke bare på konsument-siden, men også internt i datatilbyders egen virksomhet.

Det tjenstlige behovet og prinsippene for dataminimering er ofte knyttet til hvilke aktiviteter som foregår i en underenhet, i helsesektoren kan dette f.eks. være et behandlingssted. Merk at vi i denne rapporten bruker "underenhet" som generalisert begrep, og ikke som strukturen i Enhetsregisteret.

Dette betyr at behovet for presis identifisering av underenheter primært er motivert ut fra informasjonssikkerhet, slik at behandlingsansvarlige kan ha nødvendig kontroll og oversikt, selv om det for den aktuelle samhandlingen ikke nødvendigvis kan utledes et eksplisitt krav fra lovverk.

4.1.2 Kunne uttrykke hvordan en identitet er oppstått

"Det" som skal identifiseres (altså underenheten), må kunne få sin egen identitet, og dette må være en identitet som kan brukes flere ganger, i flere kontekster/systemer (t.d. samme identifikator i både asynkron meldingsutveksling og synkron datadeling) og på tvers av sektorer.

Å identifisere underenheten er forskjellig fra å gi den en rolle eller tilgang. Men samtidig må den som skal vurdere om tilgang skal kunne gis, kunne få vite hvordan identiteten har oppstått for å vurdere om en kan ha tiltro til påstand om identitet. Det er datasettet knyttet til identiteten andre aktører kan ha tillit til.

Til identiteten vil det være knyttet metadata som kan synliggjøres på ulike måter; for eksempel innebygd i et sertifikat, eller som oppslagbare metadata registrert hos en utsteder eller et register, eller fremkomme gjennom et token fra en systemløsning som Maskinporten eller Feide. Det må være tydelig hvor disse metadataene kommer fra: "hvem opprettet disse metadataene og hvor sannsynlig er det at denne påstanden er rett".

Fra person-eID kjenner vi slike sikkerhetsnivå, der ulike aspekter som identitetskontroll, styrken på autentiseringsmekanismen og tillitsnivået innad i føderasjonen "samles til et tall"; de historiske begrepene "nivå 3" eller "nivå 4". Prosjektgruppa tror at den ytterligere kompleksiteten som kommer fra datadeling, der tilgang skal styres basert på mange påstander om identiteter (feks kombinasjonen legen + pasienten + legens arbeidsgiver + sykehjemmet pasienten befinner seg på akkurat nå), gjør det uhensiktsmessig å skulle uttrykke dette i ett og bare ett "nivå". Forskjellen i sannhetsverdi for de ulike identitets-påstandene kan ha relevans for tilgangsstyringen som APIet må utføre. En identitet som er selvdeklarert vil nødvendigvis ha mindre tillit enn der en tredjepart har kontrollert et identitetsbevis. Ofte trenger man ikke det høgste tillitsnivået, men noen ganger trenger man det.

Løsninger må altså gi aktørene mulighet til å uttrykke ulike sannhetsverdier for metadata knyttet til en identitet.

Løsninger bør også vurderes opp mot hvordan de understøtter at påstanders sannhetsverdi kan endres over tid. Som eksempel vil identiteter og tilhørende autentiseringsmekanismer som ble opprettet for veldig lenge siden, kunne ha mindre tiltro enn "ferske data". Et system kan også bli kompromittert, og vil trenge tiltak før tillitsnivået kan bli reetablert.

4.1.3 Støtte flyktige strukturer

Det følger også av forrige avsnitt at løsninger må støtte at det vi i denne rapporten kaller "underenheter" er enheter som ikke nødvendigvis finnes i noe nasjonalt eller sektor-spesifikt register.

Hierarkiene som "det som skal identifiseres" inngår i kan være flyktige, de er ikke nødvendigvis regulert, hierarkiene kan være forskjellige mellom ulike forvaltningsnivåer, mellom ulike sektorer (eller tilogmed innad i en sektor), samt mellom offentlig og privat. Det

vil være svært krevende å til enhver tid skulle vedlikeholde en samlet oversikt på nasjonalt nivå over alle disse identifiserbare enhetene på en kostnadseffektiv måte.

4.1.4 Hindre for vide tilganger og gjenbruk

En av de store problemene med virksomhetssertifikater er “universalnøkkel”-utfordringen.

Dersom en spesifikk datautveksling må begrenses til utvalgte underenheter i organisasjonen, blir det viktig å tilby mekanismer som kan hindre at andre enheter i organisasjonshierarkiet får tilgang til data de ikke skal ha tilgang til. Dette blir spesielt viktig der det snakk om sensitive persondata (som i helsesektoren) eller forretningshemmeligheter (som forskningsprosjekter utsatt for industrispionasje).

Nye løsninger må derfor være utformet slik at det blir enkelt og sikkert å utstede nye autentiseringsmekanismer til forskjellige bruksområder, slik at ansvarlig personell ikke fristes til gjenbruk av slike. Autentiseringsmekanismene tilknyttet en identitet bør heller ikke lett kunne brukes av andre enheter enn de blir utstedt til.

4.1.5 Legge til rette for delegering

Utlån av virksomhetssertifikat til systemleverandører er et problem i dag, og bør unngås i fremtiden.

En enhet som samhandler bør alltid identifiseres og autentiseres som seg selv. Det medfører at en databehandler som opptrer på behandlingsansvarlig sine vegne, må ha sine egne autentiseringsmekanismer.

Dette betyr også at det må etableres mekanismer som hindrer en enhet å selv-deklarere at den opptrer på andres vegne - det må sikres at behandlingsansvarlige har gjort en aktiv delegerings-handling til databehandler. Det er et åpent spørsmål om slike krav kanskje løses bedre av de konkrete infrastrukturene som skal ta de nye løsningene i bruk.

Samtidig er ikke trolig ingen større prinsipielle forskjeller i det å delegere nedover internt i en virksomhet - altså frå hovedenhet til underenhet - som det å delegere til en ekstern enhet. Det er da også nærliggende å tenke seg flernivå kjeder av delegeringer. Løsninger som understøtter slik generalisering har trolig mer gjenbrukspotensiale enn spesialiserte delegeringsmekanismer.

4.1.6 Skalerbar og brukervennlig utstedelse

Når vesentlig flere identifikatorer og autentiseringsmekanismer skal utstedes og tas i bruk enn det vi gjør i dag, er det essensielt at løsningene for utstedelse er brukervennlige, skalerbare, kostnadseffektive og samtidig sikre. Sannsynligvis er det behov for å beskrive noen ulike prosesser for slik utstedelse, som balanserer de ulike kvalitetene som sikkerhet kontra enkelthet.

Prosjektet antar at de fleste autentiseringsmekanismene som vil lages i praksis vil være basert på asymmetrisk krypto, slik at det "bare" er å velge en god nok algoritme for å oppnå tilstrekkelig teknisk sikkerhetsnivå.

4.1.7 Understøtte tilgangskontroll basert på kobling person + enhet + system

Selv om dette prosjektet er begrenset til identifisering og autentisering av enheter og ikke fysiske personer, så ser vi fra eksemplene en klar trend om at det ofte er kombinasjonen person + enhet (eventuelt også system) som må brukes til å gjøre tilgangsbeslutninger i et API. Et API vet i utganspunktet ingenting om verken sluttbruker, system eller annan kontekst hos konsumenten, men vil ofte ha behov for slik informasjon for å kunne dele data (GDPR artikkel 5, bokstav f).

I mange tilfeller gir det også god sikkerhetsgevinst å begrense en samhandling til en innlogget bruker, i stedet for rene maskin-til-maskin samhandling der misbrukspotensiale ofte er komplette datasett på avveie.

4.1.8 Tilrettelegge for dataminimering

Det er være hensiktsmessig at data som blir utlevert skal minimeres alt etter hvilken enhet i en konsumerende virksomhet som spør. Dataminimering er et styrende prinsipp i GDPR (artikkel 5, bokstav c). I helsesektoren er det regler rundt det som kalles "Relevant og nødvendig informasjon" som også er knyttet til registrering (https://www.helsedirektoratet.no/rundskriv/helsepersonelloven-med-kommentarer/dokumentasjonsplikt#paragraf-45-utlevering-av-og-tilgang-til-journal-og-journalopplysninger)

Ved å kunne identifisere enheter på lavere nivå enn juridisk person, gjør vi det lettere for behandlingsansvarlig å gi ut en dataminimert respons.

4.1.9 Støtte flernivå strukturer

Noen av eksemplene som prosjektgruppa har fått, indikerer behov for å identifisere flere nivåer enn 2.

4.1.10 Støtte distribuerte arkitekturer

Løsninger bør etterstrebe at utstedelse av identiteter, utstedelse av autentiseringsmekanismer tilhørende en identitet, samt mekanismer for "bruksområde-begrensning" i størst mulig grad er frikoblet fra spesifikke infrastrukturer.

Dette behovet er motivert fra et arkitekturprinsipp om "løse koblinger" og mye av suksessen med eID for fysiske personer kommer av dette prinsippet er fulgt, slik at en innbyggers eID

sømløst kan “plugges inn” i mange ulike systemer innen ulike domener. eID for juridiske personer er for alle praktiske formål bygd opp på samme måte, men mangelen på mulighet for granulert identifisering og begrensninger på bruksområde skaper de utfordringene som denne rapporten peker på.

4.2 Referanser

- Personopplysningsloven, https://lovdata.no/pro/#document/NL/lov/2018-06-15-38
- Lov om elektroniske tillitstjenester, https://lovdata.no/pro/#document/NL/lov/2018-06-15-44
- NIST 800-63: Digital Identity Guidelines, https://pages.nist.gov/800-63-3/
- Normen for informasjonssikkerhet og personvern i helse- og omsorgssektoren, https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren
- Rundskriv I-2019-3 fra Helse- og Omsorgsdepartementet om Informasjonshåndtering i spesialisthelsetjenesten, https://lovdata.no/pro/#document/RDEP/rundskriv/i-2019-3/KAPITTEL_4-2

5 Referanseark for Digdir

Tittel på notat:	Innsiktsrapport – Utfordringer med virksomhetssertifikater
Digdirs notatnummer:	
Forfatter(e):	Jørgen Binningsbø, Tor Alvik
Evt. eksterne samarbeidspartnere:	Steinar Noem (NHN), Snorre Løvås (Uninett), Helle Stedøy, Jens Obsberg Andresen, Ingunn Rønningen
Saksnummer:	Saksnummer
Prosjektnummer:	
Prosjektnavn:	
Prosjektleder:	
Prosjektansvarlig avdeling:	
Oppdragsgiver(e):	
Resymé/omtale:	
Emneord:	
Totalt antall sider til trykking:	
Dato for utgivelse:	

Utgiver:	Digitaliseringsdirektoratet Postboks 1382 Vika 0114 OSLO www.digdir.no