Direktoratet for e-helse

Krav til sikkerhetsbillett ved deling av helseopplysninger

Versjon 1.0

Merknad 25.09.2024:
Dette dokumentet ble utarbeidet av Direktoratet for e-helse. Det vil bli oppdaterst som en del av arbeidet med med digital samhandling.

HITS 1220:2019

Publikasjonens tittel:
Krav til sikkerhetsbillett ved deling av helseopplysninger

Rapportnummer
HITS 1220:2019

Utgitt:
03/19

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Besøksadresse:
Verkstedveien 1, 0277 Oslo
Tlf.: 21 49 50 70

Publikasjonen kan lastes ned på:
www.ehelse.no

Innhold

1 Innledning

Data- og dokumentdeling tas i bruk på stadig flere områder innen helse- og omsorgstjenesten. En viktig del av slik samhandling er tilgangskontroll av brukere og klienter på tvers av virksomheter. Tillitskjeder må i den sammenheng etableres mellom alle parter. Sikkerhetsbilletter benyttes for å etablere slike tillitskjeder mellom samarbeidende parter.

Alle prosjekter som implementerer data- og dokumentdeling må spesifisere innholdet i en sikkerhetsbillett som aktørene kan stole på. Et minimumsinnhold i sikkerhetsbilletten bør være felles for helse- og omsorgstjenestene for å minimere arbeid hvert prosjekt har rundt dette, samtidig som det skaper en enhetlig måte å løse utfordringene som aktørene har ved spesifiseringen av sikkerhetsbilletten.

En sikkerhetsbillett inngår i mange ulike anvendelser av data- og dokumentdeling. Sikkerhetsbillett er et samlebegrep for alle typer identitets- og tilgangsbilletter uavhengig av protokoll og format.

Direktoratet for e-helse har i 2018 knyttet til seg to referanseprosjekter – Helsenorge og Velferdsteknologisk Knutepunkt. Samarbeid med referanseprosjekter har som formål å avdekke felles utfordringer sektoren har ved innføring av løsninger for data- og dokumentdeling som bør løftes for nasjonale avklaringer.

Gjennom samarbeidet med referanseprosjektene ble det prioritert å utarbeide dette dokumentet.

1.1 Normative referanser

[1] IHE Cross-Enterprise User assertion XUA

[2] IHE XUA – Provide X User Assertion – ITI-40 Spesifikasjon XUA sikkerhetsbillett

[3] Cross-Enterprise Security and Privacy Authorization (XSPA)
Profile of SAML v2.0 for Healthcare Version 2.0

[4] RFC 7519 - JSON Web Token (JWT)

[5] RFC 6749 - The OAuth 2.0 Authorization Framework

[6] OpenID Connect Core 1.0

[7] Norsk FHIR profil for Organization

[8] Norsk FHIR profil for Practitioner

[9] Norsk FHIR profil for Patient

1.2 Ikke-normative referanser

[10] Cross-Organization Data Access Profile – The Argonaut Project

[11] OAuth 2.0 Token Exchange – draft

[12] FHIR ressurs practitionerRole

[13] FHIR ressurs RelatedPerson

[14] FHIR ressurs HealthcareService

[15] FHIR dataype HumanName

[16] Personidentifikatorer

[17] Bruk av kodeverk i FHIR

[18] Norsk profil (draft) av HealthcareService

[19] FHIR kodesett for rolle

2 Brukstilfeller

2.1 Klientautentisering

Ved behandling av helse- og personopplysninger via data- og dokumentdeling er det krav om at klientene må kunne kobles til en virksomhet og være forhåndsgodkjent. En slik godkjenning vil gå ut på at virksomheten må godkjennes som en bruksorganisasjon for bruk av STS.

Som STS må jeg kunne autentisere klienten slik at jeg kan koble klienten til en forhåndsgodkjent virksomhet.

Klientautentisering er inkludert i flytene beskrevet i kapittel 2.2 og 2.3. Når STS autentiserer klienten, kan informasjon om virksomheten benyttes som påstander i sikkerhetsbilletten.

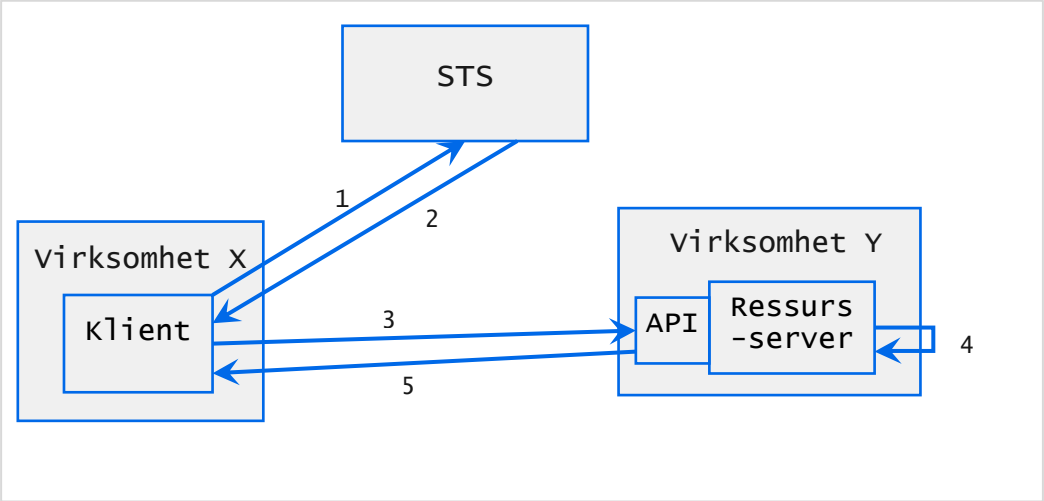
2.2 Klientautorisering

Brukerhistorie for klientautoriseringsflyt:

Som forhåndsgodkjent klient tilhørende virksomhet X ønsker jeg tilgang til datadelingsgrensesnitt(API) hos virksomhet Y (API-eier) slik at jeg kan få utført funksjonen (operasjonen) datadelingsgrensesnittet tilbyr.

Forhåndsbetingelser:

1. Virksomhet Y har inngått avtale med Virksomhet X om at X kan benytte Y sitt datadelingsgrensesnitt.
2. Virksomhet Y må ta stilling til om de krever en brukerpålogging eller ikke (altså enten maskin-til-maskin eller krav om en brukersesjon).
   Dersom de krever en brukersesjon må de sette krav til:
3. Identitetstilbyderens tillitsnivå (autentiseringsstyrke)
4. Intern eller ekstern digital identitet.
5. Hvis Virksomhet Y har tillit til Virksomhet X sine interne digitale identiteter, kan denne flyten benyttes også med innlogget bruker.
6. Virksomhet Y har selv, eller via en tiltrodd tredjepart som Y har delegert ansvaret til, registrert klienten som forhåndsgodkjent til å benytte datadelingsgrensesnittet i STS.



Figur 1 Klientautentisering

Flyt:

1. Klient spør STS om å få tilgang til datadelingsgrensesnittet. Forespørselen inkluderer en hemmelighet eller signatur som unikt identifiserer klienten.

2. STS-en kontrollerer at tilgangsforespørselen kommer fra en forhåndsgodkjent klient, sjekker om klienten har tillatelse til forespurt tilgang (scope) og utsteder og returnerer en tilgangsbillett dersom tilgang foreligger.
3. Klienten mottar tilgangsbilletten og kaller API-et med tilgangsbilletten inkludert.
4. Ressursserver kontrollerer at tilgangsbilletten er signert av STS-en og har riktig omfang i forhold til grensesnittet som er forespurt.
5. Ressursserver gjennomfører kallet og returnerer et svar.
6. Klient mottar svaret.

2.3 Brukerautentisering og klientautorisering

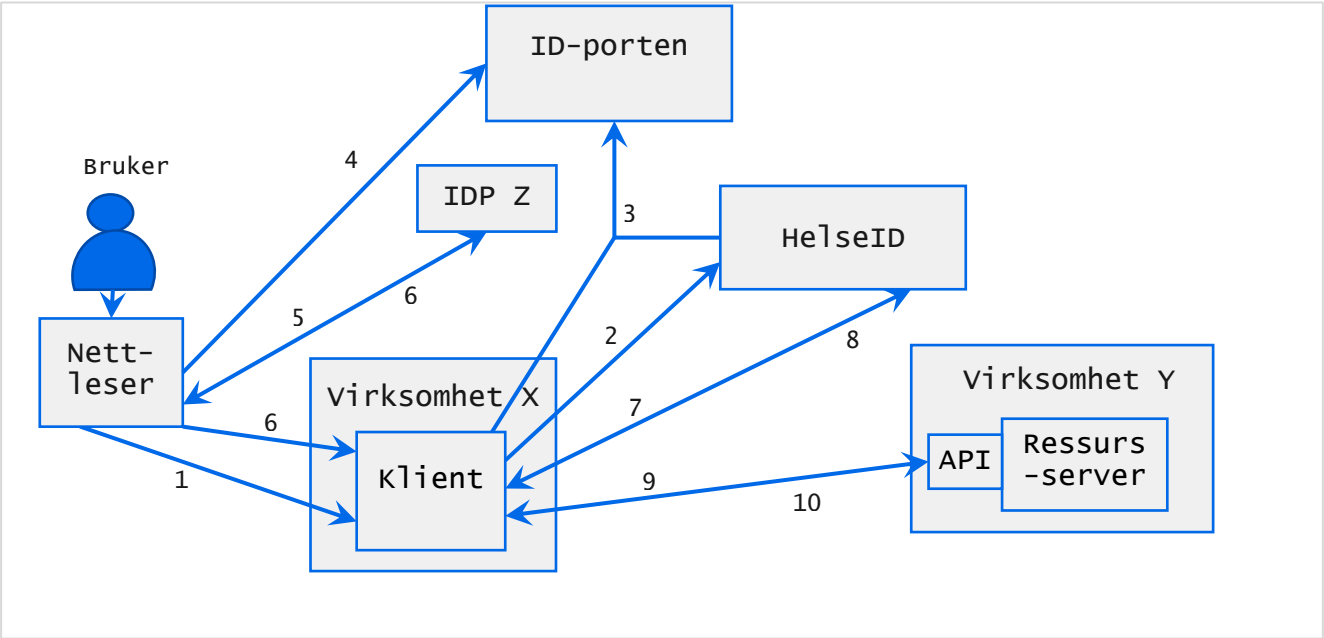
Brukerhistorie inkluderer brukerautentisering og klientautoriseringsflyt:

Som bruker av en forhåndsgodkjent klient tilhørende virksomhet X ønsker jeg tilgang til en ressurs hos virksomhet Y slik at jeg kan få utført funksjoner på ressursen som Ressursserver hos virksomhet Y tilbyr.

Forhåndsbetingelser:

1. Virksomhet Y har inngått avtale med Virksomhet X om at X kan benytte Y sitt datadelingsgrensesnitt.
2. Virksomhet Y krever at brukere hos virksomhet X er autentisert med et gitt tillitsnivå (f.eks eIDAS høy eller nivå 4) – eller at brukere er autentisert hos IdP Z.
3. Bruker hos virksomhet X må ha en elektronisk identitet på et gitt tillitsnivå (f.eks «høy» eller «4».
4. Virksomhet Y har selv, eller via en tiltrodd tredjepart som Y har delegert ansvaret til, registrert klienten som forhåndsgodkjent til å benytte datadelingsgrensesnittet i STS-en, i dette eksempelet HelseID.

For dette use caset finnes flere mulige flyter alt ettersom hvilken IDP som skal benyttes og hvilken type klient som brukeren benytter. I dette eksempelet benyttes en IDP som ID-porten tilbyr og det benyttes en standard webapplikasjon. I tillegg er den basert på at bruker velger å logge inn før benyttelse av API.



Figur 2 Brukerautentisering og Klientautentisering

Flyt:

1. Bruker ønsker å logge inn
2. Klienten ber om å få identifisert sin bruker ved å gjøre en autentiseringsforespørsel mot HelseID.
3. HelseID kontrollerer at innloggingsforespørselen kommer fra en forhåndsgodkjent klient, og omdirigerer klienten til ID-porten.
4. ID-porten ber om at bruker velger IDP. Bruker velger IDP Z og blir omdirigert til IDP Z (via klienten som ikke er vist i figuren over)
5. Bruker logger inn
6. Etter vellykket innlogging omdirigerer IDP Z nettleseren til klienten igjen med autentiseringsinformasjon (gitt at Authorization code flow benyttes).
7. Klienten mottar autentiseringsinformasjon som inkluderer en kode og spør HelseID om å få utstedt identitetsbillett en tilgangsbillett.
8. HelseID kontrollerer kode og kontrollerer at tilgangsforespørselen kommer fra en forhåndsgodkjent klient og utsteder identitetsbillett og en tilgangsbillett.
9. Klienten kaller datadelingsgrensesnittet med tilgangsbilletten
10. Ressursserver kontrollerer at tilgangsbilletten er signert HelseID og kontrollerer at riktig tillatelse er gitt med hensyn til grensesnittet som er forespurt. Ressursserver gjennomfører kallet og returnerer et svar.

2.4 Delegering og representasjon

Det finnes mange eksempler på delegering og representasjon i det daglige liv: en forelder kan representere sitt barn, en ansatt kan ha delegerte rettigheter for å utføre oppgaver på vegne av sin arbeidsgiver osv.

Delegering handler om at personer tildeles enkeltrettigheter for å agere på vegne av noen og representasjon medfører at en annen person har samme rettigheter som en selv eller en part.

Det er utenfor omfanget til dette prosjektet å beskrive flyter for hvordan slik delegering og representasjon oppstår. Likevel er det slik at i data- og dokumentdeling har ressurseier som deler data/dokumenter behov for å kjenne til hvem innlogget bruker representerer eller har fått delegert ansvar fra.

Prosjektet har sett nærmere på tre ulike varianter av delegering og representasjon:

- Foreldrerepresentasjon – En forelder representerer sitt barn og opptrer på vegne av barnet
- Helsepersonell som er ansatt i en virksomhet som yter helsehjelp representerer virksomheten og seg selv når personellet gjør oppslag på en ressurs/pasient. Dette er samme flyt som er beskrevet i kapittel 2.3.
- Personell uten tjenstlig behov delegeres rettigheter fra et annet helsepersonell med tjenstlig behov for å bistå dette helsepersonellet med å yte helsehjelp.

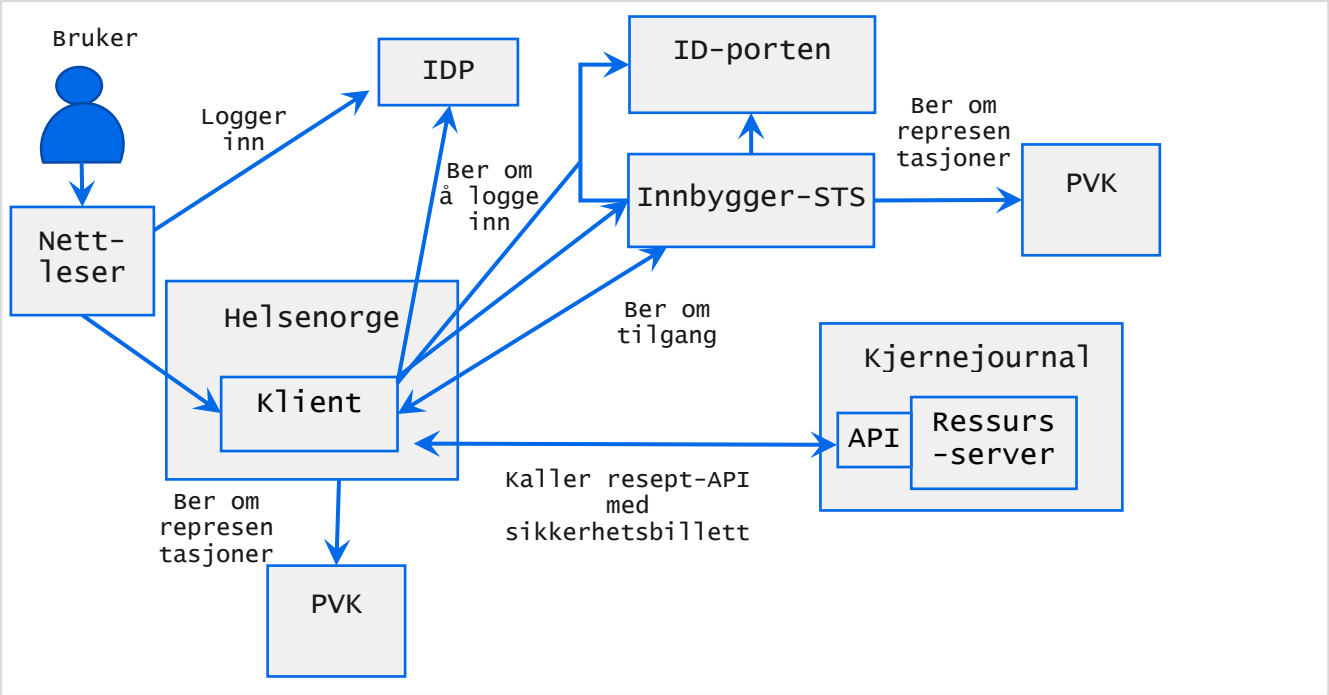
2.4.1 Foreldrerepresentasjon

Som forelder ønsker jeg å ha tilgang til å se helseopplysninger om mitt barn slik at jeg kan følge med på oppfølging i helse- og omsorgstjenesten for mitt barn.

Eksempel – innsyn resepter:

Som forelder ønsker jeg å ha tilgang til å se reseptene til mitt barn slik at jeg kan følge med på medisinbruken til mitt barn.

1. Forelder logger inn på Helsenorge ved å logge inn via Innbygger-STS og ID-porten. Innbygger-STS returnerer en reference-token til nettleser som den sender Helsenorge. Helsenorge ber Innbygger-STS om et access-token ved å bruke reference-tokenet. Access-tokenet kan benyttes for "interne" api-er. Helsenorge slår opp i personvernkomponenten for å sjekke hvem andre innlogget bruker kan representere. Personvernkomponenten returnerer en liste med personer den kan representere.
2. Forelder blir presentert personene den kan representere i Helsenorge og ber om å representere sitt barn.
3. Foreldre ber om å få se reseptene til barnet. Helsenorge ber Innbygger-STS om tilgang til å kalle kjernejournal sitt API-et på vegne av sitt barn. Innbygger-STS slår opp i personvernkomponenten og tar beslutningen om at forelder kan representere sitt barn og utsteder et access-token med et omfang som tillater kall til kjernejournal.
4. Helsenorge kaller kjernejournal sitt API for resepter for barnet og returner en liste med resepter. Dersom barnet er mellom 12 og 16, må kjernejournal filtrere bort visse typer resepter (basert på barns personvernrettigheter nedfelt i forskrifter).
5. Helsenorge viser reseptliste for forelders barn.



Figur 3 Brukerautentisering og representasjon ved API-kall.

Ansvar og tillitsforhold:

1. Innbygger-STS har ansvaret for å beskrive hvilken representasjon som innlogget bruker har valgt å bruke. Representasjonsforholdet henter Innbygger-STS fra personvernkomponenten(PVK).
2. Ressurseier (her kjernejournal) har tillit til representasjonen som innbygger-STS har beskrevet i sikkerhetsbilletten.
3. Basert på innholdet i billetten må ressurseier kunne logge hvem som har fått tilgang og billetten må derfor ha informasjon om innlogget bruker og hvem den representerer. I tillegg må ressurseier, basert på billetten, kunne håndheve personvernregler dersom dette eksisterer (f.eks når forelder representerer barn mellom 12 og 16 år, så må Kjernejournal filtrere bort enkelte resepter).

2.4.2 Personelldelegerte rettigheter

Persondelegerte rettigheter legger til grunn at personellet som skal benytte data- eller dokumentdeling i utgangspunktet ikke har tjenstlig behov, men gjør oppgaver for personell med tjenstlig behov. Eksempel: sekretær gjør oppgaver for en lege. Sekretæren har ikke tjenstlig behov uten at den har fått et delegert ansvar fra legen.

Det forutsettes at selve delegeringen av rettigheten skjer i klient-systemet og at dette ikke skjer som en del av flyten. Det gjøres mye delegering i sektoren i dag, men systemene har i liten grad støtte for slik delegering. Det finnes i midlertidig noen få eksempler på systemstøtte for slik delegering: I DIPS kan arbeidsoppgaver i "arbeidsflyt" delegeres. Dette use caset må sees på som en fremtidig use case. Strukturen i billetten tar høyde for det, men beskriver ikke hvordan dette skal gjøres

Som personell med delegert ansvar fra personell med tjenstlig behov ønsker jeg på vegne av personellet med tjenstlig behov å gjøre oppslag i en pasient sine helseopplysninger hos en annen virksomhet slik at jeg kan yte best mulig helsehjelp.

Sikkerhetsbillettflyten er den samme som er beskrevet i kapittel 2.3. I tillegg må sikkerhetsbilletten inneholde informasjon om den delegerte rettigheten samt at Ressurseier må akseptere forespørsler fra brukere uten tjenstlig behov, men med delegerte rettigheter.

3 Felles påstander for helse- og omsorgstjenesten

Teknologier som benytter sikkerhetsbillett kan deles opp i hovedgrupper: SAML-baserte billetter og JWT-baserte billetter. Hver av disse billettene vil bli behandlet adskilt i dette dokumentet.

3.1 SAML-baserte sikkerhetsbilletter

Bruk av SAML-baserte sikkerhetsbilletter (SAML token) er knyttet til bruk av "SOAP over http"-baserte grensesnitt. Slike grensesnitt er i utstrakt bruk i dag spesielt innen spesialisthelsetjenesten. Derimot er nye anvendelser av SOAP-baserte grensesnitt begrenset. Direktoratet for e-helse har anbefalt at nye anvendelser ikke bør benytte SOAP over http dersom dette ikke er krav, for eksempel slik det er i IHE XDS/XCA (Dokumentdeling).

Bruk av IHE XDS/XCA setter krav til at det benyttes SAML token, gjennom IHE profilen Cross-Enterprise User Assertion Profile (XUA) [2]. IHE XUA beskriver påstander om en autentisert identitet (bruker, applikasjon, system…) i en SAML token.

Alle anvendelser av dokumentdeling skal benytte IHE XUA som sikkerhetsbillett.

3.1.1 Felles krav til IHE XUA i helsesektoren

1. Datatyper som IHE XUA setter krav til påattributtnivå skal benyttes.
2. Subject skal alltid være innlogget bruker (eventuelt autentisert applikasjon/system)
3. ID på innlogget bruker skal benytte et nasjonalt godkjent identifikatorsystem som er støttet av aktørene. Basert på denne ID skal det kunne gjennomføres personvernmessige kontroller.
4. Når innlogget bruker er personell med tjenstlig behov:
    - Organisasjon skal være den juridisk ansvarlige organisasjonen som innlogget bruker representerer.
    - Det skal oppgis underorganisasjonsenhet dersom innlogget bruker kan knyttes til det. Innlogget bruker kan ha stillinger på flere enheter og det bør komme klart frem hvilken enhet bruker representerer. I tillegg vil dette kunne gi pasienten en bedre forståelse av hvorfor helsepersonellet aksesserte pasientens

helseopplysninger. Det kan også tenkes at det er behov for at underorganisasjonsenheten kan benyttes i en autorisasjonsregel. Det er ikke standardisert på hvilket identitetssystem som skal benyttes. Standardisering av dette vil skje i regi av Direktoratet for e-helse og HL7 Norge av FHIR ressursen HealtcareService.

- HPR-nr skal oppgis dersom personell er registrert slik at det kommer klart frem at innlogget bruker er helsepersonell.
- Rolle skal oppgis i henhold til avtalt kodeverk. Rollen skal kunne benyttes til å gi informasjon til pasienten samt til autorisasjonsregler.
- Tjenstlig behov skal oppgis i henhold til avtalt kodeverk. Dette skal benyttes til å vises pasienten samt autorisasjonsregler.

5. Dersom forespørsel gjelder en pasient skal ID oppgis ved hjelp av fødselsnummer eller d-nummer.
6. Dersom innlogget bruker representerer en annen pasient (f.eks barn), skal dette oppgis i billetten. Representasjon skal logges ved tilgang til en pasients helseopplysninger.
7. XUA sikkerhetsbilletten skal utvides med attributter som beskriver:
   - Sikkerhetsnivå/konfidensialitetsnivå (leveres normalt fra IDP)
   - Tilganger som beskriver hvilke dokumenttyper som Subject kan få tilgang til.

3.1.2 Krav til SAML-token for andre anvendelser

Dersom det er behov for bruk av SAML-token for andre felles anvendelser i helsesektoren enn dokumentdeling, og XUA ikke dekker behovet, må dette dokumentet utvides med nye krav.

For andre anvendelser hvor det er krav om SAML-token anbefales det å støtte Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML v2.0 for Healthcare Version 2.0 [3].

3.2 Sikkerhetsbilletter basert på JSON Web Token (JWT)

Dette kapittelet omhandler felles påstander for helse- og omsorgstjenesten og er spesielt knyttet til tilgangsbilletter. De påkrevde påstandene som OAUTH[5] og Open ID Connect standarden[6] definerer, er ikke inkludert.

I arbeidet med påstander har det fremkommet behov for å skille på tilgangsbilletter hvor ressurseier krever en innlogget bruker og når dette ikke kreves (typisk maskin til maskin hvor kun klientautorisering er godt nok). Når ressurseiere har behov for å vite hvem innlogget bruker er, så må informasjon om brukeren medfølge billetten. Dersom klienten opererer kun på vegne av sin virksomhet, er det ingen innlogget bruker og slik informasjon kan da ikke medfølge. I slike anvendelser er det viktig å ha med påstander som beskriver hvilken organisasjon klienten representerer. Det kan være behov for juridiske betraktninger for å

avklare hjemmel av en slik tilgang når slike klienter får tilgang til helseopplysninger. Dette er ikke vurdert som en del av dette dokumentet.

3.2.1 Kollisjonssikre påstandsnavn

I henhold til JWT-standarden[4] så finnes det 3 typer påstandsnavn: Registrerte (registrert i IANA registeret), Offentlige (kan være registrert i IANA eller være kollisjonssikre) og Private (ikke kollisjonssikre).

I dette dokumentet beskrives påstander som har påstandsnavn som er av typen "Offentlige" og med kollisjonssikre navn.

> For å sikre unike navn på felles påstander i helsesektoren skal alle påstander prefikses med "helse://"

> Alle felles påstandsnavn i helsesektoren skal være engelske

3.2.2 Angivelse av hvem som er opphavet til en påstand

I en ideell tillitsmodell bør alle stole like mye på alle påstander. Slik er det ikke i dag. En påstand fra BankID vil i dag ha større tillit enn en påstand fra en klient hos en annen virksomhet. Derfor vil påstander fra ulike kilder ha ulikt tillitsforhold. Det er derfor viktig for en autoriseringsserver som skal signere en tilgangsbillett å kunne angi hvor opphavet til de ulike påstandene er fra.

Følgende standard for dette er definert:

`helse://`	Prefiks for påstander fra STS
`helse://identity/`	Prefiks for påstander fra IDP
`helse://<register>/`	Prefiks for påstander som STS har hentet fra <register>, for eksempel HPR
`helse://client/`	Prefiks for påstander om klienten som kommer fra STS
`helse://client/claims/`	Prefiks for påstander fra klienten/fagsystem
`helse://client/ec/`	Prefiks for påstander hentet fra klientens virksomhetssertifikat

3.2.3 Påstander som nøstede strukturer

I helsesektoren vil det være behov for å inkludere påstander i sikkerhetsbilletten som er basert på kodeverk og som benytter ulike identifikatorsystemer.

Eksempler på kodeverk er adminstrative kodeverk fra volven.no, FHIR valueset, ICD-10 og SNOMED CT. Eksempler på identifikatorsystemer er: folkeregisteret, HPR, HER, enhetsregisteret.

I henhold til JSON web token standarden RFC 7519 [4] kan påstander være nøstede JSON strukturer:

```
helse://hovedpåstand: {underpåstand1, underpåstand2, underpåstand3}
```

Angivelse av påstander slik som kodeverk og identifikatorer kan benytte nøstede JSON strukturer

3.2.4 Angivelse av kodeverk

Angivelse av kodeverk i felles påstander for helsesektoren er bestemt at skal følge FHIR standarden "Coding" [17]. Eksempel (ikke-normativt):

```
"helse://client/claims/role": {
        "coding": [{
          "system": "http://snomed.info/sct",
          "code": "36682004",
          "display": "Physical therapist"
        }]}
```

3.2.5 Angivelse av identifikator

Angivelse av kodeverk i felles påstander for helsesektoren skal følge FHIR standarden "Identifier" [16].

Merk: Etter hvert skal det kunne benyttes godkjente lokale/regionale brukeridentiteter og slike identiteter har også behov for å oppgi "assigner" som er organisasjonene som er ansvarlig for å utstede identiteten. På nasjonale identiteter er dette implisitt informasjon.

Når HelseID benyttes, vil den ha ansvaret for å konstruere denne strukturen etter en vellykket autentisering hos en valgt identitetstilbyder.

3 eksempler (ikke normativt):

```
"helse://identity/person": {
    "identifier":  [{
      "system": "urn:oid:2.16.578.1.12.4.1.4.1",
      "value": "12345678901" fødselsnummer)
    }]}

"helse://client/organization": {
    "identifier":  [{
      "system": "urn:oid:2.16.578.1.12.4.1.2.101",
      "value": "123456789" (organisasjonsnummer)
```

```
    }]}
"helse://identity/person": {
    "identifier":  [{
      "system": "urn:oid:x.x.x.x.",
      "value": "12345", (ID hos lokal IDP)
       "assigner": "HSØ" (eksempel)

    }]}
```

3.2.6 Angivelse av omfang

I en tilgangsbillett oppgis et omfang (på engelsk *scope*) som et attributt med en eller flere verdier. Omfanget indikerer hva slags ressurser en tilgangsbillett skal gi tilgang til. Det er behov for å standardisere hvordan tilgang til ressurser skal oppgis i billetten. Dette arbeidet inngikk ikke i utarbeidelsen av denne versjonen av dokumentet.

3.2.7 Felles påstander i JWT tokens

3.2.7.1 request_record

Hovedpåstand `request_record` beskriver hvem/hva forespørsel gjelder. Siden dette kan være forskjellig fra den innloggede bruker, må dette beskrives i egen påstand.

Dersom forespørselen gjelder en person, så vil dette kreve logging med formål om å kunne vise innsynet til personen selv. I tillegg vil det kunne benyttes for å forstå relasjonen mellom personen og innlogget bruker som forespør.

Underpåstand	FHIR ressurs/datatype	Obligatorisk/ valgfritt	Beskrivelse
`resourcesType [patient, batch, other]`	String	Obligatorisk	Beskriver ressurstypen.
`(resourcesType = patient)`	Patient[9]		
`identifier`	Identifier[16]	Valgfritt	Dersom ressursen kan unikt identifiseres. For pasient vil dette normalt være fødselsnummer.
`name`	Text	Valgfritt	Navn på ressurs. Dette feltet bør unngås. Formålet kan være å sikre at ID og navn hører sammen. Dersom feltet inkluderes, bør det utføres analyse av den økte risikoen for eksponering av sensitiv informasjon

(resourcesType = batch)			Dersom batchen gjelder en pasient, må ressursen "patient" inkluderes.
(resourcesType = other)			Innhold må avklares for hvert enkelt bruk. Dersom forespørsel gjelder en pasient, må ressursen "patient" inkluderes.

Eksempel:

```
"helse://client/claims/request_record": {
      "requestType": "patient",
      "identifier": [{
      "system": "urn:oid:2.16.578.1.12.4.1.4.1",
      "value": "12345678901"
            }],
      "name": {
            "text": "Ola Nordmann"
      }}
```

3.2.7.2 reason_for_request

Hovedpåstand `reason_for_request` skal beskrive brukerens tjenstlige behov. Verdien kan enten peke på en tekststreng eller et kodeverk.

Formålet med denne påstanden er først og fremst for logging som skal vises pasienten. Pasienten må kunne forstå ut i fra teksten hva behovet for innsynet var. I tillegg er formålet med påstanden etterprøvbarhet av tjenstlig behov. For fremtidig bruk kan påstanden også inngå i autorisasjonsregler.

Underpåstand	FHIR ressurs/datatype	Obligatorisk/ valgfritt	Beskrivelse
coding	Coding[17]	Valgfritt	Dersom kodeverk for tjenstlig behov benyttes, skal denne påstand inkluderes

Eksempel (ikke normativt):

```
"helse://client/claims/reason_for_request": "klinisk behandling"
```

Eksempel (ikke normativt):

```
"helse://client/claims/reason_for_request": {
        "coding": [{
```

```
        "system": "http://volven.no/xxxx",
        "code": "yyyy",
        "display": "En tekst som beskriver koden"
      }]}
```

3.2.7.3 requester

Hovedpåstand `requester` skal beskrive innlogget bruker eller klient. Ofte kalt subject. `Requester.resourceType` beskriver hvilken type ressurs som er den forespørrende part. Følgende lovlige verdier finnes:

1. Practitioner: Personell med tjenstlig behov. Basert på FHIR ressursen Practitioner[8].
2. Patient: pasienten representerer seg selv. Basert på FHIR ressursen Patient [9].
3. RelatedPerson: person som representerer en pasient, eksempelvis foreldre, en med fullmakt, verge. Basert på FHIR ressursen RelatedPerson[13].
4. HealthcareService: klient som representerer en organisasjon og en tjeneste hos organisasjonen. Basert på FHIR ressursen HealthcareService [14][18] .

De 3 første gjelder når det er krav om innlogget bruker. Formålet med påstanden er da å gi nok informasjon til å i etterkant kunne forstå relasjonen som innlogget bruker har til pasienten det forespør om. Informasjonen skal brukes til logging (både for innsyn til pasient og etterprøvbarhet) og samt overholdelse av personvernregler (sperringer). Den siste (punkt 4) skal benyttes ved automatiserte klientforespørsler (maskin til maskin).

3.2.7.4 requester er en person

Når `requester` er en person er følgende påstander påkrevd:

Underpåstand	Datatype	Obligatorisk/ valgfritt	Beskrivelse
`identifier`	Identifier[16]. Følgende parametere er obligatorisk: "system" "value"	Obligatorisk. Kan inneholde flere identifier påstander	Unik id på requester + identifikasjons-system.
`name`	HumanName [15]: text (obligatorisk)	Obligatorisk.	Navn på requester

ResourceType = practitioner

Eksempel:

```
"helse://client/requester": {
    "resourceType": "Practitioner",
    "identifier": [{
      "system": "urn:oid:2.16.578.1.12.4.1.4.4",
      "value": "<HPR-ID>"
    },{
```

```
      "system": urn:oid:2.16.578.1.12.4.1.4.1",
      "value": "12345678901"
    }],
    "name": {
      "text": "Juri van Gelder"
    }
```

ResourceType = patient

Eksempel**:**

```
"helse://client/requester": {
    "resourceType": "Patient",
    "identifier": {
      "system": "urn:oid:2.16.578.1.12.4.1.4.1",
      "value": "<fnr>"
    },
    "name": {
      "text": "Ola Normann"
    },
```

ResourceType = RelatedPerson

For denne typen er innlogget bruker en annen innbygger som enten har et foreldreansvar ovenfor pasienten, pasienten har gitt en fullmakt til innlogget bruker eller innlogget bruker er verge for pasienten.

`relationship` skal baseres på Volven kodeverket 7611 som per dags dato har 3 verdier: foreldreansvar, fullmakt og vergemål.

```
"helse://client/requester": {
    "resourceType": "Relatedperson",
    "identifier": [{
      "system": "urn:oid:2.16.578.1.12.4.1.4.1"
      "value": "<fnr>"
    }],
    "relationship": [{
    "coding": [{
           "system": "http://volven.no/7611", (eventuelt benytte OID)
           "code": "FO",
           "display": "Foreldreansvar"
      }],
    "name": {
      "text": "Ola Normann"
    }}
```

3.2.7.5 requester er en automatisert klient

ResourceType = HealthcareService

Underpåstand	Datatype (FHIR ressurs)	Obligatorisk/ valgfritt	Beskrivelse
`Identifier`	Identifier[16]	Valgfritt	Dersom det er behov for en unik ID på klienten
`providedBy`	Organization[7]med følgende parametere: Identifier[16] type name	Obligatorisk. Obligatorisk Valgfritt Valgfritt	Organisasjonen som klienten representerer
`name`	String	Obligatorisk.	Navn på HealthcareService

Eksempel**:**

```
"helse://client/requester": {
    "resourceType": "HealthcareService ",
    "identifier": {
           "system": "urn:oid:2.16.578.1.12.4.1.2.102",
           "value": "<RESH-id>"
    },
    "provideBy": {
            "Organization": {
               "identifier": {
                     "system": "urn:oid:2.16.578.1.12.4.1.2.101",
                     "value": "<orgnr>"

    }}},
    "name": "HSØ responssenter"
    }
```

3.2.7.6 practitionerRole

Hovedpåstand `practitionerRole` skal beskrive ansattrolle eller rolle som beskriver relasjonen mellom pasienten og innlogget personell i organisasjonen som klienten og bruker representerer. Basert på FHIR ressursen PractitionerRole[12].

Påstanden er kun obligatorisk når `requester` er av typen "practitioner". Rollen skal kunne benyttes til både logging og utførelse av autorisasjonsregler.

Per nå finnes det ikke et kodeverk som inneholder alle gyldige roller og hver anvendelse må selv bestemme hvilke kodeverk som skal benyttes. Volven har flere kodeverk som dekker roller. FHIR har også et kodeverk som dekker dette [19].

Underpåstand	Datatype (FHIR ressurs)	Obligatorisk/ valgfritt	Beskrivelse
`Organization`	Organization[7] med følgende parametere: Identifier[16] type name partof	Obligatorisk. Obligatorisk Obligatorisk Obligatorisk Valgfritt	Organisasjonen som innlogget bruker er ansatt i. Kan inneholde hierarki av organisasjoner (bruk av "partof"). Iht FHIR så er dette feltet egentlig en referanse. Pga billettens virkemåte, så er hele ressursen inkludert.
`code`	Coding[17]	Obligatorisk.	Rolle på requester

Eksempel (ikke normativ):

```
{
   "helse://client/claims/practitionerRole":[
      {
         "Organization":{
            "identifier":[
               {
                  "system":"urn:oid:2.16.578.1.12.4.1.2.102",
                  "value":"<RESH-id>"
               },
               {
                  "system":"urn:oid:2.16.578.1.12.4.1.2.101",
                  "value":"<orgnr>"
               }
            ],
            "type":{
               "coding":[
                  {
                     "system":"http://hl7.org/fhir/organization-type",
                     "code":"dept",
                     "display":"Hospital Department"
                  }
               ]
            },
            "name":"Akuttmottak"
         },
         "code":{
            "coding":[
               {
                  "system":"http://snomed.info/sct",
                  "code":"36682004",
                  "display":"Physical therapist"
               }
            ]
         }
      }
```

```
   ]
}
```

3.2.8 Eksempel på sikkerhetsbillett ved krav om innlogget bruker

Standard påstander er ikke tatt med her. NB med forbehold om feil.

```
{
   "helse://client/claims/request_record":{
      "requestType":"patient",
      "identifier":[
         {
            "system":"urn:oid:2.16.578.1.12.4.1.4.1",
            "value":"12345678901"
         }
      ]
   },
   "helse://client/claims/reason_for_request":"klinisk behandling",
   "helse://client/requester":{
      "resourceType":"Practitioner",
      "identifier":[
         {
            "system":" urn:oid:2.16.578.1.12.4.1.4.4",
            "value":"<HPR-ID>"
         }
      ],
      "name":{
         "text":"Juri van Gelder"
      },
      "helse://client/claims/practitionerRole":{
         "Organization":{
            "identifier":[
               {
                  "system":"urn:oid:2.16.578.1.12.4.1.2.101",
                  "value":"<orgnr>"
               }
            ],
            "type":{
               "coding":[
                  {
                     "system":" http://hl7.org/fhir/organization-type",
                     "code":"dept",
                     "display":"Hospital Department"
                  }
               ]
            },
            "name":"Akuttmottak"
         },
         "code":{
            "coding":[
               {
                  "system":"http://snomed.info/sct",
                  "code":"36682004",
```

```
                  "display":"Physical therapist"
               }
            ]
         }
      }
   }
}
```

3.2.9 Eksempel på sikkerhetsbillett uten krav om innlogget bruker

Standard påstander er ikke tatt med her. NB med forbehold om feil.

```
{
   "helse://client/claims/request_record":{
      "requestType":"patient",
      "identifier":[
         {
            "system":"urn:oid:2.16.578.1.12.4.1.4.1",
            "value":"12345678901"
         }
      ]
   },
   "helse://client/claims/reason_for_request":"velferdsteknologisk
oppfølging",
   "helse://client/requester":{
      "resourceType":"HealthcareService ",
      "identifier":{
         "system":"urn:oid:2.16.578.1.12.4.1.2.102",
         "value":"<RESH-id>"
      },
      "provideBy":{
         "Organization":{
            "identifier":{
               "system":"urn:oid:2.16.578.1.12.4.1.2.101",
               "value":"<orgnr>"
            }
         }
      },
      "name":"HSØ responssenter"
   }
}
```

4 Sentrale begreper

Begrepene er basert på definisjoner fra internasjonale standarder eller utarbeidet av Helse Sør-Øst (HSØ) og av NHN (HelseID).

Begrep	Alternative begreper	Beskrivelse	Kilde
Sikkerhetsbillett	Sikkerhetsbevis, token, security token	Sikkerhetsbillett er et samlebegrep for alle typer identitets- og tilgangsbilletter uavhengig av protokoll og format.	Basert på HSØ sin definisjon
Identitetsbillett	Identitetsbevis, ID-token, identity token	En identitetsbillett representerer utfallet av en autentiseringsprosess. En identitetsbillett inneholder informasjon som entydig identifiserer en gitt bruker. Denne informasjonen er ofte statisk, Identitetsbillett signeres elektronisk av utstedelsesløsningen slik som STS. Informasjonen i identitetsbilletten kan stoles på hvis konsument kan verifisere billettens signatur, gyldighet, hvem den er utstedt til samt korrelasjon til autentiseringsforespørselen.	Basert på HSØ sin definisjon
Tilgangsbillett	Tilgangsbevis	En tilgangsbillett inneholder informasjon ut over identiteten til brukere, som gir grunnlag for å evaluere om tilgang kan innvilges. Ofte er denne informasjonen kontekstuell, for eksempel knyttet til en gitt pasient hvor en kan ha en behandlerrelasjon som implisitt innebærer et dokumentert tjenstlig behov for tilgang til informasjon om pasienten. Kommentar: Vi bruker «Access Token» når det benyttes OAUTH, og SAML token når det benyttes WS-Federation (når IHE transaksjoner benyttes), mens tilgangsbillett er et felles begrep.	Basert på HSØ sin definisjon
Påstander	Claims, Assertions	En sikkerhetsbillett består av påstander som beskriver egenskaper knyttet til ressursen i sikkerhetsbilletten, eks navn, identitet, funksjon eller oppgave, og som er relevante	Basert på HSØ sin definisjon

		for å kunne gjøre tilgangskontroll, samt ivareta krav om uavviselighet og logging. Et claim er en påstand om en ressurs eller identitet, for eksempel tilhørighet til en virksomhet, e-postadresse eller fødselsnummer.	Basert på HelseID sin definisjon
Påstandsnavn	Claim name	Påstandens navn. Skal alltid være en string.	JSON web token standarden RFC 7519
Påstandsverdi	Claim value	Påstandens verdi må være en JSON value som kan være en string, boolean, integer, JSON object eller en array.	JSON web token standarden RFC 7519
Kollisjonssikre påstander	Collision-resistant claims	Det er lov å avtale egne påstander i anvendelser av JWT tokens. Derfor er det en risiko at korte påstandsnavn kan bli tatt i bruk med forskjellige betydninger. For å unngå dette, kan påstandsnavn prefikses med unikt navnerom for å være unike på tvers av anvendelser. Dette kalles kollisjonssikre påstander.	Basert på JSON web token standarden RFC 7519
Offentlige påstandsnavn	Public claim names	Offentlige påstandsnavn er i denne konteksten navn som er kollisjonssikre og som da kan benyttes på tvers av anvendelser. I helsesektoren har vi valgt å prefikse helsesektorspesifikke påstandsnavn med "helse:". Kommentar: Offentlige påstandsnavn kan også registreres i det internasjonale registeret IANA. Dette har vi valgt å ikke gjøre.	JSON web token standarden RFC 7519
Representasjon	Impersonation	Når A representerer B, har A alle B sine rettigheter i en gitt kontekst. Alle som mottar en token som beskriver at A representerer B, må forholde seg til B. *Når A representerer B, er A den samme som B.*	Token Exchange – ietf draft
Delegering	Delegation	Når B delegerer noen av sine rettigheter til A, kan A opptre på vegne av B. A beholder sin identitet og er skilt fra B sin identitet.	Token Exchange – ietf draft

		Når B har delegert noen av sine rettigheter til A, kan A opptre som en mellompart mellom B og mottagende part	
Subjekt-token	Subject-token	En tilgangsbillett som skal representere identiteten til parten som tilgangsbillettforespørselen gjelder. "Subject" i det returnerte tilgangsbilletten vil være det samme som "subject" i identitetsbilletten.	Token Exchange – ietf draft
Aktor-token	Actor-token, TE-token, token exchange token.	En tilgangsbillett som skal representerer identiteten til mellomparten. Mellomparten vil være parten (Oauth klient) som har mottatt tilgangsrettigheter for å handle på vegne av "subjectet" (enten delegert eller på vegne av).	Token Exchange – ietf draft
Omfang	Autorisasjon, Scope	Et omfang indikerer hva slags ressurser en sikkerhetsbillett skal gi tilgang til, begrenset til det bruker har gitt (eksplisitt eller implisitt) tilgang til. Fordi et omfang kan bety tilgang til et tjenestegrensesnitt, kan et omfang formuleres som en autorisasjon. Det er dog viktig å merke seg at dette da blir en autorisasjon på klientnivå og ikke for en brukerkonto. Kommentar: Man skiller mellom identitetsnære scopes og ressursnære scopes.. F.eks kan man som et identitetsnært scope be om «email» eller «fødselsnummer». Mens for en ressurs "ehelse/vkp/medication.read"	Basert på HSØ og HelseID Basert på HSØ sin definisjon
SAML token	SAML tilgangsbillett	Tilgangsbillett for SOAP/IHE tjenester. XML basert	Basert på HSØ sin definisjon
Access token	JWT Token	Tilgangsbillett for REST tjenester inkl FHIR. OAUTH basert med JSON syntaks.	
STS	Security token service, Sikkerhets-billettjeneste	Security Token Service, sikkerhetskomponent som utsteder og elektronisk signerer sikkerhetsbillett, altså identitets- og/eller tilgangsbillett. En STS fungerer som et tillitsanker hvor anvendere stoler på de tjenester som STS tilbyr.	Basert på HSØ sin definisjon

		En STS kan implementere en eller flere autentiserings- eller autorisasjonsprotokoller. Eksempler ID Porten, HelseID, Feide. Kommentar: STS er en generisk term. Det er greit å vite at termen abstraherer protokollimplementasjoner. I praksis så har en STS konkrete roller i tilknyttet til hvilke protokoller den implementerer, slik som IdP (Identity provider), OpenId Provider, Authorization Server og STS (WS-Federation)	
Identitetstilbyder	IDP	Identitetstilbyder tilbyr autentisering som en tjeneste andre systemer og applikasjoner kan konsumere. Dette innebærer at de som benytter disse autentiseringstjenestene må stole på at identitetstilbyderen forvalter sine digitale identiteter godt og at de sørger for tilstrekkelig god sikkerhet både i forbindelse med identifisering av bruker og utveksling av informasjon om den autentiserte brukeren. I helsesektoren i Norge finnes det i dag mange identitetstilbydere, men vi skiller i hovedsak mellom tre kategorier: • Interne identitetstilbydere (eksempel: de regionale helseforetakene) • Lokale identitetstilbydere (eksempel: forskjellige systemer, f.eks EPJ, kurve osv) • Eksterne identitetstilbydere (eksempel: Buypass, Commfides, BankID)	Basert på HelseID sin definisjon
Bruker		En bruker er et menneske som bruker en registrert klient for å få tilgang til ressurser	Basert på HelseID sin definisjon
Klient	Tjenestekonsument, Konsument	En klient i denne kontekst er programvare som ønsker å få tilgang til å aksessere en ressurs, enten på vegne av en innlogget bruker eller som en del av en automatisert prosess (maskin-til-maskin). En klient kan forespørre en sikkerhetsbillett fra STS på to måter:	Basert på HSØ og HelseID sin definisjon

		• For å be om å autentisere en bruker – hvorpå det vil utstedes en identitetsbillett. • For å be om tilgang til å aksessere en ressurs – hvorpå det vil utstedes en tilgangsbillett. En klient må være registrert og konfigurert i STS. En identitetsbillett (identity token) og en tilgangsbillett (access token) kan returneres til klient i ett tjenestekall.	
Ressurs	Tjeneste, API	Ressurs er en fellesbetegnelse for en eller flere entiteter som deles med andre virksomheter/personer, og som er representert med et navn, har en eier og kan kontrolleres gjennom et API. Eierskapet er sterkt knyttet til retten til å bestemme tilgangsreglene til en ressurs. En ressurs er noe en autoriseringstjeneste skal beskytte på vegne av eieren. I HelseID skilles det mellom to typer ressurser: • Identitetsressurs - for eksempel brukeridentitet • API-ressurs - et tjenestegrensesnitt	Referanse-arkitektur datadeling
JWT	JSON Web Token	En JWT (Uttales «Djått»), også kalt self-contained token, er tredelt med JSON header, payload og signatur fra utsteders signeringssertifikat. En JWT inneholder blant annet informasjon om utsteder, mottaker, utstedelsestidpunkt, og utløpstid. Dersom det er et Id Token eller Access Token kan det også inneholde informasjon om bærende klient og eventuelt en bruker. Kommentar: Enkelte claims-typer «tilhører» protokollspesifikasjoner.	Basert på HelseID sin definisjon
Bearer token		Et bearer token er en sikkerhetsbillett som kan brukes fritt av den som måtte være i besittelse av det.	Basert på HelseID sin definisjon
Reference token		Reference token er en nøkkel som refererer til en tilgangsbillett lagret i STS, hvis innhold	

		mottakende klient kan hente ved å bruke nøkkelen.	
Refresh token		Refresh token er en sikkerhetsbillett som brukes til å fornye en tilgangsbillett.	