# Vedlegg til høringsnotat

## Innhold



## 1. GNSS og sikkerhet for korrekt loggføring av posisjonsdata i kontrollutrustning.

Som omtalt omfatter yrkestransportloven krav til at det for alle drosjeturer skal registreres geografisk posisjon med satellittbasert kommunikasjonssystem (GNSS), og at slike data skal lagres i 60 dager. Yrkestransportloven åpner for at Samferdselsdepartementet (SD) kan fastsette nærmere regler om loggføring av posisjon i forskrift, (yrkestransportloven § 9).

Som en følge av dette kravet vil det være hensiktsmessig at kontrollutrustningen registrerer GNSS-data og sørger for at disse blir lagret så lenge som yrkestransportloven krever.

GNSS-funksjonaliteten kan i utgangspunktet være en del av en heldigital løsning, der GNSS-signalene hentes fra GNSS-funksjonalitet på den mobile enheten kontrollutrustningen benyttes på eller fra andre digitale GNSS-tjenester. Kontrollutrustningen kan også utvikles slik at de GNSS-signalene som registreres og lagres blir hentet fra en GNSS-enhet fastmontert i kjøretøyet som benyttes til drosjevirksomhet.

I dette notatet vurderes sikkerhet i GNSS for de alternative løsningene for kontrollutrustning som følger av forskriftsforslaget:

1: GNSS som baserer seg stedstjenester og GNSS-mottakere i sjåføren og kundens mobile enhet

2: GNSS som baserer seg på enhet som er fastmontert i kjøretøyet.

### Generelt om GNSS-funksjonalitet og sårbarhet

Summen av kapasitet(mulighet) og intensjon til å gjennomføre tiltak for å manipulere eller endre GNSS signaler er avgjørende for hvorvidt det foreligger en trussel eller risiko. I vurderingen av GNSS-sikkerhet og er det dermed relevant å vurdere følgende:

1. Medfører det foreslåtte regelverk noen form for insentiv til å blokkere eller endre GNSS-signaler (intensjon).
2. Hvilke muligheter finnes for å forstyrre eller forfalske GNSS-signaler og hvilke tekniske barrierer som finnes eller kan introduseres som kan bidra til å redusere den praktiske muligheten til å gjennomføre dette (kapasitet).

For å vurdere den totale risikoen må også konsekvensen ved manipulasjon vurderes. Drosjer beveger seg ofte på eller i nærheten av steder der bruk av GNSS er viktig for samfunnsviktige funksjoner, f.eks. sykehus. De kan også oppholde seg på slike steder over lengre tid. Dette er et element som styrker viktigheten av å redusere sannsynligheten for at aktiv, fysisk (frekvens-basert) manipulasjon tas i bruk. Dersom forstyrrelser skjer på slike steder vil dette kunne bidra til risiko for at denne type tjenester påvirkes. I tillegg til at det er viktig å sikre riktig posisjonsdata for personlig sikkerhet for kunde og sjåfør og for riktig prisfastsetting, er det derfor viktig at utstyr som brukes i drosjer ikke påvirker omkringliggende bruk av GNSS-signal.

GNSS-mottakere er generelt sårbare for fysisk manipulasjon som jamming (støy som forstyrrer signalet) og spoofing (falske signaler).

På sikt er det noen aspekter som kan sannsynliggjøre økt bruk av fysisk manipulasjon av GNSS utstyr. Dersom det foreligger økonomisk motivasjon for å påvirke dataene om prisfastsettelse fremfor strekningsmåling i taksameter kan det gi motivasjon for å påvirke signalene. Økt motivasjon kan drive fram nye forenklede løsninger for å manipulere GNSS. Generell teknologisk utvikling og spesielt forenkling av spoofing vil sannsynliggjøre økt bruk av jamming og spoofing. Denne utviklingen styrkes av at utstyret blir billig og enkelt å bruke, samt at den tekniske kompetansen som kreves for å gjøre mer krevende spoofingangrep stadig blir mindre. Det er derfor rimelig å anta at det kan foreligge både en viss intensjon og kapasitet til økt forstyrrelse eller påvirkning av GNSS-data, jf. vurderingspunktene 1 og 2 over. Se konkret vurdering senere i dokumentet.

I det foreslåtte regelverket introduseres krav som bidrar til å redusere muligheten til, eller hvor lett det er å påvirke GNSS signalet. Dette omtales også i den konkrete vurderingen.

## Vurdering av GNSS sårbarhet i de konkrete løsningene (løsning 1 og løsning 2)

*Vurdering av intensjon (insentiv) til å blokker eller endre GNSS signal til posisjonsdata:*

GNSS-løsninger til bruk ved flåtestyring har eksistert lenge og de fleste taksameterløsninger som benyttes i dag har innebygde posisjonsløsninger. De som tilbyr drosjetjenester har normalt interesse av at dette fungerer godt. Selve oppgjøret skal i dag baserer seg på en forhåndsavtalt pris eller pris basert på strekningsmåling i taksameteret avhengig av hva som er billigst for kunden, og påvirkes ikke direkte av posisjonsdataene. Posisjonen der passasjer skal plukkes opp må nødvendigvis være avklart og registrert allerede før turen, og vanligvis vil bestemmelsesstedet også være registrert. GNSS-signaler vil også kunne benyttes til å registrere turens startsted, turens endested og tidspunkt for start og stopp, på bakgrunn av dette er det mulig å ved hjelp av kartdata beregne kjørt strekning. Der hvor det er maksimalprisreguleringen gjelder kan disse opplysningene etter endt tur benyttes til å beregne pris for oppdraget basert på en parallelltakst. Fra og med 1. november 2020 gjelder maksimalprisreguleringen i kommuner der fylkeskommunene kan eller faktisk tildeler enerett, jfr. Yrkestransportregelverket. Dette er derfor aktuelt i områder med lav befolkningstetthet. Dersom den beregnede parallelltaksten er lavere enn tilbudt pris er det den prisen som er beregnet på bakgrunn av tid og distanse som skal benyttes. I de tilfellene turen er (eller fremstår) så lang at pris beregnet i tråd med prisopplysningsforskriften er høyere enn tilbudt pris vil sjåføren slippe å redusere den tilbudte prisen. Dersom sjåføren ønsker å 'jukse til seg' denne fordelen vil det ikke hjelpe å kun blokkere (Jamme) posisjonsdata, det vil i så fall kreves at man også forfalsker kjøreruten så vil dette utgjøre en relativ høy teknisk barriere. Videre er det vanskelig å se for seg at kunde skal ha interesse av å ha med eget utstyr til å spoofe signaler i drosjen all den tid pris skal avtales på forhånd og det kun i enkelte tilfeller dette kan medføre at prisen som skal betales reduseres. Samtidig vil dette være relativt teknisk krevende og den potensielle gevinsten vil dermed ikke stå i sammenheng til innsatsen.

Det er derfor ikke lett å se økonomiske insentiver til at sjåfør eller passasjer skal blokkere (Jamme) GNSS signaler under turen for å påvirke selve betalingen for oppdraget, og det er trolig heller ikke økonomiske insentiver av stor betydning til å påvirke posisjonsdata, selv om dette ikke kan utelukkes. De foreslåtte kravene til kontrollutrustning vil ikke påvirke disse insentivene i den ene eller andre retningen i forhold til dagens situasjon siden dette er utfordringer som allerede eksisterer i dag.

Det er imidlertid noen tilfeller man kan se for seg at en sjåfør vil ønske å blokkere eller forfalske et GNSS signal:

- For å få økt tilgang til turer: Selv om selve prisen fastsettes eller avtales på forhånd så avgjør bestillingssystemet ofte hvem som tilbys turer basert på hvilke drosjer som er tilstrekkelig nære. Det kan være gunstig å være «i nærheten» av et sted eller i en sone med mange oppdrag. I hvor stor grad dette faktisk er en utfordring i dag er uvisst, men det er kjent at det har vært en utfordring med drosjer som melder seg ledig i 'feil sone'. Dette vil imidlertid ikke påvirkes av nye krav i forhold til dagens situasjon annet enn at nye krav kan medføre at det etableres høyere barrierer mot å gjøre dette.
- Sjåføren bidrar i eller har gjennomført en kriminell handling og ønsker å sette seg selv på (framstå) et annet sted. Gitt at sjåfør er registrert i kontrollutrustningen og det er krav til sikker pålogging er det vanskelig å se for seg hvordan dette kan utnyttes i en situasjon der sjåføren har en bestilt tur og er i næring. I de tilfellene sjåføren ikke er i næring vil situasjonen være som for hvilken som helst trafikant. Kravet til loggføring i yrkestransportloven dekker loggføring av drosjeturer og ikke privat kjøring. Denne typer turer vil derfor kun registreres der det benyttes såkalt elektronisk kjørebok i kjøretøyet, i disse tilfellene vil all kjøring registreres. Bruk av elektronisk kjørebok vil ikke påvirkes av den foreslåtte reguleringen.

Samlet sett vurderes det at det er lite som tilsier at det foreligger vesentlige insentiver til å manipulere GNSS signaler i drosjer, og det er ingenting som tilsier at krav til GNSS i kontrollutrustning alene bidrar til intensjon (insentiver) til å gjøre dette øker i forhold til dagens praksis.

*Vurdering av muligheter for manipulasjon av posisjonsdata og tekniske barrierer*

Sett i forhold til muligheten for å utnytte GNSS-data som en del av kontrollutrustningen er det lite som skiller de to løsningene nevnt over. Begge løsninger beskriver mottaksformer av GNSS-signaler som allerede er benyttet i ulike tjenester både innen privat og kommersiell bruk. GNSS-basert navigasjon ved bruk av mobile enheter eller som en del av kjøretøyets integrerte kontrollsystemer har vært på markedet i mange år, og brukes også i utstrakt bruk i blant annet flåtestyring og til elektroniske kjørebøker.

En løsning som fullt ut benytter seg av innebygget funksjonalitet for mottak av GNSS i en portabel kontrollutrustning (alternativ 1) som f.eks. en Pad eller smarttelefon, kan i noen tilfeller ha dårligere antenneforhold sammenlignet med en dedikert enhet som kan plasseres optimalt. Graden av forbedringspotensialet er svært avhengig av antenneutforming og i hvilken grad kjøretøyet demper signalstyrke. Det er derfor mulig at alternativ 2 kan gi en mer konsis og optimal sikring av tilstrekkelig kvalitet i mottaksstyrke, sammenlignet med noen potensielle realiseringer av alternativ 1.

Når det kommer til GNSS-data og integritet er det potensielt større forskjeller i de to alternativene. Ved bruk av løsning 1 må det forventes at eier av den mobile enheten som benyttes til å realisere kontrollutrustning har administrative rettigheter på enheten. I tilfeller hvor posisjoneringsdata leveres som en tjeneste fra operativsystem til kontrollutrustning, finnes det flere eksempler på programvare som logisk overstyrer lokasjonsdata og da effektivt foretar en logisk manipulasjon. Bortfall kan også styres dersom eier av den mobile enheten lokalt velger å skru av posisjoneringstjenesten. I de tilfellene hvor mellomlagring må benyttes grunnet manglende tilgang på internett er datagrunnlaget mer utsatt i alternativ 1 da administratorrettigheter gir økt risiko for at manipulasjon. Ved bruk av fysisk fastmonterte enheter er denne type logisk manipulasjon vanskeligere, da logisk tilgang på GNSS-data og tilgang til administrative grensesnitt kan være begrenset. Der både sjåfør og passasjer har hver sin enhet vil det være mulig å lage system som

reduserer muligheten for at sjåføren utfører denne type manipulasjon eller avdekker situasjoner der data mellom enhetene samsvarer, dette vil derfor forsterke sikkerheten. Forskjellen i sikkerhet for korrekte data vil derfor være langt lavere dersom også kundens enhet registrer posisjonsdata.

Fysisk manipulasjon av GNSS-signal eller signalstyrke er mulig for begge de skisserte løsningene. Passiv manipulasjon ved å redusere signalstyrke som treffer antennen kan i mange tilfeller være enklere å utføre ved bruk av løsning 2, da antenneplassering ofte er skjult og derfor tillater enklere bruk av omliggende installasjoner med det formål om å dempe signalstyrke. Begge alternativene er sårbare for aktiv fysisk manipulasjon av GNSS-signal. Fordelen med alternativ 2 er at man i denne løsningen muliggjør kobling til data fra kjøretøyet samt bruk av bedre antenne og signalprosessering. Ved å ta høyde for kjøretøyets egen telemetri kan kontrollutrustningen bruke dette til å danne grunnlag for barrierer eller kontrollfunksjoner som søker å avdekke fysisk aktiv manipulasjon. Videre vil bruk av en dedikert og fastmontert enhet med kjente egenskaper på antenne lettere kunne beregne hvorvidt et GNSS-signal er forsøkt passivt manipulert ved å redusere signalstyrke ved mottak, da denne installasjonstypen har mindre variable signaler enn en frittstående og portabel løsning. Faste installasjoner tillater også bruk av smartere antenner som i større grad er motstandsdyktige mot aktiv fysisk manipulasjon, da disse kan ha egenskaper for smartere signalprosessering eller som skjermer for mottak av signal fra uventede hold.

Dersom kontrollutrustningen benytter seg av GNSS-funksjonen i den mobile enheten den brukes på, vil dette gi mulighet til enkelt å bruke samme mobile enhet med kontrollutrustning i flere biler.

Det foreslåtte regelverket omfatter en bestemmelse om at «*Kontrollutrustningen skal ha funksjoner som lagrer posisjonsdata og vanskeliggjør eller avdekker manipulering av GNSS-data.*». Den konkrete praktiseringen av denne bestemmelsen vil fremgå av en veileder, det legges til grunn at dette betyr at det skal finnes funksjoner som er basert på tilgjengelig teknologi som ikke er urimelig fordyrende i kontrollutrustningen.

Et eksempel på en slik funksjon er at systemet benytter multi-GNSS mottakere, det vil si at de tar i bruk signaler fra flere enn ett system på en gang.[1] Dette vil øke sikkerheten i loggføringsdataene. Fra og med 17. mars 2022 vil det europeiske satellittnavigasjonssystemet Galileo bli påkrevd i alle smarttelefoner som følge av at Europakommisjonen har fastsatt dette i Radioutstyrsdirektivet.[2] Dette er et steg på veien til flere multi-GNSS-mottakere. Forøvrig vil det som følge av den foreslåtte bestemmelsen være rimelig å forvente at programvaren, uavhengig av om det benyttes fastmontert eller mobile enheter, inneholder relevante integritetssjekker som lett kan implementeres. Et falsk ('spoofet') signal vil for eksempel, dersom dette ikke er særlig sofistikert utført, ha en annen indikasjon av satellittplassering enn det man virkelig kan forvente på dette tidspunktet, ha feil tidssignal eller ha posisjonen og satellittplasseringen som fremstår som mer 'perfekt' enn det som er praktisk mulig. Sofistikert spoofing er ikke mulig å utelukke, men denne type funksjoner vil i alle tilfeller bidra til å høyne de tekniske barrierene mot spoofing. Videre er det naturlig som følge av det nevnte kravet å forvente at dersom GNSS signal er utilgjengelig (i lengre perioder enn det man vil kunne forvente som følge av tuneller etc.) så skal det ikke være mulig å akseptere oppdrag i løsningen. Dette siden dette kan være en indikasjon på passiv jamming / tildekking.

---

[1] Se Norsk Romsenters NRS-rapport 2013/3, «*Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur*», spesifikt side 77.

[2] *Se mer om dette her.*

Dersom kunden har app som også registrerer posisjonsdata, bidrar dette til forhøyet sikkerhet for at posisjonsdata blir registrert siden sjåføren ikke enkelt ensidig kan hindra at posisjonsdata registreres. Dette vil også kunne hindre at sjåføren installerer apper som lager falske posisjonsdata ved at systemet relativt lett vil kunne avdekke dersom det er betydelig avvik mellom posisjonen til sjåførens registreringer og registreringer på kundens telefon. Under en drosjetur er både sjåfør og passasjer inne i samme bil, så dette tiltaket vil ikke umuliggjøre fysisk manipulering, men vil øke den tekniske barrieren for manipulering. Som en negativ bivirkning av dette kan det bemerkes at dersom man først skal forstyrre GNSS signalene til begge enhetene så vil dette medføre fare for at også omliggende enheter forstyrres. Denne risikoen vurderes imidlertid som lavere enn nytten ved å ha to enheter.

Dersom kontrollutrustningen er utformet slik at den sikrer at GNSS-signaler hentes fra en fysisk fastmontert enhet i bilen som ikke kan slås av, og kontrollutrustningen kun fungerer når den er i nærheten av denne enheten, vil det medføre økt sikkerhet mot at det brukes kjøretøy som ikke er registrert som drosje. En fastmontert GNSS-enhet vil også redusere risikoen for straffbare handlinger der selve drosjeturen er premisset for handlingen, samt øke politiets muligheter til å finne spor/bevis i etterkant, siden GNSS-posisjonen blir lagret uansett hvordan den mobile enheten med kontrollutrustningen blir behandlet. En fastmontert GNSS-enhet i bilen vil også kunne skaffe informasjon om bilens totalt kjørte strekning og strekning kjørt i drosjevirksomhet, dersom det er aktuelt for f.eks. å avdekke skattesvindel. Dette vil imidlertid ikke gi informasjon om detaljer i bilens kjøremønster siden krav til loggføring kun omfatter selve oppdragene. Det er derfor i praksis mulig å få samme opplysninger ved å bruke kjøretøyets totale kilometerstand.

## 2. Nærmere beskrivelse av de aktuelle løsningene

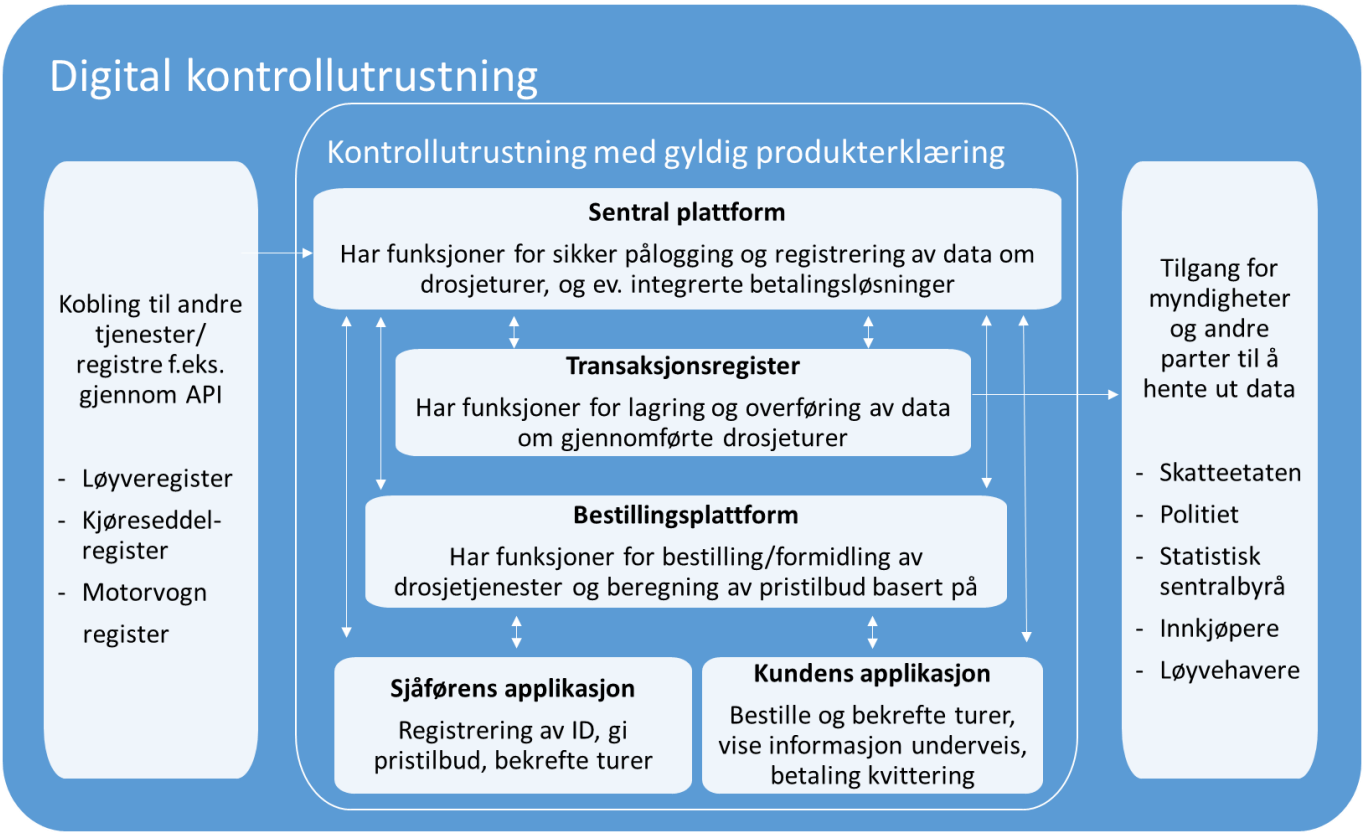
### Løsning 1: heldigital løsning

En kontrollutrustning må tilfredsstille de behov og hensyn som er beskrevet i regelverket. Det er opp til systemleverandøren å sikre at kravene til funksjoner i kontrollutrustningen oppfylles. Teknisk sett kan alle funksjonene i kontrollutrustningen ligge i én og samme løsning, eller bestå av flere komponenter og programvare i et samlet system. Hvordan markedet vil oppfylle funksjonskravene, vil derfor bero på blant annet valg av teknologi og forretningsmodell.

### Eksempel på hvordan kontrollutrustning kan oppfylle kravene i digital kontrollutrustning

Som illustrasjon på hvordan de påkrevde funksjonene kan oppfylles av systemleverandør vil vi i det følgende gi et konkret eksempel. Eksempelet under er en applikasjonsbasert digital kontrollutrustning som består av følgende hovedkomponenter og programvare:

- Sentral plattform
- Transaksjonsregister
- Bestillingsplattform
- Kundeapplikasjon
- Sjåførapplikasjon




*Figur 1: Skisse av potensiell løsning for kontrollutrustning*

**Sentral plattform** i dette eksempelet er en teknisk plattform som har sikre funksjoner for å:

- registrere opplysninger om gjennomførte drosjeturer (løyvehaver, sjåfør, avtalt pris, kjørerute, mv.)
- registrere GNSS-data som gir informasjon om drosjens posisjon (posisjonsdata kan gjøres tilgjengelig i bestillingsplattformen og skal lagres i transaksjonsregisteret, samt gir grunnlag for utskrift av kvittering med angivelse av kjørerute for gjennomførte drosjeturer) og skal kunne kobles til andre offisielle registre for kontroll av identifikasjon. Dersom nødvendig identifikasjon ikke er registrert, kan ikke kontrollutrustningen tas i bruk
- kommunisere og utveksle informasjon med øvrige hovedkomponenter

Koblinger til relevante registre skal muliggjøre verifisering av hvilken løyvehaver, sjåfør og hvilket kjøretøy som benyttes til drosjeturen. Om mulig bør verifiseringen skje online. Dette kan f.eks. løses gjennom programmeringsgrensesnitt (API) hos forvalter av de aktuelle registrene.

**Transaksjonsregisteret** lagrer opplysninger som er beregnet og registrert i den sentrale plattformen, herunder nøkkeldata om gjennomførte turer og sporingsdata. Dette vil være grunnlaget for overføring av data om skattepliktige transaksjoner til skattemyndighetene, ivaretagelse av plikter etter bokføringsforskriften, og til formidling av kvittering til kunden for gjennomførte turer.

Skattemessige opplysninger fra kontrollutrustningen skal rapporteres til skattemyndighetene på standardiserte dataformater av driftsansvarlig for kontrollutrustning, som ikke selv kan være løyvehaver. Posisjonsdata skal leveres til politiet på forespørsel. Andre myndigheter som har behov for å hente ut statistikk kan også kreve opplysninger fra transaksjonsregisteret dersom disse har hjemmel for dette. Dette kan for eksempel være Statistisk sentralbyrå og fylkeskommuner.

**Bestillingsplattformen** er den delen av løsningen som benyttes til formidling av drosjeturer og har funksjoner for å

- registrere og håndtere bestillinger av turer. Bestilling av drosjeturer basert på angitt hente- og leveringsdestinasjon skal bekreftes i plattformen. Pristilbudet basert på oppgitt bestemmelsessted beregnes basert på f.eks. kartdata og den aktuelle prisstrukturen hos formidler, og i samsvar med maksimalprisforskriften. Sjåføren skal ikke kunne påvirke prisen
- foreta kassaavstemming
- kommunisere og utveksle informasjon med sjåfør- og kundeapplikasjon
- kunne benytte posisjonsdata til hensiktsmessig flåtestyring

Bestillingsplattformen må ivareta direkte integrasjonsbehov for formidlere som Pasientreiser, skoleskyss mv. Disse representerer et stort samlet volum av transporttjenester med tilhørende behov for koordinering og utnyttelse av ressurser. Integrasjon av denne typen skal være teknologinøytralt og basert på de facto standard for datakommunikasjon (f.eks. et REST API) for utveksling av informasjon om bestilling/avbestilling/endring av transport, endringer i status i pågående transport som av- og påstigning, forsinkelser og posisjonering, samt mulighet for direkte kommunikasjon med sjåfør. Det forutsettes at behov for integrering med kontraktspartnere avtales i det enkelte tilfellet.

**Sjåførapplikasjonen** er en applikasjon på sjåførens smarttelefon, nettbrett eller annen enhet. Sjåførapplikasjonen kommuniserer og utveksler relevant informasjon med den sentrale plattformen og bestillingsplattformen.

Sjåfør logger inn på sjåførapplikasjon med kontrollerbar ID (for eksempel gjennom bank-ID, biometrisk gjenkjenning e.l.), angivelse av løyvenummer, kjøreseddel og bilens registreringsnummer.

I sjåførapplikasjonen får sjåfør melding om bestilte turer, hentested, bestemmelsessted og hvem kunden er. Sjåføren bekrefter i sjåførapplikasjonen at sjåføren kan tilby den aktuelle drosjeturen til pristilbudet som genereres i bestillingsplattformen.

Når sjåføren har bekreftet i sjåførapplikasjonen at drosjeturen er gjennomført vil kunden motta kvittering. Sjåføren får tilsvarende kvittering for utført oppdrag i sin sjåførapplikasjon.

Drosjesjåførens versjon av kundeapplikasjonen skal ha tilsvarende funksjonalitet som en ordinær kundeapplikasjon (se under). Pristilbud og bekreftelse av tur gjøres av sjåføren på vegne av kunden i sjåførapplikasjonen. Dette innebærer at drosjer med kontrollutrustninger også kan betjene kunder som ikke behersker eller ikke ønsker å bruke smarttelefon, eller som ønsker å praie drosjen på gata eller benytte drosje fra holdeplass.

**Kundeapplikasjonen** er en applikasjon eller portal på kundens smarttelefon, nettbrett, datamaskin eller annen enhet. Kundeapplikasjonen benyttes av kunden til å bestille drosjeturer og eventuelt betale. Kunden angir hentested og bestemmelsessted og får fremvist et pristilbud og bekreftelse på hvilken bil, sjåfør og løyve som skal utføre drosjeturen. Kunden kan sammenligne pristilbudet mot pristilbud fra flere tilbydere. Når kunden har akseptert pristilbudet er oppdraget akseptert, og loggføringen av drosjens posisjon starter når kunden setter seg inn i bilen. Kundeapplikasjonen skal vise bilens posisjon til enhver tid, sjåførens navn og bilde, avtalt pris mv. Dersom kunden har bestilt turen gjennom en bestillingsapplikasjon vil kunden bekrefte bestillingen gjennom applikasjonen. Situasjoner der kunden ikke dukker opp til en bestilt tur eller drosjen ikke dukker opp til en bestilt tur vil reguleres av avtalebetingelser knyttet til bruken av applikasjonen, og for øvrig få konsekvenser for kundens «rating» av leverandøren.

Når drosjen har ankommet bestemmelsesstedet og kunden har betalt, skal kunden få kvittering for betalt tur. Kunden kan velge å betale med kontanter eller på annen måte, for eksempel i applikasjonen dersom dette er mulig. Dersom kunden er innlogget i kundeapplikasjonen kan kunden ha tilgang på digital kvittering og en oversikt over alle tidligere utførte turer direkte i applikasjonen. Alternativt kan kvittering sendes digitalt til kunden på andre måter, for eksempel e-post eller SMS. Det legges i forslaget til nytt regelverk til grunn at kunden har en egen kundeapplikasjon.

Både sjåfør- og kundeapplikasjonen skal tilbys gjennom sikre distribusjonskanaler, eksempelvis Google Play og App Store, og støtte krav til universell utforming og personvern, samt unngå diskriminering av kunder i henhold til likestillings- og diskrimineringsloven.

## Løsning 2: fastmontert GNSS-funksjon

I dette avsnittet beskrives teknisk hva som kan ligge i et eventuelt nærmere krav til loggføringsfunksjonen for posisjonsdata, dersom det kreves at loggføringsfunksjonen sikres med GNSS-enhet fysisk fastmontert i bilen (løsning 2). Det skisseres alternative løsninger som kan benyttes for å imøtekomme et eventuelt krav.

Hensikten med nærmere krav om at loggføring av posisjonsdata skal implementeres med en GNSS-enhet med fysisk tilknytning til kjøretøyet, er å gi høyere sikkerhet for korrekte GNSS-data, for slik å øke sikkerheten for passasjer og sjåfør. I tillegg vil en GNSS-funksjon fastmontert i kjøretøyet, utgjøre en ekstra kontrollmulighet for skattemyndighetene med hensyn til korrekt skatteoppgjør siden data med dette blir sikrere.

For ivareta sikkerhet for at posisjonsdata er pålitelige og komplette, legges det til grunn at det ikke må være lett å miste eller slå av GNSS-sporingen, for eksempel ved å slå av kontrollutrustningens posisjonsfunksjon på den mobile enheten, eller ved at telefonenheten går tapt. Vi legger derfor til grunn at en fastmontert enhet både må inneholde en egen GNSS-mottager og sende disse dataene uavhengig av mobil enhet.

I det følgende er det beskrevet tre potensielle tekniske løsninger for fastmontert GNSS-funksjon som grunnlag for posisjonsdata som registreres og lagres av kontrollutrustningen.

A. *Løsning der eksisterende taksametersystem benyttes som den fastmonterte enheten*
B. *Løsning der posisjonsenhet som benyttes til system for flåtestyring eller elektronisk kjørebok benyttes og som er sikkert tilkoblet kjøretøyet*
C. *Løsning som er bygget for formålet, og forsterket med tilkobling til kjøretøyets systemer*

### A. Løsning der GNSS system som er en del av eksisterende taksametersystem benyttes som den fastmonterte enheten

Dagens regelverk for taksametre omfatter kun taksameter som måleinstrument og de funksjonene som er relatert til dette. I praksis så omfatter taksametersystemene som benyttes mye mer:

- GNSS enhet for flåtestyring og oppdragsstyring og for å oppfylle krav til loggføring av kjørerute
- Funksjoner for pålogging av sjåfør
- Lagring og overføring av transaksjonsdata til drosjesentral eller annen aktør

- Baksystemer som håndterer lagring av data, systemtilgang og rapportering til skattemyndigheter

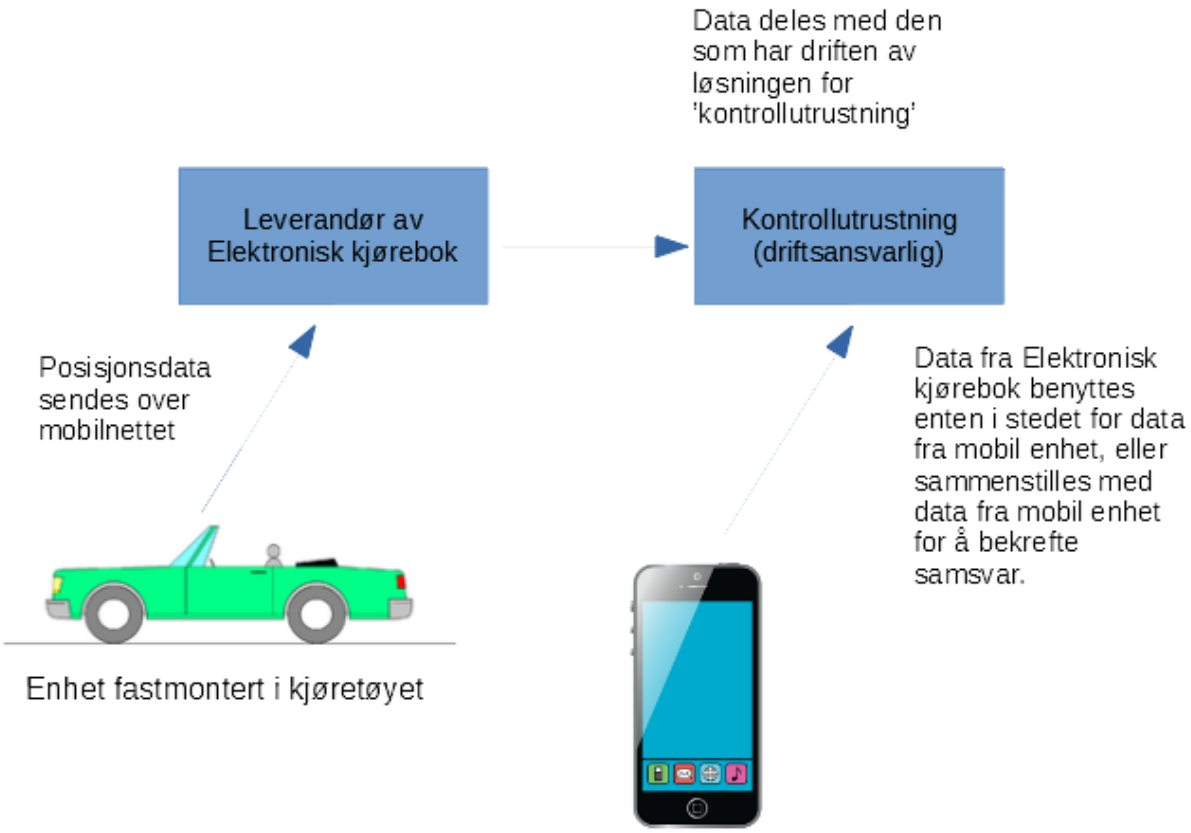
I praksis oppfyller dermed dagens taksametersystem i stor grad i praksis de funksjonelle kravene som foreslås for kontrollutrustning. Selv om selve taksameterfunksjonen ikke lenger blir det mest kritiske så er disse systemene ferdig utviklet og tilgjengelig, det vil dermed utgjøre en liten barriere for eksisterende løyvehavere å ta i bruk dette. Dagens taksametersystem er videre konstruert for å kunne koples (plomberes) sikker til kjøretøyet.

### B. Bruk av og samarbeid med leverandører av eksisterende system for flåtestyring og dokumentasjon av bruk av kjøretøy

Det finnes mange leverandører av teknologi for å dokumentere bruk og posisjon av kjøretøy. Det vanligste bruksformålet til slike løsninger er såkalte 'elektroniske kjørebøker', men også flåtestyringsverktøy eller forskjellige typer alarmer og sikkerhetsløsninger, bruker denne type systemer. En elektronisk kjørebok består av en GNSS-enhet koblet til bilen som dokumenterer hver enkelt tur som foretas. GNSS-enheten sender kjøreloggen til en 'kjørebok' på nett som alltid er oppdatert. Siden dette er løsninger som i stor grad allerede finnes og er installert i kjøretøy som brukes til næringsvirksomhet, kan det tenkes at det er kostnadseffektivt å bruke disse løsningene også til å ivareta nærmere krav til loggføringsfunksjonen, jf. yrkestransportloven § 9.

En forutsetning for at dette er en løsning som er mulig å realisere er at det er kommersiell interesse blant dagens leverandører av elektroniske kjørebøker til å understøtte den type funksjonalitet, det vil si å tilby de nødvendige datagrensesnittene i løsningen. Det må også foreligge databehandleravtaler som omfatter alle aktørene. Det er selvsagt også en mulighet for at leverandører av denne typen systemer ønsker å utvikle porteføljen til å også å utvikle kontrollutrustninger for å komplementere eksisterende løsninger.

Denne løsningen kan brukes ved at man enten sammenstiller data fra den elektroniske kjøreboken for å bekrefte samsvar mellom posisjonene i disse løsningene og posisjonen i kontrollutrustningen i ettertid (etter endt tur), eller at man bruker posisjonsdata fra disse løsningene i 'sanntid' dersom dette er teknisk mulig.




*Figur 2: Skisse av potensiell løsning der GNSS-signal sikres med elektronisk kjørebok*

**Kostnader**

Løsningen krever at det må være montert elektronisk kjørebok i kjøretøyene som benyttes. Dette er typisk et løpende abonnement med en kostnad på kr 2 000 til 3 000 per år. Mange næringsdrivende benytter allerede denne type løsninger, så det antas at denne kostnaden i seg selv ikke vil utgjøre en stor etableringsbarriere. Det må imidlertid i tillegg lages funksjonalitet for eksport av data fra løsningen, og det vil påløpe kostnader knyttet til drift og utvikling av dette.

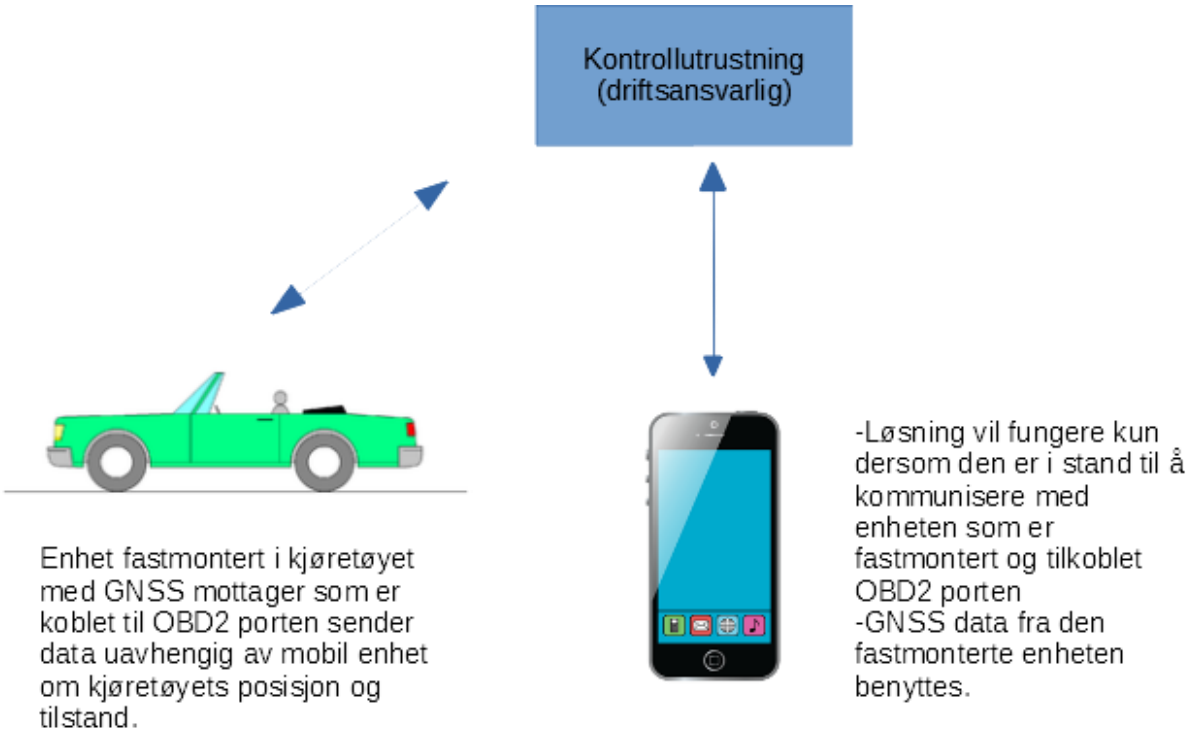
Siden det allerede finnes leverandører av kjørebøker som håndterer posisjonsdata gjennom GNSS-teknologi, vil en slik løsning sannsynligvis representere den løsningen for fastmontert GNSS-logging som vil kreve minst av investeringer og nyutvikling.

**Sikkerhet**

Dette systemet vil ikke ha høyere sikkerhet enn dagens 'elektroniske kjørebok'. I dag er det er ingen konkrete krav til sikker tilkobling eller plombering av enheten til kjøretøyet. Mange leverandører har tilgjengelige instruksjoner for egenmontering, og det er dermed relativt lett å flytte enhetene mellom kjøretøy, selv om systemene ofte registrerer 'strømbruddshendelser', som kan gi en indikasjon på at noe har skjedd. Dersom det skal kreves sikker tilkobling til kjøretøyet, det vil si plombering som utføres av verksted, vil dette øke kostnaden for løsningen. Det bør derfor forutsettes at det kun kan brukes løsninger som kan tilkobles sikkert til kjøretøyet.

**C. Bruke enhet i kjøretøyet som er bygd for formålet med GNSS-mottaker, eventuelt i kombinasjon med tilkobling til kjøretøyets telemetri.**

Så godt som alle kjøretøy i dag har en såkalt OBD2-port. Denne porten (kontakten) har som hensikt å skaffe til veie diagnosedata om kjøretøyet og brukes blant annet av bilverksteder til feilsøking. OBD2-porten kan gi statisk informasjon om kjøretøyet, for eksempel kjøretøyets identifikasjonsnummer (VIN), eller dynamisk informasjon om motorstatus eller hastighet (ikke posisjon). Dette er data som kan sammenstilles med GNSS-data fra en fastmontert enhet i bilen, for å øke sikkerheten for korrekte data. Det er da mulig å lage en kontrollutrustning som kun kan brukes dersom den mobile enheten med kontrollutrustningen befinner seg på tilnærmet samme posisjon som kjøretøyet og den fastmonterte GNSS-senderen når denne befinner seg i riktig kjøretøy. Denne type løsning kan dermed omtales som en såkalt 'black box'-løsning, siden den er i stand til dokumentere bruken av kjøretøyet uavhengig av mobil enhet.




*Figur 3: Skisse av potensiell løsning ved bruk av bilens OBD2-port og enhet for GNSS-signal montert i bilen*

**Kostnader**

Det forutsettes at det brukes en egen enhet som er tilpasset formålet som kan kobles til OBD2-porten og som også inneholder GNSS-mottager. Med tanke på strømbrudd eller bortfall av datanettverk vil det også være behov for en viss lagringskapasitet i enheten. Enkelte leverandører av elektroniske kjørebøker har også løsninger som kan kobles til denne porten.

Løsningen krever at den som utvikler kontrollutrustningen også sørger for hardware som kobles til kjøretøyet og som kan kommunisere med den mobile enheten. Det vil både være utviklingskostnader til dette, og produksjonskostnader per enhet. Siden denne enheten også må inneholde en GNSS-enhet eller-antenne, vil dette være en betydelig høyere kostnad enn for løsningen som er skissert i

avsnittet over, både med tanke på utviklingskostnader og enhetskostnader. Det vil trolig være nødvendig å utvikle eller tilpasse løsninger spesielt. Det kan derfor ikke utelukkes at enhetskostnader kan komme til å være like høye som kostnader til dagens taksametre (se avsnitt **Feil! Fant ikke referansekilden.**).

**Sikkerhet**

Dette eksemplet representerer den mest komplette løsningen av de tre løsningene og den løsningen som gir best mulighet for å utvikle en løsning som sikrer god datakvalitet. Denne løsningen vil kunne danne en barriere mot feil posisjonsdata, og det vil være krevende å forfalske posisjonsdata ved bruk av denne løsningen, forutsatt at systemleverandøren har ivaretatt sikkerheten i programvaren på en god måte. Det vil ved tilkobling til kjøretøyets OBD2-port også være mulig å dokumentere med relativt god sikkerhet hvilket kjøretøy som er benyttet.

## Oppsummering

Nærmere krav til at loggføringen av drosjeturer skal sikres ved en fastmontert enhet i kjøretøyet, kan sammen med funksjoner i programvaren for kontrollutrustning bidra til høyere sikkerhet for korrekte posisjonsdata.

Sikkerhet for korrekte posisjonsdata oppnås imidlertid ikke automatisk ved fysisk tilknytning, og må vurderes i sammenheng med krav til datakvalitet i løsningen totalt sett. For eksempel må det etableres løsninger i programvaren som skal forhindre drift dersom posisjonsdata mangler eller at data ikke samsvarer med annen informasjon, uavhengig av krav til tilkobling.