NTNU
Det skapende universitet

Personvernhensyn ved innsamling av dynamiske data

Studie av anvendelsesområder for AutoPASS

Marte Hellum Olaisen

Master i kommunikasjonsteknologi
Oppgaven levert: Juni 2007
Hovedveileder: Steinar Andresen, ITEM
Biveileder(e): Sven L. Pihl, CIBER

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Oppgavetekst

Utvidelse av eksisterende teknologier og nyutvikling av teknologiske løsninger kan være med på å effektivisere trafikkavviklingen på norske veier. Intelligente transportsystemer (ITS) ser ut til å være en del av fremtiden innen transportsektoren, og en utvidet bruk av AutoPASS vil kunne involveres i systemene. AutoPASS er det norske systemet for elektronisk betaling av bompenger. Trafikkdata samlet inn fra AutoPASS-brikker kan eventuelt benyttes til andre formål. Dette åpner opp for nye anvendelsesområder i årene som kommer. Bruken av AutoPASS vil kunne medføre at bilistene legger igjen elektroniske spor når de ferdes på norske veier. Personvernlovgivning og Datatilsynet kan dermed sette begrensninger for anvendelsene, og må tas hensyn til når nye anvendelsesområder og rutiner for behandling av data diskuteres.

Formålet med masteroppgaven er på bakgrunn av dette å se på mulige anvendelsesområder for AutoPASS, og evaluere disse med tanke på personvern. Oppgaven går ut på å kartlegge eksisterende bruk av AutoPASS, samt se på nye muligheter. Med utgangspunkt i krav om tilfredstillende personvern skal nåværende praksis vurderes og eventuelle endringer foreslås.

Oppgaven gitt: 17. januar 2007
Hovedveileder: Steinar Andresen, ITEM

Sammendrag

Bruk av IKT i transportsektoren gir muligheten til å øke trafikksikkerheten, minke miljøbelastningen og effektivisere trafikkavviklingen. AutoPASS heter det norske systemet for elektronisk betaling av bompenger, og AutoPASS er et eksempel på hvordan IKT kan benyttes for å effektivisere bompengebetalingen i Norge. AutoPASS muliggjør kommunikasjon mellom vegsystem og trafikanter, og legger tilrette for en rekke anvendelser utover betaling av bompenger.

Teknologier som krever behandling av personopplysninger kan medføre at brukerne legger igjen elektroniske spor. Teknologisk utvikling åpner opp for en rekke anvendelser som fører til økt registrering og bruk av personopplysninger. Oppmerksomhet rundt personvern har på bakgrunn av dette økt i den senere tid. AutoPASS er en teknologi som innebærer behandling av personopplysninger, og utfordrer følgelig personvernet. Utvidelser av AutoPASS vil også utfordre personvernet gjennom en økning i omfanget av opplysninger som samles inn. Med utgangspunkt i personvern kartlegger jeg i denne oppgaven eksisterende bruk av AutoPASS, og ser videre på nye anvendelsesområder for teknologien.

Tendensen i eksisterende og utprøvde anvendelser er økt samordning av betalingssystemer for ulike transporttjenester. Eksisterende anvendelse av AutoPASS er i hovedsak for bompengebetaling og reisetidsmålinger. AutoPASS prøves også ut som betalingsmiddel for ferge og parkering. Utvikling av et AutoPASS betalingskort pågår i dag, og visjonen for kortet er at det skal fungere som betalingsmiddel for alle transporttjenester. Parallelt med utvidelser innad i Norge pågår det både nordiske og europeiske prosjekter som jobber mot en samordning av bompengebetaling på tvers av landegrensene.

ITS (Intelligente Transportsystemer) er betegnelsen på bruk av IKT i transportsektoren, og det utvikles stadig nye ITS-løsninger som et resultat av den raske teknologiutviklingen. ITS kan deles inn i ulike anvendelsesområder, og anvendelsesområdene jeg har valgt å se på i denne oppgaven er (1) trafikantinformasjon, (2) overvåkning og kontroll og (3) betalingssystem. Innen de tre utvalgte områdene kan det skisseres flere mulige anvendelser av AutoPASS. Trafikantinformasjon åpner opp for mer sanntidsinformasjon til trafikanter

gjennom ulike informasjonstjenester, eksempelvis en tjeneste for dynamisk informasjon til fergetrafikanter. Under området overvåkning og kontroll kan AutoPASS anvendes for å realisere et overvåkningssystem for farlig gods i vegnettet. Datainnsamling fra AutoPASS kan også gi et bedre datagrunnlag for planlegging av veier og infrastruktur. AutoPASS som betalingssystem er anvendelsesområdet som omfavner den største mengden datafangster, og som skaper de største utfordringene for personvernet. Dette på grunn av at betalingstjenester i de fleste anvendelsene krever behandling av personopplysninger. Med tanke på miljøet kan AutoPASS benyttes for vegprising, et system som beregner avgifter på bakgrunn av et kjøretøys belastning på miljøet i utsatte områder. Vegprising krever et tettere oppsett av målepunkter enn i dag, og innkreving av miljøavgift fra tungtransport kan på samme måte beregnes ut i fra belastningen den påfører miljøet.

Oppsummert ser vi at en utvidelse av AutoPASS til å inkludere flere anvendelser medfører flere registreringer av bevegelser i vegnettet. Denne informasjonen kan brukes for å kartlegge reisemønster, og muligheten for misbruk er tilstede. Fokus på hvordan personvernet utfordres og tas hensyn til i dag kan gi nyttige innspill når nye anvendelser utvikles. Eksisterende praksis i henhold til personvern kan dermed videreutvikles eller forbedres på bakgrunn av erfaringer. Når krav til behandling av data utarbeides for nye anvendelser må personvernet tas hensyn til, og det må rettes oppmerksomhet mot de utfordringene som følger av en utvidelse av AutoPASS. Sammenlagt skaper flere anvendelser nye utfordringer med tanke på samordning og muligheten for kobling av datafangster.

Forord

Denne masteroppgaven markerer slutten på min sivilingeniørutdanning innen Kommunikasjonsteknologi ved NTNU. Oppgaven har et halvt års omfang, og er utført ved Institutt for Telematikk med fordypning innen området telekommunikasjon, organisasjon og samfunn (TOS). Fordypningsområdet har gitt meg muligheten til å studere det som interesserer meg mest; samspillet mellom teknologi og samfunn. I denne oppgaven ser jeg på personvernutfordringer ved anvendelser av AutoPASS, og oppgaven er i så måte ikke rent telematisk.

Arbeidet med oppgaven har vært meget lærerikt, men også til tider krevende. Mye tid har gått med til å oppnå forståelse og finne informasjon om problemområdet. Oppgaven er utformet i samarbeid med CIBER Norge AS, og jeg vil rette en takk til veileder Sven Pihl for all hjelp og støtte under arbeidet med oppgaven. Professor Steinar Andresen har vært min veileder fra instituttet, og fortjener en takk for all veiledning og hjelp. Jeg vil også takke informantene fra Q-Free og Statens Vegvesen for gode innspill og nyttig informasjon. Helt til slutt vil jeg takke Amund for alle gode forslag til forbedringer av oppgaven.

Trondheim 14. juni 2007,
Marte Hellum Olaisen

Innholdsfortegnelse

Figur- og tabelliste

Forkortelser

ASECAP	European Association with tolled motorways, bridges and Tunnels
ARKTRANS	ARKitektur for TRANSportområdet
ASB	AutoPASS Samordnet Betaling
BST	Beacon Service Table
CALM	Continous Air-interface Long and Medium range
CEN	European Committee for Standardization
CESARE	Common Electronic fee collection System for an ASECAP Road tolling European system
CS	Central System
CSSS	Central System Security Server
DSRC	Dedicated Short Range Communication
EETS	European Electronic Tolling Service
EFC	Electronic Fee Collection
EMK	Den Europeiske Menneskerettskonvensjonen
EPC	Electronic Parking Consulting
EU	Den Europeiske Union
FAD	Fornyings- og Administrasjonsdeparementet
GPS	Global Positioning System
GSM	Global System for Mobile communications
IEEE	Institute of Electrical and Electronics Engineers
IKT	Informasjons- og Kommunikasjonsteknologi
IPv6	Internet Protocol version 6
ISO	Industry Standards Organization
ITS	Intelligente TransportSystemer
JD	Justisdepartementet
NorITS	Nordic Interoperability for Tolling Systems
OBE	On Board Equipment
OBU	On Board Unit
RFID	Radio Frequency Identification
RSE	Road Side Equipment
RSU	Road Side Unit
SD	Samferdselsdepartementet
SV	Statens Vegvesen

TC	Technical Commitee
TØI	Transportøkonomisk Institutt
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
VST	Vehicle Service Table
WiMax	Wireless Metropolian Area Networks
WLAN	Wireless Local Area Network

1 Innledning

I den offentlige debatten har fokuset på personvern økt som følge av omfattende utvikling og bruk av teknologi som produserer elektroniske spor. I *Personvernrapporten 2007* peker Datatilsynet (2007a) på hvordan utbredelsen av RFID-brikker gjør det enklere å spore enkeltpersoners bevegelser i samfunnet. Med innføring av RFID i både pass og bankkort i tillegg til i AutoPASS, vil kartleggingen av bevegelser bli meget omfattende. Teknologien er nyttig og forenkler hverdagen for brukerne i mange tilfeller, men den medfører også større mulighet for overvåkning. Personvernet er i følge Datatilsynet (2007a) derfor i en brytningstid, med en stadig mer omfattende registrering og bruk av personopplysninger.

Transportsektoren står ovenfor mange utfordringer med tanke på det økende behovet for transport i samfunnet, og hovedutfordringen er *"å utvikle et transportsystem med god fremkommelighet, der hensyn skal tas til miljø og trafikksikkerhet*" (SV 2006a). Informasjons- og kommunikasjonsteknologi (IKT) kan gi et viktig bidrag i prosessen mot å endre situasjonen, og målet med økt bruk av IKT i transportsektoren er å skape et effektivt, miljøvennlig og sikkert transportsystem (TØI 2004b). Anvendelser av de mulighetene IKT gir er nødvendig for å nå dette målet, og jeg mener at anvendelsene må ta hensyn til personvernet. Enkelte anvendelser innebærer behandling av persondata, og kan medføre at brukeren legger igjen elektroniske spor. Hvorvidt dette skaper vansker for personvernet er avhengig av hvordan teknologien anvendes.

Teknologirådet (2005) betegner AutoPASS som et velkjent eksempel på en teknologi som utfordrer personvernet gjennom registrering av brukerens bevegelser. I dag forbinder de fleste AutoPASS med bompengebetaling, men teknologien legger også tilrette for andre anvendelser. Noen anvendelser er allerede under utprøving, mens andre befinner seg på et tankestadium. Ved å utnytte de mulighetene AutoPASS-teknologien gir, kan nye anvendelser bidra til å endre situasjonen i transportsektoren. Jeg ser på en vurdering av personvern i henhold til AutoPASS som et meget aktuelt tema, spesielt med tanke på mulige utvidelser i anvendelsen av teknologien.

1.1 Problemstilling og problemområde

For en konkretisering av problematikk rundt hensynet til personvern har jeg valgt AutoPASS og dynamiske data som studieområde i oppgaven. Dynamiske data kan karakteriseres ved at de kontinuerlig oppdateres (se kapittel 4), og begrepet kan benyttes om data som samles inn ved bruk av AutoPASS. En illustrasjon på dette er at data som forteller hvilken bomstasjon en bil sist passerte vil oppdateres når bilen passerer en ny bomstasjon. Det er nettopp denne dynamikken som legger tilrette for nye anvendelser av AutoPASS, og som samtidig skaper nye utfordringer for personvernet. Personvernhensyn ved innsamling av dynamiske data er derfor aktuelt å se på i sammenheng med både eksisterende og nye anvendelser av AutoPASS.

I denne oppgaven vil jeg se på hvilke anvendelser av AutoPASS som eksisterer i dag, og hvilke nye anvendelser av AutoPASS som kan komme i fremtiden. Jeg vil også se på hvordan både eksisterende og nye anvendelser utfordrer personvernet, og vurdere praksis i henhold til personvern i dag og for fremtiden. Formålet med oppgaven kan oppsummeres i tre punkter:

- Kartlegge eksisterende anvendelser av AutoPASS.
- Se på nye anvendelsesområder for AutoPASS.
- Vurdere anvendelsene og praksis i henhold til personvern.

Problemområdet i oppgaven omfavner samspillet mellom teknologi og samfunn. AutoPASS utfordrer personvernet, mens personvernet stiller krav til AutoPASS. Gjensidig påvirkning mellom AutoPASS og personvern gjør at nye anvendelser av AutoPASS skaper nye utfordringer for personvernet, mens personvernet på bakgrunn av utfordringene stiller nye krav til anvendelsene. Kunnskap om hvordan anvendelsene av AutoPASS i dag utfordrer personvernet kan dermed benyttes for å ta hensyn til personvernet når nye anvendelser utvikles.

1.2 Avgrensninger

For at oppgaven ikke skal bli for generell har jeg gjort noen avgrensninger i omfanget. Personvernhensyn ved innsamling av dynamiske data kan være aktuelt for mange teknologier, men i denne oppgaven er studieområdet avgrenset til AutoPASS. Oppgaven vil se på hvilke anvendelser som allerede eksisterer eller er utprøvd, men er begrenset til å se på et realistisk utvalg nye anvendelsesområder. Med hensyn til oppgavens omfang har jeg også valgt å utelate økonomiske vurderinger, selv om økonomi kan være en viktig drivkraft for utvidelser av AutoPASS. Oppgaven er en tverrfaglig studie som omfatter både teknologi og samfunn, og tekniske utfordringer og detaljer i AutoPASS er utelatt for å gi plass til betraktninger om personvern. Detaljer i henhold til sikkerhetsmekanismer som kryptering og lignende er følgelig ikke fokusert på i oppgaven. Jeg har også begrenset oppgaven til å ikke gå dypt inn i problematikk rundt eierskap og organisering, og vil ikke gi noen løsning på hvordan ansvarsfordelingen i AutoPASS bør være med tanke på offentlige og private aktører.

1.3 Metode

Problemstillingen er retningsgivende for valg av forskningsmetode, og valget av metode er dermed avgjørende for hvordan jeg har valgt å tilnærme meg problemstillingen. Det er vanlig å dele inn forskningsmetode i to hovedgrupper; kvalitative og kvantitative metoder. Kvantitative metoder går i bredden av problemområdet, og ønsker å oppnå resultater i form av målbare (kvantiserbare) enheter. Kvalitativt orienterte metoder går i dybden av materialet som undersøkes, og innebærer innhenting av mange opplysninger om få undersøkelsesenheter. (Dalland 1993)

En kvalitativ tilnærming til problemstillingen vil gi grunnlag for en omfattende forståelse av problemområdet. I denne oppgaven har jeg gjennomført en kvalitativ litteraturstudie supplert med ustrukturerte intervjuer. Dette innebærer at intervjuene har tatt form som samtaler hvor spørsmålene ikke har vært ferdig formulert på forhånd (Dalland 1993:34). Informantene ble valgt ut fordi de har god kunnskap på undersøkelsesområdet, og representerer utviklingsmiljøene involvert i AutoPASS. Utvelgelsen samsvarer med Thagaards anbefalinger om strategisk

utvalg i kvalitative studier, og innebærer at man "*velger informanter som har egenskaper eller kvalifikasjoner som er strategiske i forhold til problemstillingen*" (Thagaard 2002:53). Jeg har hatt kontakt med 5 informanter i perioden 01. mars til 15. mai 2007, og jeg gjennomførte intervjuer av to av disse. Resten av kommunikasjonen har foregått via e-post.

Datainnsamlingen fra litteratur er gjort for å oppnå forståelse rundt problemområdet, og valget av litteratur er dermed med på å presisere problemstillingen. Tema i oppgaven er AutoPASS, personvern og dynamiske data, og problemstillingen er knyttet til personvernhensyn ved innsamling av dynamiske data. Datainnsamlingen om AutoPASS, personvern og dynamiske data fremhever sammenhengen mellom de tre områdene, og danner grunnlaget for oppgaven som i hovedsak er teoretisk. Rapporten er i seg selv er sluttprodukt av studien som er gjennomført.

Litteratur og kilder

Mye av informasjonen om AutoPASS er funnet enten på Internett eller gjennom kontakt med Statens Vegvesen og Q-Free. AutoPASS er et teknologiområde under utvikling, og det finnes ikke mange bøker på området. Beste kilde til informasjon om videre utvikling av AutoPASS har derfor vært Internett, og da spesielt de offentlige nettsidene til AutoPASS, Statens Vegvesen, ITS Norway og Samferdselsdepartementet. En del av teknologien bak AutoPASS har vært utviklet over flere år og er dokumentert i bøker og standarder. AutoPASS spesifikasjonene er en omfattende dokumentsamling eid av Statens Vegvesen. Med tanke på masteroppgavens omfang og begrensninger har jeg ikke hatt anledning til å sette meg ytterligere inn i denne samlingen, men intervju av representanter fra Vegdirektoratet og Q-Free har gitt meg mye informasjon på området. Grunnet begrenset tilgang på informasjon om AutoPASS kan kildene som er brukt være noe subjektive, og viser i hovedsak synspunkter fra sitt ståsted. For å oppnå en balanse med tanke på personvern har jeg benyttet kilder og rapporter fra Datatilsynet sammen med vedtak i Personvernnemnda. SINTEF har gjort mye arbeid om bruk av IKT i transportsektoren, og har utarbeidet en rekke rapporter som har vært nyttige for å skape forståelse rundt problemområdet.

Mitt bidrag

Vurdering av hvordan hensynet til personvern praktiseres i dag er nyttig grunnlag i vurderinger av nye anvendelser. Jeg oppfatter eksisterende arbeider om personvern som mer generelle i forholdet til teknologi, mens jeg i denne oppgaven fokuserer på personvern i en konkret teknologi, nemlig AutoPASS. Utvidet bruk av IKT i transportsektoren gir ikke bare positive konsekvenser i form av et bedre transportsystem, men skaper også utfordringer utover de tekniske. Gjennom å rette oppmerksomhet på personvernutfordringene med AutoPASS kan oppgaven være med på å skape oppmerksomhet rundt utfordringer med annen bruk av IKT i transportsektoren.

Jeg har i denne oppgaven kartlagt eksisterende og utprøvde anvendelser av AutoPASS på bakgrunn av en omfattende datainnsamling, og vurdert disse opp mot personvern. Videre har jeg diskutert mulige nye anvendelser for AutoPASS som en del av ITS. Ideen bak de fleste nye anvendelsene har jeg hentet fra eksisterende arbeider som *Nasjonal Transportplan,* mens andre har jeg kommet frem til gjennom samtaler med faglærer og veileder. Hvordan ideene kan realiseres med AutoPASS er derimot mitt eget bidrag. Jeg har også diskutert løsningene mine i henhold til personvern, og gitt noen forslag til hvordan personvernet kan ivaretas. Alle vurderinger gjort av anvendelsene med hensyn på personvern representerer mitt bidrag.

Målgruppe

Målgruppen for oppgaven er personer som jobber med AutoPASS og planlegging av fremtidige anvendelser av teknologien. Oppgaven kan også være av interesse for andre som jobber med IKT-utvikling, både generelt og innen transportsektoren. Med tanke på at oppgaven ser på AutoPASS gjennom en personvernsvinkling, er den også aktuell for personer som jobber med eller interesserer seg for personvern, selv om de ikke er tilknyttet transportsektoren.

1.4 Oppbygning

Oppgavens teoretiske del omfatter andre, tredje og fjerde kapittel. Kapittel 2 er en beskrivelse av domenet i oppgaven. Her introduseres AutoPASS og plasseres i sammenheng med annen bruk av IKT i transportsektoren. Utfordringer for

personvernet blir også introdusert, og det gis en kort beskrivelse av teknologien bak AutoPASS. Kapittel 3 er en teoretisk gjennomgang av hva som ligger bak hensynet til personvern. Nasjonale og internasjonale bestemmelser som regulerer behandling av personopplysninger blir gjennomgått og oppsummert som et sett viktige personvernprinsipper, nyttige for videre vurdering av personvern. Kapittel 4 tar for seg dynamiske data, og viser hvordan slike data er aktuelle i sammenheng med AutoPASS og personvern.

Funnene fra den kvalitative studien beskrives i femte og sjette kapittel av oppgaven. Kapittel 5 tar for seg AutoPASS i dag og ser på hvilke anvendelser som er i bruk, under utprøving og under utarbeidelse. Samordning på tvers av landegrenser er et aktuelt tema i denne sammenheng og presenteres sist i kapittelet. Nye anvendelser blir deretter gjennomgått i kapittel 6, og her ser vi på hvilke løsninger fremtidens transportsystem kan bestå av. I begge kapitlene vil anvendelsene fortløpende diskuteres i henhold til personvern.

Kapittel 7 ser på praksis for personvern gjennom en diskusjon rundt hvilke krav som bør stilles til behandling av data ved en utvidelse av AutoPASS til å omfatte flere anvendelser. Her gjenopptas viktige diskusjonspunkter angående personvern fra kapittel 5 og 6, med utgangspunkt i teorien. Kapittel 8 markerer avslutningen for oppgaven gjennom en konkluderende oppsummering. Her foreslås også områder for videre studier og arbeid.

2 Domenebeskrivelse: AutoPASS

I dette kapittelet vil jeg gi en beskrivelse av domenet AutoPASS, og se på AutoPASS i sammenheng med målsetningene for teknologi i transportsektoren. Utvidet bruk av informasjons- og kommunikasjonsteknologi (IKT) i transportsektoren gir mange nye muligheter, og disse kan skisseres opp som anvendelsesområder for intelligente transportsystemer (ITS). Kapittelet introduserer deretter utfordringer for personvernet ved bruk av teknologi som AutoPASS. Innen domenet er det en rekke elementer som er nyttige å se på før det til slutt gis en kort beskrivelse av teknologien bak AutoPASS.

2.1 Bakgrunn

AutoPASS heter det norske systemet for elektronisk betaling av bompenger (AutoPASS 2007a). Tjenesten er rettet mot kjøretøy som ofte benytter avgiftsbelagte transportstrekninger, som for eksempel bompengefinansierte motorveger, bruer og tunneler. Flere av de manuelle bomstasjonene er automatiserte og byttet ut med AutoPASS-teknologi. Resultatet er at kjøretøyene ikke trenger å stoppe ved passering av betalingspunkt dersom de har skaffet seg en AutoPASS-avtale. Hensikten med AutoPASS er å gjøre betalingen av vegtransporttjenester så enkel som mulig for brukerne. I dag realiseres dette med en AutoPASS-brikke som monteres i frontruten på kjøretøyet, og denne registreres elektronisk når betalingspunktene passeres. Dette øker effektiviteten og bedrer trafikkflyten, samtidig som det er kostnadsbesparende (IBM 2006). Det er en målsetning å få et felles betalingssystem for alle tjenester innen vegtransport i Norge, og AutoPASS-brikkene er blant annet prøvd ut som betalingsmiddel for parkering og på ferger. (Vermesan et al. 2005) Norge er blant de ledende landene i verden innen utvikling av samordnede bompengesystemer, og arbeidet med å innføre AutoPASS i Norge ble startet av Statens Vegvesen i 1998 (Ibid.). AutoPASS (2007b) forteller at betaling av bompenger for å finansiere vegutbygging i Norge ikke er noe nytt fenomen. Allerede for flere hundre år siden var det vanlig å betale for bruk av vegnett og broer. Omfanget av bompengefinanisering har dog økt i løpet av de siste 20 årene, mye på grunn av trafikkøkning og da økende behov for utbygginger og investeringer i vegnettet. Problemer med kødannelser i de største

byene i Norge var en utslagsgivende faktor for utbygging av en rekke bomringer på slutten av 80-tallet. Formålet med bomringene er dog rent finansielt, og er ikke ment som en regulering av trafikken. (AutoPASS 2007b) Inntekter fra bomringer brukes til finansiering av infrastruktur for lokal kollektivtrafikk i tillegg til finansiering av vegprosjekter (SD 2004:67). Verdens første bomstasjon med elektroniske betaling ligger i Ålesund, og ble åpnet allerede i 1987 (Trondsen 2006a). I dag er det 23 AutoPASS-anlegg i Norge av 45 bompengeanlegg totalt. 1,2 millioner AutoPASS-brikker er i bruk. (SV 2007a)

2.2 Teknologi i transportsektoren

Samferdselsdepartementet (2002:3) ønsker at økt bruk av IKT i transportsektoren skal *"øke sikkerheten i transportsektoren, øke utnyttelsen av kapasiteten i transportinfrastrukturen, [og] øke nytten for brukerne av transportsystemene"*. AutoPASS er et eksempel på hvordan IKT benyttes for å realisere et elektronisk betalingssystem for bompenger. AutoPASS øker både utnyttelsen av kapasitet i transportinfrastrukturen og nytten for brukerne. Kapasiteten øker som et resultat av bedre trafikkflyt gjennom bomstasjonene og færre problemer relatert til kødannelser. Systemet øker dermed også nytten for brukerne, som ved bruk av AutoPASS slipper å stoppe for å betale bompenger, og slipper å stå i kø. Sammenlagt medfører dette en effektivisering av bompengeinnkrevingen på norske veger. Samferdselsdepartementet (2002:6) peker på nettopp effektivitet som en av flere områder hvor IKT kan bidra positivt i transportsektoren gjennom *"en effektiv utnyttelse av eksisterende transportinfrastruktur"*. To andre viktige områder er trafikksikkerhet og miljø. Bruken av IKT i transportsektoren gir muligheten til å *"øke trafikksikkerheten gjennom bedre trafikkstyring, trafikkovervåking og utstyr i det enkelte transportmiddel"* (Ibid.). Miljøbelastningen fra transportsektoren kan også påvirkes gjennom en utvidet bruk av IKT, ved å legge tilrette for miljøbesparende tiltak. Effektivitet, sikkerhet og miljø refereres ofte til som tre viktige transportpolitiske målsetninger, og visjonen er følgelig at IKT kan bidra til en mer effektiv, mer miljøvennlig og mer trafikksikker transport (TØI 2004b:5). AutoPASS er en ikke bare en teknologi som kan benyttes for betaling av bompenger. Teknologien gjør det mulig for trafikanter og vegsystem å kommunisere. Dette innebærer at AutoPASS legger til rette for en rekke tjenester som benytter denne typen kommunikasjon.

2.2.1 Transportpolitikk og ITS

I *Nasjonal Transportplan* (SD 2004:7-8) skisseres det opp fire hovedmål for transportpolitikken:

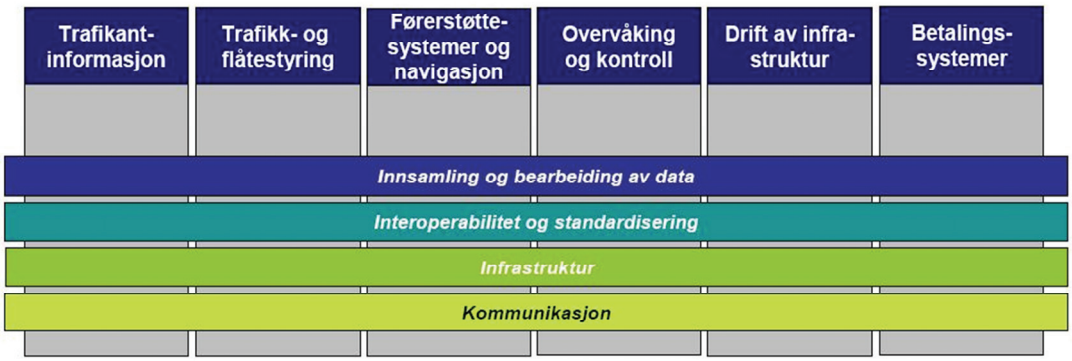
- *Færre drepte og alvorlig skadde i vegtrafikken*, og fortsatt høy sikkerhet i andre transportformer
- *Mer miljøvennlig bytransport* – med redusert bilavhengighet og økt kollektivtrafikk.
- *Bedre fremkommelighet i og mellom regioner*, for å fremme utvikling av levedyktige distrikter, vekstkraftige bo- og arbeidsmarked og dekke næringslivets transportbehov
- *Et mer effektivt transportsystem,* hvor blant annet økt bruk av konkurranse benyttes for å få et best mulig transporttilbud for de samlede ressursene til transportformål.

ITS står for Intelligente Transportsystemer og er en betegnelse som benyttes for bruken av IKT i transportsektoren. ITS kan hjelpe til med å nå de fire hovedmålene, og samtidig bidra til en optimalisering av eksisterende transportsystemer. Målet med innføringen av ITS er i følge Bang og Wahl (2007:1) *"å forbedre transportsystemet i form av bedre fremkommelighet, bedre effektivitet, bedre trafikksikkerhet, reduserte kostnader, og økt nytte for brukerne av transportsystemene og samfunnet for øvrig"*. Det utvikles stadig nye ITS-løsninger som et resultat av den raske teknologiutviklingen, og felles for alle løsningene er at de benytter seg av elektroniske data. Innsamling og kvalitetssikring av data er sentrale oppgaver i ITS. Innsamlede data kan være nyttige i flere ulike systemer, og det er derfor viktig å sikre muligheter for deling og gjenbruk. Dette kan gjøres gjennom bruken av et felles rammeverk for ITS-løsningene. (Bang & Wahl 2007)

Eksempel på et slikt rammeverk er ARKTRANS (ARKitektur for TRANSportområdet), som er et nasjonalt rammeverk for transportsystemer. Rammeverket skal bidra til et bedre samspill mellom informasjonssystemer og transporttjenester, og følgelig en bedre tilrettelegging for samordning av person- og godstransporten i Norge. (SD 2004)

2.2.2 Anvendelsesområder for ITS

ITS kan deles inn i 6 ulike anvendelsesområder, illustrert i figur 2.1. Anvendelsesområdene er avhengige av noen sentrale grunnsteiner, representert ved de 4 horisontale boksene. Som nevnt er innsamling og bearbeiding av data en viktig del av ITS; uten data vil ikke løsningene fungere. Interoperabilitet og standardisering gjør det mulig å samordne de ulike tjenestene, og en forutsetning for det er datakommunikasjon og muligheten for distribusjon av data. For å kunne realisere ITS-løsningene og kommunikasjon mellom transporttjenester trengs det også en infrastruktur. (Bang & Wahl 2007)



Figur 2.1 Anvendelsesområder for ITS (Bang & Wahl 2007)

Anvendelsesområdene jeg har valgt å se videre på i sammenheng med AutoPASS er trafikantinformasjon, overvåkning og kontroll og betalingssystemer. Valget er gjort på bakgrunn av at AutoPASS i dag faller inn under området for betalingssystemer, mens de to andre anvendelsesområdene er interessante med tanke på nye muligheter med AutoPASS.

Trafikantinformasjon er et sentralt anvendelsesområde for ITS, og skal sikre trafikantene tilstrekkelig informasjonsgrunnlag til å kunne ta beslutninger om reiser eller kjøreoppdrag. Dette er informasjon som i stor grad etterspørres i dagens samfunn, og innebærer informasjon om alt fra kollektivtakster og rutetider til tilstanden på vegnettet. Dynamisk sanntidsinformasjon er nyttig som datagrunnlag i denne sammenhengen, sammen med statisk informasjon (kapittel 4 vil se nærmere på ulike datatyper og databehandling).

Overvåkning og kontroll omfatter tiltak for å overvåke og kontrollere trafikken. Dette innebærer overvåking av trafikkstrømmer og trafikkavvikling, potensielle konfliktsituasjoner og lignende. Overvåkning ligger ofte til grunn for trafikantinformasjon, og de to områdene er relatert til hverandre.

Betalingssystemer er nødvendige for å kunne ta betalt for ulike transporttjenester. I elektroniske betalingssystemer gjennomføres betalingen ved bruk av en elektronisk billett eller brikke. Integrering av slike betalingssystemer er under utvikling i dag, og gjør det mulig å benytte seg av samme betalingsmiddel i flere transporttjenester. Dette innebærer også bruk av samme brikke for å betale for bompassering, fergebillett og parkering, som med AutoPASS. (Bang & Wahl 2007)

2.2.3 Utfordringer for personvernet

En av de største personvernutfordringene ved bruk av AutoPASS omhandler retten til anonym ferdsel. *Personvernrapporten 2007* peker på at retten til å være anonym er et viktig personvernprinsipp. *"Borgeren har krav på å kunne ferdes anonymt. Når nye teknologiske løsninger tas i bruk, skal det legges til rette for at retten til anonym ferdsel fortsatt blir ivaretatt"* (Datatilsynet 2007a:5). AutoPASS er en teknologi som innebærer behandling av personopplysninger. Det betyr at AutoPASS behandler opplysninger som kan knyttes til enkeltpersoner. Opplysningene inneholder blant annet navn og adresse til personen som har inngått en AutoPASS-avtale og fått en AutoPASS-brikke, samt hvilke passeringer av bomstasjoner brikken gjør. Det er derfor ikke bare trafikkrelaterte konsekvenser av bruken av teknologi som dette. Personverninteresser utfordres av bilistenes ønske om en effektiv passering av bomstasjoner. Det samme gjelder for tiltak og teknologier som skal øke trafikksikkerheten. En avveining mellom hensynet til personvern og de transportpolitiske målsetningene gjøres dermed når transportsektoren velger å ta i bruk en teknologi. For bilistene er det snakk om en avveining mellom personverninteresser og egne interesser når de tar i bruk teknologien, på bakgrunn av hvilke interesser de anser som viktigst for seg selv.

En utvidelse av AutoPASS til å omfatte andre anvendelsesområder enn bompengebetaling vil medføre flere utfordringer for personvernet. Som en del av ITS vil det stilles krav til databehandling og deling av data mellom ulike

anvendelser. Personopplysningene vil kunne knyttes til enda flere tjenester, og behandles på flere steder. Behandlingen av personopplysninger er regulert av juridiske rammer som vi kommer tilbake til i kapittel 3.

2.3 Systemelementer i AutoPASS

Det er flere elementer involvert i AutoPASS-systemet; *utsteder, bompengeselskap, operatør, vegkantutstyr, AutoPASS-brikke, bruker, sentral konto og avtaleverk* (Foss 2005). Ansvaret til utstedere er å inngå AutoPASS-avtaler, sende ut AutoPASS-brikker og opprette sentrale konti. I dag er det bompengeselskapene som er utstedere. Bompengeselskapene vil også ha rollen som operatør, og har da ansvaret for å drive bomstasjoner eller andre betalingspunkter som samler inn data fra AutoPASS-passeringer. Retten til å drive et bompengeselskap er i dag konsesjonsbelagt. Det kreves uten unntak Stortingsvedtak før et selskap kan begynne med innkreving av bompenger (Furan 2007). Alle bompengeselskaper har et sentralsystem (CS) som behandler passeringer av bomstasjoner som tilhører bompengeselskapet. Sentralsystemet behandler også passeringer av fremmede bompengeselskap gjort av "sine" avtaler. Vegkantutstyr kalles utstyret montert i betalingspunktene for å kunne kommunisere med AutoPASS-brikken, dette kan for eksempel være det fysiske betalingspunktet i en bomstasjon. Personer eller organisasjoner som benytter seg av AutoPASS kan kalles brukere, og alle brukere har sin egen sentrale konto som administreres av bompengeselskapet. Denne kontoen inneholder informasjon om brukerens rettigheter, gjerne i form av betalingsinformasjon. Rettigheter, forpliktelser, roller og ansvar, oppgaver og daglig drift av AutoPASS reguleres av et sett avtaler og retningslinjer samlet i et AutoPASS-avtaleverk. En AutoPASS-avtale er selve avtalen mellom bruker og utsteder. (Foss 2005)

2.3.1 AutoPASS-avtale

For å kunne benytte seg av AutoPASS må brukeren inngå en avtale med en utsteder. Avtalen definerer betingelsene knyttet til bruken av AutoPASS, og ved å skrive under på en slik avtale har brukeren akseptert avtalens vilkår. Frivillig samtykke fra den registrerte er et juridiske krav for å kunne registrere og behandle personopplysninger, og gjennom avtalen gir brukeren samtykke til dette

(JD 2000). Punkt 9 i avtalen omhandler personvern, og 9.1 sier at *"all bruk av brikken vil bli registrert i forbindelse med betalingskontroll, fremstilling av anonymisert statistikk, og eventuelle opplysninger til kunden. Registreringen skjer i overensstemmelse med personopplysningslovens bestemmelser"* (AutoPASS 2007c). Punkt 9.2 spesifiserer videre at brikken kan brukes for anonym datainnsamling, uten at personopplysninger behandles. Kunden kan også henvende seg til bompengeselskapet for informasjon om behandlingen av opplysninger om seg selv. Opplysningene skal i henhold til punkt 9.3 kun benyttes for administrasjon av AutoPASS-tjenestene. Siste delpunkt under personvernpunktet omhandler sletting av passeringsopplysninger. Dette skal gjøres så raskt som mulig etter at faktura er betalt, og ved uenigheter om betalingsplikt skal opplysningene lagres inntil kravet er gjort opp eller rettslig avgjort. (Ibid.)

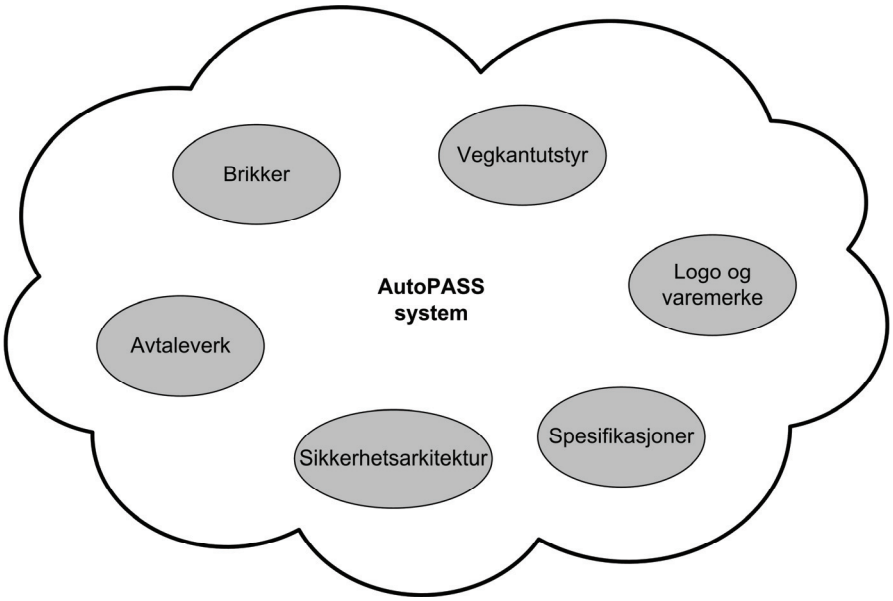
2.4 Beskrivelse av AutoPASS-teknologi

Teknologien som muliggjør AutoPASS kalles Radio Frequency IDentification (RFID), og faller inn under kategorien for automatiske identifiseringsteknologier. Automatisk identifisering er i mange tilfeller meget tidsbesparende, siden data ikke trenger å registreres manuelt. Samtidig gir det en høyere nøyaktighet for data som registreres (RFID Journal 2007a). Automatiske identifikasjonssystemer brukes for å gi informasjon om objekter i bevegelse, for eksempel biler. RFID er en generell betegnelse på identifisering av flyttbare objekter ved bruk av radiobølger. Teknologien anvendes i mange ulike sammenhenger, blant annet innen varehandel, adgangskontroll og betalingssystemer (Vermesan et al. 2005). AutoPASS er et eksempel på en anvendelse av RFID-teknologi for betaling av bompenger. For mer informasjon om RFID og virkemåte, se appendiks A.

2.4.1 System og spesifikasjoner

AutoPASS-systemet bygger på et sett av spesifikasjoner som sikrer både teknisk og funksjonell samordning mellom de ulike tjenestene som tilbys gjennom AutoPASS. Spesifikasjonene omfatter AutoPASS-brikker, vegkantutstyr, sentralsystemer, grensesnitt mellom systemelementer, sikkerhetsarkitektur, varemerker og avtaleverk (illustrert i figur 2.2). AutoPASS er en nasjonal standard for vegkantutstyr og brikker, og Statens Vegvesen er både eier og forvalter av system

og spesifikasjoner. Konseptet bak AutoPASS er hentet fra det europeiske forsknings- og utviklingsprosjektet CESARE II, og det er mulig at en samordning av bompengesystemer i Europa vil baseres på dette prosjektet (se kapittel 5.7.2). AutoPASS er dog en forenkling av modellen beskrevet i CESARE. (Foss 2005)



Figur 2.2 Komponenter og rammeverk i AutoPASS-systemet (basert på Foss 2005)

Sentrale standarder bak AutoPASS-spesifikasjonene omhandler Electronic Fee Collection (EFC) og Dedicated Short Range Communication (DSRC).

Electronic Fee Collection brukes som en samlebetegnelse for alle systemer designet for å samle inn avgifter fra brukere på en ikke-manuell måte, for kjøretøyrelaterte transporttjenester. Avgiften samles inn gjennom utveksling av data, eksempelvis via et luftgrensesnitt, og gjør det mulig for brukeren å betale for en tjeneste med elektroniske verdier lagret i en sentral konto. Ved bruk av EFC trenger dermed ikke brukeren å gjøre noe for å betale avgiften. EFC er relatert til applikasjoner som bompengeinnkreving, vegprising og parkering. Det finnes en rekke standarder om EFC innen vegtransport og trafikktelematikk (ISO 2003). Technical Committee 278 i det europeiske standardiseringsorganet CEN (CEN TC 278) er et eksempel på en mye brukt samling av standarder innen vegtransport og trafikktelematikk, som beskriver anvendelsen av Dedicated Short Range Communication (DSRC) for elektronisk betaling av bompenger (Furan 2007).

Dedicated Short Range Communication er en protokoll som tillater kommunikasjon i høy fart, på kort til medium avstand mellom kjøretøy og vegkant, eller mellom kjøretøy (IEEE 2007). DSRC er et subsett av RFID-teknologien, og benyttes i hovedsak som protokoll for elektronisk betaling av bompenger. AutoPASS er et av systemene som benytter seg av DSRC-protokollen, og AutoPASS ble godkjent av CEN TC 278 i januar 2003 (Skadsheim 2003).

3 Hensynet til personvern

I dette kapittelet forklares begrepet personvern, og hvorfor hensynet til personvern er aktuelt for denne oppgaven. Det finnes flere tilnærminger til personvernbegrepet, og kapittelet tar for seg ulike fokus på personvern og hvilke interesser som er utgangspunkt for interesseteorien innen personvern. Behandling av personopplysninger er regulert av både nasjonale og internasjonale bestemmelser, og vi skal se nærmere på disse. Helt til sist vil personvernet oppsummeres som noen konkrete prinsipper.

3.1 Personvern

Det registreres i stadig økende grad opplysninger og informasjon om enkeltpersoners bevegelser i samfunnet. Vi legger igjen elektroniske spor når vi ringer i mobiltelefonen, tar ut penger i minibanken, er på internettkafé og sender e-post, eller betaler for en bompassering med AutoPASS. På grunn av bruk av teknologi som dette, fokuseres det i økende grad på personvern i dag. Spesielt rettes det oppmerksomhet mot at registrering og innsamling av personlige opplysninger kan føre til misbruk av opplysningene og krenkelse av personlig integritet. Til tross for at teknologiutviklingen er med på å forenkle hverdagen, så forsterker økt behandling av personopplysninger sjansen for overvåkning. Ulempen med økt overvåkning er muligheten til å sammenlagt kunne avdekke og kartlegge en hel del om en persons bevegelser. Overvåking krenker den personlige integriteten ved at grensene mellom private og tilgjengelige opplysninger viskes ut. Bruk av teknologi som krever registrering og behandling av personopplysninger er med på å forsterke overvåkningen. Det blir også vanskeligere for enkeltpersoner å holde oversikten over hvilken informasjon som lagres om dem, og hvor denne informasjonen lagres til en hver tid (Teknologirådet 2007).

Begrepet personvern kan defineres på mange ulike måter. Personvern knyttes gjerne til *"enkeltindividers mulighet for privatliv, selvbestemmelse og selvutfoldelse"*, og et vesentlig element er *"at personer i utgangspunktet skal kunne bestemme hva andre skal få vite om hans eller hennes egne personlige forhold"* (FAD 2007). Dette bygger på tanken om at alle har rett til privatliv, og at man selv

kan bestemme hvilke opplysninger man ønsker å dele med omverdenen. Direktør i Datatilsynet, Georg Apenes (som sitert i Datatilsynet 2007a), peker på at personvernet i 2007 spenner over et stort område, fra normal folkeskikk om å respektere andres privatliv, til lovgivning om behandling av personopplysninger. Lover og regler skal være med på å sikre at personopplysninger behandles med respekt, og at tilgangen til opplysningene begrenses til formålstjenlig bruk. Schartum og Bygrave (2004:13) peker på at personvern i akademiske miljøer og Datatilsynet praksis gjerne defineres som *"vernet av den enkeltes interesse i å kunne kontrollere behandling av opplysninger om seg selv"*. Personvern sammenlignes dermed ofte med beskyttelsen av personlig integritet. Samtidig er ikke begrepet personlig integritet i seg selv en dekkende forklaring, og andre aspekter er derfor knyttet til hver enkelts mulighet til å bestemme over andres innsyn i personlige forhold, og muligheten til å bestemme hvordan andre kan tre inn i ens private liv (Ibid.:14).

Det finnes mange tilnærminger til personvernbegrepet, og Ravlum (TØI 2004a:7) peker på at én slik tilnærming kan gjøres gjennom tre ulike innfallsvinkler: Det integritetsfokuserte personvern, det maktfokuserte personvern og det beslutningsfokuserte personvern. Dette innebærer ikke en deling av personvernbegrepet i tre, men er heller et hjelpemiddel for å kunne se hvilke deler personvernbegrepet er satt sammen av. I en gitt situasjon trenger ikke bare et fokusområde å være gjeldende. Det finnes situasjoner hvor man kan fokusere på personvernet gjennom alle tre områdene.

Integritetfokusert personvern

Personlig integritet er et uttrykk for ønsket om å ha kontroll over opplysninger om seg selv, spesielt opplysninger som oppleves som personlige. Dette er utgangspunkt for det integritetsfokuserte personvernet, og bygger på retten til "privacy", hvor personopplysninger betraktes som privat eiendom. Fokuset strekker seg dog lengre enn at personopplysninger ikke skal utveksles uten samtykke, det tar også hensyn til den grunnleggende retten til å være i fred, uavhengig av om det innebærer deling av personopplysninger eller ikke. (TØI 2004a)

Digitalisering gjør at informasjon blir tilgjengelig via helt nye medier, og gjerne i større utspredning. Krenkelser av personlig integritet gjennom IKT, eksempelvis

gjennom publisering av bilder uten samtykke, aktualiserer spørsmålet om "personopplysningsvern". Schartum og Bygrave (2004:26) peker på at *"IKT forstørrer og forverrer virkningene av integritetskrenkelsen"*. Personvernet sier som nevnt at hver enkelt skal få bestemme hva andre skal få vite om hans eller hennes personlige forhold. I denne sammenheng er det i hovedsak snakk om vern av personopplysninger, og personvernet kan flyttes over i en ny dimensjon kalt "personopplysningsvern" (FAD 2007). Det er denne dimensjonen som i hovedsak er behandlet i lovverket, som vi kommer tilbake til.

Maktfokusert personvern

Retten til å beskytte seg mot maktmisbruk står sentralt i det maktfokuserte personvernet. Misbruk av personopplysninger kan medføre en forskyvning i maktbalansen mellom to ulike parter. Dette kan være maktbalansen mellom borger og stat eller arbeidstaker og arbeidsgiver, og et maktovertak kan gi maktholder en overlegen posisjon. Offentlige myndigheter kan eksempelvis benytte personopplysninger til å effektivisere utøvelsen av autoritet, og dermed styrke sin posisjon ovenfor borgerne (TØI 2004a, FAD 2007).

Beslutningsfokusert personvern

Personopplysninger benyttes ofte som beslutningsgrunnlag, eksempelvis ved søknad om lån i en bank eller ved en jobbsøknad, og det stilles derfor et krav til at opplysningene beslutningstaker har tilgang til er korrekte. For å sikre at behandlingen av personopplysninger gir riktige og rettferdige avgjørelser må det i følge Ravlum (TØI 2004a:8) stilles krav til behandlingen av personopplysningene. Her er det også viktig å se på forutsetningene om at opplysningene vil kunne benyttes som beslutningsgrunnlag en gang i fremtiden.

3.2 Personverninteresser

Personvern kan beskrives som *"et knippe ideelle interesser som tillegges enkeltmennesker"* (JD 1997:21). Dette er bakgrunnen for interessemodellen som beskriver personverninteresser. Interessemodellen kan brukes uavhengig av hvilket fokus på personvern som velges; integritets-, makt- eller beslutningsfokus. Vektleggingen av interessene kan variere avhengig av fokus. Interessemodellen danner grunnlaget for interesseteorien som vi skal se nærmere på. Det finnes også

interesser som ikke er relatert til personvern, og dette medfører at personverninteressene ofte må veies opp mot andre interesser. I enkelte tilfeller kan dette medføre interessekonflikter.

3.2.1 Interesseteori

Når man snakker om personverninteresser er det vanlig å skille mellom individuelle og kollektive interesser. Individuelle interesser handler om den enkeltes rett til å ha kontroll over opplysninger om seg selv, mens kollektive interesser beskriver interessene individer har sammen som gruppe i å ivareta kontroll over opplysninger om gruppen og dens medlemmer (JD 1997).

De individuelle interessene kan oppsummeres som fire områder: diskresjon, innsyn, fullstendighet og privatlivets fred. Diskresjon er en meget sentral interesse, og handler om muligheten til å kontrollere tilgang til og bruk av opplysninger samlet inn om seg selv. For å kunne kontrollere dette må den enkelte ha innsyn i hvilke opplysninger som registreres. Dette gir muligheten til å sikre at opplysningene er riktige og fullstendige. Fullstendighet bygger dermed på ønsket om at beslutninger på bakgrunn av personopplysninger skal tas på et korrekt og fullstendig grunnlag. Sist men ikke minst har man rett til å få være i fred, og verne om eget privatliv. Denne interessen er ikke knyttet til personopplysninger i like stor grad, men omhandler privatliv i en større sammenheng, uavhengig av om det er snakk om registrering av personopplysninger eller ikke. (TØI 2004a)

De kollektive interessene går ut på ønsket om en borgervennlig forvaltning, et robust samfunn og et begrenset overvåkningsnivå. En borgervennlig forvaltning kan uttrykkes ved ønsket om at forvaltningen skal fremstå som menneskelig og forståelig for borgerne. Automatisering er et problemområde som står sentralt i de kollektive interessene. Saksbehandlingen kan gjennom automatisering føles upersonlig dersom den gjøres av en datamaskin alene, og dette kan skape avstand mellom enkeltmenneskene og forvaltningen. Borgervennlighet handler i denne sammenheng om at borgerne bedre skal kunne forstå hva som ligger til grunn for saksbehandlingen, og at resultatet til en viss grad er beregnelig i forkant. Automatisering skaper også redsel for at samfunnet skal bli mer sårbart, og mindre robust. Den kollektive interessen om et robust samfunn bygger dermed på

ønsket om høy sikkerhet ved elektronisk informasjonsbehandling. Interessen om et begrenset overvåkningsnivå går ut på at samfunnet må vernes mot maktmisbruk og urimelig kontroll. Her kommer vi inn på problematikk rundt lagring av informasjon i store registre, og faren ved sammenkobling av slike registre for å skaffe flere opplysninger. Et register kan på egenhånd være harmløst, men slått sammen med et annet register vil det plutselig kunne gi store mengder informasjon, og havne i konflikt med personvernet. (JD 1997, TØI 2004a)

3.2.2 Interessekonflikt

I mange tilfeller kan personverninteresser komme i et motsetningsforhold til hverandre. Av de individuelle interessene er det spesielt ønsket om diskresjon som havner i konflikt med andre interesser. Grunnen til dette er at diskresjon medfører en avgrensing av informasjonstilgangen. Spesielt ønsket om fullstendighet utfordrer diskresjonsnivået. I saksbehandlinger vil dette bety at begrenset tilgang til opplysninger settes opp mot fullstendig innsikt i opplysninger. Dette medfører en konflikt mellom hensynet til diskresjon og hensynet til at all nødvendig informasjon er tilgjengelig. (JD 1997)

Schartum og Bygrave (2004:37) minner om at personverninteressene ikke er enerådende, og at en sentral del av personvernretten er å veie personverninteressene opp mot andre interesser. Som forbrukere har man gjerne andre interesser som ikke nødvendigvis omhandler personvern. Ved bruk av AutoPASS havner eksempelvis retten til anonym ferdsel og diskresjon i konflikt med ønsket om effektivitet. Bilister som benytter seg av AutoPASS har gjennom avtale samtykket til at personopplysninger kan behandles, og har valgt effektivitet foran anonymisering av sin ferdsel på norske veger. Den individuelle interessen om diskresjon utfordrer dermed interesser utover personvernet. Både forbrukerinteresser og kommersielle interesser kan havne i konflikt med personvernet. Personifisert markedsføring på bakgrunn av registrerte opplysninger er et eksempel på en anvendelse med kommersiell interesse som står i motsetning til personvernet. Ofte er det slik at personvernet blir taperen i avveininger mellom personverninteresser og andre interesser. Et resultat av den økte redselen for terror i verdenssamfunnet er eksempelvis at personvernet må vike for en økning i overvåknings- og kontrolltiltak (FAD 2006). Den kollektive

interessen om et begrenset overvåkningsnivå, samt den individuelle interessen om diskresjon utfordres gjennom slike tiltak. Samtidig ønsker man å kunne leve i et robust samfunn som beskytter mot farer som terror, og i denne sammenheng ønsker de kollektive interessene å opprettholde en viss grad av overvåkning og kontroll. Hensynet til samfunnet går i slike tilfeller foran hensynet til enkeltpersoner, og setter de kollektive interessene foran de individuelle. Alle mennesker er en del av samfunnet, og mange godtar dermed tiltak som dette. For å løse interessekonflikter, både mellom ulike personverninteresser og mellom personvern og andre interesser, må det gjøres balanserte avveininger (JD 1997).

3.3 Juridiske rammer

Registrering og behandling av personopplysninger er regulert både gjennom nasjonalt lovverk og internasjonale bestemmelser. I Norge er elektronisk behandling og innsamling av personopplysninger underlagt personopplysnings-loven som implementerer internasjonale personvernprinsipper hentet fra blant annet EUs personverndirektiv.

3.3.1 Nasjonale bestemmelser

Personopplysningsloven[1] er den norske loven om behandling av personopplysninger, og formålet med loven er *"å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger",* jf. § 1 (JD 2000). Samtidig skal loven bidra til at behandlingen av personopplysninger skjer i samsvar med grunnleggende personvernhensyn, og at *"behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger"* blir ivaretatt (Ibid.). Personopplysningsloven er en videreføring av personregisterloven av 1978. I personopplysningsloven reguleres behandlingen av opplysninger uavhengig av om opplysningene er organisert i registre, databaser eller på en annen måte (Schartum & Bygrave 2004:102). Lovens § 2 definerer ulike begreper som er nyttige for å kunne tolke lovens bestemmelser:

> "1) personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson,

[1] *Lov om behandling av personopplysninger (personopplysningsloven)*

2) behandling av personopplysninger: enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter,
3) personregister: registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen,
4) behandlingsansvarlig: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes,
5) databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige,
6) registrert: den som en personopplysning kan knyttes til,
7) samtykke: en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv,
8) sensitive personopplysninger: opplysninger om

a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning
b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling
c) helseforhold
d) seksuelle forhold
e) medlemskap i fagforeninger".

Loven gjelder for *"behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler",* og *"annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister"* (JD 2000). I AutoPASS registreres og behandles personopplysninger ved bruk av elektroniske hjelpemidler og systemet faller dermed inn under lovens gyldighetsområde.

Det stilles vilkår for behandlingen av personopplysninger i lovens § 8:

"Personopplysninger (jf. § 2 nr. 1) kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller behandlingen er nødvendig for a) å oppfylle en avtale med den registerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås, b) at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse, c) å vareta den registrertes vitale interesser, d) å utføre en oppgave av allmenn interesse, e) å utøve offentlig myndighet, eller f) at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan ivareta en berettiget

> interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen".

Loven stiller altså som utgangspunkt at den registrerte (jf. § 2 nr. 6) skal samtykke i behandlingen av personopplysningene, men det kan også foretas avveininger mot andre lovmessige eller samfunnsmessige hensyn. For AutoPASS må vilkåret om samtykke fra den registrerte etterkommes, og dette gjøres gjennom AutoPASS-avtalen. Behandling av personopplysninger er følgelig nødvendig for å oppfylle avtalen.

I tillegg til personopplysningsloven gjelder noen supplerende bestemmelser gitt i en egen forskrift. Denne forskriften refereres til som personopplysnings-forskriften[2], og inneholder utfyllende krav til informasjonssikkerhet ved behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler. Informasjonssikkerhet kan defineres som tiltak iverksatt for å sikre konfidensialitet, integritet og tilgjengelighet for informasjonen. Med konfidensialitet menes det at informasjon ikke skal være tilgjengelig uten autorisasjon. Begrepet integritet betyr at informasjon ikke skal kunne endres eller ødelegges av uautoriserte, mens tilgjengelighet innebærer at informasjonen er tilgjengelig for autoriserte som trenger den for å utføre pålagte oppgaver (Dataforeningen 2007). Kravene til informasjonssikkerhet spesifiseres i personopplysningsforskriftens kapittel 2, og er et supplement til § 13 i personopplysningsloven som sier at *"den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger"* (FAD 2000). AutoPASS er et informasjonssystem som må oppfylle kravene som stilles til informasjonssikkerhet i personopplysningsforskriften.

Forvaltningsorganer

Datatilsynet og Personvernnemnda er begge myndighetsutøvende organer opprettet i medhold av personopplysningsloven. Datatilsynet er opprettet for å kontrollere at personopplysningsloven følges, og er et uavhengig forvaltningsorgan som fungerer som både tilsyn og ombud for personvern i Norge. EUs

[2] *Forskrift om behandling av personopplysninger (personopplysningsforskriften)*

personverndirektiv (art. 28 nr. 1) stiller krav om at tilsynsmyndighetene må være uavhengige, og uavhengigheten realiseres ved at klager på vedtak gjort av Datatilsynet ikke behandles av Justisdepartementet, men av Personvernnemnda (Schartum & Bygrave 2004:172). Datatilsynets oppgaver går ut på å *"identifisere farer for personvernet og gi råd om hvordan de kan unngås eller begrenses"* (Datatilsynet 2007b). Samtidig skal Datatilsynet informere om både nasjonal og internasjonal utvikling i behandling av personopplysninger, og om problematikk rundt slik behandling. *Personvernrapporten 2007* (Datatilsynet 2007a) er eksempelvis en rapport som forteller om hvilke ulike personvernutfordringer dagens samfunn står ovenfor. Klager på vedtak gjort av Datatilsynet blir tatt opp i Personvernnemnda, opprettet for å behandle klagene i medhold av personopplysningslovens §43 (Personvernnemnda 2007). Personvernnemnda er også et uavhengig forvaltningsorgan, og både Datatilsynet og Personvernnemnda er underlagt Fornyings- og Administrasjonsdepartementet.

3.3.2 Internasjonale bestemmelser

Det norske regelverket for beskyttelse av personvern er underlagt flere internasjonale bestemmelser, og det kan ikke vedtas lover i Norge som avviker fra disse. Retten til privatliv er et viktig prinsipp som følger både av den europeiske menneskerettskonvensjonen (EMK), artikkel 8, og som står sentralt i EUs personverndirektiv (95/46 EF). Personverndirektivet handler mer konkret om *"beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av sådanne opplysninger"* (TØI 2004b). Alle de nordiske landene har underlagt seg EMK og implementert personverndirektivet i egne lovverk. Dette medfører at lovgivningen må tilfredsstille noen sentrale og grunnleggende personvernprinsipper, gjengitt i kapittel 3.4.

3.4 Personvernprinsipper

Internasjonale personvernprinsipper og den norske personopplysningsloven er med på å sette rammene for hvordan behandlingen av personopplysninger skal foregå. Datatilsynet har som oppgave å "vokte" over personverninteressene, og gi råd for hvordan personopplysningene bør behandles. Det er derfor interessant å se på hvilke retningslinjer Datatilsynet jobber ut fra for å sikre at personvernet

opprettholdes. *Personvernrapporten 2007* (Datatilsynet 2007a) oppsummerer Datatilsynets tolkninger av de juridiske rammene rundt personvern som en rekke viktige personvernprinsipper. Alle prinsippene bygger på den grunnleggende tanken om at *"den enkelte skal ha bestemmelsesrett over personopplysninger om seg selv"* (Ibid.:5). Personvernprinsippene er gjengitt i tabell 3.1.

Personvernprinsipp	*Beskrivelse*
Saklig begrunnelse	Saklig begrunnelse for behandling av personopplysninger. Opplysningene skal samles inn til uttrykkelige angitte og legitime formål og brukes i overensstemmelse med disse.
Frivillig samtykke	Registreringen av personopplysninger skal i størst mulig grad være basert på et frivillig, uttrykkelig og informert samtykke. Opplysninger i offentlige registre hvor registrering er pliktig, skal være lovhjemlet.
Opplysningsplikt for behandlingsansvarlig	Ved innhenting av personopplysninger har den enkelte uoppfordret rett til å vite om det er frivillig eller obligatorisk å oppgi personopplysningene, hvilket formål opplysningene skal brukes til, og om de vil ble utlevert til andre
Rett til innsyn	Den behandlingsansvarlige skal bistå den registrerte med å gi innsyn i hvilke opplysninger som er lagret, hva de skal brukes til og hvor de er hentet fra.
Registreringen skal være riktig	Opplysninger som registreres, skal være korrekte og ajourførte.
Feilaktige opplysninger skal rettes	Feilaktige personopplysninger skal endres, slettes eller sperres.
Unødvendige opplysninger skal slettes	Overskuddsinformasjon og opplysninger som ikke lengre er nødvendig for formålet med registreringer, skal slettes.
Informasjonssikkerhet skal ivaretas	Den behandlingsansvarlige skal sørge for tilfredsstillende informasjonssikkerhet. Det må kunne dokumenteres at rutiner og tiltak som sikrer personopplysninger, blir etterlevd i praksis. I det offentlige må risikovurderingene også omfatte borgernes ulike forutsetninger for å ivareta egen informasjonssikkerhet.
Strengere regler ved følsomme opplysninger	Behandling av følsomme personopplysninger er underlagt særlig strenge regler.
Retten til å være anonym	Borgeren har krav på å kunne ferdes anonymt. Når nye teknologiske løsninger tas i bruk, skal det legges til rette for at retten til anonym ferdsel fortsatt blir ivaretatt.
Rett til manuell vurdering	Den registrerte har rett til å få en manuell vurdering av avgjørelser som fullt ut er basert på automatisk behandling av personopplysninger, dersom avgjørelsen er av vesentlig betydning for vedkommende.

Tabell 3.1 Personvernprinsipper (Datatilsynet 2007a)

4 Dynamiske data

Oppgavetittelen forteller at oppgaven skal se på personvernhensyn ved innsamling av dynamiske data. I dette kapittelet vil jeg forklare hva som ligger i begrepet dynamiske data og hvorfor dette er aktuelt for AutoPASS. Videre er det interessant å se på hvilke ulike typer dynamiske data som finnes. For denne oppgaven er dynamiske trafikkdata mest relevante, og en beskrivelse av verdikjeden for trafikkdata med involverte parter er nyttig for å oppnå forståelse av hvordan innsamling av dynamiske data kan påvirke personvernet.

4.1 Databehandling

"Dynamiske trafikkdata karakteriseres ved at de oppdateres kontinuerlig. De beskriver for eksempel tilstanden på vegnettet eller de rådende trafikkforhold" (Wahl, Haugen & Lillestøl 2006). Det skilles ofte mellom statiske og dynamiske data, og i motsetning til dynamiske data så karakteriseres statiske data ved at de sjelden oppdateres. Ordet dynamisk beskriver bevegelse og forandring, mens ordet statisk viser til noe som er preget av uforanderlighet (Kunnskapsforlaget 2007). Ved passering av en bomstasjon samles det inn passeringsdata fra AutoPASS-brikkene. Formålet med innsamlingen er i hovedsak å samle inn de data som trengs for å gjennomføre en elektronisk betaling av bompasseringen. Samtidig kan summen av passeringer i samme tidsrom fortelle noe om rådende trafikkforhold. Forholdene vil være under kontinuerlig endring, som et resultat av at dataene som samles inn er dynamiske.

Behandling av personopplysninger representerer (jf. § 2 i personopplysningsloven) all bruk av personopplyninger, fra innsamling og lagring til bearbeiding og sammenkobling. Kapittel 2 i personopplysningsforskriften tar for seg informasjonssikkerhet med tanke på *"behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler der det for å hindre (...) tap av anseelse eller personlig integritet er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene"* (FAD 2000). For systemer som AutoPASS medfører dette at det må gjennomføres bestemte sikkerhetstiltak for å oppnå et tilfredsstillende sikkerhetsnivå for behandlingen av personopplysninger.

En jevnlig gjennomgang av informasjonssystemet er også nødvendig for å verifisere at sikkerhetstiltakene faktisk er etablert og fungerer som ønsket (jf. § 2-5).

4.1.1 Datainnsamling

Innsamling av data gjøres på bakgrunn av hvilke formål dataene er tiltenkt. For AutoPASS samles det inn data om passeringer av bomstasjoner. Dette innebærer data som tid, sted og hvilken AutoPASS-brikke som passerte. Passeringen forteller ikke noe om hvem som kjørte bilen brikken var plassert i. I tilfeller der det tas bilde av en passering, er det også kun registreringsnummeret som bli avbildet, ikke personer som befinner seg i bilen. Sensitive opplysninger samles ikke inn ved passering av en bomstasjon, i samsvar med reguleringer i personopplysningsloven. (Personvernnemnda 2005) Innsamling av passeringsdata benyttes som betalingsgrunnlag i AutoPASS betalingssystem. Samtidig kan det også samles inn trafikkdata, som kan benyttes til å eksempelvis gjennomføre reisetidsmåling på en vegstrekning. Ulike datafangster er dermed nyttige til ulike formål.

4.1.2 Ulike typer dynamiske data

Det finnes flere typer dynamiske data. Sett i henhold til vegtrafikk kan man avgrense begrepet til å omfatte klimadata, miljødata og trafikkdata. Klimadata er data om vær og føreforhold, mens miljødata er eksempelvis luftforurensning. Trafikkdata sier noe om trafikkavvikling, reisetid og kø eller forsinkelser. Dynamiske data som helhet forteller noe om situasjonen i det tidsrommet datainnsamlingen foretas, og kan kalles sanntidsdata. Fokus i denne oppgaven er i hovedsak på trafikkdata, men også klimadata og miljødata kan komme til å spille en større rolle for fremtidig bruk av AutoPASS. Behovet for innsamling av trafikkdata kan oppsummeres i tre punkter. Trafikkdata trengs for (1) statistikk og statistiske beskrivelser av trafikken på vegnettet, (2) sanntidsanvendelser for trafikkstyring, overvåkning og informasjonstjenester både internt og ovenfor publikum og (3) trafikkontroll (SV 2001:2). Innsamling av data i et målepunkt kan prinsipielt brukes for å dekke alle formålene, og en samordning av systemene som samler inn ulike typer trafikkdata kan være hensiktsmessig for et større datagrunnlag (Ibid.). En slik samordning kan derimot havne i konflikt med personvernet ved deling og sammenkobling av ulike datafangster, og må tas

hensyn til når datafangstene behandles. Behovet for dynamisk trafikkdata er knyttet til ønsket om effektivitet og sikkerhet i trafikken. Innsamling og analyse av trafikkdata kan hjelpe til med å nå disse målene. Dette forutsetter ikke nødvendigvis at dataene må knyttes til bestemte kjøretøy eller brikker, og datainnsamlingen bør i slike tilfeller være anonym i samsvar med personvernprinsippet om anonym ferdsel.

4.1.3 Dynamiske data og personvern

En del av personopplysningene som registreres ved inngåelse av AutoPASS-avtalen kan sees på som statiske data. Dette er opplysninger som navn, personnummer og adresse, som ikke oppdateres så ofte. I seg selv utfordrer denne registreringen personvernet, og sammen med registreringer om hvor AutoPASS-brikken har passert blir utfordringen enda større. Passeringsdata kan sees på som dynamiske data, og sammenlagt kan det med tilgang til alle registreringene knyttet til en avtale kartlegges mye om en persons bevegelser. Dynamiske data sammen med statiske data gjør kartleggingen enda mer komplett. I dag finnes det to logger for dynamiske data på selve AutoPASS-brikken. Den ene loggen er forbeholdt transaksjoner, det vil si passering av bomstasjon, og har plass til totalt 100 passeringer. Ved passering av bomstasjon kan det dermed hentes ut reisedata fra loggfilen. Dynamiske data som dette kan benyttes for fremstilling av anonymisert statistikk. Den andre loggen er forbeholdt anonyme reisetidsmålinger og har plass til 4 passeringer. Det er mulig å lese de dynamiske loggfilene uten å lese brikke-ID. På denne måten kan personvernet ivaretas. (Nyre 2007) Enkelte bruksområder krever likevel at de dynamiske dataene knyttes til brikken, og det er i slike tilfeller personvernet utfordres. Potensialet for å bruke dynamiske data til andre formål enn det de er samlet inn for er til stede. Sammenkobling av datafangster fra flere ulike transporttjenester kan dermed bidra til økt overvåkning. Gjennom avtaler som samordner alle dynamiske bevegelser i transportsektoren og som tilbyr én faktura for alle tjenestene benyttet, vil hensynet til personvern utfordres ytterligere.

Informasjonssikkerhet

Det stilles som nevnt krav til tilfredsstillende informasjonssikkerhet ved behandlingen av personopplysninger. Personopplysningsforskriften (FAD 2000)

spesifiserer at klare ansvars- og myndighetsforhold for bruken av informasjonssystemet som behandler opplysningene må etableres. Dette innebærer en konfigurering av systemet for å tilfredsstille kravene til informasjonssikkerhet (§ 2-7). Med konfigurasjon menes selve utformingen av informasjonssystemet, inkludert sammenkobling av ulike systemelementer. Tilfredsstillende informasjonssikkerhet betyr at systemet skal sikres mot uautorisert adgang, og at autorisert personell hos behandlingsansvarlige kun kan benytte systemet for å utføre pålagte oppgaver. Personell må også pålegges taushetsplikt i tilfeller hvor konfidensialitet er nødvendig. I § 2-11 spesifiseres det at *"personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig"* (FAD 2000). Samordning av systemer kan medføre slike overføringer mellom involverte aktører. Sikkerhetstiltak skal sikre at det ikke forekommer uautorisert tilgang til eller bruk av informasjonssystemet for å skaffe personopplysninger.

4.2 Verdikjede for trafikkdata

På veien fra innsamling til bruk vil datafangsten bevege seg gjennom flere trinn, og det er i sammenheng med trafikkdata interessant å se nærmere på denne prosessen. Informasjonsverdikjeden er utgangspunktet for en mer detaljert verdikjede som inkluderer verdiøkning og aktører. Før informasjonsverdikjeden introduseres er det nyttig å se på hva som ligger i begrepet brukere av trafikkdata.

4.2.1 Brukere av trafikkdata

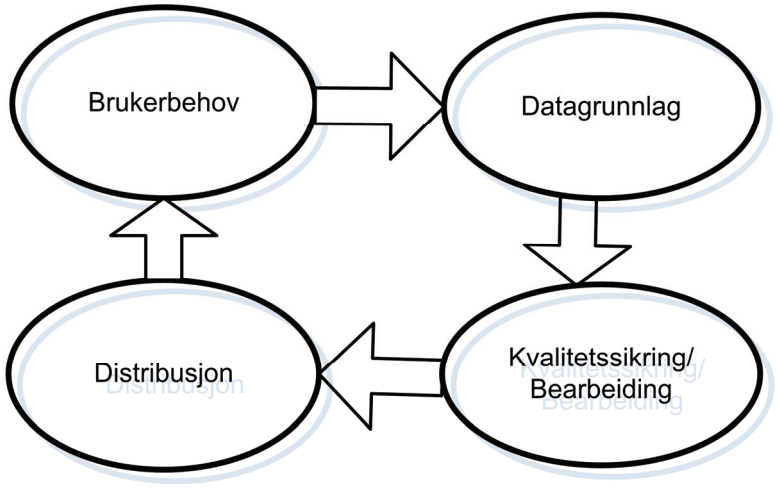
I følge Wahl og Skjetne (2005:3) kan man dele brukere av trafikkdata inn i fem kategorier:

- De individuelle trafikantene
- Vegholder
- Transportører
- Kollektivselskaper
- Næringslivet

Individuelle trafikanter bruker trafikkdata til optimalisere egen reiserute i vegnettet. Vegholder er ansvarlig for drift og vedlikehold av vegen, og bruker trafikkdata til å administrere disse oppgavene. Trafikkovervåkning, trafikkteknisk drift og trafikkstyring er alle oppgaver som krever tilgang på trafikkdata. Transportørene bruker trafikkdata for en optimalisering av egen virksomhet, og kollektivselskapene er på samme måte som transportørene avhengig av trafikkdata for å optimalisere transporten av passasjerer. Siste kategori av trafikkdatabrukere er næringslivet, som er avhengige av god logistikk for å oppnå effektivitet. Planlegging av transport er en viktig del av konkurransedyktigheten til en bedrift, og trafikkdata trengs for å optimalisere planleggingen. (Ibid.)

4.2.2 Informasjonsverdikjeden

For at dynamisk trafikkinformasjon skal være nyttig for en bruker må den etter innsamling både bearbeides og relateres til interessegrad og behov for brukeren. Det hele kan ses på som en prosess som beveger seg fra innsamling av data til selve anvendelsen av den. Resultatet er en informasjonsverdikjede satt sammen av 4 trinn: Datagrunnlag, kvalitetssikring og bearbeiding, distribusjon og brukerbehov.



Figur 4.1 Hovedelementer i informasjonsverdikjeden (Basert på Wahl et al. 2006)

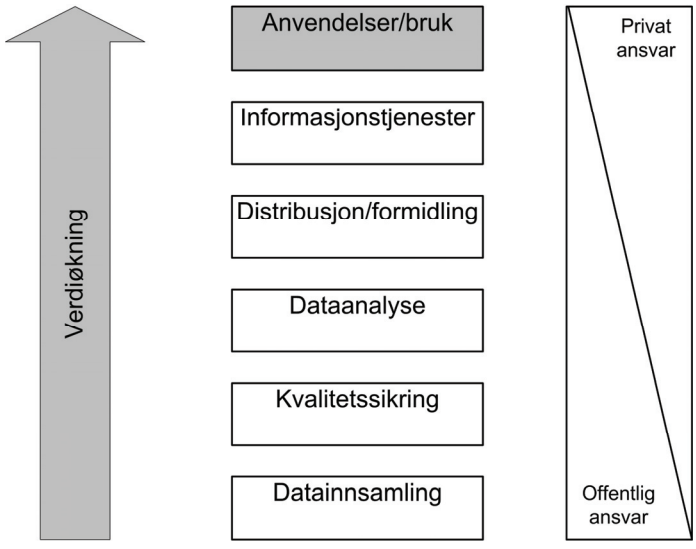
Figur 4.1 viser hvordan verdikjeden beveger seg fra datagrunnlaget, som er basis for kjeden, videre til kvalitetssikring og bearbeidelse av datagrunnlaget for å skape informasjon av verdi for brukerne. Herfra distribueres informasjonen til brukere, og siste ledd omhandler følgelig brukernes behov, som både tilsvarer enden og utgangspunktet for verdikjeden. Brukerbehovene bestemmer hvilke data som skal

samles inn, og verdikjeden er derfor illustrert som en sirkel uten endelig start og stopp. (Wahl et al. 2006)

Informasjonsverdikjeden kan brukes for å se på ulike tilfeller der det samles inn dynamiske data for å dekke brukernes behov for informasjon. Sammenligner vi verdikjeden med betaling av bompenger med AutoPASS, vil datagrunnlaget kunne sees på som de data som samles inn ved passering av bomstasjon. Passeringsdata vil videre kvalitetssikres og bearbeides for å kunne skape informasjon for brukeren, som i dette tilfellet er bompengeselskapet som ønsker betaling fra AutoPASS-abonnenten. Ferdig bearbeidet informasjon om passeringen distribueres deretter til betalingssystemet som kan gjennomføre betalingstransaksjonen for abonnenten og bompengeselskapet. Brukerbehovet representerer her bompengeselskapets behov for tilstrekkelig passeringsdata, for å elektronisk kunne ta betalt for en bompassering.

4.2.3 Verdiøkning langs verdikjeden

En mer detaljert verdikjede er vist i figur 4.2, og illustrerer hvordan verdien på data øker jo lengre opp i verdikjeden man kommer.



Figur 4.2 Verdikjede for informasjon (Basert på Wahl et al. 2003)

Etter innsamling systematiseres og kvalitetssikres dataene, før de analyseres for å skape informasjon. Denne informasjonen distribueres til ulike brukergrupper, som

benytter informasjonen som grunnlag i sine informasjonstjenester. Helt til slutt benyttes informasjonen til å ta beslutninger eller fatte tiltak. Ansvaret for innsamlingen av data ligger hos Statens Vegvesen, mens mot toppen av verdikjeden har private aktører i større grad kommet inn på markedet. Dette er illustrert til høyre i figur 4.2, hvor det private ansvaret øker jo lengre opp i verdikjeden man beveger seg. Spørsmål om organisering og eierskap av trafikkdata aktualiseres ved inkludering av private aktører. (Wahl & Skjetne 2005) I samsvar med avgrensningene for oppgaven presentert i kapittel 1.3 vil ikke oppgaven si noe konkret om hvordan dette spørsmålet skal besvares. (For mer informasjon om mulige løsninger se Wahl & Skjetne 2005)

For AutoPASS er det i hovedsak de tre første trinnene i verdikjeden som er gjeldene i dag. Når man beveger seg videre oppover i verdikjeden, til distribusjon, informasjonstjenester og bruk, involveres andre aktører enn Statens Vegvesen og bompengeselskapene. Flere tjenester involverer flere aktører, og da gjerne private aktører. For personvernet betyr dette at informasjon vil deles mellom flere parter. Personopplysningsforskriften stiller sikkerhetskrav til alle trinnene i verdikjeden, da alle trinnene representerer en form for behandling av opplysninger. Elektronisk overføring av personopplysninger skal kun overføres fra behandlingsansvarlig til aktører som tilfredsstiller kravene til informasjonssikkerhet i personopplysningsforskriften (§ 2-15, FAD 2000).

Organisatorisk sett kan man dele inn verdikjeden i ulike roller; sensoreier, datainnsamler, dataeier, datadistributør, kvalitetsansvarlig og tjenesteleverandør. Sensoreier er aktøren som eier utstyret som benyttes til registrering av data. Dersom registreringen innebærer personopplysninger må sensoreier sørge for at utstyret er sikret mot uautorisert adgang. Datainnsamler har ansvaret for den praktiske innsamlingen og lagringen av data. Innsamling av personopplysninger er regulert av personopplysningsloven, og lagringen må oppfylle kravene om konfidensialitet, integritet og tilgjengelighet. Dataeier er eier av innsamlet data, mens datadistributør videreformidler data til brukere. Kvalitetskontroll av data er avhengig av bruksområde, og er ansvaret til kvalitetsansvarlig. Siste rolle er tjenesteleverandørene, som formidler informasjonen til brukerne, eksempelvis trafikkmeldinger i NRK og P4.

5 AutoPASS i dag

I dag benyttes AutoPASS i hovedsak for betaling av bompenger, og i dette kapittelet skal vi se nærmere på hvordan dette foregår. Med referanse til kapittel 2.2 faller AutoPASS i denne sammenheng inn under anvendelsesområdet betalingssystemer, og teknologien er prøvd ut som betalingsmiddel på ferger og for parkering. AutoPASS benyttes i tillegg til reisetidsmålinger, og denne anvendelsen kan enten representere området overvåkning og kontroll eller trafikantinformasjon, avhengig av hva målingene benyttes til. I dette kapittelet skal vi se hvordan tjenestene er tenkt realisert, og diskutere fortløpende hvilke utfordringer de skaper for personvernet. Med mål om å utvide AutoPASS til å inkludere kollektivtransport er et AutoPASS-kort under utvikling. I kapittel 5.3 presenterer jeg AutoPASS-kortet som et trinn på veien mot en samordning av elektronisk billettering i Norge. Det skjer også mye med tanke på internasjonal samordning av bompengesystemer, og kapittelet ser til slutt på utviklingstrekk i Norden og Europa.

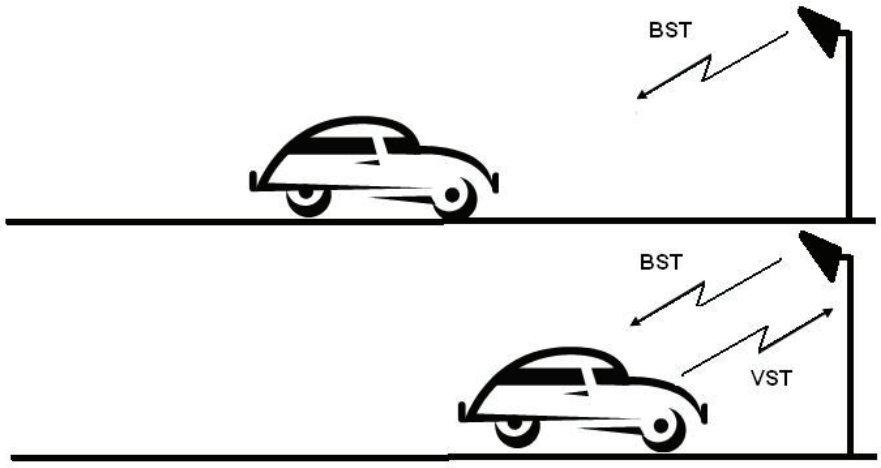
5.1 Betaling av bompenger

AutoPASS benyttes i alle anlegg med elektronisk innkreving av bompenger i Norge, og AutoPASS er dermed i omfattende bruk i de største bompengeanleggene. De anleggene som ikke benytter AutoPASS i dag er gjerne så små at det ikke er lønnsomt med elektronisk innkreving, og behovet er derfor ikke tilstrekkelig til å innføre AutoPASS. (Furan 2007)

5.1.1 Virkemåte AutoPASS

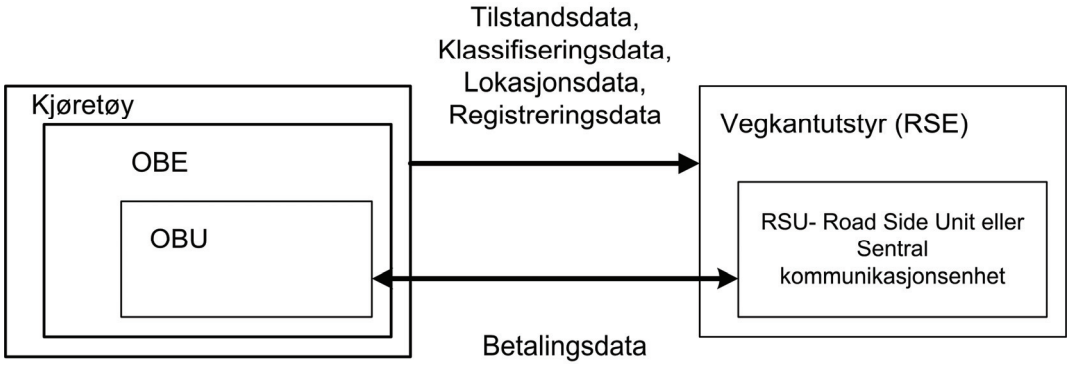
I henhold til internasjonale standarder for Electronic Fee Collection kalles utstyret som befinner seg i kjøretøyet for On board Equipment (OBE). Vegkantutstyr kalles tilsvarende for Road Side Equipment (RSE). Utveksling av data mellom RSE og OBE for å gjennomføre en elektronisk betaling kalles en transaksjon. Transaksjonsmodellen for elektronisk bompengebetaling (EFC) ved bruk av Dedicated Short Range Communication består av to faser; initialiseringsfasen og transaksjonsfasen. Formålet med initialiseringsfasen er å sette opp

kommunikasjon mellom RSE og OBE-er som har beveget seg inn i en DSRC-sone. I denne fasen gjennomføres en utveksling av Beacon Service Table (BST) og Vehicle Service Table (VST) (se figur 5.1). For å kunne gå over i transaksjonsfasen må initialiseringsfasen fullføres, og i transaksjonsfasen gjennomføres selve betalingen. (ISO 2004a)



Figur 5.1 Initialiseringsfasen (basert på ISO 2004a)

Enheten som kommuniserer med vegkantutstyret kalles On Board Unit (OBU) og er en del av OBE. Kommunikasjonen mellom kjøretøy og vegkantutstyr kan illustreres som i figur 5.2. For å kunne gjennomføre en betalingstransaksjon utveksles det betalingsdata mellom OBU'en og vegkantenheten (RSU'en) eller den sentrale kommunikasjonsenheten. Denne kommunikasjonen foregår i samsvar med DSRC-standarden. Vegkantutstyret kan også samle inn data fra kjøretøyet, som eksempelvis registreringsnummer (ved bruk av video). (ISO 2003)



Figur 5.2 Grensesnitt mellom kjøretøy og vegkantutstyr (basert på ISO 2003)

AutoPASS følger denne transaksjonsmodellen. OBU er AutoPASS-brikken, og RSE er vegkantutstyret som består av en leser (RSU). I alle AutoPASS-anlegg finnes det vegkantutstyr som registrerer biler som passerer med AutoPASS-brikker, og ved en vanlig bompassering forekommer følgende handlingsforløp:

1. Leseren i bomstasjonen sender kontinuerlig ut en BST, som inneholder informasjon om hvilken bomstasjon som passeres, og hvilke brikker som aksepteres som betalingsmiddel her.
2. Dersom en brikke mottar en BST den kan kommunisere med, svarer den med en VST, som forteller hvilken type brikke det er og hvilken applikasjon som benyttes.
3. Leseren i bomstasjonen spør etter mer informasjon fra brikken gjennom en GET_SECURE.request. (Dette er informasjon som brikke ID, transaksjonsteller, status osv.)
4. Brikken svarer med å sende en GET_SECURE.response sammen med en kryptigrafisk sjekksum over de data som sendes, samtidig som den teller opp transaksjonstelleren.
5. Leseren verifiserer at mottatte data er korrekte ved bruk av den kryptografiske sjekksummen.
    a. Dersom alt er i orden gis det grønt lys for passering og dataene sendes videre til baksystemet. Passeringen, med tid og sted, skrives til brikken.
    b. Dersom data fra brikken ikke kan verifiseres gis det rødt lys for passering, og det tas bilde av kjøretøyet, som sammen med dataene sendes til baksystemet.

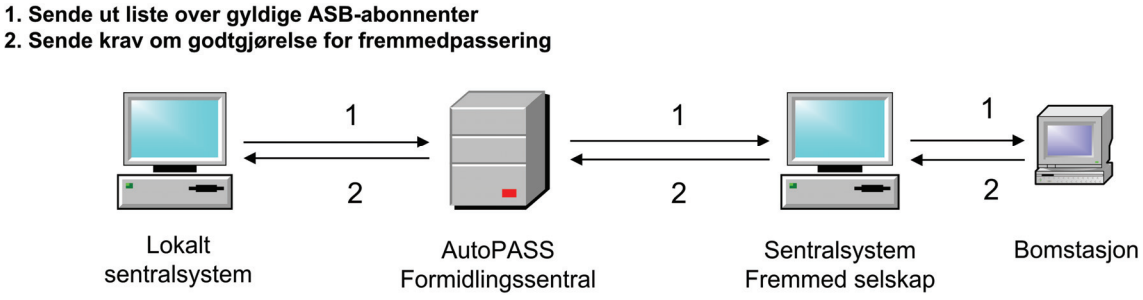
Trinn 1 og 2 i handlingsforløpet representerer initialiseringsfasen, og denne må gjennomføres før transaksjonsfasen kan starte. I trinn 3 til 5 gjennomføres selve transaksjonen for bompengebetalingen. Dette er et handlingsforløp som benyttes når det er penger involvert i transaksjonen, eller når det av annen grunn må være helt sikkert at det er riktig brikke det kommuniseres med (korrekt brikke-ID). Det er også mulig å hente ut data fra brikken uten å benytte kryptering, men da gis det ingen garanti på at brikke-ID er korrekt. (Nyre 2007)

5.1.2 AutoPASS Samordnet Betaling (ASB)

"Formålet med ASB er at trafikanten gjennom kontrakt med ett bompengeselskap skal kunne benytte sin AutoPASS brikke til betaling i andre bompengeanlegg og fergestrekninger – uten å gjøre noen ny avtale med et annet selskap" (AutoPASS 2003). For å nå målsetningen om et felles betalingssystem for alle vegtjenester i Norge, ble AutoPASS Samordnet Betaling (ASB) innført i 2004. ASB representerer en samordning av bompengebetalingen i Norge. Resultatet av ASB er at kunden kan benytte sin AutoPASS-brikke som betalingsmiddel når han passerer en bomstasjon, uavhengig av om det er dette bompengeselskapet brikkeavtalen tilhører. ASB tilbys av alle bomstasjoner som tilbyr betaling med AutoPASS. (Ibid.)

Dataflyt for ASB

For å benytte seg av ASB må kunden angi dette i sin AutoPASS-avtale. Hver dag lager sentralsystemene til bompengeselskapene oppdaterte lister over egne abonnenter som ønsker å benytte seg av ASB. Denne listen sendes videre til en felles AutoPASS formidlingssentral, opprettet for å håndtere dataflyten mellom de ulike bompengeselskapene. Formidlingssentralen sender kontinuerlig ut en sammenslått og oppdatert liste over alle ASB-abonnentene til alle bompengeselskapene. Figur 5.3 viser dataflyten ved distribuering av liste over gyldige ASB-abonnenter, og ved utsendelse av betalingskrav for "fremmedpasseringer".



Figur 5.3 Kommunikasjon ASB (basert på AutoPASS 2003)

Hver ASB-brikke opererer med to nøkkelringer, en *home key* for passering av bomstasjoner under bompengeselskapet de tilhører, og en *foreign key* for passering av andre bomstasjoner. For passering av fremmede bompengeselskap benyttes *foreign key*, og det leses av hvor brikken kommer fra, både land og hvor i landet.

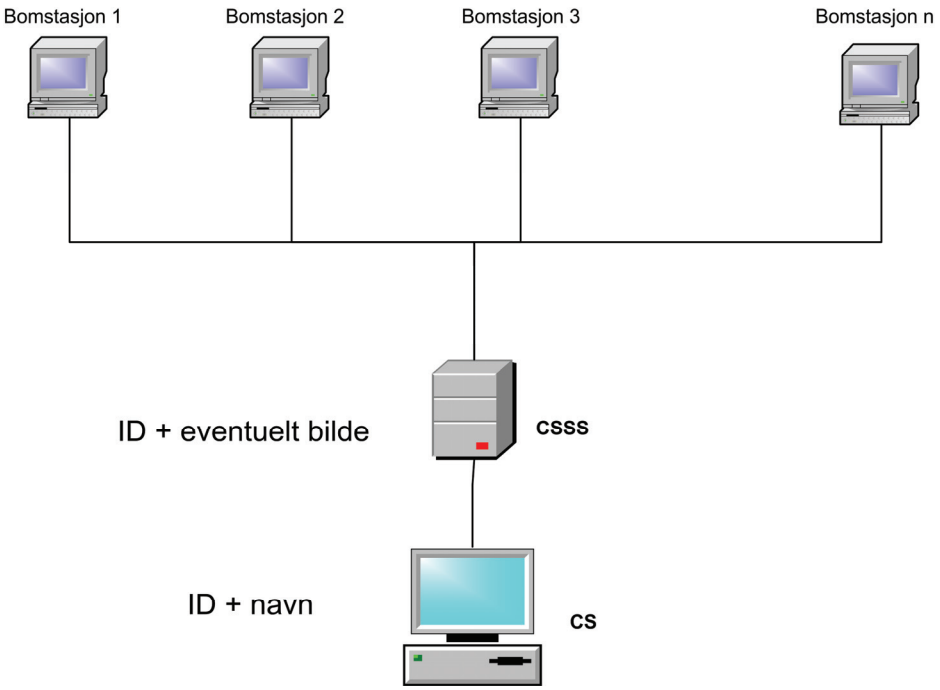
Det vil si at en brikke utstedt i Oslo vil ha en tallkode sammensatt av både tallverdi for Norge og Oslo, samt et serienummer. Dette utgjør til sammen brikke-ID. Ved passering av en bomstasjon under et annet selskap enn det brikken tilhører, sjekkes abonnenten opp mot listen over godkjente ASB-abonnenter. Alle godkjente fremmedpasseringer lagres lokalt i sentralsystemet til bompengeselskapet før de sendes til formidlingssentralen. Herfra videreformidles informasjon om hvilke fremmedpasseringer abonnenter fra de ulike selskapene har gjort. Bompengeselskapene må følgelig betale for "sine" fremmedpasseringer til de bompengeselskapene som har stilt betalingskravene, samt kreve betaling fra abonnentene som har gjort passeringene. Ved fremmedpasseringer vil ikke personinformasjon behandles av det fremmede bompengeselskapet, og ulovlige passeringer vil bli tatt bilde av. Ulovlige passeringer kan være passeringer gjort av brikker som ikke er tilknyttet ASB. (Furan 2007)

ASB gjør det mulig for brukeren å kjøre gjennom alle AutoPASS-anlegg med samme avtale. I henhold til personvern gjør ASB det mulig å kartlegge alle bevegelsene som gjøres av brikken rundt om i AutoPASS-anleggene. Til tross for denne kartleggingen velger mange å ta i bruk ASB. Brukeren får én faktura med alle sine passeringer, og dette for mange meget praktisk. Fakturaen utstedes av bompengeselskapet brikken tilhører, og tilgang til alle passeringsopplysninger er mulig derfra.

Databehandling i bompengeselskapene

Et bompengeselskap kan ha flere tilhørende bomstasjoner. Alle bomstasjoner underlagt et bompengeselskap er tilknyttet et felles sentralsystem (CS) for selskapet. En illustrasjon av databehandlingen ved bompasseringer vist i figur 5.4. Bomstasjonene 1 til n er underlagt samme konsesjon og bompengeselskap, og er koblet sammen med en sikkerhetsserver, Central System Security Server (CSSS), gjennom et Virtuelt Privat Nettverk (VPN). Forbindelsen mellom bomstasjon og CSSS er dermed kryptert. Når en brikke passerer bomstasjon n, sender stasjon n inn brikke-ID og eventuelt bilde til CSSS. Denne sender så videre samme informasjonen til sentralsystemet, og først her kobles ID med navn. Kommunikasjon mellom sentralsystemet og CSSS går via et vanlig lokalnettverk, men siden både CSSS og sentralsystemet står i en sikret sone er de beskyttet mot ikke-autorisert tilgang. Med tanke på personvern er ikke tilgang på

personopplysninger knyttet til en kunde mulig før informasjonen er sendt til sentralsystemet. Dette betyr at ved passeringer, både fremmede og lokale, vil ikke bomstasjonene vite noe om hvem som passerer, annet enn brikke-ID. (Furan 2007) Databehandlingen fra sentralsystemet forgår som beskrevet ovenfor som dataflyten i ASB.



Figur 5.4 Databehandling i bompengeselskapene (basert på Furan 2007)

5.2 Bomstasjoner

Det finnes flere ulike typer bomstasjoner i Norge, og skillet mellom dem avhenger av graden av automatisering. De tre typene bomstasjonene som finnes er:

- Betjente bomstasjoner
- Ubetjente bomstasjoner med automater
- Automatiske bomstasjoner

Betjente bomstasjoner er som navnet tilsier betjent av personell. Det vil si at betalingen av bompenger skjer manuelt, og det er ikke mulig å benytte AutoPASS-brikken for betaling. Ubetjente bomstasjoner med automater gir muligheten til

passering både med og uten AutoPASS-brikke. Kjøretøy uten brikke kan betale kontant for passeringen i automater. Automatiske bomstasjoner, tidligere kalt helautomatiske, opererer helt uten betjening eller automat. Kjøretøy med brikke passerer og betaler på vanlig måte, mens kjøretøy uten brikke blir tatt bilde av ved passering. I slike tilfeller kan fører betale kontant for passeringen på nærmeste bensinstasjon som tar i mot betaling for bompasseringer. Dersom fører ikke betaler for passeringen kontant innen tre dager sendes faktura i posten til den personen kjøretøyet er registrert på. (Wærsted 2007)

5.2.1 Påvirkning av personvernet

Lagring av passeringer

Det spesifiseres i punkt 9.4 i den generelle AutoPASS avtalen at *"opplysninger om hver enkelt passering skal slettes så raskt som mulig etter at fakturaen er betalt. Ved tvist om betalingsplikten oppbevares opplysningene inntil kravet er gjort opp eller rettslig avgjort"* (AutoPASS 2007c). Lokalt i bomstasjonene lagres det en reservekopi av alle passeringer. Her ligger opplysningene ustrukturert, og er ikke tilgjengelig for andre enn teknikere, som bruker opplysningene i forbindelse med feilsøking. Passeringene overføres også til sentralsystemet for bompengeselskapet, og her skjer avregning av passeringene normalt innen en time. Lagringstiden er avhengig av hvilken type avtale brikken har; om den forutsetter etterbetaling av passeringen, eller om den har klippekort, månedskort eller årskort. Ved forhåndsbetaling, som med klippekort og periodeabonnement, skal det ikke utstedes noen faktura, og opplysningene trenger ikke å lagres i systemet. Passeringsinformasjonen lagres alltid en måned lengre enn de trengs for regnskapsformål og lignende. Dersom en ugyldig brikke passerer en bomstasjon, blir det tatt bilde av bilens registreringsnummer. Dette bildet brukes ikke til å gi informasjon om fører eller passasjerer, men sendes til sentralsystemet for optisk avlesning av registreringsnummer. Denne avlesningen gjøres innen fem dager etter passeringen. Dersom brikken har en gyldig avtale skjer avregningen som normalt etter avlesingen, men dersom brikken ikke har en gyldig avtale vil det sendes et krav til bileieren. Før kravet sendes ut vil passeringen ligge "på vent" i fem dager, slik at bilisten har mulighet til å betale for passeringen på eksempelvis en bensinstasjon. I dette tilfellet slettes opplysningene en måned etter betalingen

er gjort. Ved fremmedpasseringer vil lagringstiden være noe lengre enn beskrevet ovenfor. (Personvernnemnda 2005) Lagringstiden av opplysningene tar dermed til etterretning prinsippet om at unødvendige opplysninger, som ikke lengre er nødvendige for formålet med registreringen, skal slettes.

Grunnen til at lagringstid er viktig kan knyttes opp mot muligheten for gjenbruk av informasjon i ettertid. Gjennom maktfokuset på personvern er det en fare for at denne informasjonen kan benyttes eksempelvis av politiet i etterforskning av en sak eller av skattemyndigheter for å avsløre svindel. Maktbalansen mellom myndighetene og bilisten vil forskyves dersom myndighetene har mulighet til å benytte passeringsopplysninger fra AutoPASS som bevismateriale uten at bilisten har samtykket til en slik behandling. Et eksempel på en aktuell nyhetssak er at Skatteetaten har fått tilgang til passeringsdata fra bompengeselskaper (SV 2007b). Skattemyndighetene ønsker tilgang til disse opplysningene for å kunne kontrollere at de samsvarer med det som er oppgitt i selvangivelsen. Dette betyr at personopplysningene blir benyttet som beslutningsgrunnlag for avgjørelser gjort av skattemyndighetene. Dette er klart en utfordring for personvernet, og Datatilsynet mener at det kreves lovgrunnlag for å hente ut slik informasjon (Engesvik 2007, 27. februar). Med lovgrunnlag mener Datatilsynet at de må ha rettslig kjennelse for å få tilgang til slike opplysninger. I slike tilfeller må det gjøres avveininger mellom bilistenes personverninteresser og samfunnets interesse i å oppklare lovstridige forhold.

Passering av automatiske bomstasjoner uten AutoPASS-brikke

Kostnader for fakturering av enkeltpasseringer er ofte like høy eller høyere enn selve passeringssummen, og det er opp til det enkelte bompengeselskap å vurdere om summen skal innkreves. Spesielt gjelder dette passering av turister, som ofte ikke har kompatibel brikke. Til innkreving av avgifter fra utenlandske kjøretøy benyttes et engelsk firma kalt EPC (Electronic Parking Consulting), som har spesialisert seg på innkreving av parkerings- og bompengeavgifter. Innad i Norge blir faktura tilsendt en gang i måneden, avhengig av antall passeringer. Det sendes i lengste tilfelle faktura etter tre måneder, hvor alle passeringer av én bomstasjon i tidsrommet er summert. (Wærsted 2007) En sammenfatning og totalfakturering av alle passeringer av bomstasjoner gjort av et kjøretøy vil kunne oppfattes som overvåkning, og vekker spørsmål rundt personvern. Dette er spesielt

aktuelt ved fakturering gjennom EPC av passeringer gjort av turister, dersom disse vil sammenfattes på en felles faktura. Sammenlagt vil alle passeringene av bomstasjoner i landet kunne kartlegge hvordan kjøretøyet har beveget seg rundt på norske veger.

Anonymt alternativ

Retten til anonym ferdsel er et sentralt personvernprinsipp, og Datatilsynet ønsker følgelig at det skal finnes et anonymt alternativ for passering av alle typer bomstasjoner. Ved kontant betaling i betjente bomstasjoner og ved myntinnkast i automater, opprettholdes muligheten til å passere anonym. Problemene oppstår ved passering av automatiske bomstasjoner. Muligheten for å betale for en bompassering på en bensinstasjon i etterkant av en passering er i realiteten ikke et anonymt alternativ. Det tas bilde av bilen som passerer, og dersom betaling av passeringen ikke er gjort på en bensinstasjon etter tre dager, utstedes det en regning med opplysninger om passeringer, kjøretøy og skyldig beløp. Det er dermed mulig i etterkant av passeringen, å identifisere en bilist uten at vedkommende har samtykket om det (Personvernnemnda 2005).

Ved spørsmål om opprettelse av automatiske bomstasjoner ble det stilt et krav fra Datatilsynet om at det må finnes et reelt anonymt alternativ for de som ønsker å ferdes sporfritt på norske veger. Samtidig ønsket Datatilsynet at det skulle pålegges konsesjonsplikt for behandlingsansvarlige for de automatiske bomstasjonene. Dette var ikke Statens Vegvesen enig i, og klaget inn vedtaket fra Datatilsynet til Personvernnemnda (se Personvernnemnda 2005). Resultatet av tvisten ble et pålegg om at det skal tilbys et "sporfritt" alternativ, og at det må gis konsesjon til behandlingsansvarlige i de automatiske bomstasjonene. I konsesjonen pålegges behandlingsansvarlig å sikre at *"(1) lengste lagring av reservekopi i bomstasjon ikke overstiger 72 timer, (2) behandling i sentralsystemet fører til sletting av opplysninger innen en time i normaltilfelle og (3) innen 24 timer for fremmedpasseringer, samt at tilgangen til data baseres på tjenstlige behov"* (Personvernnemnda 2005). Det "sporfrie" alternativet innebærer dermed at passeringsopplysningene slettes nokså umiddelbart etter passering av bomstasjon. Ellers foregår behandlingen i utgangspunktet som for en vanlig avtale. Alle bompengeselskapene tilbyr et "sporfritt" alternativ, en såkalt alternativ AutoPASS-avtale, for trafikkanter som ønsker å ferdes så sporfritt som mulig

(Wærstedt 2007). Dersom den alternative brikken av en eller annen grunn ikke blir lest av riktig vil det tas bilde at kjøretøyet. Et helt anonymt alternativ for passering av automatiske bomstasjoner finnes foreløpig ikke. Fordelen med den alternative avtalen er at brukeren inkluderes i rabattordninger tilknyttet bruk av AutoPASS, noe som ikke er mulig med andre "anonyme" løsninger som kontantbetaling, og betaling i bensinstasjon etter passering.

Interessekonflikt ved alternativ avtale

Alle passeringer gjort av den alternative brikken slettes senest etter 72 timer fra registrene i bomstasjonen, og med dette fraskriver kunden seg muligheten til å kunne motta og kontrollere regning for passeringene (Jonassen 2006, 15. april). Hensynet til personvern blir dermed stilt opp mot forbrukerhensynet. Valget av en alternativ avtale vil svekke forbrukerrettighetene til abonnenten, mens valget av en "vanlig" avtale medfører registrering av passeringer og da avkall på enkelte personverninteresser. Selv om brikken er sporfri, og registreringer i bomstasjonene slettes etter 72 timer, så lagres de 100 siste passeringene likevel på brikken. Dette vil kunne endres i fremtiden, da lagring av informasjon på brikken ikke er umulig å fremdrive, og gjør brikken mindre sporfri. Per i dag gjøres denne lagringen av passeringer som en kvittering for kunden, dersom det skulle oppstå uenigheter rundt om en passering er riktig registret eller ikke.

Én brikke per kjøretøy

Prinsippet bak AutoPASS er at én brikke kun skal benyttes av ett kjøretøy. I den generelle AutoPASS-avtalen står dette nedfelt i punkt 3.4: *"Kunden kan ikke benytte Brikken i andre motorvogner enn det som er angitt i denne avtalen"* (AutoPASS 2007c). Statens Vegvesen kan på denne måten gjennomføre trafikkanalyser i større grad enn dersom brikken ikke var fastlåst til et kjøretøy. For bilistene kan dette føles som et kontrolltiltak, som gjør at kjøretøyet til enhver tid kan spores gjennom enveiskobling mellom brikke og kjøretøy. Dersom brikken skulle kunne benyttes av flere kjøretøy vil det potensielt kunne føre til misbruk, for eksempel ved plassering av en brikke fra et "billig" kjøretøy i et dyrt. Brukerne kan likevel oppfatte fastlåsing av brikke til et kjøretøy som urettferdig. Når man kjøper klippekort på buss eller annen kollektivtransport, gjerne for å få rabatt på billettene, kan kortet benyttes av flere personer. For AutoPASS er praksisen en annen, og avtaler med forhåndsbetalte antall passeringer kan ikke flyttes mellom

kjøretøy på samme måte som klippekort kan flyttes mellom personer. Selv om en bruker eier to kjøretøy i samme klasse, har han ikke i utgangspunktet lov til å flytte brikken mellom kjøretøyene. Dette er en diskusjon som Datatilsynet har involvert seg i, og tilsynet har ytret ønske om at avtalene ikke skal knyttes til et bestemt kjøretøy, men heller til kunden (Personvernnemnda 2005). Eksempel på en situasjon hvor praksisen ser ut til å tilsvare Datatilsynets ønske, er ved bruk av leiebil når egen bil er på verksted. I denne situasjonen er det vanlig å flytte AutoPASS-brikken over i leiebilen (Faglærer Steinar Andresen 2007).

I henhold til samordning av bompengebetalingen i Europa vil prinsippet om én brikke per kjøretøy være en nødvendig forutsetning. Det samme gjelder for mulige nye anvendelsesområder. Det er ønskelig, spesielt fra Statens Vegevesens side, at alle kjøretøy skal være utstyrt med en AutoPASS-brikke i fremtiden. Problemet med et eventuelt offentlig pålegg om bruk av brikke er at ingen kjøretøy kan ferdes på norske veger uten å registreres. Dette vil gjøre det enda vanskeligere å kunne opprettholde muligheten til anonym ferdsel, og vil kunne oppleves som en krenkelse av den personlige integriteten.

5.3 AutoPASS smartkort og elektronisk billettering

Et smartkort er et kort utstyrt med enten en mikroprosessor og en minnebrikke, eller kun en minnebrikke. Smartkort utstyrt med mikroprosessor kan prosessere data lokalt på kortet, og dette betyr at data både kan slettes, legges til eller behandles på annen måte på kortet. Kort uten mikroprosessor kan derimot bare foreta en forhåndsdefinert operasjon, som for eksempel ved forhåndsbetalte telefonkort, og krever tilkobling til ekstern prosesseringskraft for å utføre operasjonen. En av ulikhetene mellom smartkort og vanlige kredittkort med magnetstripe er at smartkortet kan inneholde mer informasjon og flere funksjoner. Smartkortene blir også sett på som et sikkerhetsmessig godt alternativ til det tradisjonelle kredittkortet. (Sun 2007) Et AutoPASS smartkort (heretter kalt AutoPASS-kort) er et slikt kort, med data og funksjonalitet tilsvarende en AutoPASS-brikke. AutoPASS-kortet betinger at man i større grad foretar betalingen manuelt, ved at kortet må kommunisere med en kortleser. Dette innebærer kommunikasjon på kortere avstand enn for brikken. Kortet er ikke låst til kjøretøy slik AutoPASS-brikken er, og øker fleksibiliteten for mulige

anvendelsesområder. Et slikt kort kan utvides til betalingsmiddel for alle transporttjenester, inkludert kollektivtransport. Dette fordrer en tilrettelegging og samordning av elektroniske billetteringssystemer i Norge. *Håndbok 206* for elektronisk billettering er utarbeidet med formål om en slik samordning, og fungerer som en nasjonal standard for elektronisk billettering. *Håndbok 206* er delt i tre, hvor første del beskriver nasjonale retningslinjer for elektroniske billetteringssystemer. Del 2 beskriver krav og anbefalinger til regional og internasjonal samordning, mens del 3 omhandler tekniske spesifikasjoner for nasjonal interoperabilitet. Alle elektroniske billetteringssystemer i Norge er pålagt å følge *Håndbok 206*, og dette skal sikre samordning av systemene. Samordning defineres i *Håndbok 206* i tre ulike ledd; teknisk samordning, funksjonell samordning og avtalemessig samordning. Teknisk samordning sørger for at to enheter kan kommunisere, mens funksjonell samordning sikrer at data behandles og forstås likt på begge sider av kommunikasjonslinken. Avtalemessig samordning omhandler ansvar- og rollefordeling, rutiner for feilhåndtering og juridiske forhold. For brukeren betyr dette at samme billettmedium kan benyttes for ulike transporttjenester. (Trondsen 2006b)

Målsetninger knyttet til samordning av elektroniske billetteringssystemer er nedskrevet i *Håndbok 206* som M30 til M34 (SV 2004:10):

M 30 - Elektronisk billettering skal bidra til utvikling av et samordnet transportsystem med flere reiserelasjoner for kundene og færre ulikheter som følge av ulike transportmidler, trafikkselskaper og/eller myndighetsområder.

M 31 - Kunden skal kunne bruke samme billettmedium og produkt hos ulike transportselskaper og på ulike transportmidler på tvers av geografiske områder og myndighetsområder for alle reiser innenfor kollektivtilbudets felles annonserte dekningsområde.

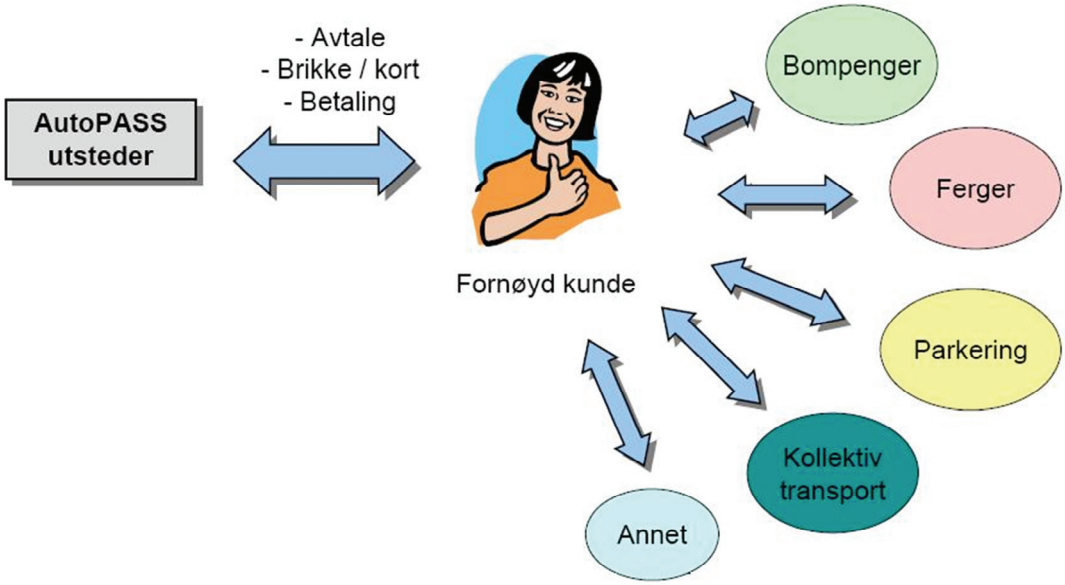
M 32 - Elektronisk billetteringssystemer skal baseres på internasjonale (ISO) og europeiske (CEN) standarder, slik at en oppnår en systemarkitektur som er basert på åpne og standardiserte grensesnitt både med hensyn til kommunikasjon og utveksling av informasjon og med hensyn til samordning av elektroniske billetteringssystemer.

M 33 - Et billettmedium skal kunne ha plass til og kunne håndtere flere produkter slik at de reisende oppnår en tilfredsstillende grad av

fleksibilitet med hensyn på valg og bruk av ulike produkter for ulike transporttjenester.

M 34 - Det skal finnes minst et nasjonalt produkt som kan benyttes i alle elektroniske billetteringssystemer.

Målsetningene viser at ved en samordning av elektronisk billettering på nasjonalt plan settes kunden i større grad i fokus, og med ett kort kan han betale for alle transporttjenester. Dette samsvarer med visjonen for AutoPASS-kortet, illustrert i figur 5.5, hvor kunden fremstilles som meget fornøyd og positiv. Kunden trenger kun én avtale, én brikke eller et kort og får én faktura for alle transporttjenestene som er benyttet.



Figur 5.5 Visjon AutoPASS (Trondsen 2006a)

AutoPASS-kortet er under utvikling, men er ikke i bruk enda. Kortet kan enten være knyttet til en sentral konto på samme måte som AutoPASS-brikken, eller det kan "lades" med en forhåndsinnbetalt sum. Dette innebærer at kortet inneholder elektroniske verdier. Tanken er at AutoPASS-kortet skal fungere som hovedbetalingsmiddel på ferger, siden takstregulativer gjør det vanskelig å benytte AutoPASS-brikken (se kapittel 5.4). I tillegg til å være kompatibelt med AutoPASS skal det utvikles i samsvar med *Håndbok 206*. Målet er at kortet skal være tilgjengelig i løpet av 2007. (Trondsen 2006a)

Reell konkurrent til eksisterende betalingskort?

Et AutoPASS-kort vil kunne benyttes som betalingsmiddel for flere tjenester enn AutoPASS-brikken, som er fastlåst til kjøretøy. Dette kan være kommersielle tjenester som parkering, eller tjenester som ikke er direkte knyttet til transportsektoren og Statens Vegvesen. I denne sammenheng stiller jeg spørsmål ved om et AutoPASS-kort er et reelt alternativ til eksisterende betalingskort. De fleste har i dag VISA-kort eller en annen form for betalingskort. Vil kundene da se nytten av å bruke sin AutoPASS-konto for betaling av flere tjenester når det i prinsippet er det mulig å benytte VISA-kortet for samme formål? Det er ikke sagt at kunden vil synes det er praktisk å ha enda et kort med tilsvarende funksjonalitet. Mange banker utsteder i dag smartkort med magnetstripe, selv om det foreløpig er magnetstripen som benyttes mest. Løsningen for AutoPASS kan dermed baseres på betalingskortene og teknologien som allerede finnes. For avtaler med forhåndsbetaling låser kunden fast elektroniske verdier i AutoPASS-kortet, og spørsmålet er i denne sammenheng knyttet til om kunden vil benytte seg av dette tilbudet. Jeg har valgt å ikke gå dypere inn i denne diskusjonen i oppgaven.

5.3.1 Implikasjoner for personvernet

En utvidelse av AutoPASS-avtalen til å omfavne et AutoPASS-kort medfører innsamling av enda flere opplysninger som kan knyttes til person. Spesielt dersom kortet skal kunne benyttes til betaling for alle transportmidler. I tillegg til å registrere personopplysninger ved inngåelse av AutoPASS-avtalen, vil det samles inn opplysinger om bruken både innenfor og utenfor AutoPASS-anleggene. Data vil lagres i ulike registre, både hos bompengeselskap og kollektivselskap, og en kobling av registrene kan ses på som en trussel mot personvernet. Gjennom kobling vil det for eksempel være mulig å spore reisemønsteret til en gitt person, og dette strider i mot prinsippet om personlig integritet. *Håndbok 206* er oppmerksom på problematikk rundt personvernet i samordnede billetteringssystemer, og peker på at det oppstår en interessekonflikt *"mellom kundens behov for beskyttelse av sin integritet og kundens, kollektivselskapet og andre operatørers behov for sikkerhet"* (SV 2004:71). Sikkerheten innebærer ved etterskuddsbetaling at operatøren skal kunne dokumentere for betalingskravene som kunden stilles ovenfor. For kundens

del vil lagring av informasjon om transaksjoner på kortet være kundens bevis på at tjenestene faktisk er betalt. Flere overordnede krav for å beskytte den personlige integriteten er beskrevet i et eget kapittel i håndboken, og har som mål å redusere muligheten for misbruk av innsamlet informasjon (for mer informasjon se kapittel 5.2 i SV 2004).

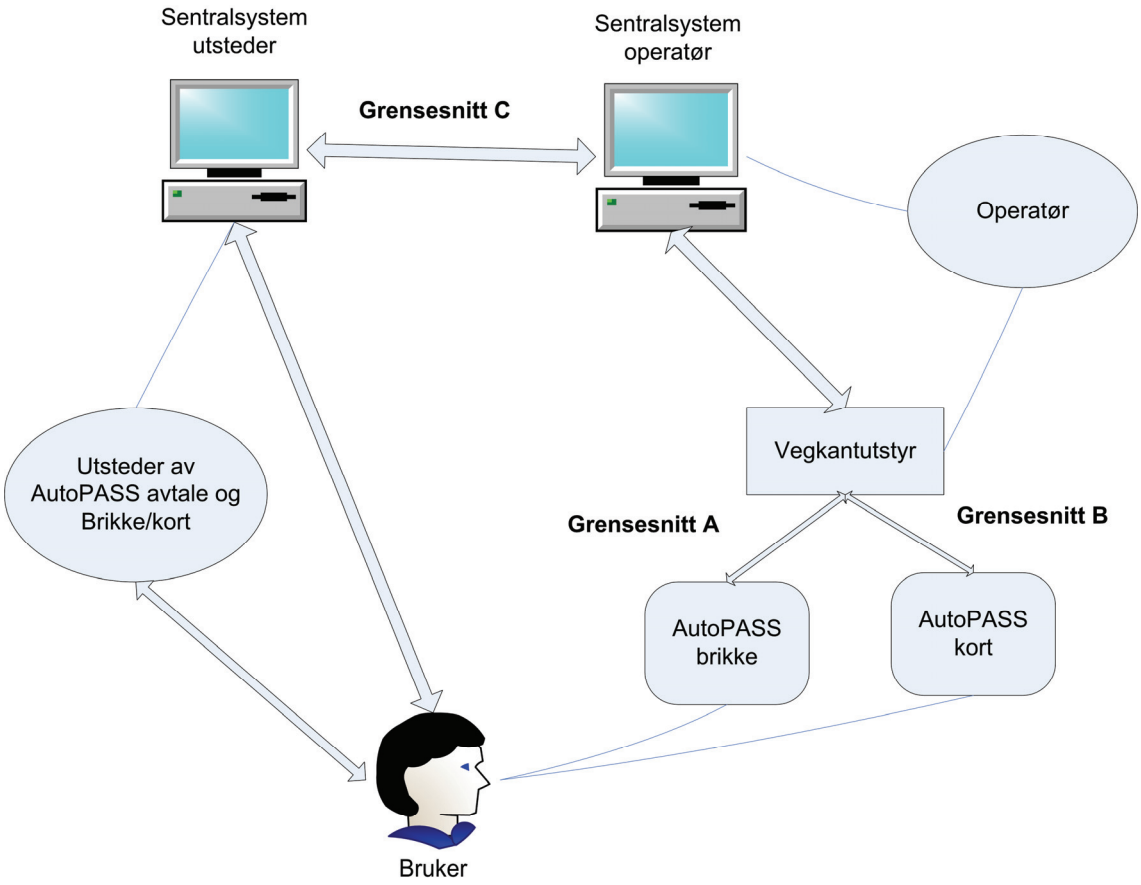
5.4 AutoPASS Ferge

AutoPASS kan som nevnt benyttes som betalingsmiddel på ferger. Dette gjøres mulig gjennom egne felter for ombordkjøring, der det er installert vegkantutstyr for avlesning av brikken. På samme måte som ved passering av bomstasjon trenger ikke bilen å stoppe for å betale. En tilsvarende avlesning må da også gjøres ved avkjøring dersom fergen har flere anløp med ulike billettpriser. Et alternativ til betaling med AutoPASS-brikken er ved bruk av AutoPASS-kort, dersom et slikt kort vil realiseres (AutoPASS 2003). De tekniske innretningene for å betale fergebilletter med AutoPASS-brikken er allerede på plass, men takstregulativer for billetteringen gjør bruken vanskelig. Fullstendig automatisering av en fergestrekning vil kun være økonomisk på meget trafikkerte strekninger, der mannskapet kan spare inn på å slippe manuell innkreving. Enkelte fergestrekninger i Norge er lite trafikkerte, og på disse strekningene vil ikke installasjon av tekniske løsninger for AutoPASS være lønnsomt (Furan 2007). I slike tilfeller har mannskapet tid til å ta manuelt betalt.

5.4.1 Krav til AutoPASS Ferge

"For å kunne anvende AutoPASS-brikkene og AutoPASS-kortene som betalingsmedia innenfor fergesektoren, kreves det at fergeselskapene har et sentralsystem med tilsvarende funksjonalitet som de sentralsystemene som bompengeselskapene i dag benytter for AutoPASS-brikkene som betalingsmedia" (Foss 2005:10). Fergeselskapenes sentralsystemer vil inngå som en del av ASB-systemet, og betaling av fergebilletter vil foregå deretter. På samme måte som for innkreving av bomavgift vil applikasjonen for kommunikasjon mellom vegkant og brikke baseres på internasjonale og europeiske standarder for DSRC og EFC. Bruken av AutoPASS-kort, og da kommunikasjonen mellom kort og kortleser, baseres på *Håndbok 206* for elektronisk billettering. (Ibid.)

Figur 5.6 viser sammenhengen mellom involverte parter for AutoPASS i fergesektoren. Det er tre viktige grensesnitt merket av i figuren; A, B og C. Grensesnitt A og B er begge mellom bruker og operatør, og kommunikasjonen går enten via AutoPASS-brikke og vegkantutstyr (A), eller via AutoPASS-kort og kortleser (B). Grensesnitt C representerer linken mellom operatør og utsteder. Utsteder er kan være en annen enn det selskapet passeringen gjøres hos, som en del av ASB. Som vi så i kapittel 5.1.2 går kommunikasjonen mellom operatør og utstedere i realiteten via en AutoPASS-formidlingssentral, som ikke er vist på figur 5.6. Formidlingssentralen *"samler inn, kontrollerer, pakker og sender videre data til riktige mottakere"* (Foss 2005:10). Modellen for bruk av AutoPASS i fergesektoren samsvarer med modellen for ASB.



Figur 5.6 Sammenheng mellom involverte parter (Basert på Foss 2005)

Takstregulativer

Fergesektoren er i dag regulert av et komplekst Riksregulativ som ikke lar seg inkludere i ASB på noen enkel måte. Slik det er nå kan man bare betale per kjøretøy med AutoPASS-brikken, og betaling av passasjerer lar seg vanskelig inkludere i systemet. Passasjerer i kjøretøyene kan inkluderes i kjøretøystaksten, men passasjerer som reiser uten kjøretøy faller utenfor. Fergesektoren opererer med lengdeklasser for kjøretøy, og det har blitt stilt forslag om at antallet lengdeklasser må reduseres (Amdal 2006). Mange av fergeselskapene holder ikke bare på med fergetransport, men også med buss og hurtigbåt. Dette kompliserer takststrukturen for ferge, buss og hurtigbåt ytterligere. En del av fergeselskapene har allerede samordnet billetteringen mellom egne transportmidler, spesielt med tanke på passasjerer. (Ibid.) Det finnes rabattordninger for passasjerer, for eksempel for studenter, men disse er gjerne ulike fra fylke til fylke. For å forenkle takststrukturen både for trafikantene og fergeselskapene, pågår det nå en revisjon av takstsystemene. Målet er blant annet å oppnå effektiviseringsgevinster, og samtidig unngå at en endring i takstene vil skape negative utslag for trafikantene (SD 2006).

Prøveprosjekt: Flakk – Rørvik

Bruken av AutoPASS for fergebetaling har blitt testet ut på ulike fergestrekninger, blant annet på riksfergestrekningen mellom Flakk og Rørvik. Siden 2006 har det vært mulig benytte AutoPASS for betaling av fergebilletten på denne strekningen. De som ikke har AutoPASS-brikke eller ikke ønsker å betale med brikken kan kjøre ombord i et manuellfelt, og betaler på vanlig måte. Fergestrekningen har fungert som et prøveprosjekt for et nytt Riksregulativ for fergetakster, og prosjektet er enda ikke avsluttet. (AutoPASS 2007d)

5.4.2 Personvern og ferge

Utvidelsen av AutoPASS til å inkludere flere tjenester enn bompengebetaling gjør at kartlegging av en brikkes bevegelser blir enda mer komplett. Dette betyr at inkluderingen av fergebetaling i AutoPASS, som en del av ASB, også havner i konflikt med prinsippet om anonym ferdsel. Registreringene utvides fra passering av bomstasjon til å inkludere bevegelser til havs. Gjennom ASB vil alle passeringer behandles av tilhørende bom- eller fergeselskap, og disse vil få omfattende oversikt

over egne brikkers bevegelser. Til tross for en økende kartlegging vil tjenesten være nyttig, spesielt for transportører og yrkessjåfører som ofte benytter avgiftsbelagte strekninger med fergedekning. Tjenesten vil gjøre det enklere for trafikantene å betale for seg dersom de allerede har en AutoPASS-avtale, og så lenge nye takstregulativer ikke gir negative utslag vil effektivitetsgevinstene kunne gjøre tjenesten attraktiv både for næringsliv og privattrafikk.

5.5 AutoPASS Parkering

Betaling av parkering med AutoPASS-brikken er en annen AutoPASS-tjeneste i prøvefasen. Foreløpig må brukere som ønsker å benytte seg av tilbudet registrere brikken hos parkeringsselskapet som tilbyr tjenesten, men Vegdirektoratet ønsker å inkludere denne tjenesten i AutoPASS Samordnet Betaling i løpet av 2007. Prøveprosjekter har vært gjennomført i to parkeringshus i Oslo, og det er planer om å utvide tjenesten til flere. Ved bruk av AutoPASS for parkering registreres brikken ved inn og utkjøring, og total bruk avregnes en gang i måneden. Brukeren sparer dermed tid ved at bommen åpnes automatisk ved inn- og utkjøring av parkeringshusene, og de slipper å stoppe for å betale. (AutoPASS 2007e)

5.5.1 Park & ride

Park & ride er et konsept innenfor transportsektoren som går ut på å parkere bilen for å ta kollektivtransport videre. Dette er spesielt nyttig for tungt trafikkerte innfartsårer til store byer som for eksempel Oslo. Park & ride ved Asker stasjon er nå under utprøving, og baserer seg på bruk av AutoPASS-brikke for reisetidsmåling og betaling av parkering. Dette innebærer at bilistene kan parkere bilen på Asker stasjon, og ta eksempelvis toget videre inn til byen. Løsninger som dette kan gjøre at bilistene heller anvender kollektivtransport når de skal inn til Oslo, og trafikkbelastningen på vegen vil minke. For at Park & ride skal være et godt alternativ for bilistene kreves en samordning mellom AutoPASS og billetteringssystemene for kollektivtransporten. Innføringen av et AutoPASS-kort vil kunne være med å forenkle konseptet. (Skadsheim 2006)

5.5.2 Personvern og parkering

Gjennom en tjeneste for betaling av parkering beveger AutoPASS seg inn på det kommersielle markedet. Private aktører som parkeringsselskaper vil kunne disponere datafangster hentet fra AutoPASS-brikkene. I henhold til verdikjeden i kapittel 4.2 har vi beveget oss lengre mot toppen, og mot anvendelse og bruk av innsamlet data til tjenester som ikke lengre er under ansvarsområdet til konsesjonsbelagte bompenge- eller fergeselskaper. Parkering medfører innsamling og lagring av informasjon, og utgjør enda en registrering av kjøretøyets bevegelser. En slik tjeneste vil likevel være attraktiv for kundene, som gjennom en samordning med betalingssystemer for kollektivtransport vil kunne benytte AutoPASS parkering som en del av for eksempel en helhetlig Park & Ride tjeneste.

5.6 Reisetidsmåling

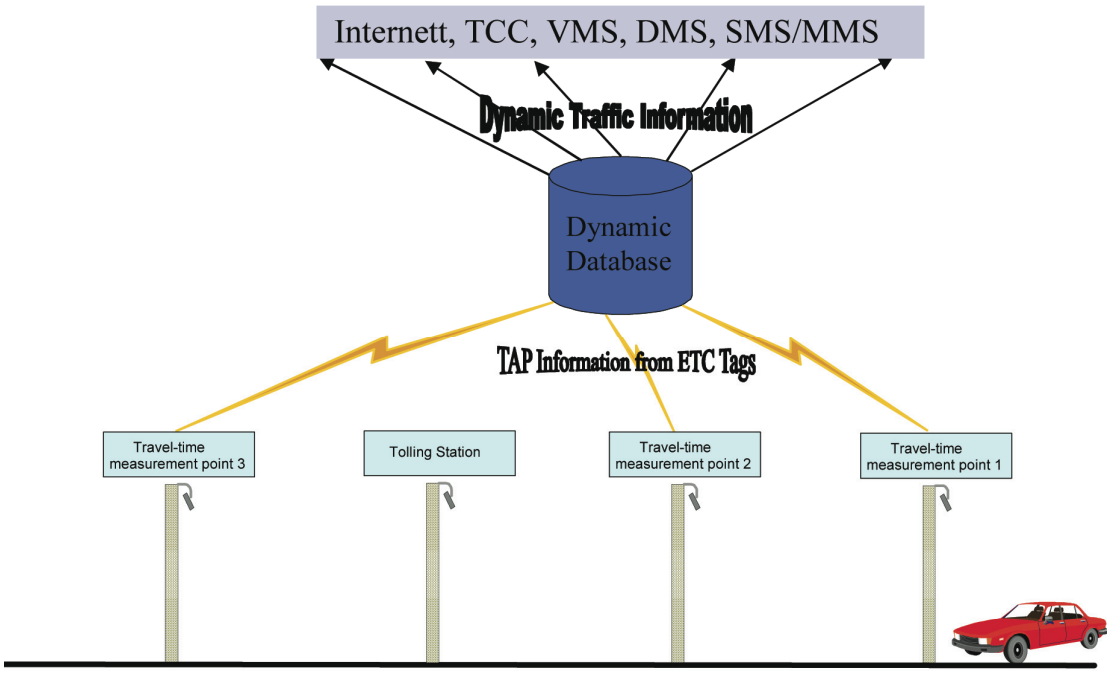
AutoPASS-teknologien er ikke bare nyttig for betaling av avgifter, den kan også benyttes for å samle inn ulike trafikkdata. Trafikkdata kan være data om reisetid eller forsinkelser på en vegstrekning, og danner et viktig grunnlag i trafikkanalyser. Trafikkanalyser kan benyttes for å beregne fremkommelighet på en vegstrekning, og reisetidsmålinger kan være et nyttig hjelpemiddel for å eksempelvis finne ut om det er tidsbesparende å rute om en vegstrekning eller ikke. Trafikkdata fra reisetidsmålinger kan også inngå som datagrunnlag i informasjonstjenester, og kan dermed brukes enten for overvåkning og kontroll av trafikken eller som grunnlag i trafikantinformasjon som sikrer trafikantene et tilstrekkelig informasjonsgrunnlag. I dag benyttes AutoPASS for reisetidsmålinger på E18 i Vestfold.

For å kunne regne ut reisetid for et kjøretøy på strekningen A til B, må brikken registreres i begge punktene. Med tanke på personvern kreves det at disse registreringene er anonyme, og det er utviklet et anonymt reisetidssystem som baserer seg på muligheten til å skrive informasjon til AutoPASS-brikken. I stede for å registrere brikke-ID, lagres heller passeringen av målepunktet på selve brikken. Passeringen leses deretter av på neste målepunkt, og utregninger av reisetid kan gjøres på bakgrunn av passeringsdata. På AutoPASS-brikken finnes det to logger for behandling av dynamiske data, og den ene har plass til fire passeringer forbeholdt reisetidsmålinger (Nyre 2007).

5.6.1 Systembeskrivelse

Når en brikke passerer et målepunkt, lagres passeringen i loggfilen på brikken. Det som skrives til brikken er tid og sted for passeringen. Sted er representert med en identifikator for den aktuelle leseren. Ved passering av neste målepunkt leses hele loggfilen, og reisetiden mellom ulike målepunkter kan regnes ut, basert på passeringene lagret i loggfilen og den nye passeringen. Den eldste av de fire passeringene blir så overskrevet med data for den nye passeringen. Systemet leser dermed aldri brikke-ID eller annen informasjon som kan kobles til bil eller person, og målingene er anonyme. (Nyre 2007)

Figur 5.7 viser hvordan et slikt systemet kan bygges opp. TAP er informasjon om tid og sted (Time And Place) som lagres i brikken ved passering av et målepunkt Brikken er referert til som en Electronic Toll Collection (ETC) tag i figuren. TAP-informasjonen (passeringen) registreres i en database for dynamiske data (baksystemet), og distribueres videre som dynamisk trafikkinformasjon via utvalgte kommunikasjonsmedier. Det er bare TAP som leses fra brikken.



Figur 5.7 Illustrasjon av system for reisetidsmåling (Haugen 2005)

Ved passering av et målepunkt vil alltid det samme handlingsforløpet forekomme. Passering av en bomstasjon mellom to målepunkter har ingenting å si for reisetidsmålingen, siden passeringene av bomstasjoner lagres i en egen logg. På en vegstrekning som illustrert i figur 5.7, med først to målepunkter, så en bomstasjon og så et målepunkt igjen, vil datainnsamlingen skje på følgende måte (Haugen 2005):

Passering av første målepunkt (Travel-time measurement point 1):

1. Leseren leser loggfilen
2. Leseren overskriver den eldste passeringen med den nye
3. Leseren sender alle fem passeringene (fire fra loggfilen) til baksystemet som regner ut reisetidene

Passering av andre målepunkt (Travel-time measurement point 2):

1. Leseren leser loggfilen
2. Leseren overskriver den eldste passeringen med den nye
3. Leseren sender alle fem passeringene (fire fra loggfilen) til baksystemet som regner ut reisetidene

Passering av en bomstasjon (Tolling station):

1. Normal AutoPASS-transaksjon gjennomføres, og lagrer passeringen i loggen for passering av bomstasjon
2. Loggpekeren inkrementeres

Passering av tredje målepunkt (Travel-time measurement point 3):

1. Leseren leser loggfilen
2. Leseren overskriver den eldste passeringen med den nye
3. Leseren sender alle fem passeringene (fire fra loggfilen) til baksystemet som regner ut reisetidene

Baksystemet bearbeider de data som er samlet inn fra målepunktene, og kan på bakgrunn av reisetidene gjøre en veloverveid trafikkanalyse. Det er dog mange faktorer som kan påvirke reisetiden, eksempelvis vær og føreforhold, ulykker og kødannelser, og disse må tas til etterretning når trafikkanalysene gjøres.

5.6.2 Personvern og reisetidsmålinger

I AutoPASS-avtalen spesifiseres det at bruk av brikken for anonymisert datainnsamling ikke skal medføre behandling av personopplysninger (AutoPASS 2007c). Dette realiseres for reisetidsmålinger gjennom bruk av den dynamiske loggen. For personvernet er anonymitet spesielt viktig med tanke på at slike data ikke senere skal kunne benyttes som beslutningsgrunnlag, for eksempel i en rettssak. Datainnsamlingen for reisetidsmålinger oppfyller kravene om anonymitet, men gir ikke bilistene noen mulighet til å samtykke om hva datainnsamlingen skal brukes til. Det er likevel vanlig praksis i transportsektoren å gjøre anonyme datainnsamlinger som dette, og i henhold til personvernet er slike registreringer lovlig når de ikke kan knyttes til person.

5.7 Samordning i Norden og Europa

NorITS er et samarbeidsprosjekt som jobber mot en samordning av de nordiske bompengesystemene (NORdic Interoperability for Tolling Systems). Målet er full interoperabilitet mellom eksisterende og kommende EFC-operatører i Norden. Dette betyr at en bruker kun trenger én avtale og én brikke for å kunne passere alle bompengeanlegg i Norden, og brukeren vil motta kun én faktura (Hansen 2005). I praksis kan NorITS ses på som en utvidelse av AutoPASS-tjenesten. Dette innebærer en funksjonell og geografisk utvidelse av AutoPASS Samordnet Betaling. EU-direktivet om elektronisk betaling (EFC-direktivet) krever at det skal jobbes mot en samordnet løsning i de europeiske landene. Gjennom NorITS ligger dermed de nordiske landene godt an i arbeidet med å oppfylle den felles europeisk målsetningen. Samtidig gir NorITS viktig input til utviklingen av et felles europeisk betalingssystem. (SD 2005)

5.7.1 AutoPASS EasyGo

Et resultat av arbeidet i NorITS er AutoPASS EasyGo, en tjeneste som gjør det mulig å benytte AutoPASS-brikken ved passering av bompengeanlegg på Øresundsbroen og Storebæltsbroen. Norge, Sverige og Danmark har dermed samordnet sine systemer for elektronisk betaling av bompenger på enkelte strekninger. I tillegg til passering av de to broene kan brikken benyttes på enkelte

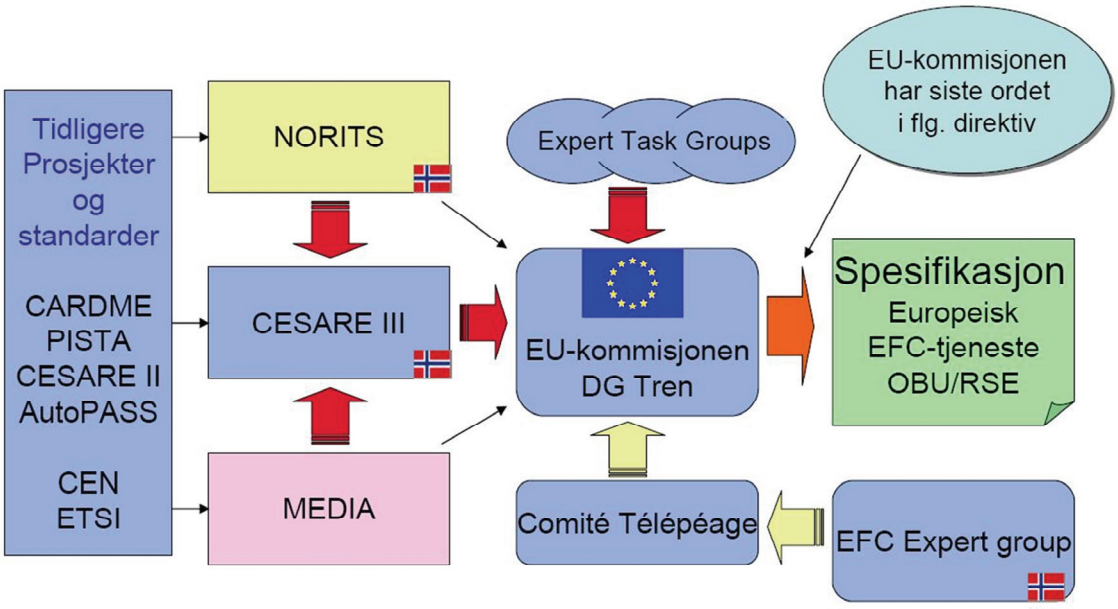
fergeforbindelser i Sverige og Danmark. Passering av bompengeanleggene i Sverige og Danmark foregår på samme måte som i Norge, og faktura vil bli tilsendt i etterkant av passeringen. Kunder fra Sverige og Danmark kan benytte sine BroBizz-brikker[3] i alle AutoPASS-anleggene i Norge, samt på fergestrekningen Flakk – Rørvik. (EasyGo 2007)

5.7.2 Europeisk utvikling

CESARE er et europeisk forsknings- og utviklingsprosjekt som jobber for *"å innføre operabilitet i alle bompengesystemer i Europa, basert på en felles tjeneste, en felles spesifikasjon og et felles avtaleverk"* (AutoPASS 2003). CESARE står for Common Electronic fee collection System for an ASECAP Road tolling European system. Prosjektet er ledet av ASECAP[4], som er en europeisk paraplyorganisasjon for bompengeselskaper. CESARE-prosjektet kan sees på som sammensatt av 4 ulike faser, og prosjektet er nå i fase III (CESARE III). Arbeidet som gjøres i NorITS og med CESARE III er med på å påvirke den europeisk utviklingen (se figur 5.8). Arbeidet leder frem til felles spesifikasjoner for en europeisk EFC-tjeneste, og spesifikasjonene fordrer interoperabilitet mellom alt av vegkantutstyr (RSE) og brikker (OBU). EU-direktiv 2004/52 handler om interoperabilitet mellom EFC-systemer i Europa. Direktivet baserer seg på prinsippet om én avtale og én brikke, og definerer begrepet European Electronic Tolling Service (EETS). EETS er en tilleggstjeneste for eksisterende EFC-tjenester som kreves implementert for interoperabilitet mellom bompengeanlegg i Europa. Neste generasjons AutoPASS-brikker må kunne utføre en EETS-transaksjon i tillegg til en AutoPASS-transaksjon, og de må håndtere kravene til sikkerhet for EETS. Tidsrammen satt i EU-direktivet ønsker at den nye brikken skal foreligge i 2009, og at det skal være mulig å lagre data om kjøretøyet på brikken. I første omgang skal brikken innføres for tungbiler, og i 2011 skal den være innført i alle kjøretøy. Dette betyr at brikken i 2011 kan benyttes for å betale for alle europeiske EFC-tjenester. (Trondsen 2004)

[3] BroBizz er navnet på betalingssystemet som benyttes på Øresunds- og Storebæltsbroen, og er et system tilsvarende AutoPASS.

[4] ASECAP – Assosiation Européenne des Comcessionaires d'Autorutes et d'Ouvreages à Péage



Figur 5.8 Influensveier til europeisk utvikling (Trondsen 2006a)

Figur 5.8 viser at Norge er med på å påvirke den europeiske utviklingen for EFC-systemer gjennom deltakelse i NorITS, CESARE III og som medlemmer av en EFC ekspertgruppe. Arbeidet med EETS foregår i 12 ekspertgrupper (Expert Task Groups) innenfor Comité Télépéage. Gruppene jobber med alt fra teknisk utredning av DSRC til klassifisering av kjøretøy og sertifisering av utstyr og systemer. Arbeidet med EETS har fortsatt en del uavklarte forhold, og innholdet i den felles betalingstjenesten er fremdeles usikkert. (Trondsen 2006a)

5.7.3 Personvern på tvers av grensene

En samordning av bompengeinnsamlingen i Europa vil medføre registrering av passeringer i et enda større geografisk område. Med tanke på personvern betyr dette en ytterligere spredning av personopplysninger. EUs personverndirektiv ønsker som vi så i kapittel 3.3.2, å beskytte personer med tanke på både behandling og utveksling av personopplysninger. Alle land som har implementert personverndirektivet oppfyller i følge personopplysningslovens § 29 (JD 2000) kravene om forsvarlig behandling av personopplysninger, og utveksling av opplysninger mellom land er regulert av lovverk. Implementeringen kan likevel være ulik fra land til land, og behandlingen følger de nasjonale retningslinjene.

6 Nye anvendelser av AutoPASS

Teknologiutvikling er med på å skape nye muligheter for transportsektoren. AutoPASS har vist seg å ikke bare kunne benyttes til elektronisk innkreving av bompenger, men også til betaling av fergebilletter og parkering. I tillegg har brikken vist seg nyttig for reisetidsmålinger. Foreløpig er anvendelsesområdene begrenset til dette, men den raske utviklingen av nye løsninger gjør at teknologien kan og vil inkluderes i nye anvendelser. Økt fokus på nytteverdien av IKT i transportsektoren legger til rette for nye løsninger, og Samferdselsdepartementets strategi for IKT innebærer *"bedre, tryggere og mer effektiv transport – med IKT"* (SD 2004:52). Sett fra et teknologisk og transportpolitisk synspunkt er dette meget bra, men det er viktig å være oppmerksom på at nye løsningene også kan skape nye utfordringer for personvernet.

I dette kapittelet vil jeg ta for meg mulige nye anvendelsesområder for AutoPASS og RFID-teknologi, som kan komme på bakgrunn av utvikling innen området for intelligente transportsystemer og tjenester. Anvendelsene kan sees i sammenheng med transportpolitiske målsetninger, samtidig som de også skaper utfordringer for personvernet. Sist i kapittelet vil jeg presentere en ny kommunikasjonsteknologi som kan bli viktig for ITS i fremtiden.

6.1 ITS og AutoPASS

Kapittel 2.2 introduserte noen viktige transportpolitiske målsetninger sammen med begrepet intelligente transportsystemer. Oppsummert ønsker målsetningene å oppnå høy trafikksikkerhet og et miljøvennlig, effektivt og fremkommelig transportsystem. ITS kan hjelpe til med å nå disse målene. Anvendelsene av ITS kan deles inn i 6 ulike områder, og i sammenheng med AutoPASS valgte jeg å se videre på trafikantinformasjon, overvåkning og kontroll og betalingssystemer. Alle tre anvendelsesområdene omhandler innsamling av dynamiske data. For fremskaffelse av trafikantinformasjon trengs det et omfattende datagrunnlag som inkluderer sanntidsinformasjon om trafikksituasjonen. Et bredt datagrunnlag er også nødvendig for å få et komplett overblikk ved overvåking og kontroll av trafikken. Siste anvendelsesområde er betalingssystemer, og en samordning av

betalingssystemer for ulike deler av transportsektoren krever data for å gjennomføre betalingstransaksjoner på tvers av transporttjenestene.

Med utgangspunkt i de tre anvendelsesområdene for ITS vil jeg nå definere noen eksakte muligheter for utvidet bruk av AutoPASS. Anvendelsene kan også sees på som tiltak for å komme noen skritt nærmere de transportpolitiske målsetningene. I ITS-strategien for *Nasjonal Transportplan 2010-2019* (SV 2006a) pekes det på mange mulige ITS-løsninger som kan komme i fremtiden. Løsningene er enda ikke utarbeidet, og eksisterer foreløpig bare som ideer. Med utgangspunkt i noen av disse ideene vil jeg se videre på hvordan de kan realiseres med AutoPASS. Løsningene jeg skisserer forutsetter at lagringskapasitet på brikkene ikke setter noen begrensning for anvendelsen.

6.1.1 Overvåkning og kontroll

Overvåkning av farlig gods

Farlig gods er en fellesbetegnelse på kjemikalier, stoffer og produkter med egenskaper som representerer en fare for mennesker og miljø dersom det skulle oppstå et uhell (DSB 2007). Kjøretøy som transporterer farlig gods er i dag merket med et oransje skilt. Noen oransje skilt er merket med tall som representerer farene knyttet til det farlige godset, og et UN-nummer som angir hvilket farlig gods som transporteres. En oversikt over farenummer er gitt i tabell 6.1.

0	Ingen betydning	6	Giftig
2	Gass	7	Radioaktivt
3	Brannfarlig væske eller gass	8	Etsende
4	Brannfarlig fast stoff	9	Risiko for voldsom reaksjon
5	Oksiderende	x	Farlig reaksjon med vann

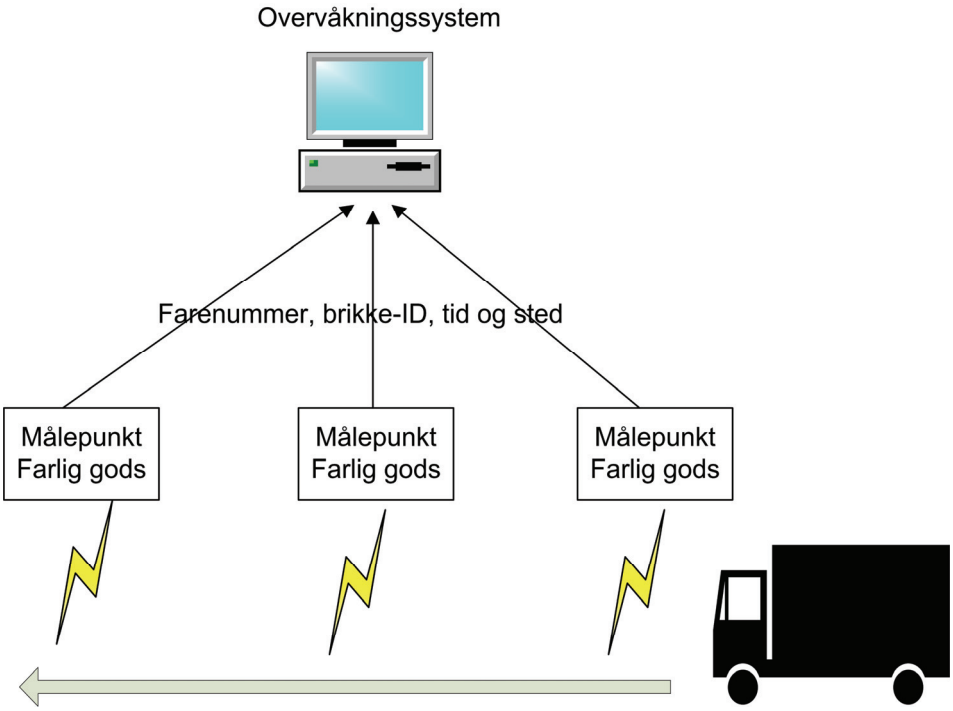
Tabell 6.1 Oversikt over farenummer for farlig gods (DSB 2005)

Farenummeret er satt sammen av flere siffer, der første siffer representerer primærfare, mens 2. og 3. siffer representerer sekundærfare. Dersom det er to like siffer betyr det en forsterking av faren, mens tall med 0 bak betyr ingen sekundærfare. (DSB 2005)

For å unngå at kjøretøy som frakter farlig gods involveres i ulykker og hendelser er det nyttig å ha en oversikt over hvor kjøretøyene befinner seg. Dette kan være spesielt nyttig på utsatte strekninger som tunneler (SV 2006a). Et overvåkningssystem vil ha oversikt over hvor det farlige godset befinner seg på et gitt tidspunkt. Systemet vil eksempelvis kunne se hvilke kjøretøy som befinner seg inne i en tunnel ved en ulykke, og hvilke kjøretøy er på veg mot denne tunnelen. På denne måten vil redningsmannskapene være mer forberedt på hva som venter på skadested, eller kjøretøy med farlig gods kan stoppes før de kjører inn i en ulykkessone.

Overvåkningssystem med AutoPASS

For å kunne benytte AutoPASS i et overvåkningssystem som dette må alle kjøretøy med farlig gods ha en AutoPASS-brikke. På brikken kan det lagres farenummer i tillegg til brikke-ID. Farenummeret vil kunne leses av i ulike punkter, og som for reisetidsmålinger kan det lages en logg som lagrer passeringene kjøretøyet gjør av punktene. Passeringene sammen med farenummer og eventuelt brikke-ID sendes videre fra leseren i punktet til et baksystem. Overvåkningssystemet vil ut i fra passeringsloggen kunne se hvilken veg kjøretøyet beveger seg, og har på bakgrunn av farenummeret oversikt over hvilke typer farlig gods som kjører i ulike retninger. For at systemet skal fungere må det plasseres ut lesere på strategiske steder av den utsatte strekningen, og disse må kobles opp mot et baksystem som behandler registreringene som vist i figur 6.1 Overvåkningssystemet kan videre kobles opp mot utrykningsmyndighetene, slik at de raskt kan skaffe seg oversikt ved utrykning. Et overvåkningssystem som dette kan være med på å øke trafikksikkerheten. Ved rask hjelp under en ulykke som involverer farlig gods kan overvåkningssystemet være nyttig også med tanke på miljøet, ved å hindre at det farlig godset skaper store ødeleggelser for miljøet i området hvor ulykken finner sted.



Figur 6.1 Overvåkningssystem for farlig gods

Planlegging av veier og infrastruktur (godstransport)

Ved areal og transportplanlegging (ATP) er det ofte vanskelig å få etablert et tilstrekkelig sikkert datagrunnlag for å gjøre gode analyser og ta veloverveide avgjørelser (Faglærer Steinar Andresen 2007). For å skaffe et bedre datagrunnlag for planlegging av veier og infrastruktur kan AutoPASS benyttes for innsamling av data. På samme måte som ved overvåkning av farlig gods kan det innføres et overvåkningssystem av annen godstransport gjennom plassering av målepunkter på strategiske steder. Ulike typer gods kan betegnes ved ulike tallkoder lagret på brikken, og det kan velges å ikke lese brikke-ID for å anonymisere informasjonen. For analyse- og planleggingsformål kan trafikkdata fra AutoPASS-brikken være med på å fremskaffe grunnlagsdata uten tilknytning til kjøretøy. Datagrunnlaget kan benyttes for å utvikle en effektiv infrastruktur, blant annet gjennom strategisk plassering av godsterminaler. Vegnettet kan også utvides og tilpasses faktisk belastning. Med tanke på logistikk vil sanntidsdistribuering av informasjon om godstransport kunne effektivisere virksomheten for transportørene og næringslivet, men dette krever kobling til kjøretøy. Et mulig hinder for en slik kobling er frykten for at informasjonen skal misbrukes for å overvåke

konkurrerende transportørers marked og for å skaffe seg konkurransefortrinn. For et rent statistisk formål kreves det dog ikke kobling til kjøretøy.

Utfordringer for personvernet ved overvåkningssystemer

Et overvåkningssystem for farlig gods krever at samtlige kjøretøy som frakter farlig gods er utstyrt med en brikke. Dette kan gjennomføres ved et pålegg om bruk av brikke i slike kjøretøy, og AutoPASS-avtalen kan knyttes til bedriften som eier kjøretøyet. Yrkestrafikk av denne sort trenger dermed ikke direkte tilknytning til privatpersoner, og krever ikke lagring av personopplysninger på samme måte som for privattrafikk. Overvåkning av farlig gods trenger gjennom denne løsningen dermed ikke å utfordre personvernet i noen betydelig grad. Det vil dog være mulig for bedriften å knytte en passering til en bestemt sjåfør i etterkant, og dette kan skape vansker. For å gjøre systemet enda mer anonymt er det mulig å ikke lese brikke-ID på samme måte som for reisetidsmålinger. Da vil oversikten kun være basert på type farlig gods. For annen type gods vil et overvåkningssystem gi størst gevinster med tanke på planlegging av veier og infrastruktur. Dette systemet krever også at kjøretøyene er utstyrt med brikke, men krever heller ikke at avtalen knyttes til enkeltpersoner. Datainnsamlingen kan også i denne sammenheng basere seg på type gods uten å lese brikke-ID, og løsningen vil ikke skape problemer for personvernet.

6.1.2 Betalingssystem

Automatisk innkreving av miljøavgift

Et annet ITS-satsningsområde for vegtransport retter seg mot målet om en mer miljøvennlig bytransport gjennom *"et system basert på RFID/AutoPASS for automatisk innkreving av miljøavgifter fra tungbilklasser med høy forurensningsgrad i utsatte områder"* (SV 2006a:35). Dette innebærer en utvidelse av AutoPASS til å inkludere en tjeneste for innkreving av miljøavgifter fra tungbiler som forurenser mye. For å kunne samle inn miljøavgifter må AutoPASS-brikken inneholde informasjon om hvilken miljøklasse tungbilen faller inn under. På samme måte som ved overvåking av farlig gods krever løsningen at alle tungbiler er utstyrt med brikke. Som vi så i kapittel 5.7 tilsier europeisk utvikling og EU-direktiv 2004/52 at alle tungbiler skal pålegges bruk av brikke innen 2009, samt at det skal være mulig å lagre informasjon om kjøretøy på brikken. Dersom

direktivet innføres vil alle tungbiler utstyres med brikker som inneholder informasjon som eksempelvis miljøklasse. Avhengig av takster og avgiftssystem kan betalingssystemet regne ut miljøavgiftene. Det holder nødvendigvis ikke å kreve miljøavgifter fra tungbiler som kjører inn i et utsatt område. Dersom miljøavgiften skal kreves inn i eksempelvis bomstasjonene trenger tungbilen bare å betale en engangssum for å kjøre ubegrenset mye innenfor bomringene. Oppsett av flere lesere og målepunkter kan gjøre at avgiften i større grad tilsvarer belastningen som påføres miljøet i området. Ved å registrer kjøremønster og dermed hvor mye og hvor langt tungbilen har kjørt i det utsatte området, vil avgiften kunne regnes ut dynamisk, og som vi skal se vil avgiftsalternativer for vegprising kunne benyttes som grunnlag for utregningene. Passeringer av lesere kan lagres i en logg på brikken på samme måte som for overvåkning av farlig gods og reisetidsmålinger. Sammenlagt kan data fra de ulike leserne plassert rundt i vegnettet benyttes til formål som innkreving av miljøavgift, reisetidsmålinger, overvåkning av farlig gods og som input til sanntids trafikkinformasjonstjenester. Et tettere oppsett av lesere kan også benyttes for vegprising med mål om å begrense trafikken i utsatte områder. Dette vil være positivt for miljøbelastningen i områdene. En slik løsning vil kunne gjøre det fristende å jukse, eksempelvis ved å benytte en brikke med ”feil” miljøklasse i henhold til tungbilen for å få lavere avgifter.

Vegprising

“Hensikten med vegprising er at det enkelte kjøretøy skal belastes med en avgift som reflekterer de kostnader og ulemper som en kjøretur i et gitt vegsystem medfører for andre enn dem som tar beslutning om den enkelte kjøretur eller transport“ (TIØ 2000). Vegprising kan være et nyttig virkemiddel for å unngå problemer som skyldes høy trafikkbelastning. I byer som er plaget med mye trafikk og forurensing kan vegprising være en utslagsgivende faktor for bedring av forholdene. Vegprising vil medføre økte kostnader for bilistene, noe som kan gjøre at flere velger andre fremkomstmidler enn bilen. Positive virkninger av vegprising kan dermed være at biltrafikken i byene minker, og at flere bytter til kollektivtransport. En forutsetning er at kollektivtilbudet utvides og bedres i samsvar med etterspørselen. Løsninger som Park & Ride (som ble introdusert i kapittel 5.5.1) er et godt alternativ for bilister som normalt benytter egen bil hele vegen. Vegprising vil dermed være en del av en felles transportpolitisk strategi som medfører endringer i

reiseadferd og etterspørsel etter kollektivtransport. Det finnes i følge Transportøkonomisk institutt (2000) flere alternativer til den tradisjonelle bompengeavgiften som de største byene i Norge opererer med i dag. Alternativene er innsamling av avgifter på bakgrunn av tid, distanse eller område. En tidsavgift vil avhenge av tiden et kjøretøy beveger seg innenfor et avgrenset området i en bestemt tidsperiode. Ulemper med en slik løsning er at den kan medføre at hastigheten øker og at dette igjen går ut over trafikksikkerheten. Distanseavgiften avhenger av distansen et kjøretøy legger bak seg i løpet av en bestemt periode, innenfor et gitt område. Siste alternativ er en fast avgift for å benytte et kjøretøy innenfor et avgrenset område i en tidsperiode. Denne avgiften kan kalles områdeavgift. (TØI 2000) Løsninger som dette kan medføre både ulemper og fordeler i forhold til bompengesystemet som er i bruk i dag, men er løsninger som kan tas opp til vurdering. For innkreving av miljøavgifter kan et av disse alternativene benyttes som bakgrunn for beregning av avgift.

AutoPASS-kort

På vegen mot en samordning av betalingssystemer for trafikktjenester kan AutoPASS-kortet være et foregangsprosjekt. Å kunne benytte et slikt kort som betalingsmiddel for alle transporttjenester vil forenkle reisen for trafikantene. Samtidig kan det legge tilrette for større bruk av kollektivtransport. Som en del av AutoPASS Samordnet Betaling kan kortet benyttes for alle tjenester tilknyttet.

Personvern ved betalingssystemer og vegprising

Tungbiler kan bli pålagt bruk av AutoPASS-brikke, og AutoPASS kan benyttes til innkreving av miljøavgifter. AutoPASS-avtalen for tungbilene vil på samme måte som ved overvåking av farlig gods tilhøre bedriften som eier tungbilen, og registrering og behandling av data for tungbilen trenger ikke knyttes til person. Innsamling av miljøavgift fra tungbiler brukt i yrkessammenheng utfordrer dermed ikke personvernet på samme måte som for privattransport. Ved innføring av vegprising i et bestemt område vil utfordringene for personvernet være knyttet til en økning i antall registreringer. For private bilister kan dette føles som overvåking og bidrag til kartlegging av bilistenes reisemønster. All kartlegging havner i konflikt med prinsippet om anonym ferdsel. Både utvidelse av betalingssystemer til å inkludere vegprising og bruk av AutoPASS-kort vil utfordre personvernet.

6.1.3 Trafikantinformasjon

Sanntids trafikkinformasjon

AutoPASS kan inkluderes i et større system for innsamling av dynamiske trafikkdata. Sammen med andre datafangster kan trafikkdata fra AutoPASS benyttes som grunnlag for trafikantinformasjon og resultere i reduserte reisetider og bedret fremkommeligheten for trafikantene. Sammenlagt påvirker dette effektiviteten i transportsystemet med utgangspunkt om at informasjonen distribueres i sanntid. Informasjon om trafikkavvikling og situasjonen i vegnettet kan være nyttig for flere formål, og et anvendelsesområde kan oppfylle mer enn ett transportpolitisk mål. Gjennom tilgang på tilstrekkelig informasjon og tilrettelegging av betalingssystemer, vil eksempelvis Park & Ride løsninger være et viktig bidrag til at bilistene bytter fra bil til kollektivtransport. Dette vil minke miljøbelastningen som biltrafikken påfører byene. En samordning av betalingssystemer vil forenkle bruken av kollektivtransport. AutoPASS-kortet er en løsning som er med på å gjøre akkurat dette. Tilgang på trafikantinformasjon, både med tanke på biltrafikk og på reiser med kollektive transportmidler, er kritisk for å få til slike løsninger.

Dynamisk informasjon om ferge

En mulighet for AutoPASS ferge er å utvide sin tjeneste til å tilby informasjon om kø og ventetider til sine trafikanter. Som en del av en større ITS-løsning vil det også kunne distribueres informasjon om endringer i rutetider (SV 2006a). Datagrunnlag for en dynamisk informasjonstjeneste for ferge kan bygge på data samlet inn fra AutoPASS-brikkene sammen med andre datafangster. Dynamiske vegskilt på veg mot fergeleiet kan informere trafikantene om når både første og neste ferge skal gå. Det kan også informeres om hvor lang kø det er på fergeleiet, og antatt ventetid. Gjennom muligheten til å skrive til brikken kan det legges inn informasjon om at kjøretøyet skal ta en ferge. Den dynamiske informasjonstjenesten kan da knyttes opp mot et en ITS-løsning i kjøretøyet som distribuerer informasjonen direkte til føreren. På denne måten vil informasjonen kun distribueres ved etterspørsel. Dette kan effektivisere trafikkavviklingen på ferger og fremkommeligheten i vegnettet, spesielt for yrkestransport.

Personvern

Kobling av datafangster for å tilby utvidede informasjonstjenester kan havne i konflikt med personvernet. Økt innsamling av data, og bruk av data i flere anvendelser, kan fremskaffe informasjon som i utgangspunktet ikke var tiltenkt de ulike datainnsamlingene. Et eksempel på bruk av data på denne måten er gjennom personifisert reiseinformasjon, som for eksempel ved en informasjonstjeneste for fergetrafikanter. Informasjonstjenester som dette vil på bakgrunn av en helhetlig kartlegging av reisemønster gi informasjon om forventet reisetid på en vegstrekning, hvilket nummer i fergekøen kjøretøyet er, buss- og togruter og så videre. Dette kan være meget nyttig informasjon for brukeren, men medfører også utfordringer for personvernet. Den personlige integriteten utfordres gjennom en kartlegging av bevegelser, ikke bare på vegen, men også til havs og ved bruk av kollektivtransport.

6.1.4 Oppsummering av nye anvendelser

De nye anvendelsene jeg har sett på representerer de tre anvendelsesområdene for ITS i transportsektoren. Overvåking av farlig gods i vegnettet er en anvendelse innenfor området overvåking og kontroll som vil kunne bedre trafikksikkerheten og minke det farlige godsets belastning på miljøet ved ulykker. Grunnlagsdata og statistikkinnsamling fra godstransport kan benyttes for å gjennomføre analyser og ta gode avgjørelser ved areal og transportplanlegging. Automatisk innkreving av miljøavgift og vegprising er begge eksempler på nye muligheter for betalingssystemer. Anvendelsene vil kunne minke miljøbelastningen, og samtidig minke trafikkbelastningen i utsatte områder. Innføring av et AutoPASS-kort kan sees på som et effektiviseringstiltak, samtidig som det sammen med sanntidsinformasjon til trafikanter kan påvirke miljøet positivt, ved at det blir enklere for å benytte seg av kollektivtransport. Økt tilgang på trafikantinformasjon vil også legge tilrette for Park & Ride, som sammen med dynamisk fergeinformasjon vil være med på å øke fremkommeligheten i vegnettet. For personvernet er de fleste utfordringene knyttet til en økning i antall registreringer ved bruk av AutoPASS for flere tjenester. Problemet er at flere registreringer øker muligheten for kartlegging og overvåking av bevegelser i trafikken.

6.2 RFID-teknologi i ITS

RFID vil ikke bare kunne inkluderes i nye ITS-løsninger gjennom AutoPASS. Det er flere tilfeller hvor RFID-teknologi kan benyttes i transportsektoren, og noen av mulighetene introduseres her.

Elektroniske kant- og midtlinjer

For å redusere antall ulykker som følge av at et kjøretøy kommer over i feil kjørebane eller kjører utenfor vegbanen, kan det utvikles et varslingssystem basert på RFID-teknologi. Dette kan gjennomføres ved å plassere passiv RFID-teknologi i kant- og midtlinjer på vegbanen, og en leser i kjøretøyet. Når bilen passerer kant- eller midtlinje vil leseren oppdage RFID-brikkene, og det utløses et lydsignal for å påkalle førerens oppmerksomhet. I tilfeller der føreren sovner av eller bare er uoppmerksom vil signalet gjøre at føreren kan manøvrere kjøretøyet i riktig retning igjen. Dette er et tiltak som kan forbedre trafikksikkerheten. (SV 2006a, SV 2006b)

Trådløs identifisering av kjøretøy

Ved hjelp av elektroniske nummerskilt er trådløs identifisering av kjøretøy mulig. Informasjon om kjøretøyets eiermessige, sikkerhetsmessige og avgiftsmessige tilstand kan lagres i en RFID-brikke og dermed registreres automatisk (SV 2006a). På denne måten kan kontrollen av kjøretøy effektiviseres. Dette er informasjon som også kan lagres på AutoPASS-brikken, og som krever at alle kjøretøy er utstyrt med brikke.

Prioritering av kjøretøy i lyskryss

RFID kan kombineres med trafikksignalsystemer for å prioritere utrykningskjøretøy i lyskryss (SV 2006a). Dersom et utrykningskjøretøy er på veg mot et lyskryss kan annen trafikk stoppes, slik at utrykningskjøretøyet kan slippe gjennom med absolutt prioritet. Utrykningskjøretøy kan utstyres med en RFID-brikke som vil oppdages når de er på veg mot et lyskryss. Signalsystemet kan handle deretter, og gi prioritet til utrykningskjøretøyet. Dette kan gjennomføres ved at all annen trafikk inn mot krysset får rødt lys slik at uttrykningskjøretøyet har fri bane gjennom. Et slikt system kan også realiseres ved bruk av GPS, og er et tiltak som vil bedre trafikksikkerheten.

Gebyrordning for piggdekk

En annen mulighet med ITS er en effektivisering av gebyrordningen for piggdekkbruk. Dette kan realiseres gjennom en løsning som gjør det enklere å betale for piggdekkgebyret og å overvåke at gebyret er betalt. Løsningen kan benytte sensorer for å fange opp piggdekkbruk, sammen med informasjon fra en RFID-brikke, eksempelvis AutoPASS eller elektroniske nummerskilt, som forteller om piggdekkgebyret er betalt eller ikke (SV 2006b). Det er også mulig med automatisk innkreving av gebyr ved bruk av AutoPASS-brikken. Dette betyr at bilistene ikke trenger å betale gebyret manuelt, men at en innkreving gjøres automatisk ved passering av et kontroll og betalingspunkt for piggdekkgebyr. AutoPASS må da utvides til å også tilby denne betalingstjenesten.

6.2.1 Personvern og utvidet bruk av RFID.

Bruk av RFID-teknologi i kant- og midtlinjer er i utgangspunktet en punkt til punkt tjeneste, der informasjon om passeringer ikke skal benyttes til annet enn å påkalle oppmerksomhet i en gitt situasjon. Dersom informasjonen lagres og tenkes brukt til andre formål, vil personvernet aktualiseres. Andre formål kan være å bruke informasjonen som beslutningsgrunnlag i eksempelvis forsikringssaker som følge av en ulykke. Det samme gjelder for bruk av RFID for prioritering av utrykningskjøretøy. Lagring av informasjon gjør at den potensielt kan knyttes til bestemte kjøretøy og personer i en senere sammenheng. Utfordringene for personvernet er i denne sammenheng, som for AutoPASS, knyttet til kartlegging og mulighetene for bruk av informasjon til annet enn opprinnelig formål.

Elektroniske nummerskilt vil inneholde informasjon om et kjøretøys avgiftsmessige status og tilstand. Som nevnt kan denne informasjonen også lagres på AutoPASS-brikken. Det samme gjelder for betaling og kontroll av piggdekkgebyr. Vi har allerede sett på andre mulige utvidelser av AutoPASS i sammenheng med anvendelsesområder for ITS, og sammen med utvidelsene i dette avsnittet kan tjenestekjeden for AutoPASS bli meget omfattende. Alle tjenestene innebærer behandling av data, og i de situasjonene det er snakk om personopplysninger vil kravene til forsvarlig behandling måtte oppfylles i lys av personopplysningsloven og forskriften. Bruk av RFID-teknologi, selv om den ikke skal inngå som en del av AutoPASS, medfører at kjøretøyene legger igjen

elektroniske spor. Hensynet til personvern er dermed viktig å være klar over når tjenestene utvikles.

6.3 Kommersiell bruk av AutoPASS

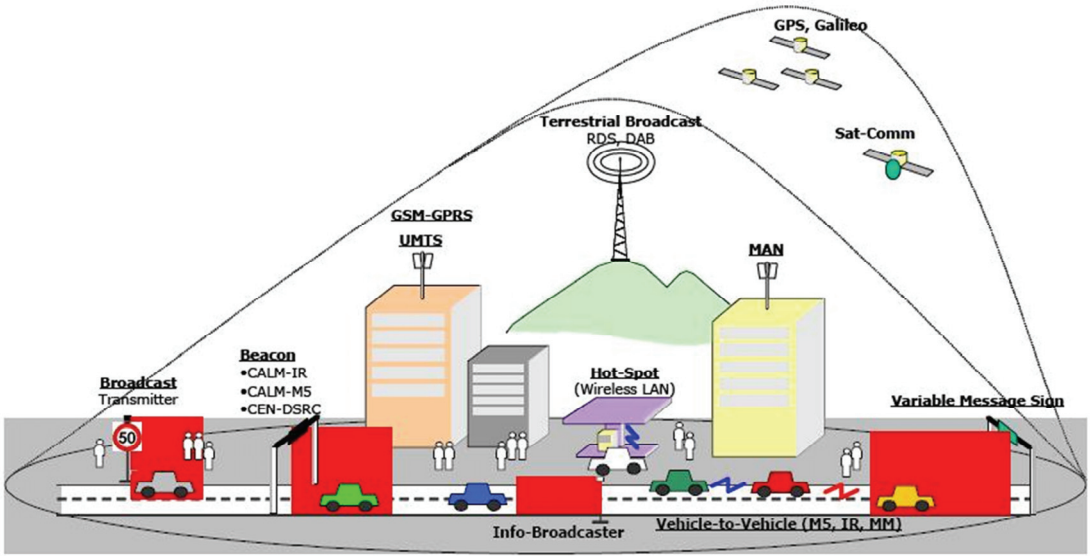
AutoPASS som elektronisk betalingstjeneste kan utnyttes på et kommersielt nivå. Dette involverer private aktører på samme måte som med bruk av AutoPASS for betaling av parkering. Eksempler på mulig kommersiell bruk er betaling av bilvask eller bensin på bensinstasjon og betaling av mat på McDonalds Drive-in. Eksemplene innebærer automatisk betaling for tjenesten eller varene som kjøpes, og brukeren trenger i prinsippet ikke gjøre noe aktivt for å gjennomføre handelen. Slike tjenester vekker spørsmål om eierskapen til AutoPASS. Dersom teknologien benyttes til formål som dette, er det ikke lengre sagt at AutoPASS-brikken skal eies av Statens Vegvesen. Som vi så i kapittel 4.2.3 er datafangster tradisjonelt sett organisert av offentlige myndigheter som Statens Vegvesen, mens private aktører i større grad står for distribusjon til brukere gjennom ulike informasjonstjenester. Spørsmål om eierskap og organisering av AutoPASS aktualiseres på samme måte som for eierskap til trafikkdata når private aktører involveres.

6.4 Fremtidsblikk: CALM

Kommunikasjonsteknologi er en forutsetning for å kunne tilby og utvikle ITS-løsninger. AutoPASS gjøres mulig gjennom RFID-teknologi og DSRC. En sentral kommunikasjonsteknologi for fremtidige ITS-løsninger er en standard under utvikling kalt Continous Air-interface Long and Medium range (CALM). CALM tar sikte på å til enhver tid kunne benytte beste tilgjengelige kommunikasjons-ressurser. Dette betyr at CALM er en kommunikasjonsløsning som alltid velger beste tilgjengelige trådløse kommunikasjonsmedium, og som har muligheten til å bytte fra et medium til et annet dersom det skulle være nødvendig. CALM inkluderer dermed bruk av eksisterende kommunikasjonsteknologier som blant annet GSM, UMTS, GPS, WLAN, WiMax og DSRC. Siden CALM er basert på IPv6[5] er den også kompatibel med Internettjenester. Konseptet er utviklet for å

[5] *IPv6 – Internett Protokoll versjon 6*

kunne tilby en lagdelt tjeneste som muliggjør kontinuerlig kommunikasjon mellom kjøretøy, mellom kjøretøy og infrastruktur, og mellom infrastruktur. CALM kan sees på som bredbånd i bil, og en skisse av teknologien er vist i figur 6.2. AutoPASS er representert ved CEN-DSRC, og kan inkluderes i CALM. (ISO 2004b)



Figur 6.2 Skisse over CALM (ISO 2004b)

CALM åpner opp for en rekke applikasjoner som kan være med på å forbedre både trafikksikkerhet og trafikkadministrasjon. Noen anvendelsesområder er allerede nevnt i forbindelse med AutoPASS og RFID. Eksempler på andre fremtidige muligheter er listet opp under.

Automatisk bremsevarsling

- Kommunikasjon mellom kjøretøy.
  - Dersom kjøretøyet foran bremser vil fører varsles.
  - Applikasjonen kan også ta over kontrollen og bremse dersom fører ikke gjør det.

Rødlysvarsling

- Kommunikasjon mellom infrastruktur og kjøretøy.
  - Varsling dersom kjøretøyet kjører mot rødt lyd.

Kollisjonsvarsling

- Kommunikasjon mellom kjøretøy eller mellom infrastruktur og kjøretøy.
  - Varsling dersom kjøretøyet holder på å kollidere med en annen bil eller noe annet.

Automatisk vurdering av fartsgrenser

- Kommunikasjon mellom kjøretøy og infrastruktur eller mellom infrastruktur.
  - Infrastrukturen kan endre fartsgrensen i henhold til gjeldene kjøreforhold.
  - Kjøretøy kan for eksempel gi beskjed til infrastruktur dersom der er lite friksjon på vegen, og dermed glatt, slik at fartsgrensen kan reduseres.

Variable meldingstavler

- Kommunikasjon mellom infrastruktur
  - Kan informere om rådene trafikkforhold.
  - Kan vise fartsgrensen i øyeblikket.

eCall

- Kommunikasjon mellom kjøretøy og infrastruktur
  - Dersom bilen havner i en ulykke vil bilen selv varsle om dette til utrykningsmyndighetene.
  - Utrykningsmannskapet får beskjed om hvor ulykken har skjedd med en gang.

ITS og CALM legger tilrette for flere nye muligheter innen transportsektoren. Visjonene er mange og store, men realisering av enkelte av løsningene ligger et stykke frem i tid foreløpig. Det er mange utfordringer knyttet til utvidet bruk av ITS-løsninger, og en av de største er hensynet til personvern. Under utvikling av nye løsninger kan det være nyttig å forholde seg til noen konkrete krav i henhold til personvern og behandling av data.

7 Krav til behandling av data

En utvidelse av AutoPASS til å omfatte flere anvendelsesområder betyr at flere former for datafangst knyttes til systemet. Jeg vil i dette kapittelet se på hvordan denne utvidelsen kan påvirke personvernet, og hvordan kravene til behandling av data bør ta høyde for de nye utfordringene som skapes. Data i denne forbindelse representerer alle datafangster i AutoPASS-systemet, både dynamiske trafikkdata og persondata, og behandlingen av data omfatter alt fra innsamling og lagring til sammenkobling og bruk.

Det eksisterer allerede regelverk som setter rammene for behandling av personopplysninger i elektroniske informasjonssystemer. Vi skal først se litt på elektronisk databehandling og oppsummere viktige personvernområder, før vi ser videre på hvordan behandling av data kan kontrolleres med tanke på personvern. Anvendelsene vi har sett på i oppgaven vil deretter raskt oppsummeres og plasseres i tilhørende ITS-anvendelsesområde. Utvidelsen av AutoPASS til å inkludere flere anvendelser vil gi nye utfordringer for personvernet som det er interessant å se litt nærmere på. Til sist i kapittelet vil praksis rundt personvern i dag og i fremtiden kort diskuteres.

7.1 Elektronisk databehandling

I kapittel 3.3.1 så vi at informasjonssystemer som elektronisk behandler personopplysninger er underlagt personopplysningsloven. Loven inneholder konkrete retningslinjer for behandling med utfyllende krav til informasjonssikkerhet beskrevet i personopplysningsforskriften. Juridisk sett finnes det dermed en rekke regler for databehandling i informasjonssystemer som AutoPASS. Som utgangspunkt for tilfredsstillende behandling skal bedrifter kun behandle opplysninger som er av interesse for forretningsvirksomheten. En utvidelse av AutoPASS til å inkludere flere tjenester betyr en utvidelse av forretningsvirksomheten, og hvilke opplysninger som er av interesse kan følgelig endres. Dette kan medføre både begrensninger og utvidelser av omfanget personopplysninger som registreres.

Som vi så i kapittel 3.2.2 utfordres personverninteressene stadig av interesser som ikke representerer personvern, eksempelvis forbrukerinteresser og kommersielle interesser. Spesielt havner ønsket om diskresjon og anonymitet i konflikt med andre interesser. Avveininger mellom ulike interesser gjøres dermed når man velger å ta i bruk en tjeneste. Tjenestene er som regel harmløse på egenhånd, men summen av tjenester kan være uheldig for personvernet. ITS legger tilrette for en rekke nye tjenester og løsninger innen transportsektoren, og noen av tjenestene produserer på lik linje med AutoPASS elektroniske spor. Det er nettopp mengden av slike spor Datatilsynet er bekymret for i *Personvernrapporten 2007*, på bakgrunn av potensialet for misbruk ved kartlegging og overvåking. Med økt fokus på personvern og hvilke regler og retningslinjer som gjelder for databehandling i denne sammenheng, kan utviklingen av nye tjenester i større grad rettes mot å ivareta personvernet.

Sammenlagt må praksis for behandling av data fokusere på flere områder for å ta tilstrekkelig hensyn til personvernet. En oppsummering av viktige personvernområder berørt i oppgaven følger under, og vil diskuteres i kapittelet.

- Anonymitet
    - Dersom formålet ikke krever behandling av personopplysninger bør anonymiteten ivaretas.
    - Sporfrie alternativer må tilbys så fremt det er mulig.
- Lagring og gjenbruk
    - Kravene som stilles til informasjonssikkerhet må oppfylles gjennom å sikre opplysningenes integritet, konfidensialitet og tilgjengelighet.
    - Konsekvente retningslinjer for utlevering og bruk av opplysninger i etterkant må utarbeides og følges.
- Kobling av datafangster
    - Muligheter for kobling av datafangster for å skaffe ny informasjon utover formålet med innsamlingen må hindres.
- Samarbeid og samordning
    - En oppklaring av ansvarsforhold er viktig når databehandlingen involverer flere aktører.
    - Krav til databehandling må gjelde alle involverte aktører.

- Personvernet må ivaretas hos alle involverte aktører gjennom avtaleverk.
- Unødig spredning av opplysninger må hindres.

7.1.1 Kontroll i henhold til personvern

Elektronisk databehandling stiller krav til informasjonssystemene, og kravene innebærer rutiner for behandlingen. Ved utvidelser av informasjonssystemer til å inkludere flere datafangster omfatter databehandlingen også mulighet for sammenkobling, og dette er det nødvendig å være oppmerksom på i henhold til personvern. Når rutiner og systemkrav utarbeides er det viktig å kontinuerlig kontrollere at personverninteressene ivaretas. Ansvaret for kontrollen bør ligge både hos de som utvikler anvendelsene og de som gjennomfører utvidelsene. Kontrollen må gjøres med utgangspunkt i regler og krav fra nasjonale bestemmelser, og jeg vil liste opp tre kontrollpunkter som tar for seg viktige utfordringer for personvern ved utvidelse av informasjonssystemer.

1. Kontroll av datafangst.
    - Hva er formålet med datainnsamlingen?
    - Er integritet, konfidensialitet og tilgjengelighet tilstrekkelig sikret?
2. Kontroll av mulige koblinger mellom datafangster.
    - Er det mulig å koble datafangster for å skaffe mer informasjon?
3. Kontroll av hvilke informasjonstjenester som kan bygge på datafangstene.
    - Setter formålet med innsamlingen noen grenser for anvendelsen av datafangsten?
    - Er det noen begrensninger for utvalget av informasjonstjenester?

Kontrollpunktene kan benyttes for å vurdere et informasjonssystem i henhold til personvern. Hvor streng kontrollen av de ulike delene skal være avhenger av om det fra offentlig hold velges en strengere eller svakere oppfølging av personvern. Som vi har sett stilles det allerede en rekke vilkår for databehandling gjennom lover og regler, men tolkningen av disse avhenger av det offentlige. Datatilsynet legger i stor grad retningslinjer for oppfølging av personvernet i Norge, og da også tolkningen av lovverket.

Kontroll av datafangst i første punkt omhandler bevissthet rundt formålet med innsamlingen. Personvernprinsippet om saklig begrunnelse for innsamlingen fra kapittel 3.4 må oppfylles, sammen med vilkårene for lovlig behandling oppført i personopplysningsloven. Sikring av data innebærer krav om autorisert tilgang til og bruk av dataene som er samlet inn, samt at dataene til en hver tid skal være korrekte. Integritet, konfidensialitet og tilgjengelighet er som vi har sett tidligere viktig for personvernet, spesielt med tanke på informasjonssikkerhet. Andre kontrollpunkt er rettet mot muligheten for sammenkobling av datafangster. I tilfeller hvor sammenkobling brukes for å få tilgang til mer informasjon vil den utgjøre en stor utfordring for personvernet. Siste punkt omhandler kontroll av informasjonstjenester, og er viktig å være oppmerksom på for å unngå misbruk av data ved nye anvendelser. Dette punktet vil være avhengig av kontrollen i punkt to, hvor muligheten for kobling av datafangster kan danne grunnlaget for en informasjonstjeneste. De tre punktene er i utgangspunktet alle avhengige av hverandre, og en streng eller svak oppfølging av personvernet vil avgjøre hvordan kontrollen gjennomføres.

Personifiserte informasjonstjenester og markedsføring er anvendelser av datafangster som kan bli lovlig dersom det velges en svakere oppfølging av personvernet fra det offentlige. Det kan åpnes opp for bruk av datafangster fra AutoPASS til å eksempelvis tilby personifiserte informasjonstjenester som baserer seg på kartlegging. Dette kan enten være tjenester som dyttes på brukeren (”push”) eller som etterspørres (”pull”). AutoPASS trafikantinformasjon kan tilby slike informasjonstjenester, og dynamisk fergeinformasjon introdusert i kapittel 6.1.3 er et eksempel på en personifisert tjeneste som kan etterspørres. En informasjonstjeneste som kan dyttes på brukeren er personifisert markedsføring. Kartlegging av en brukers reisemønster kan benyttes for å sende brukeren reklame om eksempelvis en restaurant som ligger på en vegstrekning han benytter ofte. Informasjonstjenestene er dermed av ulik interesse for brukerne, og i et samfunn hvor det ikke settes begrensninger for bruken av data vil det kunne utvikles en rekke slike tjenester, uavhengig av om brukerne ønsker det eller ei. Alle aktører som har tilgang til datafangstene vil kunne utnytte dette for å drive kartlegging og tilby slike tjenester, og det kan dermed være fristende å bruke datafangstene for annet enn det opprinnelige formålet. Kontinuerlig kontroll og

oppfølging av personvern i henhold til de retningslinjer som gis fra det offentlige er derfor viktig.

7.2 AutoPASS datafangster

Vi har i denne oppgaven har sett på flere mulige anvendelser av AutoPASS-teknologien. Noen av anvendelsene er allerede under utprøving, mens andre foreløpig befinner seg på et tankestadium. En utvidelse av AutoPASS-systemet til å inkludere alle anvendelsene presentert i oppgaven vil medføre et stort omfang av datafangster.

I kapittel 6 så vi på noen mulige anvendelser av AutoPASS som en del av ITS i fremtiden. Tabell 7.1 oppsummerer de nye mulighetene med tilknytning til AutoPASS anvendelsesområde.

AutoPASS anvendelsesområde	**Ny anvendelse (Transportmål)**	**Utfordring**	**Hensyn til personvern**
Overvåkning og kontroll	Planlegging av veier og infrastruktur (Effektivitet og fremkommelighet)	Mulighet for kartlegging og bruk av informasjon til andre formål.	Anonyme innsamlinger ikke knyttet til kjøretøy.
	Overvåkning av farlig gods (Trafikksikkerhet og miljø)		Anonyme innsamlinger eller knytte avtalen til bedrift
Betalingssystem	Miljøavgift (Miljø)		Kreves avtale for å utføre en betalingstransaksjon. Avtalen kan knyttes til bedrift.
	Vegprising (Miljø)	Mulighet for kartlegging og overvåkning av privatpersoners reisemønster.	Lagringstid og gjenbruk av data må begrenses. Sporfrie alternativer såfremt det er mulig.
Trafikantinformasjon	Sanntids trafikkinformasjon (Effektivitet, fremkommelighet og miljø)	Samordning gir økt utveksling av data. Kobling av datafangster utover innsamlingens formål.	Kontrollere muligheten for kobling av datafangster. Begrense anvendelsen av datafangster i informasjonstjenester.
	Dynamisk fergeinformasjon (Effektivitet og fremkommelighet)		

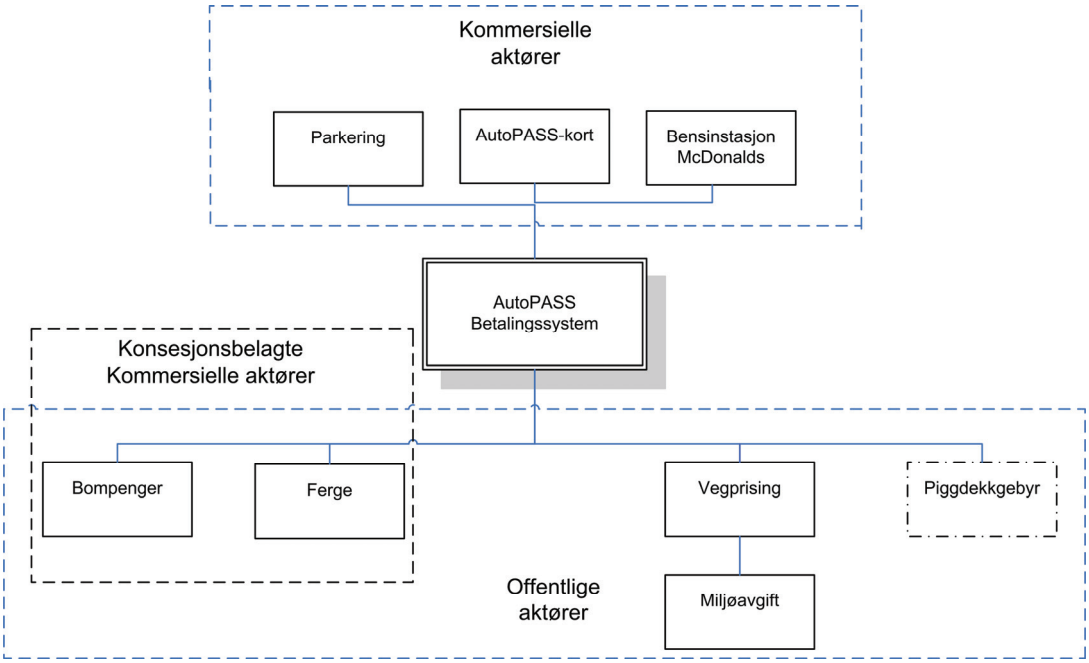
Tabell 7.1 Nye anvendelser tilknyttet AutoPASS anvendelsesområder

Tabellen viser hvilke transportmål anvendelsen er med på å oppfylle og hvilke utfordringer anvendelsene gir for personvernet. Siste kolonne ser kort på hvordan hensynet til personvern kan ivaretas, og vi ser at utfordringene for flere av anvendelsene samsvarer med problematikken representert i kontrollpunktene fra 7.1.1. Kontrollpunktene kan benyttes for å kontrollere at personvernet tas tilstrekkelig hensyn til for utvidelsen av AutoPASS.

7.2.1 Anvendelsesområder og datafangster

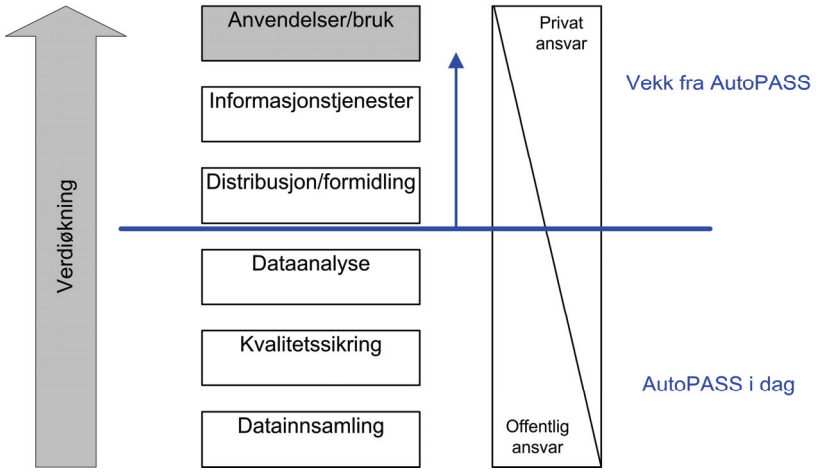
AutoPASS betalingssystem kan samle inn data for betaling av bompengeavgift, fergebillett, miljøavgift på bakgrunn av et vegprisingsystem og vegprising som en egen anvendelse. Realisering av et AutoPASS-kort muliggjør datafangster fra enda flere tjenester, inkludert kollektivtransport, og vil på samme måte som med parkering og andre kommersielle tjenester åpne opp for flere private aktører. Figur 7.1 viser at datafangstene kan benyttes for å tilby betalingstjenester av både kommersielle og offentlige aktører. Det er ikke sagt at alle anvendelsene vil tilbys som en del av AutoPASS, selv om muligheten er tilstede. Belastningen på betalingssystemet kan potensielt bli ganske stor, og det kan stilles spørsmål om AutoPASS er robust nok til å takle et slikt omfang av tjenester. Teknologien kan sette begrensninger for antall tjenester det er praktisk å legge til systemet. En økning i antall tjenester vil medføre en økning i antall transaksjoner. Dersom tjenestene er avhengige av at flere transaksjoner gjøres på selve brikken vil belastningen på brikken gå opp. Med tanke på etterbehandling av innsamlede data vil ikke kapasiteten være et problem.

Betaling av piggdekkgebyr er en tjeneste tenkt utviklet med RFID-teknologi, og er tatt med i figur 7.1 for å vise at den også er mulig å inkludere i AutoPASS betalingssystem.



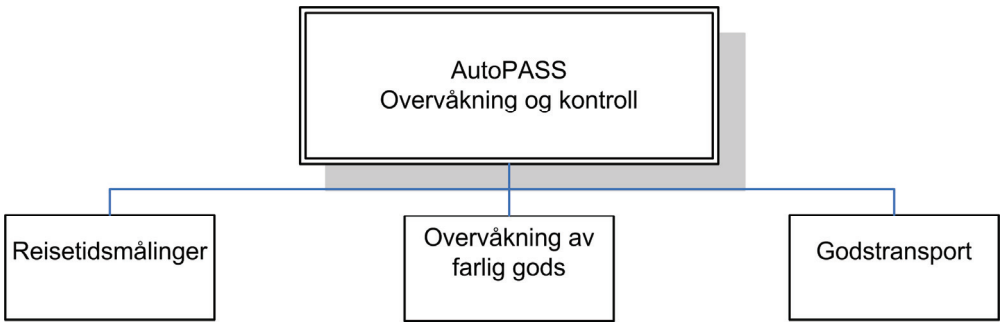
Figur 7.1 Datafangster for AutoPASS betalingssystem

AutoPASS involverer gjennom sitt betalingssystem hele verdikjeden i kapittel 4.2.3, og verdikjeden er vist i figur 7.2 med noen ekstra markeringer. For datafangster som faller inn under offentlig ansvarsområde vil situasjonen for AutoPASS være som i dag, mens inkludering av kommersielle tjenester gjør at systemet beveger seg mot toppen av verdikjeden. For slike anvendelser kan økonomiske hensikter spille en større rolle med tanke på at verdien av dataene øker jo lengre opp i verdikjeden man kommer. Flere tjenester og involvering av private aktører gjør at systemet beveger seg lengre unna den funksjonaliteten AutoPASS har i dag.



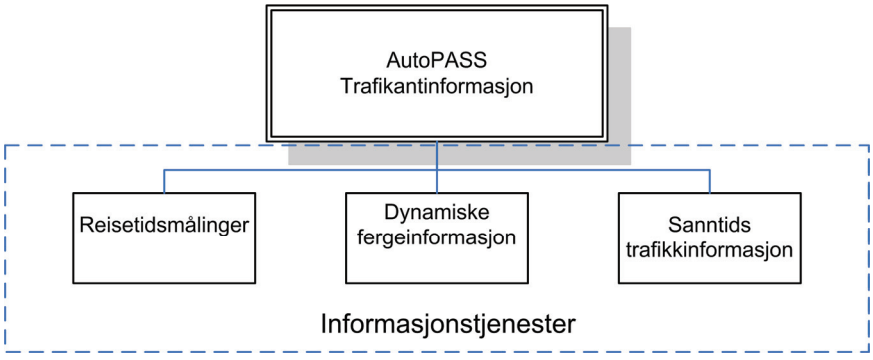
Figur 7.2 Verdikjeden fra kapittel 4.2.3 med markeringer

De fleste tjenestene vi har sett på i oppgaven faller inn under anvendelsesområdet betalingssystem, og AutoPASS betalingssystem kan bli meget omfattende. Innenfor områdene overvåkning og kontroll og trafikantinformasjon er omfanget noe mindre. Datafangster innen overvåkning og kontroll muliggjør grundige trafikkanalyser som kan bedre trafikkavviklingen. Innsamling av data fra godstransport kan gi et tilfredsstillende datagrunnlag ved planlegging og dimensjonering av veier og infrastruktur. Datagrunnlag fra reisetidsmålinger og overvåkning av farlig gods er også nyttig for overvåkning og kontroll, og disse anvendelsene er illustrert i figur 7.3.



Figur 7.3 Datafangster for AutoPASS overvåkning og kontroll

Siste anvendelsesområde er trafikantinformasjon, som også kan benytte datafangster fra reisetidsmålinger. Trafikantinformasjon representerer et utvalg informasjonstjenester som retter seg direkte mot brukerne. Vi har nå beveget oss noen trinn lengre opp i verdikjeden. Innsamling av data gjøres fremdeles gjennom AutoPASS-brikken, men dataene anvendes som grunnlag i informasjonstjenester, gjerne tilbudt av private aktører. Aktørene kan potensielt ta betalt for informasjonstjenestene, som et resultat av at tjenestene tilfører brukerne stor verdi. Figur 7.4 viser hvilke datafangster som kan danne grunnlaget for informasjonstjenester innen AutoPASS trafikantinformasjon.



Figur 7.4 Datafangster for AutoPASS trafikantinformasjon

Reisetidsmålinger karakteriseres som trafikkdata, og gir informasjon om forventet reisetid, kø eller forsinkelser på en vegstrekning. Dette er informasjon som brukerne kan finne nyttig i flere sammenhenger. Tjenester som tilbyr sanntids trafikkinformasjon kan benytte reisetidsmålinger sammen med data om andre forhold i trafikken. Dynamisk fergeinformasjon kan også i stor grad basere seg på et bearbeidet datagrunnlag fra reisetidsmålinger sammen med annen sanntids trafikkinformasjon. I mange tilfeller er datafangstene overlappende, og data samlet inn for et formål kan også være nyttig for et annet. I kapittel 4.1.2 så vi at innsamling av data fra et målepunkt potensielt kan brukes for å dekke flere behov for trafikkdata. Dette taler for en økt samordning av systemer og følgelig økte muligheter for kobling av datafangster.

7.2.2 Utfordringer ved utvidelse av AutoPASS

Hvor store utfordringer inkludering av flere tjenester i AutoPASS skaper for personvernet avhenger av hvor strenge kravene til databehandling er. Sammenlagt har vi i denne oppgaven sett at de største utfordringene ved en utvidelse av AutoPASS er økningen i antall registreringer av personers bevegelser, og muligheten for overvåkning og kartlegging. Dette utfordrer den personlige integriteten, og enkelte av tjenestene vi har sett på står i direkte konflikt med prinsippet om anonym ferdsel. Som vi så i kapittel 3.2.1 eksisterer det en kollektiv interesse om et begrenset overvåkningsnivå i samfunnet, og inkludering av et stort antall tjenester i AutoPASS vil utfordre denne interessen. Brukerne kan likevel se på utvidelsene som meget praktiske, spesielt for AutoPASS betalingssystem som forenkler betalingen av flere transporttjenester. Det er dermed ikke sagt at personverninteressene vil sette en stopper for slike utvidelser, men de vil heller legge retningslinjer for databehandlingen.

Kobling av datafangster

AutoPASS-systemet vil inkludere alle tre anvendelsesområdene vist i figur 7.1, 7.3 og 7.4. Muligheten til å koble datafangster innenfor et område og på tvers av områdene er tilstede. Innsamling av en datafangst gjøres i utgangspunktet for et bestemt formål, og en kobling mot en annen datafangst kan gi informasjon utover det opprinnelige formålet med datainnsamlingen. Registrering av alle bevegelser i transportsektoren, fra passering av bomstasjoner eller målepunkter for vegprising

til bruk av kollektivtransport, medfører kartlegging av brukernes reisemønster. Denne kartleggingen kan oppfattes som overvåkning, og på grunn av muligheten for misbruk av slik informasjon representerer kobling av datafangster en utfordring for personvernet. For alle datafangster som ikke skal knyttes til person kreves det som for reisetidsmålinger, at innsamlingene er anonyme. Dette gjelder innsamling av trafikkdata som skal benyttes for trafikkanalyser, og ikke som grunnlag i betalingstransaksjoner eller andre tjenester som krever kobling til person.

Et tettere oppsett av målepunkter, som i tillegg kan samle inn data for flere formål, vil utfordre personvernet dersom det ikke stilles konkrete krav til databehandlingen. Kravene må derfor i samsvar med kontrollpunkt 2 (i 7.2) ta hensyn til mulighetene for sammenkobling av innsamlede data, og være oppmerksom på at økt tetthet mellom målepunkter betyr flere registreringer og styrker potensialet for kartlegging.

Samarbeid

AutoPASS vil med nye tjenester involvere både offentlige og private aktører, og dette medfører økt samarbeid. For å kunne samarbeide kreves det en tydelig rolledeling mellom aktørene, noe som innebærer en avklaring av forhold rundt eierskap og organisering. Hvem har ansvaret for de ulike trinnene i verdikjeden? Hvordan sikres tilstrekkelig datakvalitet, og hvilke anvendelser av dataene er akseptable? AutoPASS er i dag forvaltet av Statens Vegvesen, og denne typen offentlig kontroll er med på å sikre tilstrekkelig kvalitet og informasjonssikkerhet for datafangstene som representerer grunnlaget i verdikjeden. Det offentlige ansvaret inkluderer trinnene frem til distribusjon, og fra dette punktet kommer private aktører mer og mer inn på banen (se figur 7.2). Data som samles inn gjennom AutoPASS kan benyttes i kommersielle tjenester og distribueres mellom flere aktører. Vi har sett at tjenestene ikke må være direkte knyttet til transportsektoren og de opprinnelige transportpolitiske målsetningene med AutoPASS. En oppklaring av forholdene rundt eierskap og organisering ved involvering av flere private aktører er viktig på et tidlig stadium av involveringsprosessen. Rolle og ansvarsfordeling er i dag spesifisert i et AutoPASS-avtaleverk som vi så i kapittel 2.3, og utvidelser av AutoPASS må inkluderes i avtaleverket. Krav til databehandling vil omfatte alle involverte aktører, og alle

må oppfylle kravene til informasjonssikkerhet for utveksling av data. I henhold til kontrollpunkt 3 i 7.2 vil kontrollen av informasjonstjenester kunne gjøres på basis av hvilke aktører som velges å inkluderes i samarbeidet.

Samordning

Samordning av betalingssystemer i transportsektoren medfører utveksling av data mellom flere aktører. I Norge legges det tilrette for samordning gjennom *Håndbok 206* som ble introdusert i kapittel 5.3, og alle elektroniske betalingssystemer i Norge skal bygge på denne. For AutoPASS betalingssystem stilles det krav til samordning gjennom nasjonale retningslinjer, og utvikling av rammeverk som ARKTRANS skal være med på å bedre samspillet mellom ulike ITS-systemer. *Håndbok 206* definerer samordning i tre ledd; teknisk, funksjonell og avtalemessig, og i alle leddene må personvernet tas hensyn til. Ved teknisk samordning kan personvernet tas hensyn til gjennom mekanismer for fysisk sikring av data. Funksjonell samordning fordrer lik behandling av dataene hos alle parter. Med tanke på at samordning medfører samarbeid mellom flere parter, vil en avtalemessig samordning være med på å avklare ansvarsforhold og rollefordeling, tilsvarende som i AutoPASS avtaleverk. Samordning av betalingssystemer er ikke bare en mulighet innad i Norge, og som vi så i kapittel 5.7 er arbeidet mot en samordning av bompengebetaling i Norden allerede i gang gjennom AutoPASS EasyGo. Neste trinn i utviklingen er en europeisk samordning, og samordning på tvers av landegrensene medfører registrering av bevegelser i et enda større geografisk område.

Utfordringene med samordning er knyttet til muligheten for kartlegging gjennom en økning i antall registreringer. Samordning av tjenester gjennom bruk av en felles avtale som AutoPASS Samordnet Betaling (ASB) som ble presentert i kapittel 5.1.2 medfører nettopp dette, gjennom at alle bevegelser registreres på samme sted og sammenfattes på én faktura. Deling av datafangster mellom flere aktører kan bety at personopplysninger vil behandles flere steder, og representerer også en utfordring for personvernet. Krav til behandling av data med tanke på samordning må utarbeides med utgangspunkt i å beskytte den personlige integriteten. Behandling av personopplysninger bør begrenses til å kun gjelde den behandlingsansvarlige aktøren, ikke alle involverte aktører i samordningen. På denne måten vil ikke opplysningene være like sårbare for spredning. Samordning

trenger dog ikke være mellom systemer som behandler personopplysninger, og innsamling av dynamiske data uten persontilknytning kan være nyttig for flere transportformål. Slike systemer krever at anonymiteten opprettholdes, og kravene til databehandling må ta hensyn til dette.

7.3 Personvern i praksis

Det største anvendelsesområdet for AutoPASS i dag er bompengebetaling. Anvendelsen ble gjennomgått i kapittel 5.1, etterfulgt av en diskusjon rundt hvordan dagens løsning tar hensyn til personvern i kapittel 5.2. Viktige personverntema ved dagens praksis for bompengebetaling omfatter personvernprinsippet om anonym ferdsel, lagringstid for passeringsopplysninger, muligheten for gjenbruk og konseptet én brikke per bil. Dette er tema som også er interessante når vi ser på eventuelle endringer i praksis ved en utvidelse av AutoPASS. Forskjellen mellom utfordringene for dagens AutoPASS og en utvidelse av AutoPASS, er det store omfanget av datafangster som kan tillegges systemet i fremtiden. Graden av kartlegging og overvåkning er i dag beskjeden i forhold til hva den kan bli. Som vi har sett er det nettopp en økning i registreringer av bevegelser som skaper utfordringer for personvernet ved en utvidelse av AutoPASS.

Anonym ferdsel

Det finnes ikke noe reelt anonymt alternativ for passering av automatiske bomstasjoner i dag, og den alternative avtalen er løsningen for de som ønsker å ferdes så sporfritt som mulig. Ved inkludering av andre tjenester enn bompengebetaling er det nødvendig å se på muligheten for tilsvarende alternative løsninger dersom anonymitet vanskelig lar seg gjøre. For å redusere omfanget av elektroniske spor brukeren legger igjen ved bruk av AutoPASS er dette et viktig utgangspunkt. For databehandling som ikke skal knyttes til personopplysninger vil anonyme løsninger kunne gjennomføres på tilsvarende måte som for reisetidsmålinger, gjennom bruk av den dynamiske loggen på AutoPASS-brikken.

Lagring og gjenbruk

I AutoPASS-systemet i dag stilles det krav til lagringstid for passeringsopplysninger, og dette er viktig med tanke på mulighetene for gjenbruk.

På dette området har det vært gjennomført en noe inkonsekvent praksis ved utlevering av opplysninger til andre enn behandlingsansvarlig i etterkant. Politiet har måttet gå gjennom retten for å få tilgang til opplysninger, mens Skatteetaten, som vi så i kapittel 5.2.1, har fått utlevert opplysninger fra bompengeselskaper ved direkte forespørsel. Dette er inkonsekvent, og er med på å svekke troverdigheten til AutoPASS med tanke på personvern. Konsekvente retningslinjer for slike situasjoner bør utarbeides, spesielt dersom systemet skal utvides til å inkludere flere datafangster og tjenester. Et utgangspunkt for retningslinjene bør være at tilgang til opplysninger, i samsvar med intensjonene i personopplysnings-forskriften, enten er autorisert eller tillatt gjennom rettslig kjennelse. Retningslinjene vil sette en stopper for tilslag på forespørsler som faller utenfor rettslig interesse, og de behandlingsansvarlige vil være sikrere på hvilke regler for bruk som gjelder. Dette gjelder ikke bare i sammenheng med utlevering av opplysninger til myndighetene. Opplysningene kan være nyttige for private aktører, eksempelvis innen godstransport kan transportører være meget interessert i konkurrentenes ferdsel i vegnettet for å avdekke hvilket marked de opererer innenfor. Utlevering av slike opplysninger vil svekke tilliten til systemet.

Ønsket om sporfrihet kan medføre strengere krav til hvilke dynamiske data som lagres på brikken, da disse potensielt kan misbrukes for å overvåke reisemønster og kartlegge hvilke målingspunkter brikken har passert. Det kan innføres begrensninger for hvilke dynamiske data som lagres på AutoPASS-brikken dersom dataene ikke er tilstrekkelig sikret. For å unngå utilsiktet tilgang til de dynamiske loggene på brikken må det innføres gode mekanismer for å beskytte informasjonen mot uautorisert adgang og observasjoner utenfor systemet, og det må ikke kunne stilles tvil om at mekanismene er tilstrekkelige. Gjennom slike mekanismer vil også tilliten til systemet fra brukerne øke. Flere av anvendelsene vi har sett på benytter seg av dynamiske logger på brikken, og dette er derfor meget viktig for at anvendelsene skal kunne realiseres.

Èn brikke per kjøretøy

Med utgangspunkt i europeisk utvikling ser det ut til at kjøretøy vil pålegges bruk av AutoPASS-brikke i fremtiden. Resultatet vil være en økning i antall registreringer og større mulighet for kartlegging. Personvernsinteressene som taler for å hindre enveiskobling mellom brikke og kjøretøy blir nedprioritert for

nytteverdien av en slik kobling. Dette gjør det enda vanskeligere å opprettholde muligheten for anonym ferdsel på norske veier i fremtiden. Et nødvendig krav for å kunne realisere løsninger som innsamling av miljøavgift og overvåking av farlig gods og annen godstransport, er nettopp et slikt pålegg om bruk av brikke. I dette tilfellet trenger ikke anvendelsene å involvere behandling av personopplysinger, og en slik praksis vil ikke utfordre personvernet på samme måte som i andre anvendelser.

Overvåkningssamfunnet

Et samfunn preget av overvåkning og kontroll av borgerne er skrekkscenariet når man snakker om en økning av antall tjenester som innebærer registrering av persondata og som medfører gjenlegging av elektroniske spor. For å unngå at dette blir den nye virkeligheten må det sørges for at tilrettelegging av tjenester i AutoPASS-systemet ikke åpner opp for overvåkning og misbruk. Dette kan sikres gjennom krav til databehandling, og begrensninger for databehandlingen ligger som vi har sett i behandling av personopplysninger. Hensynet til personvern bør inkluderes i kravene allerede når de utarbeides, og på denne måten blir personvernet tatt vare på fra første stund. Når en ny tjeneste inkluderes i AutoPASS er kontrollpunktene vi så på i 7.1.1 nyttige for å vurdere utvidelsen henhold til hvilke utfordringer den skaper for personvernet. Kobling av datafangster, samarbeid og samordning skaper som vi har sett nettopp slike utfordringer, og sammenlagt må praksis for behandling av data fokusere på flere områder for å ta tilstrekkelig hensyn til personvernet.

Fokus på personvern

Vi har sett at nye anvendelser av AutoPASS og innføring av nye tjenester som behandler personopplysninger må kreves implementert slik at hensynet til personvern ivaretas. Bevisstheten rundt personvernproblematikk må økes både hos de som utvikler tjenester og anvendelser, og hos brukerne. For brukerne er det viktig at de er bevisste på hvilke tjenester de velger å benytte med tanke på hvilke personvernutfordringer tjenestene skaper for dem. Brukerne kan gjennom sin forbrukermakt være med på å bestemme hvilke anvendelser de synes er akseptable.

Offentlige tilsynsmyndigheter (som Datatilsynet) har ansvaret for at personvernet

ivaretas, og i offentlige skriv må det rettes fokus mot hvordan dette kan gjøres. Tydelige retningslinjer fra det offentlige som beskriver hvordan personopplysninger kan skjermes og integriteten bevares, kan oppklare uklarheter i henhold til databehandling. Under utvikling av ny teknologi og nye tjenester bør Datatilsynet involveres tidlig i prosessen, da de er retningsgivende organ for oppfølgingen av personvern i Norge. Jeg ser at det er mye som kan gjøres for å rette fokus mot personvern i Norge, og det er viktig at dette gjøres allerede nå. Dette gjelder ikke bare med tanke på AutoPASS, men også andre tjenester i transportsektoren og i andre samfunnssektorer. For AutoPASS bør strategi og planer for fremtiden inneholde krav til databehandling som tar hensyn til personvernet, på bakgrunn av de utfordringene jeg har sett på i denne oppgaven.

8 Konklusjon

I denne oppgaven har jeg sett på både eksisterende og nye anvendelser av AutoPASS. Mulighetene viser seg å være mange, og anvendelsene kan være med på å fremme effektivitet og sikkerhet i trafikken, samt minke belastningen som trafikken påfører miljøet. Samtidig som anvendelsene kan gi store gevinster, medfører de en økning av registreringer av brukernes bevegelser i transportsektoren. Dette skaper utfordringer for personvernet gjennom muligheten for detaljert kartlegging av brukernes reisemønster, og vi har sett at økt overvåkning og misbruk av innsamlede data er potensielle farer ved utvidelser av AutoPASS.

Det er ikke alle anvendelsene som krever behandling av personopplysninger. Innsamling av dynamiske data for analyseformål kan gi store fordeler i transportsektoren, men fordrer i mange tilfeller anonymitet. Gjennom bruk av den dynamiske loggen på AutoPASS-brikken er det mulig å gjennomføre anonyme datainnsamlinger. Løsningen er realisert for reisetidsmålinger i dag, og kan benyttes i fremtidige anvendelser som ikke krever kobling til kjøretøy. Det kan også velges å lese brikke-ID sammen med dynamiske data lagret på brikken, og for anvendelser som vegprising og innkreving av miljøavgift er dette nødvendig for å kunne gjennomføre betalingstransaksjoner. Overvåkning av farlig gods kan realiseres uten å lese brikke-ID, og overvåkningssystemet vil gi en oversikt over farlig gods som befinner seg i vegnettet. Data samlet inn fra godstransport for planleggingsformål krever ikke kobling til kjøretøy, og skaper et stort forbedringspotensial for areal og transportplanlegging som mangler et tilstrekkelig datagrunnlag i dag. Trafikkdata samlet inn fra AutoPASS kan også benyttes for å tilby trafikantene sanntids trafikkinformasjon gjennom ulike informasjonstjenester. Innenfor anvendelsesområdene trafikantinformasjon, overvåkning og kontroll og betalingssystem er mulighetene for utvidelser av AutoPASS mange. Det er AutoPASS betalingssystem som ser ut til å ville belastes mest, og samtidig skape de største utfordringene for personvernet. Betalingssystemet inkluderer eksisterende og utprøvde anvendelser som bompengebetaling, fergebetaling og parkering, og alle krever behandling av personopplysninger.

Vi har sett at både eksisterende og nye anvendelsesområder beveger seg mot en økning i samordning, både nasjonalt og internasjonalt. Flere av datafangstene kan benyttes for flere formål, og legger dermed tilrette for samordning mellom ulike anvendelser. Samtidig øker muligheten for kobling av datafangster på bakgrunn av økningen i dataomfanget, og dette skaper nye utfordringer for personvernet. Kobling av datafangster kan utnyttes for å fremskaffe informasjon utover formålet med den enkelte datafangst. Samordning involverer også flere aktører, og legger tilrette for økt samarbeid. Dette krever en oppklaring i ansvarsforhold mellom involverte aktørene. Utvidelser av AutoPASS ser ut til å kunne inkludere flere private aktører i fremtiden, og legger tilrette for flere kommersielle anvendelser. Nye informasjonstjenester kan i strid med personvernet benytte seg av kartlegging for å tilby personifiserte tjenester. For nye informasjonstjenester vil dermed kontrollen i henhold til personvern være avgjørende for hvilke av tjenestene som vil realiseres.

Økt fokus på personvern og hvilke juridiske rammer som allerede finnes for behandling av personopplysninger i informasjonssystemer som AutoPASS, gjør at nye anvendelser kan utvikles med hensyn til personvern. Erfaringer fra eksisterende og utprøvde anvendelser viser hvilke personvernutfordringer AutoPASS står ovenfor i dag, og erfaringene bør utnyttes under utviklingen av nye anvendelser. Personvernet kan videre sikres gjennom krav til behandling av data. Kravene må utarbeides med utgangspunkt i retningslinjene som allerede finnes i lovgivning, samtidig som de tar hensyn til mulighetene for kobling av datafangster og spredning av opplysninger gjennom en utvidelse av anvendelsesområdene.

8.1 Videre arbeid

Denne oppgaven er begrenset av både tid og omfang, og jeg har derfor vært nødt til å gjøre noen avgrensninger av innholdet. Dette betyr ikke at områdene jeg har utelatt fra studien ikke er viktige å se nærmere på, tvert i mot er det flere av dem som kan undersøkes videre.

Anonymiseringsteknologi og sikkerhetsmekanismer

Jeg har i denne oppgaven sett på hvilke utfordringer personvernet skaper for eksisterende og nye anvendelser av AutoPASS. I denne sammenheng kunne det

vært interessant å ha sett mer spesifikt på teknologier som fremmer personvern og anonymitet. For videre studier av AutoPASS vil det være nødvendig å vurdere hvilke ulike anonymiseringsteknologier og sikkerhetsmekanismer som kan bidra til å sikre personvernet ved en utvidelse av systemet. Jeg har kun sett på én mulig løsning for anonymisering gjennom praksis for reisetidsmålinger, men en studie av alternative løsninger hadde også vært nyttig.

Ansvarsfordeling

Vi har sett at involvering av flere aktører i AutoPASS åpner opp for en diskusjon rundt ansvarsfordeling mellom offentlige og private aktører. Bakgrunn for diskusjonen er spørsmålet om eierskap og organisering av datafangster i AutoPASS, dersom systemet åpnes opp for flere aktører. En avklaring rundt denne problematikken kan legge til rette for samordning og samarbeid i fremtiden.

Kommersielle aktører og interesseavveining

Vi har sett at verdien av data øker jo lengre opp i verdikjeden dataene beveger seg, og det kan dermed ligge kommersielle motiv bak utvikling av anvendelser og informasjonstjenester. I hvilken grad økonomi vil påvirke utviklingen av AutoPASS er et interessant område for videre arbeid. Kommersielle interesser kan i denne sammenheng havne i konflikt med personverninteresse. Hvilke interesser som blir tatt hensyn til, er avhengig av praksis for interesseavveining. Personvernloven håndheves i dag med bruk av skjønn, og tydeligere retningslinjer for avveininger mellom personvern og andre interesser kan derfor være nyttig å utarbeide så fremt det er mulig.

Målepunkter

Flere av anvendelsene jeg har sett på i oppgaven krever oppsett av flere målepunkter. Hvordan disse målepunktene bør plasseres for å danne en effektiv infrastruktur for datainnsamling kan studeres videre. Spesielt er dette interessant med tanke på hvordan AutoPASS kan gi et tilstrekkelig godt datagrunnlag i areal og transportplanlegging, og hvordan vegprising kan benyttes for å skape et praktisk hovedvegsystem for å avlaste utsatte områder.

AutoPASS-kort

Hvorvidt AutoPASS-kortet er en reell konkurrent til eksisterende betalingskort er et interessant spørsmål som kan undersøkes videre. I denne forbindelse kan

AutoPASS-kortet vurderes opp mot alternative løsninger basert på allerede eksisterende teknologi. Undersøker i henhold til brukerbehov kan gi nyttig input om hvilke forventninger brukere har til et slikt kort, og om de vil benytte seg av det.

9 Referanser

Amdal, E. (2006). *Status ferjebillettering*. Lastet ned 22.04.07, fra http://www.its-norway.com/default.asp?FILE=items/771/120/Amdal-Fergebillettering.pdf

AutoPASS (2003). Systembeskrivelse for AutoPASS – Samordnet betaling (ASB). Lastet ned 01.03.07, fra http://www.autopass.no/profil/autopass_okt03/Systembeskrivelse.pdf

AutoPASS (2007a). Sist besøkt 22.05.07, http://www.autopass.no

AutoPASS (2007b). *Bompenger i Norge*. Lastet ned 01.03.07, fra http://www.autopass.no/bompenger_norge.stm

AutoPASS (2007c). *Generelle bestemmelser - AutoPASS-avtalen*. Lastet ned 01.03.07, fra http://www.autopass.no/pdf/AutoPASS_GenAvtalebet.pdf

AutoPASS (2007d). *AutoPASS Fosen*. Lastet ned 22.04.07, fra http://www.autopass.no/autopass_ferje/autopass_fosen.stm

AutoPASS (2007e). *AutoPASS parkering*. Lastet ned 22.04.07, fra http://www.autopass.no/autopass_veg/parkering.stm

AutoPASS (2007f). *En ny generasjon brikketeknologi*. Lastet ned 26.02.07, fra http://www.autopass.no/om_autopass/brikketeknologi.stm

AutoPASS (2007g). *Brikkebytte 2007*. Lastet ned 01.03.07, fra http://autopass.no/om_autopass/brikkebytte.stm

Bang, B. & Wahl, R. (2007). *ITS – IKT i transportsektoren*. SINTEF rapport TF50 A07010. Lastet ned 02.03.07, fra http://www.sintef.no/upload/Teknologi_og_samfunn/Veg%20og%20samferdsel/Rapporter/A07010_ITS%20-%20IKT%20i%20transportsektoren.pdf

Dalland, O. (1993). *Metode og oppgaveskriving for studenter*. Oslo: Universitetsforlaget.

Dataforeningen (2007). *Faggruppen for informasjonssikkerhet*. Lastet ned 23.05.07, fra http://dataforeningen.no/?module=Articles;action=ArticleFolder.publicOpenFolder;ID=912

Datatilsynet (2007a). *Personvernrapporten 2007*. Lastet ned 21.04.07, fra http://www.datatilsynet.no/upload/Dokumenter/publikasjoner/aarsmeld/personvernrapport_liten.pdf

Datatilsynet (2007b). *Datatilsynets oppgaver*. Lastet ned 16.04.07, fra http://www.datatilsynet.no/templates/Page____954.aspx

DSB (2005). *Informasjon om farlig gods – Merking*. Lastet ned 01.05.07, fra http://www.dsb.no/File.asp?File=Publikasjoner/faresedler2005.pdf&Framework=normalt

DSB (2007). *Transport av farlig gods*. Lastet ned 01.05.07, fra http://www.dsb.no/infogroup.asp?infogroupID=1012&Rightmenu=H_Transport_farliggods

EasyGo (2007). *EasyGo – Om tjenesten*. Lastet ned 01.03.07, fra http://70.86.111.194/~easygo/index.php?option=com_content&task=view&id=20&Itemid=35

Engesvik, G. (2007, 27. februar). Her vil futen snoke. *Aftenposten*. Lastet ned 23.05.07, fra http://www.aftenposten.no/nyheter/iriks/article1661069.ece

FAD (2000). *Forskrift om behandling av personopplysninger (personopplysningsforskriften). (*FOR-2000-12-13-1265). Lastet ned 23.05.07, fra http://lovdata.no/for/sf/fa/fa-20001215-1265.html

FAD (2006). *Eit informasjonssamfunn for alle*. (St.meld. nr. 17 (2006-2007)). Lastet ned 16.04.07, fra http://www.regjeringen.no/Rpub/STM/20062007/017/PDFS/STM200620070017000DDDPDFS.pdf

FAD (2007). *Personvern*. Lastet ned 16.04.07, fra http://www.regjeringen.no/nb/dep/fad/Tema/personvern/Hva-er-personvern.html?id=448290

Finklenzeller, K. (2003). *RFID handbook: fundamentals and applications in contactless smart cards and identification* (2. utgave). Chichester, England Hoboken, N.J.: Wiley

Foss, Trond (2005). *Systembeskrivelse AutoPASS Ferge*. Lastet ned 22.04.07, fra http://www.sf-f.kommune.no/sff/k2pub.nsf/viewAttachments/C1256B3B0048DA1DC1257006003B3534?OpenDocument&frame=yes

Furan, S. (2007). Informant fra Q-Free. Kontakt via e-post og møte den 14.03.07.

Hansen, M. (2005). *NorITS – skandinavisk interoperabilitet*. Norvegkonferansen 2005, Sarpsborg. Lastet ned 27.04.07, fra http://www.norvegkonferansen.com/nedlast/Norvegkonferansen%20NORITS%20-%20Skandinavisk%20interoperabilitet%20.ppt

Haugen, Torbjørn (2005). *Evaluation of a travel time information system*. Lastet ned 26.04.07, fra http://www.sintef.no/upload/SystemEvaluation_Paper.pdf

IBM (2006). *Overview of Radio Frequency Identification*. (IBM Redbook). Lastet ned 26.02.07, fra http://www.redbooks.ibm.com/redbooks/pdfs/sg247147.pdf

IEEE (2007). *Dedicated Short Range Communication*. Lastet ned 02.03.07, fra http://grouper.ieee.org/groups/scc32/dsrc/index.html

ISO (2003). *Road Transport and Traffic Telematics – Electronic Fee Collection (EFC) – Systems architecture for vehicle related transport services.* (ISO/TS 17573).

ISO (2004a). *Road Transport and Traffic Telematics – Electronic Fee Collection - Application interface for DSRC.* (ISO 14906).

ISO (2004b). *The CALM handbook.* (ISO TC204 – ETSI ERM TG37).

JD (2000). *Lov om behandling av personopplysninger (personopplysningsloven).* (LOV-2000-04-14-31). Lastet ned 01.02.07 fra http://lovdata.no/all/nl-20000414-031.html

JD (1997). *Et bedre personvern – forslag til lov om behandling av personopplysninger.*(NOU 1997: 19). Lastet ned 15.02.07, fra http://www.regjeringen.no/Rpub/NOU/19971997/019/PDFA/NOU199719970019000DDDPDFA.pdf

Jonassen, Arild M. (2006, 15. april). Ønsker brikke i alle biler. *Aftenposten.* Lastet ned 26.02.07, fra http://www.aftenposten.no/nyheter/iriks/article1275237.ece

Kunnskapsforlaget (2007). Sist besøkt 01.05.07, www.ordnett.no

Nyre, Å. (2007). Informant fra Q-Free. Kontakt via e-post.

Personvernnemda (2005). *PVN-2005-11: Klage på vedtak om pålegg om konsesjonsplikt for helautomatiske bomstasjoner.* Lastet ned 01.03.07, fra http://www.personvernnemnda.no/vedtak/2005_11.htm

Personvernnemda (2007). *Personvernnemda.* Lastet ned 16.04.07, fra http://www.personvernnemda.no/index

RFID Journal (2007a). *What is RFID? RFID (Radio Frequency Identification) Technology news & Features.* Lastet ned 26.02.07, fra http://www.rfidjournal.com/article/articleview/1339/1/129/

RFID Journal (2007b). *FAQ, RFID Tags.* Lastet ned 26.02.07, fra http://www.rfidjournal.com/faq/18/68

RFID Journal (2007c). *The basics of RFID technology.* Lastet ned 26.02.07, fra http://www.rfidjournal.com/article/articleview/1337/1/129/

SD (2002). *Fra A til B...Bedre, tryggere og mer effektiv transport- med IKT.* Lastet ned 01.03.07, fra http://www.regjeringen.no/upload/kilde/sd/bro/2002/0005/ddd/pdfv/149264-ikt_i_transportsektoren.pdf

SD (2004). *Nasjonal Transportplan 2006-2015*. (St. mld. Nr. 24). Lastet ned 01.03.07, fra http://www.regjeringen.no/Rpub/STM/20032004/024/PDFS/STM200320040024000DDDPDFS.pdf

SD (2005). *Om ein del saker på Samferdselsdepartementets område.* (St.prp. nr. 64 (2004-2005)). Lastet ned 21.04.07, fra http://www.vegvesen.no/region_ost/prosjekter/rv2/rapporter/stprp64.pdf

SD (2006). *Om ein del saker på Samferdselsdepartementets område. (*St.prp. nr. 65 (2005-2006)). Lastet ned 22.04.07, fra http://www.regjeringen.no/Rpub/STP/20052006/065/PDFS/STP200520060065000DDDPDFS.pdf

Schartum, D.W. & Bygrave, L.A. (2004). *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger*. Bergen: Fagbokforlaget.

Skadsheim, A. (2003). *National road user charging in Norway.* Lastet ned 17.04.07, fra http://vianovatransit.no/oldweb/Presentation%20London%20March%202003.pdf

Skadsheim, A. (2006). *Innfartsparkering i Asker*. Seminar om elektroniske billetteringssystemer 12.09.06. Lastet ned 17.04.07, fra http://www.vianovatransit.no/pdf/AskerPark&RideSeptember2006.pdf

Sun (2007). *Smart Card Overview*. Lastet ned 08.06.07, fra http://java.sun.com/products/javacard/smartcards.html

SV (2001). *Fellessystem for dynamiske data – mulighetsstudie.* Lastet ned 02.03.07, fra http://www.vegvesen.no/its_pa_veg/Fellessyst_dynamiske_data/FSDD_Mulighetsstudie.pdf

SV (2004). *Elektronisk billettering.* (Håndbok 206-1). Lastet ned 26.04.07, fra http://www.vegvesen.no/vegnormaler/hb/206/handbok206-1_v8_2004-03-26.pdf

SV (2006a). *Nasjonal transportplan 2010-2019. ITS – Intelligente transport systemer. Overblikk, visjon og mulighetsområder.* Lastet ned 01.03.07, fra http://www.itsnorway.no/default.asp?FILE=items/820/120/20061222_its_overblikk_visjon_mulighet.pdf

SV (2006b). *Målrettet, troverdig og effektiv bruk av ITS på veg mot et bedre samfunn. ITS-strategi for Statens Vegvesen*. (Høringsutkast)

SV (2007a). *Bompenger*. Lastet ned 14.02.2007, fra http://www.vegvesen.no/servlet/Satellite?cid=1046077049608&pagename=vegvesen%2FPage%2FSVVsubSideInnholdMal&c=Page

SV(2007b). *Vegen og vi*. Nr. 5/07, 15. mars, 6. årgang. Lastet ned 23.04.07, fra http://www.vegvesen.no/vegenogvi/05_07/skjerm/05_2007.pdf

Teknologirådet (2005). *Teknologier som setter spor*. Lastet ned den 17.04.07, fra http://www.teknologiradet.no/FullStory.aspx?m=104&amid=487

Teknologirådet (2007). *Notat om personvern i samferdselssektoren*. Lastet ned 17.04.07, fra http://www.teknologiradet.no/Høring_om_personvern_i_samferdselssektoren_VO05W.pdf.file

Thagaard, T. (2002). *Systematikk og innlevelse - en innføring i kvalitativ metode* (Vol. 2. utgave). Bergen: Fagbokforlaget.

Trondsen, J. (2004). *AutoPASS – Bruk av infrastrukturen og fremtidsmuligheter*. ITS-konferansen Gardermoen 29.09.04. Lastet ned 16.04.07 , fra http://www.its-norway.com/default.asp?FILE=items/361/120/Autopass%20og%20fremtiden.pdf

Trondsen, J. (2006a). *Elektronisk billettering – Håndbok 206*. Seminar ITS Norway 12.09.06. Lastet ned 16.02.07, fra http://www.its-norway.com/default.asp?FILE=items/771/120/Trondsen-HB206.pdf

Trondsen, J. (2006b). *Elektronisk betaling og billettering – Norsk og internasjonal utvikling*. Norvegkonferansen Ålesund 2006. Lastet ned 17.02.07, fra http://www.norvegkonferansen.com/nedlast/Elektronisk%20betaling%20og%20billettering%20-%20Jacob%20Trondsen,%20Vegdirektoratet.pdf

TØI (2000). *A5 Vegprising. –A, Tiltak som påvirker transportomfang og transportmiddelfordeling : Miljøhåndboken*. Lastet ned 18.04.07 fra http://miljo.toi.no/index.html?25800

TØI (2004a). *Makt, Beslutning og Integritet – IKT og personvern i transport*. (TØI rapport 703/2004). Lastet ned 01.03.07, fra http://www.toi.no/getfile.php/Publikasjoner/T%D8I%20rapporter/2004/703-2004/703-2004.pdf

TØI (2004b). *Personvern og forbrukerrettigheter i transport*. Nordisk seminar. (TØI rapport 745/2004). Lastet ned 01.03.07, fra http://www.toi.no/getfile.php/Publikasjoner/T%D8I%20rapporter/2004/745-2004/745-2004.pdf

Vermesan, O. , Taylor, S., Myhre, B., Skjeggestad, V. & Jensen, G. U. (2005). *RFID – Teknologi for et trådløst samfunn*. Elektronikk 6-2005. Lastet ned 25.02.07, fra http://www.sintef.no/upload/IKT/9022/Elektronikk_2005-06_32-35.pdf

Wahl, R., Flø, M., Haugen, T., Bang, B. & Lillestøl, P.J. (2003). *Dynamisk transportinformasjon – Kunnskapsstatus*. STF22 A03305. Lastet ned 26.04.07, fra http://www.sintef.no/upload/A03305_Dynamisk%20transportinformasjon.pdf

Wahl, R. & Skjetne, E. (2005). *Organisering og eierskap til trafikkdata.* SINTEF rapport STF A05090. Lastet ned 26.04.07, fra http://www.sintef.no/upload/A05090_Rapport%20organisering%20og%20eierskap.pdf

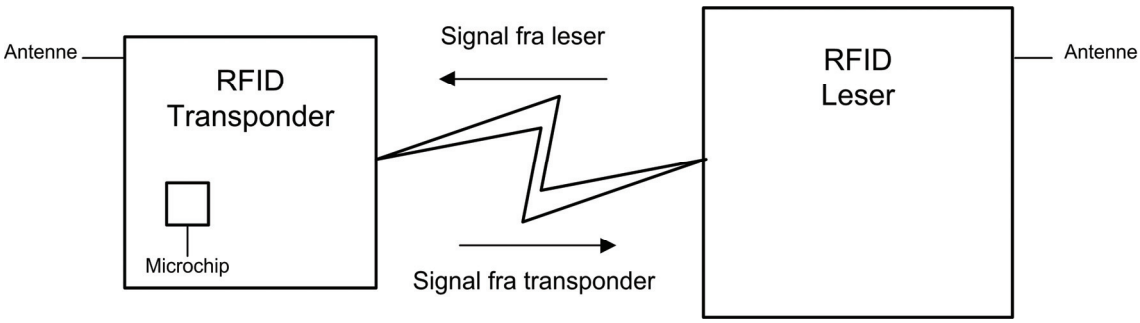
Wahl, R., Haugen, T. & Lillestøl, P.J. (2006). *DynamIT – Dynamiske Informasjonstjenester for Transportsektoren.* SINTEF Rapport STF A05230. Lastet ned 02.03.07, fra http://www.sintef.no/upload/A05230_DynamIT_Sluttrapport.pdf

Wærsted, K. (2007). Informant fra Vegdirektoratet. Møte den 27.03.07.

Appendiks A : RFID

A.1 Virkemåte

Et RFID-system består alltid av to komponenter; en RFID-transponder og en RFID-leser. Transponderen er festet til objektet som skal identifiseres, eksempelvis i en AutoPASS-brikke festet til en bil, og her lagres informasjon om objektet. For å lese denne informasjonen fra transponderen trengs det en leser. Avhengig av design og teknologien som brukes, kan denne enten bare lese fra transponderen, eller både lese og skrive til den. (Finkenzeller 2003)

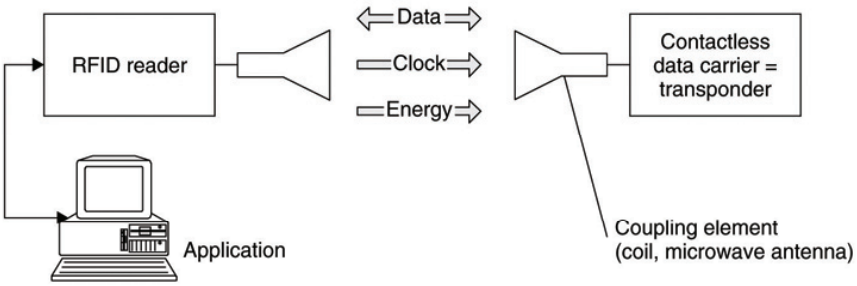


Figur A.1 Hovedkomponentene i RFID-systemer; Transponder og Leser

En typisk RFID-transponder består av en microchip koblet til en antenne, mens en typisk RFID-leser består av en eller flere antenner som sender ut radiobølger og mottar signaler fra RFID-transponderen (se figur A.1). Prinsippet bak RFID-systemene er dermed at man plasserer en transponder, en microchip med antenne, på eksempelvis en bil, og bruker en leser for å lese data fra microchipen ved bruk av radiobølger. Leseren sender deretter videre informasjonen hentet fra transponderen i digital form til et datasystem, slik at disse dataene kan benyttes for å skape forretningsverdi. Et eksempel er betaling av bompenger, enten gjennom forhåndbetaling eller fakturering i etterkant av passering av en bomstasjon. (RFID Journal 2007a)

Figur A.2 viser prinsippet bak et RFID system og kommunikasjonen mellom hovedkomponentene. Klokkepuls, energi og data sendes mellom leser og transponder, og leseren er videre koblet til en applikasjon, datasystemet som

behandler mottatt data. Klokkepulsen brukes for synkronisering av leser og transponder.



Figur A.2 Overføring av data i et RFID-system (Finkenzeller 2003:7)

A.2 Aktive og passive RFID-transpondere

Det finnes flere ulike RFID-teknologier, og en faktor som skiller ulike systemer fra hverandre er strømtilførsel til transponderen. Passive RFID-transpondere har ikke egen strømtilførsel, men får strøm fra RFID-leseren. Leseren sender ut elektromagnetiske bølger, som igjen induserer en strøm i antennen på transponderen. Aktive RFID-transpondere har derimot egen strømtilførsel, vanligvis et batteri, som tilfører all eller deler av strømmen som trengs til transponderen (Finkenzeller 2003). Semi-passive transpondere bruker batteri for å "kjøre" microchipens kretssystem, mens de kommuniserer ved å trekke strøm fra leseren. Aktive og semi-passive transpondere er nyttige for å spore verdifulle objekter over lengre avstander, men koster mer en passive transpondere som derfor er nyttige for identifisering av lav-kost objekter. (RFID Journal 2007b)

A.3 Frekvens og rekkevidde

En annen viktig karakteristikk på ulike RFID-systemer er frekvensen de operer på, og da rekkevidden til systemet. *"Operasjonsfrekvensen til et RFID-system er frekvensen som leseren sender på"* (Finkenzeller 2003:13). De ulike operasjonsfrekvensene er videre delt inn i klasser:

- Lav frekvens, LF (30-300 kHz)
- Høy frekvens, HF (3-30 MHz)
- Ultrahøy frekvens, UHF (300 MHz – 3 GHz)
- Mikrobølge (>3 GHz)

RFID-systemene kan også skilles fra hverandre med tanke på hvilken avstand transponderen kan lese fra. I henhold til frekvensbåndet som benyttes skilles det mellom:

- nærlesning (0-1cm)
- fjernlesning (0-1m)
- langdistanse lesning (>1m)

Radiobølgene oppfører seg ulikt på ulike frekvenser, og riktig frekvens må derfor velges ut i fra hva systemet skal benyttes til. (RFID Journal 2007a) Rekkevidden for en anvendelse avhenger av flere ting (Finkenzeller 2003:26):

- nøyaktighet ved posisjonering av transponder
- minimumsavstand mellom transpondere i praktisk operasjon
- farten til transponderen i sonen der leseren opererer

A.4 RFID og AutoPASS

Aktive RFID systemer er vanlig å bruke for sporing av objekter over lange avtander, og opererer ofte på 455 MHz, 2.45 GHz eller 5.8 GHZ. Leseavstanden for aktive RFID-systemer er gjerne mellom 20 og 100 meter, og de faller dermed inn under gruppen for langdistanse leseavstand (RFID Journal 2007c). AutoPASS kan klassifiseres som et aktivt RFID-system, og opererer på frekvensbåndet 5.8 GHz (AutoPASS 2007f). AutoPASS-brikken er en aktiv transponder, og er tilkoblet et batteri for strømtilførsel. Det gjennomføres i løpet av 2007 derfor en utbytting av alle AutoPASS-brikker som er fem år eller eldre, som følge av at batteriene begynner å bli tomme (AutoPASS 2007g).