

19



Bureau voor de  
Industriële Eigendom  
Nederland

11 1011501

12 C OCTROOI<sup>20</sup>

21 Aanvraag om octrooi: 1011501

51 Int.Cl.<sup>7</sup>  
G08G1/01, G08G1/09

22 Ingediend: 09.03.1999

41 Ingeschreven:  
12.09.2000

73 Octrooihouder(s):  
Wiebren de Jonge te Almere-Stad.

47 Dagtekening:  
12.09.2000

72 Uitvinder(s):  
Wiebren de Jonge te Almere-Stad

45 Uitgegeven:  
01.11.2000 I.E. 2000/11

74 Gemachtigde:  
Drs. A.J.W. Hooiveld c.s. te 2517 GK Den Haag.

54 Het Traffic Information & Pricing (TIP) systeem.

57 De vinding betreft een klasse van systemen voor het verzamelen en/of verspreiden van informatie m.b.t. verkeer, waarbij op zodanige wijze informatie over individuele personen en/of voertuigen kan worden verzameld en gecontroleerd op betrouwbaarheid, dat toch voldoende (privacy)bescherming kan worden geboden tegen onrechtmatige tracering van individuele personen en/of voertuigen. Ook kunnen uitbreidingen, verfijningen of eventuele andere veranderingen later gemakkelijk worden aangebracht.

De bedoelde systemen kunnen o.a. gebruikt worden voor het opleggen van allerlei verkeersheffingen en dus ook voor 'rekeningtransport', waaronder tenminste begrepen rekeningrijden, -varen en/of -vliegen.

Bij rekeningrijden kunnen dan b.v. alle afgelegde afstanden in rekening worden gebracht en kan het tarief, indien gewenst, voor elke afgelegde afstandseenheid worden gerelateerd b.v. aan de plaats waar, de datum waarop, het tijdstip waarop en/of de verkeersdrukte waarbij die afstandseenheid is afgelegd, aan het merk, model, bouwjaar, versnellingsbak- en/of motortype van het gebruikte voertuig, aan de ingeschakelde versnelling, het toerental, het brandstofverbruik, de geluidsproductie, de snelheid en/of de snelheidsveranderingen waarmee die afstandseenheid met dat voertuig is afgelegd, en/of aan de daarbij veroorzaakte milieuvuiling.

Een andere toepassing is b.v. de bestrijding van geluidshinder door vliegtuigen.

**Sleutelwoorden:** privacybescherming, tracering, fraudebestendigheid, controle, identificatie, semi-identificatie, agent, jager, intermediair, tellerstand, tol, verkeersheffing, totaalheffing, milieuvuiling, brandstofverbruik, lawaai, file-informatie, cruise control, automatische ijking, rollenbank, taximeter, tachograaf, black box.

NL C 1011501

De inhoud van dit octrooi komt overeen met de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekeningen.

# Het Traffic Information & Pricing (TIP) systeem

## Inleiding

5 In deze inleiding geven we allereerst een beschrijving van het door ons gebruikte begrip verkeersinformatiesysteem, laten we zien waar verkeersinformatiesystemen zoal voor gebruikt kunnen worden en geven we een aantal eigenschappen die een verkeersinformatiesysteem bij voorkeur moet hebben. Daarna geven we een korte beschrijving van een aantal kenmerkende aspecten van tot de vinding behorende verkeersinformatiesystemen, i.e. van TIP-systemen. Vervolgens gaan we eerst nader in op een specifieke, belangrijke toepassing, nl. het opleggen  
10 van verkeersheffingen, om daarna een nadere karakterisering te geven van TIP-systemen (uitsluitend of mede) voor het in rekening brengen van heffingen. Na een vergelijking met bestaande systemen geven we tenslotte een overzicht van de verdere inhoud van de tekst, waarin nadere uitleg gegeven wordt.

## Verkeer en infrastructuur

15 Verkeer maakt gebruik van een (deel van een) *infrastructuur*, i.e. de verzameling van alle voorzieningen t.b.v. het verkeer, zoals b.v. een verkeersnetwerk bestaande uit verkeerswegen en allerlei bijbehoren. Bijvoorbeeld bestaat de infrastructuur in het geval van scheepvaartverkeer o.a. uit waterwegen, havens, radarposten, bakens, (satelliet)navigatiesystemen en scheepscommunicatiesystemen, zoals b.v. marifoon. We hopen met dit voorbeeld  
20 geïllustreerd te hebben dat het begrip infrastructuur ruim moet worden opgevat.

Met het begrip *verkeer* wordt hier niet alleen bedoeld op 'fysiek' verkeer (zoals transport over, onder en/of door land, water en lucht), maar ook op 'logisch' verkeer (zoals b.v. berichtenverkeer in computernetwerken en/of economisch verkeer). Hoewel TIP-systemen eventueel in aangepaste vorm kunnen worden gebruikt bij zulke  
25 andere vormen van verkeer<sup>1</sup>, beperken we ons in het navolgende tot 'fysiek' verkeer. Om de beschrijving van TIP-systemen en van de daarvoor nodige en/of gebruikte technieken niet onnodig te compliceren, concentreren we ons in de voorbeelden en de verdere uitleg meestal op het geval van wegverkeer. Een ter zake kundige kan op basis van de gegeven uitleg zelf een, waar nodig aangepaste, beschrijving maken voor andere vormen van verkeer of transport. De gegeven voorbeelden en genoemde varianten dienen alleen ter illustratie en mogen dus niet  
30 begrepen worden als opgelegde beperkingen.

## Verkeersinformatie en verkeersheffing

De term *verkeersinformatie* gebruiken wij voor elke relevante informatie m.b.t. verkeer in de meest ruime zin, waaronder tenminste begrepen informatie over de betreffende infrastructuur, over relevante (b.v. aan het verkeer  
35

---

<sup>1</sup> Denk b.v. aan het in rekening brengen van gegevenstransport of misschien zelfs aan tamelijk extreme gevallen als b.v. elektronische heffing van omzet-, loon- en/of inkomstenbelasting.

deelnemende of deelgenomen hebbende) voertuigen en/of personen, over het gebruik van voertuigen en over andere relevante aspecten, zoals b.v. verkeersdrukke, weersgesteldheid of andere gebruiksomstandigheden<sup>2</sup>.

De term *verkeersheffing* gebruiken wij niet alleen voor verkeersbelastingen, zoals b.v. motorrijtuigenbelasting en tolheffing, maar ook voor allerlei andere kosten die op een of andere wijze gerelateerd zijn aan verkeersdeelname, zoals b.v. verkeersboetes, vervoerkosten en verzekeringspremies. Denk bij vervoerkosten b.v. aan de kosten voor gebruik van openbaar vervoer en bij verzekeringspremies b.v. aan de premies voor autoverzekeringen, waarbij de hoogte van de premie b.v. af zou kunnen hangen van het aantal afgelegde kilometers en/of van de plaats waar die kilometers zijn afgelegd. (B.v. omdat het risico op schade per afgelegde kilometer op een autosnelweg lager is dan op secundaire wegen of in een stadscentrum.) Bovendien verstaan we onder verkeersheffingen niet alleen heffingen op actieve verkeersdeelname, zoals b.v. bij rekeningrijden, maar ook op passieve 'deelname', zoals b.v. bij parkeerheffingen. Kortom, de term verkeersheffing heeft evenals de term verkeersinformatie bij ons een (zeer) ruime betekenis.

## 15 Verkeersinformatiesysteem

Bij het verzamelen en/of verspreiden van verkeersinformatie is er sprake van, wat wij zullen noemen, een *verkeersinformatiesysteem*. Een verkeersinformatiesysteem kan b.v. gebruikt worden voor het *verzamelen* van informatie over verkeersdrukke op resp. de benuttingsgraad van (delen van) het wegennet, over filevertragingen, over brandstofverbruik, over veroorzaakte milieuvervuiling en/of m.b.t. verschuldigde verkeersheffingen. Een verkeersinformatiesysteem kan eventueel (ook) gebruikt worden voor het *verspreiden* van informatie over b.v. afstanden, snelheidsbeperkingen, filevertragingen, buitentemperatuur, luchtvervuiling<sup>3</sup> en/of mistbanken.

Een verkeersinformatiesysteem *kan* voor verschillende doeleinden benut worden, zoals b.v. voor:

- 25 • het ondersteunen van verkeersbeheer, in ruime zin; denk b.v. aan verkeersregulering, verkeersstellingen, het volgen van de loop van verkeersstromen en het meten van hun gemiddelde snelheid, het bepalen van de onderlinge afstand tussen voertuigen, het detecteren van files en het meten van filevertragingen, maar ook aan het bepalen en/of plannen van de behoefte aan uitbreiding van de infrastructuur, want beheer (in ruime zin) van de infrastructuur valt hier ook onder.
- 30 • het verbeteren van de verkeersveiligheid; b.v. door continue en efficiënte(re) snelheidscontroles, door onverwijld waarschuwing voor mistbanken en/of door cruise controls automatisch lokale, via zenders verspreide snelheidslimieten te laten respecteren.
- 35 • het verzamelen van informatie over het brandstofverbruik van voertuigen in de praktijk; de resultaten kunnen b.v. uitgesplitst worden naar merk, model, bouwjaar, versnellingsbaktype, motortype, snelheid, acceleratie, ingeschakelde versnelling, toerental, motortemperatuur, weersomstandigheden, etc.

<sup>2</sup> Bijvoorbeeld kan in het geval van scheepvaartverkeer informatie over de watergetijden relevant zijn. Zie ook de volgende voetnoot.

<sup>3</sup> Denk aan het (tijdig) waarschuwen voor ernstige luchtvervuiling in b.v. tunnels. Luchtvervuiling is een voorbeeld van gebruiksomstandigheden.

- het zo nauwkeurig mogelijk bepalen van milieuvervuiling veroorzaakt door (een deel van) het verkeer; b.v. ten behoeve van het maken of nakomen van afspraken over beperking van milieuvervuiling.
- het berekenen en evt. ook in rekening brengen van verkeersheffingen; alleen prijsberekening, zoals b.v. het geval kan zijn bij vervoer per taxi of bij verzekeringspremies, of ook het daadwerkelijk in rekening brengen, zoals b.v. het geval kan zijn bij openbaar vervoer of bij rekeningrijden; een belangrijk aspect bij dit alles is de mogelijkheid tot meer of betere *variabilisering*.
- het verbeteren van de wetshandhaving; b.v. door geautomatiseerde constatering van allerlei verkeersovertredingen, door automatische en betrouwbare identificatie, door koppelen van verkeersovertredingen aan individuele personen t.b.v. een strafpuntensysteem, door betere automatisering en grotere betrouwbaarheid van de afhandeling van verkeersboetes en/of door het bestrijden van diefstal van voertuigen door snelle en eenvoudige opsporing.
- het ondersteunen van het beheer, in ruime zin, van een wagenpark<sup>4</sup>; b.v. het wagenpark van een taxi-, autoverhuur- of transportbedrijf.

## 15 Het TIP-systeem

Het TIP-systeem<sup>5</sup> is een verkeersinformatiesysteem dat voor alle genoemde doeleinden gebruikt kan worden. Zowel voor elk doel apart, als tegelijkertijd voor meerdere of mogelijk zelfs alle doelen<sup>6</sup>. Vanwege zijn brede toepasbaarheid kan het TIP-systeem met recht een *multifunctioneel verkeersinformatiesysteem* genoemd worden. Omdat bij het TIP-systeem (alle of een deel van) de toepassingen eventueel ook kunnen worden samengevoegd tot één samenhangend groter geheel, kan men ook spreken van een geïntegreerd multifunctioneel verkeersinformatiesysteem.

### De instantie

Gezien de vele en diverse taken die een TIP-systeem kan verrichten, is het zeer wel denkbaar dat er meerdere instanties betrokken zijn bij de diverse toepassingen. In zo'n geval zal het TIP-systeem waarschijnlijk beheerd worden door één of meerdere van de betrokken instanties of door een aparte, niet direct bij één van de specifieke toepassingen betrokken instantie. De beheerder is (resp. de gezamenlijke beheerders zijn) verantwoordelijk voor het TIP-systeem en voor de dienstverlening aan de overige betrokken instanties. Beheer is hier weer bedoeld in ruime zin en omvat dus o.a. onderhoud, beveiliging, aanpassing, uitbreiding, in werking houden, etc.

Om onze uitleg niet onnodig te compliceren zullen we in het vervolg ter aanduiding van één of meerdere van de bovenbedoelde instanties (incl. de beheerder) vaak gebruik maken van de aanduiding *de instantie* (of: een instan-

<sup>4</sup> Dit punt hoort misschien (voor een deel) thuis onder het ruime begrip verkeersbeheer.

<sup>5</sup> We spreken vaak van 'het systeem', hoewel het feitelijk gaat om een klasse van vele systemen met bepaalde kenmerken.

<sup>6</sup> Wij benadrukken hier voor alle duidelijkheid ten overvloede dat men ook informatie over b.v. snelheden en/of door verkeer veroorzaakte milieuvuiling kan (willen) verzamelen zonder die informatie ook te gebruiken voor wetshandhaving en/of verkeersheffingen.

tie). De enkelvoudige term instantie kan dus worden gebruikt voor de aanduiding van een bepaalde afzonderlijke instantie, die verantwoordelijk is voor of belang heeft bij een specifieke toepassing, maar ook voor alle (of een deel van de) betrokken instanties gezamenlijk. Soms gebruiken we ook de omschrijving informatie verzamelende en/of controlerende instantie.

5

### Een aantal gewenste eigenschappen

Een verkeersinformatiesysteem moet bij voorkeur tenminste de volgende eigenschappen hebben:

- zo veel mogelijk geautomatiseerd zijn;  
10 dit is o.a. van belang i.v.m. snelheid en gebruikskosten; snel verzamelen en verspreiden van recente informatie is van belang, evenals het zoveel mogelijk vermijden van personeelskosten.
- functioneren zonder hinder voor het verkeer;  
dit is o.a. tamelijk eenvoudig te realiseren door zenders en ontvangers te gebruiken.
- zorgen voor voldoende privacybescherming;  
15 dit betreft m.n. privacybescherming m.b.t. bewegingspatronen, oftewel het tegengaan (i.e. het niet praktisch uitvoerbaar resp. makkelijker maken) van onrechtmatige *tracering* van individuele, uniek identificeerbare personen en/of voertuigen<sup>7</sup>.
- garanderen van voldoende betrouwbaarheid van de verzamelde informatie;  
20 dit betreft o.a. voldoende *fraudebestendigheid*, wat m.n. van belang is als de verzamelde informatie gebruikt wordt voor het berekenen en/of in rekening brengen van verkeersheffingen.

In het algemeen kunnen de twee eerstgenoemde eigenschappen, althans voor een groot deel, op een tamelijk voor de hand liggende wijze gerealiseerd worden, nl. door het inzetten van computers, zenders en ontvangers. Realisatie van de twee laatstgenoemde eigenschappen is veel moeilijker, zeker in combinatie. Immers, het houden van  
25 een zekere mate van toezicht is onontbeerlijk voor o.a. het bereiken van (een deel van) de gewenste fraudebestendigheid. En voor controles<sup>8</sup> is het i.h.a. nodig om het gecontroleerde te identificeren. Dus controles en identificatie gaan i.h.a. hand in hand. Maar unieke identificatie van personen en/of voertuigen bij het verzamelen en/of controleren van informatie vormt een bedreiging voor de privacybescherming, omdat dit vaak tracering van de betreffende personen en/of voertuigen mogelijk maakt of vergemakkelijkt. Met bovenstaande grove redenering  
30 hopen we voldoende te hebben toegelicht dat uitoefening van controle i.h.a. bemoeilijkt wordt als tegelijkertijd de privacy beschermd moet worden (en omgekeerd).

<sup>7</sup> 'Privacybescherming m.b.t. bewegingspatronen' en 'tegengaan van onrechtmatige tracering' betekenen bij ons hetzelfde. De toevoeging 'm.b.t. bewegingspatronen' laten we vaak en de toevoeging 'onrechtmatige' laten we soms achterwege. Ook spreken we vaak van 'voorkomen' i.p.v. 'tegengaan' of 'niet praktisch uitvoerbaar maken'. Wat precies bedoeld wordt, zal i.h.a. blijken uit de context.

<sup>8</sup> Controle en toezicht zijn, of worden door ons in ieder geval gebruikt als, synoniemen. Controleren omvat dus ook toezicht houden.

## Globale karakterisering van TIP-systemen

Op basis van de hierboven gegeven toelichting kunnen we stellen dat verkeersinformatiesystemen zich m.n. van elkaar zullen onderscheiden wat betreft de wijze waarop gezorgd wordt voor adequate controle en/of privacybescherming<sup>9</sup>. Het zal dan ook geen verbazing meer wekken dat het TIP-systeem zich van andere verkeersinformatiesystemen onderscheidt m.n. wat betreft deze twee aspecten en wat betreft de mogelijkheid tot het combineren van die twee. Voor alle duidelijkheid benadrukken wij dat het TIP-systeem de mogelijkheid biedt om alle genoemde eigenschappen te combineren. We zijn nu toe aan een eerste, beknopte karakterisering van het TIP-systeem.

De klasse van verkeersinformatiesystemen behorend tot onze vinding, i.e. het TIP-systeem, wordt vooral gekenmerkt door de wijze waarop gezorgd wordt voor:

- de eigenschap dat door (resp. voor) de instantie bepaalde informatie over personen en/of voertuigen, en m.n. ook over *individuele* personen en/of voertuigen, verzameld kan worden en (voor zover nodig) *gecontroleerd* kan worden op betrouwbaarheid;
- de eigenschap dat de instantie daarbij niet hoeft te vertrouwen op de *fraudebestendigheid* van componenten in voertuigen anders dan eventueel aanwezige *agenten* (zie hieronder);
- de eigenschap dat daarbij onrechtmatige *tracering* van individuele, uniek identificeerbare personen of voertuigen kan worden voorkomen.

### Tracering

Het zal inmiddels duidelijk zijn dat we met de laatste eigenschap bedoelen dat de informatie verzamelende en/of controlerende instantie i.h.a. geen toegang hoeft te krijgen, of redelijkerwijs zelfs kan krijgen, tot (privacy gevoelig beschouwde) informatie over het bewegingspatroon van een bepaald voertuig of een bepaalde persoon waarvan de identiteit achterhaald kan worden. Een nadere toelichting wordt gegeven in het hoofdstuk over tracering.

### Fraudebestendigheid en controles

Strikt genomen is er pas sprake van fraudebestendigheid als er geen enkele vorm van fraude mogelijk is. In de praktijk spreekt men vaak al van *fraudebestendigheid* als er sprake is van bestandheid tegen elke bekende, praktisch uitvoerbare, lonende vorm van fraude waartegen men zich wenst te wapenen. Wij gebruiken de term *fraudebestendig* m.n. in deze laatste betekenis. Straks gaan we in het hoofdstuk over fraudebestendigheid nog wat nader in op deze term en het gebruik ervan. We geven dan ook een nadere toelichting op de betekenis van de term fraudebestendig(heid) toegepast op een individuele component.

Fraude door in of vanuit een voertuig onjuiste informatie te verstrekken wordt tegen gegaan door *controles* uit te voeren op verstrekte informatie. Controles kunnen dus zorgen voor tenminste een deel van de fraudebestendig-

<sup>9</sup> Hier wordt met privacybescherming natuurlijk het voorkomen, i.e. het tegengaan, van tracering bedoeld.

heid. Informatie kan echter niet alleen onjuist zijn t.g.v. (pogingen tot) fraude, maar ook te goeder trouw door b.v. onnauwkeurigheid of slecht functioneren van bepaalde apparatuur. Controles op de betrouwbaarheid van informatie zijn dus bruikbaar voor meer dan alleen fraudebestrijding. Omdat beide termen nauw met elkaar samenhangen, worden ze in deze tekst soms toch min of meer als een soort van synoniemen gebruikt.

5

### **Agent**

De term *agent* gebruiken we voor elke uit apparatuur en/of programmatuur bestaande component waarvoor geldt dat deze:

- 10
- bij tijd en wijle t.b.v. de instantie actief één of meerdere taken uitvoert in een voertuig, èn
  - fraudebestendig moet zijn (gezien vanuit het oogpunt van de instantie).

15 We merken wellicht ten overvloede op dat in het laatstgenoemde punt al opgesloten ligt dat de correcte uitvoering van de in het eerste punt genoemde taak essentieel is voor de bescherming van de belangen van de instantie en dus voor de correcte werking van het verkeersinformatiesysteem. M.a.w. een agent behartigt in het voertuig belangen van (resp. vertegenwoordigt) de betrokken instantie en betreft een component op het juist, i.e. ongemani-  
puleerd, functioneren waarvan de instantie kan en moet vertrouwen, juist ook in de vanuit het oogpunt van  
fraudebestrijding door de instantie als onveilig te bestempelen omgeving gevormd door een voertuig.

20 Wat een agent precies is of kan zijn, zal ongetwijfeld duidelijker worden door lezing van de gehele tekst. Denk bij de door een agent uit te voeren taken (in ieder geval voorlopig) m.n. aan het namens de instantie (deels of volledig) uitoefenen van controle op de betrouwbaarheid van bepaalde door andere componenten in het voertuig verstrekte informatie. In het hoofdstuk over TIP-systemen wordt een uitgebreide opsomming gegeven van taken die door een agent verricht kunnen worden.

25

### **Karakterisering van de werkwijze m.b.t. het tegengaan van tracering**

De wijze waarop bij een TIP-systeem gezorgd kan worden voor privacybescherming m.b.t. bewegingspatronen wordt m.n. gekenmerkt door het gebruik van tenminste één van de volgende drie elementen:

- 30
- *semi-identificaties*;  
semi-identificaties kunnen, zoals we later zullen laten zien, gebruikt worden voor het privacy veilig verzamelen van bepaalde informatie, zoals b.v. voor het volledig automatisch en tot op de minuut nauwkeurig bepalen van de op datzelfde moment gerealiseerde filevertragingen uitgedrukt in minuten; meer i.h.a. helpt het gebruik van niet unieke semi-identificaties om het gebruik van privacy bedreigende, unieke identificaties van voertuigen en/of personen terug te dringen.
- 35
- *agenten*;  
agenten kunnen, zoals we later zullen laten zien, o.a. gebruikt worden voor het op zodanige wijze verzamelen en controleren van allerlei informatie dat het gebruik van privacy bedreigende, unieke identificaties van voertuigen en/of personen niet, of nog maar nauwelijks, nodig is.

40

- *jagers en/of intermediairs;*

jagers en/of intermediairs kunnen, zoals we later zullen laten zien, gebruikt worden om vanuit een voertuig verzonden informatie die wel degelijk uniek identificerende gegevens m.b.t. de betreffende persoon en/of het betreffende voertuig bevat, buiten het voertuig (i.e. in de buitenwereld) op een zodanige wijze te verzamelen, dat er voldoende bescherming wordt geboden tegen onrechtmatige tracering.

### **Karakterisering van de werkwijze m.b.t. het uitvoeren van controles**

De wijze waarop bij een TIP-systeem door een instantie gezorgd kan worden voor controle op de betrouwbaarheid van, en dus fraude kan worden tegengegaan met, bepaalde in of vanuit het voertuig verstrekte informatie, waaronder m.n. ook allerlei *tellerstanden*, kent twee verschijningsvormen:

- alleen controles door de instantie *op afstand*;

de belangen van de instantie worden dan afdoende beschermd zonder dat één van de betrokken individuele componenten in een voertuig (zender, ontvanger, sensoren, meters, tellers, verbindingen, e.d.) fraudebestendig hoeft te zijn.

- alle of een deel van de controles door de instantie m.b.v. *agenten in de voertuigen*;

de belangen van de instantie worden dan afdoende beschermd zonder dat één van de *andere* betrokken individuele componenten in een voertuig (zender, ontvanger, sensoren, meters, tellers, verbindingen, e.d.) fraudebestendig hoeft te zijn.

Omdat we het verkeer niet onnodig willen hinderen, ligt het voor de hand om (tenminste een deel van) de benodigde controles op afstand uit te voeren, d.w.z. (een deel van) de controles op de betrouwbaarheid van de vanuit voertuigen via hun zender verstuurd informatie buiten de voertuigen te laten plaatsvinden. Het gebruik van bepaalde identificaties lijkt (in ieder geval) bij controles (op afstand) moeilijk te vermijden.

Er zal blijken dat de aanpak met agenten meer resp. betere mogelijkheden biedt dan de aanpak met uitsluitend controles op afstand<sup>10</sup>. Toch kan met uitsluitend controles op afstand al verrassend veel bereikt worden. Latere hoofdstukken geven hierover meer details.

### **Verkeersheffingen m.b.v. een verkeersinformatiesysteem**

Zoals eerder gemeld, is het mogelijk om een verkeersinformatiesysteem (mede of uitsluitend) te gebruiken voor verkeersheffingen, waaronder tenminste ook begrepen tol, verkeersboetes, motorrijtuigenbelasting, verzekeringspremies en parkeerheffingen. Omdat dit een zeer belangrijke toepassing is, gaan we nu uitgebreider in op deze mogelijkheid. In deze sectie ligt de nadruk bij de te geven toelichting op rekeningrijden. Ook bij de verdere behandeling en uitleg in latere hoofdstukken staat deze toepassing vaak centraal. Dat wij onze aandacht primair richten op rekeningrijden heeft niet alleen te maken met het belang ervan, maar juist ook met het feit dat deze

<sup>10</sup> Deze laatste aanpak betitelen we ook wel eens (slordigweg) als de aanpak zonder agenten, hoewel dat strikt genomen zeker niet hetzelfde is.



toepassing geschikt is om een flink deel van de mogelijkheden die het TIP-systeem biedt, te illustreren en uit te leggen.

5 Rekeningrijden kan gebruikt worden louter als vorm van belastingheffing, maar b.v. ook als *milieumaatregel* en/of als maatregel ter verbetering van de *bereikbaarheid* van bepaalde gebieden op bepaalde tijden. Bij gebruik als milieumaatregel wil men, ook in filevrije gebieden, ongebreidelde groei van de hoeveelheid verkeer tegen- gaan of de hoeveelheid verkeer misschien zelfs verminderen, omdat verkeersdeelname altijd gepaard gaat met het verbruiken van energie en met een zekere mate van milieuvervuiling.

10 Hoewel deze laatste uitspraak kwalitatief zonder meer juist is, mag niet worden vergeten dat er kwantitatief grote verschillen kunnen zijn in de mate van veroorzaakte milieuvervuiling. Denk hierbij bijvoorbeeld aan de ver- schillen tussen diverse soorten transport (b.v. personenauto's vs. autobussen, maar meer in het algemeen b.v. luchttransport vs. vervoer over water of treinverkeer vs. wegverkeer), tussen diverse soorten voortstuwingsappa- ratuur (b.v. electromotoren vs. motoren met inwendige verbranding, maar ook het ene type benzinemotor vs. een  
15 ander type) en tussen de voor het transport gebruikte brandstoffen (b.v. zonne-energie vs. fossiele brandstoffen of LPG vs. benzine).

Bij het opleggen van een verkeersheffing kan het, b.v. omwille van de rechtvaardigheid, gewenst zijn om *alle* kilometers (of welke afstandseenheid dan ook) te belasten en daarbij kilometers die onder gelijke relevante om- standigheden (zeg, met precies hetzelfde soort voertuig, zelfde snelheid, zelfde soort brandstof, etc.) worden  
20 afgelegd, gelijk te belasten. Stel even dat in een bepaald land een verkeersheffing uitsluitend ingevoerd wordt als milieumaatregel, dan lijkt het bijvoorbeeld billijk om kilometers afgelegd in een stedelijke omgeving van dat land even zwaar te belasten als kilometers op het platteland, tenminste als ze onder dezelfde relevante omstandigheden (in dit geval dus: met dezelfde gevolgen voor het milieu) zijn afgelegd. Immers, voor het milieu in een bepaalde  
25 regio maakt het i.h.a. weinig uit of de vervuilende uitlaatgassen op het platteland of in een stedelijke omgeving binnen die regio zijn geproduceerd.

Maar het kan ook gewenst zijn om, zelfs bij gelijke vervuiling, het tarief voor afgelegde kilometers wel degelijk te laten variëren, b.v. afhankelijk van verkeersdrukte of van tijd en plaats. Dit soort tarifieringen kunnen bijvoor- beeld ingezet worden ter verbetering van de bereikbaarheid van bepaalde gebieden op bepaalde tijden, b.v. door  
30 bestrijding van files tijdens spitsuren.

In deze tekst houden we ons liefst verre van een discussie over (de juistheid van) allerlei redenen om verkeershef- fingen op te (willen) leggen. Wel merken we op dat het gunstig is voor de algemene geschiktheid van een ver- keersinformatiesysteem voor het opleggen van allerlei verkeersheffingen, als tarifieringen zodanig ingericht kun- nen worden, dat aan allerlei mogelijke wensen, waaronder de twee hierboven genoemde, tegemoet kan worden  
35 gekomen.

Het tarief voor een afgelegde afstandseenheid moet dus bij voorkeur afhankelijk *kunnen* worden gemaakt van  
40 (resp. er moeten dus *betrouwbare* waarden *kunnen* worden vastgesteld van) zoveel mogelijk variabelen, zoals

b.v. van de datum en tijd waarop (nauwkeuriger geformuleerd: van de precieze periode waarin), de plaats waar en/of de verkeersdrukte waarbij die afstandseenheid is afgelegd, van (een deel van) de volledige *typering* (i.e. het merk, model, bouwjaar, versnellingsbak- en motortype, e.d.) van het gebruikte voertuig, van de soort brandstof, het brandstofverbruik, de ingeschakelde versnelling, de hoeveelheid lawaai, de aard en hoeveelheid van de veroorzaakte milieuvervuiling, de gemiddelde snelheid, het toerental, de snelheidsverandering(en) en/of de toerentalverandering(en) waarmee die afstandseenheid met dat voertuig is afgelegd.

#### Eventueel gebruik van afgeleide informatie

10 Tussen bepaalde variabelen bestaat een zeker verband. Bijvoorbeeld bestaat er voor elk voertuig van een bepaald bouwjaar, merk en model dat is uitgerust met een bepaald versnellingsbak- en motortype, een verband tussen het brandstofverbruik op een bepaald moment en een aantal andere grootheden op datzelfde moment, zoals b.v. de buitentemperatuur, de snelheid, het toerental en de acceleratie. Iets soortgelijks geldt voor de hoeveelheid geproduceerd lawaai en voor de veroorzaakte luchtvervuiling. Als zo'n verband ook kwantitatief voldoende nauwkeurig bekend is, kan het gebruikt worden voor het voldoende nauwkeurig bepalen van afgeleide waarden, i.e. voor het voldoende nauwkeurig berekenen of afleiden van bepaalde grootheden uit andere.

20 Voldoende nauwkeurig afgeleide waarden kunnen op twee manieren gebruikt worden, nl. voor controles, i.e. vergelijking met een (volgens opgave) werkelijk gemeten waarde, of voor het achterwege laten van bepaalde metingen. Van de eerstgenoemde mogelijkheid is b.v. sprake bij controles op de betrouwbaarheid van opgegeven brandstofverbruik. Van de tweede mogelijkheid is b.v. sprake als men de aard en hoeveelheid van de luchtvervuiling op een bepaald moment veroorzaakt door een bepaald motorvoertuig bepaalt zonder op dat moment bij het betreffende voertuig de aard en hoeveelheid van de uitlaatgassen daadwerkelijk te meten en te analyseren<sup>11</sup>.

#### 25 Een karakterisering van het TIP-systeem bij gebruik voor verkeersheffingen

Een belangrijk kenmerk van TIP-systemen (mede) bedoeld voor het opleggen van verkeersheffingen is, dat aan alle eerder genoemde wensen tegemoet kan worden gekomen. Kenmerkend voor de bij deze laatstbedoelde systemen gebruikte wijze van controle is, dat m.n. ook fraude met bepaalde tellerstanden kan worden tegengegaan, zodat de bedoelde verkeersinformatiesystemen ook betrouwbare informatie over tellerstanden kunnen verzamelen. Dit heeft tot gevolg dat de verzamelde informatie ook gebruikt kan worden voor het op fraudebestendige wijze opleggen van een *totaalheffing*. (In het volgende hoofdstuk komen we terug op dit begrip, dat een heffing betreft waarbij het totale 'verbruik' in b.v. kilometers of b.v. in een zekere milieuvervuilingseenheid in rekening

<sup>11</sup> Hoewel wij er vanuit gaan dat het daadwerkelijk meten en analyseren van de uitlaatgassen van elk voertuig te kostbaar is, kan het in principe wel. Het daadwerkelijk meten vanuit een motorvoertuig in het verkeer van de totale hoeveelheid lawaai die door datzelfde voertuig wordt voortgebracht (dus incl. geluid door luchtstroming langs het voertuig), lijkt echter ondoenlijk, ook al vanwege de eventuele nabijheid van veel ander verkeer. Het tamelijk nauwkeurig afleiden van de totale geluidsproductie van een voertuig uit andere gegevens lijkt daarom zelfs geboden.

kan worden gebracht.) Dus kan o.a. ook tegemoet gekomen worden aan de wens om *alle* afgelegde kilometers (hectometers, mijlen, of welke afstandseenheden dan ook) in rekening te kunnen brengen.

Kort samengevat omvat het TIP-systeem dus o.a. een klasse van systemen voor het berekenen en evt. ook in rekening brengen van verkeersheffingen waarbij *alle* afgelegde afstanden in rekening kunnen worden gebracht, waarbij het tarief per afgelegde afstandseenheid (b.v. per kilometer) op velerlei wijzen kan variëren, waarbij ook extra kosten voor het gebruik van bepaalde weggedeelten (tolwegen, bruggen, tunnels, e.d.) in rekening kunnen worden gebracht, waarbij voldoende privacybescherming en fraudebestendigheid kunnen worden geboden en waarbij (zoals we later zullen laten zien) uitbreidingen, verfijningen of eventuele andere veranderingen later gemakkelijk kunnen worden aangebracht. Het tarief voor een afgelegde afstandseenheid kan bij het TIP-systeem afhankelijk gemaakt worden van allerlei variabelen, zoals b.v. de verkeersdrukte, het type van het voertuig (i.e. merk, model, bouwjaar, versnellingsbak- en motortype, e.d.), de soort brandstof, het brandstofverbruik, de ingeschakelde versnelling, het lawaai, de gemiddelde snelheid, het toerental, de snelheidsveranderingen en/of de toerentalveranderingen waarmee de afstandseenheid is afgelegd, en/of de datum en tijd waarop (nauwkeuriger geformuleerd: de precieze periode waarin) deze afstand is afgelegd. Een opmerkelijk aspect is dus dat het mogelijk is om allerlei milieuvervuiling (zoals b.v. lawaai en luchtvervuiling) veroorzaakt door het gebruik van een bepaald voertuig in rekening te brengen, zonder bij het betreffende voertuig steeds de aard en omvang van die vervuiling daadwerkelijk te hoeven analyseren en meten. Voor alle duidelijkheid benadrukken we hier alvast dat ons systeem niet alleen geschikt is voor totaalheffingen, maar ook voor andere heffingen, zoals grens- en trajectheffingen (zie het volgende hoofdstuk).

#### **De behoefte aan het TIP-systeem t.b.v. verkeersheffingen**

Momenteel wordt in bepaalde landen al op diverse manieren belasting geheven op verkeer in ruime zin. Denk hierbij o.a. aan belasting op de aankoop, het bezit en het gebruik van voertuigen. Bij deze bestaande vormen van verkeersheffing kan niet of onvoldoende rekening worden gehouden met o.a. de mate, de plaatsen en de tijdstippen van gebruik van een voertuig en met de mate van de resulterende milieuvervuiling.

Bijvoorbeeld speelt bij de accijnsheffing op brandstoffen, die valt onder de derde genoemde vorm van belastingheffing, de mate van gebruik wel degelijk een rol. Maar toch schiet ook deze vorm van verkeersheffing duidelijk te kort. Immers, er kan o.a. geen rekening worden gehouden met de plaats en/of het tijdstip van gebruik, noch met het feit dat een bepaalde hoeveelheid brandstof meer of minder milieuvriendelijk verbruikt kan worden. Daarnaast komt nog het praktische probleem dat de accijnzen op brandstoffen meestal niet naar believen verhoogd of verlaagd kunnen worden zonder serieuze problemen te creëren. Denk hierbij o.a. aan de gevolgen voor pomphouders in grensgebieden en aan het eventuele verlies van belastinginkomsten door legale en/of illegale import van brandstoffen uit een buurland. Kortom, de bestaande vormen van verkeersheffing kunnen nog onvoldoende tegemoet komen aan de wens tot meer of betere *variabilisering*<sup>12</sup>.

<sup>12</sup> Als b.v. het type van een voertuig gebruikt wordt als variabele, kan men de tarieven relateren aan de milieu(on)vriendelijkheid van voertuigen van dat type en aldus via de tarieven de aankoop van de meest milieuvriendelijke voertuigen veel gericht stimuleren.

Er is dus wel degelijk behoefte aan een praktisch bruikbaar, doeltreffend en flexibel systeem voor het opleggen en/of variabiliseren van allerlei verkeersheffingen, zoals b.v. heffingen voor het gebruik van een voertuig (rekening houdend met b.v. de mate, de plaatsen en/of de tijdstippen van gebruik en/of de mate van veroorzaakte vervuiling) en voor het gebruik van bepaalde weggedeelten (tolwegen, -bruggen, -tunnels, e.d.), zonder dat daarbij de privacy van de gebruiker of betaler hoeft te worden geschonden. Het TIP-systeem is zo'n systeem. Daarnaast kan het TIP-systeem o.a. voldoen aan de wens om op elk moment direct, goedkoop en privacy veilig filevertragingen uitgedrukt in minuten (of een andere tijdseenheid) te kunnen bepalen.

## 10 Vergelijking met bestaande systemen voor verkeersheffingen

Voor verkeersheffingen zijn al veel systemen bedacht. Vaak betreft dit tolsystemen waarbij alleen tol wordt geheven bij het passeren van bepaalde tolpunten. Zulke tolsystemen ondersteunen dus alleen het soort heffing dat we *grensheffing* (zie het volgende hoofdstuk) zullen noemen. Grensheffingen vormen een tamelijk grof en beperkt bruikbaar middel dat in veel gevallen te kort schiet. Ze kunnen wel gebruikt worden voor een verbetering van de bereikbaarheid, maar zijn niet geschikt voor gebruik als milieumaatregel<sup>13</sup>. Bovendien is een nadeel dat gebruik van grensheffingen vaak leidt tot allerlei onrechtvaardige situaties.

Stel b.v. dat rondom een bepaald gebied een volledig sluitend cordon van tolpunten aangebracht wordt als maatregel ter verbetering van de bereikbaarheid, i.e. om tijdens spitsuren tol te heffen (en zodoende de toegang tot dat gebied m.b.v. een motorvoertuig te ontmoedigen) met de bedoeling het wegennet binnen dat gebied tijdens spitsuren enigszins te ontlasten. In de geschetste situatie kunnen sommigen dit gebied gedurende de spitsuren continu doorkruisen en het betreffende wegennet dus continu belasten na slechts één keer (om het gebied tijdens de spitsuren te betreden) of zelfs géén enkele keer (als ze voor het begin van de spitsuren al binnen het gebied zijn) tol te hebben betaald. Echter, anderen moeten voor een kort, eenmalig ritje tijdens de spitsuren wel (resp. evenveel) tol betalen. Of ze moeten voor meerdere korte ritjes zelfs meerdere keren tol betalen.

Ons is geen enkel systeem bekend dat, net als het TIP-systeem, fraudebestendig is en per persoon en/of per voertuig *vele* vormen van *totaalheffing* op kan leggen, zoals b.v. m.b.t. het (totale) brandstofverbruik, de (totale) geluidsproductie en/of de (in totaal) veroorzaakte milieuv vervuiling. Er is ons in ieder geval geen enkel bestaand systeem bekend waarbij de geluidsproductie en/of de emissie of, algemener, de milieuv vervuiling veroorzaakt door individuele voertuigen tamelijk nauwkeurig berekend wordt, laat staan een systeem waarbij zulke berekeningen een rol spelen bij het in rekening brengen van een verkeersheffing. Ook kennen wij geen systeem dat kan controleren of het in of vanuit een voertuig opgegeven brandstofverbruik klopt, i.e. geloofwaardig is. Kortom, voor zover ons bekend is het TIP-systeem uniek wat betreft het aantal aspecten waarover betrouwbare informatie kan worden verzameld. (Denk b.v. ook nog aan verkeersdrukte.) Als gevolg daarvan is het TIP-systeem ook uniek wat betreft de mate waarin diverse vormen van totaalheffing kunnen worden opgelegd.

<sup>13</sup> We gaan hier niet nader in op de argumenten waarop deze bewering berust. We merken alleen op dat grensheffingen in principe zelfs een nadelig effect kunnen hebben op het milieu, omdat verkeer tolpunten zoveel mogelijk zal proberen te mijden.

Wel bestaat er een klein aantal systemen dat, net als het TIP-systeem, gebruikt kan worden voor het opleggen van de ene specifieke vorm van totaalheffing waarbij alle afgelegde kilometers in rekening worden gebracht. Echter, voor zover ons bekend geldt voor al deze systemen tenminste dat ze òf onvoldoende bescherming bieden tegen tracering, òf dat ze gebruik maken van een (relatief duur) Global Positioning System (GPS), òf dat ze onvoldoende dan wel minder fraudebestendig zijn, òf dat ze voor het bereiken van voldoende fraudebestendigheid uitgebreid(er) gebruik moeten maken van fysieke beveiligingen.

#### Enkele unieke aspecten van het TIP-systeem

10

Een uniek aspect van het TIP-systeem is derhalve dat allerlei totaalheffingen kunnen worden gerealiseerd en dat gezorgd kan worden voor goede bescherming tegen fraude en tegen tracering van individuele, uniek identificeerbare personen en/of voertuigen zonder dat fysieke beveiliging van betrokken componenten in voertuigen, anders dan eventueel aanwezige agenten, tegen fraude noodzakelijk is en zonder dat gebruik hoeft te worden gemaakt van GPS.

15

Daarnaast heeft het TIP-systeem nog veel meer te bieden. B.v. de mogelijkheid om volledig automatisch en zeer privacy veilig de meest recente informatie te verzamelen over filevertragingen uitgedrukt in minuten, wat veel informatiever is dan informatie over files in kilometers. Verder noemen we hier nog de mogelijkheid om op privacy veilige en/of fraudebestendige wijze voertuigen te identificeren en om beter inzicht te verwerven in de feitelijke verkeersstromen, de mogelijkheid om stelselmatig betrouwbare praktijkgegevens te verzamelen over b.v. het brandstofverbruik per voertuigtype en de mogelijkheid om diefstal van voertuigen effectief te bestrijden.

20

#### Beschrijving van en toelichting op de vinding resp. de conclusies

25

De uitvinding is gekenmerkt door een werkwijze voor het verzamelen van verkeersinformatie door een instantie

- a) waarbij gebruik wordt gemaakt van in althans een deel van de voertuigen aanwezige middelen ter verstrekking van informatie,
- b) waarbij uit (de ontvangst van) de vanuit voertuigen verstrekte informatie direct of indirect verkeersinformatie wordt afgeleid,
- c) waarbij onrechtmatige tracering van individuele personen en/of voertuigen wordt voorkomen,
- d) waarbij de betrouwbaarheid van de in of vanuit voertuigen verstrekte informatie voor zover nodig wordt gecontroleerd,
- e) waarbij de instantie niet hoeft te vertrouwen op de fraudebestendigheid van individuele componenten in voertuigen anders dan eventueel een per voertuig klein aantal agenten, en
- f) waarbij geen gebruik hoeft te worden gemaakt van een GPS (Global Positioning System).

30

35

#### Toelichting:

Wat korter (en minder precies) geformuleerd beschrijft conclusie 1 (een werkwijze voor) een fraudebestendig verkeersinformatiesysteem dat onrechtmatige tracering voorkomt zonder gebruik te hoeven maken van een GPS.

40

1011501

Het begrip *verkeersinformatie* moet in de meest ruime zin worden opgevat, zoals eerder in dit inleidende hoofdstuk al is geïllustreerd. Onder verkeersinformatie verstaan we zowel collectieve informatie als individuele informatie. Onder collectieve informatie verstaan wij informatie over verzamelingen met meerdere personen of voertuigen. Denk bv. aan informatie over verkeersstromen en/of over gemiddeld brandstofverbruik e.d. Individuele informatie betreft informatie over individuele personen en/of voertuigen.

Onder individuele informatie vallen o.a. voertuiginformatie, persoonsinformatie, gebruiksinformatie en omstandighedeninformatie. De term voertuiginformatie wordt beschreven in het hoofdstuk over TIP-systemen en persoonsinformatie spreekt voor zich. Onder gebruiksinformatie valt zowel informatie over het gebruik van het voertuig (afgelegde kilometers, veroorzaakte vervuiling, tijdstip, etc.; zie eerder in dit inleidende hoofdstuk voor nog veel meer voorbeelden) als informatie over de bestuurder en/of gebruiker en/of betaler. Onder omstandighedeninformatie valt informatie over diverse omstandigheden bij het gebruik, zoals bv. verkeersdrukte, weersomstandigheden, luchtvervuiling, e.d. Onder verkeersinformatie valt ook nog informatie over de infrastructuur. Deze vorm van verkeersinformatie wordt door het verkeersinformatiesysteem vaak alleen verspreid, maar kan evt. ook voor een deel via het verkeersinformatiesysteem worden verzameld.

De term *instantie* wordt hier en in volgende conclusies gebruikt als eerder beschreven in dit inleidende hoofdstuk. De term kan dus evt. staan voor één of meerdere instanties.

De term *voertuigen* moet zodanig worden verstaan dat het in ieder geval alle mogelijke vervoermiddelen omvat. Merk op dat als men het TIP-systeem wil gebruiken voor het in rekening brengen van de vervoerskosten van openbaar vervoer, dan in bepaalde gevallen elke passagier beschouwd moet worden, i.e. moet fungeren, als een virtueel vervoermiddel voor de middelen ter verstrekking van informatie. Immers, de verstrekking van de informatie kan dan eventueel plaatsvinden voor en/of na het betreden van het feitelijke, reële voertuig van het openbare vervoersysteem. (B.v. bij het betreden en verlaten van het perron.) Hoewel een passagier het bedoelde informatieverstrekkingmiddel dan evengoed zal meenemen in het feitelijke voertuig, vindt de communicatie met de instantie in zo'n geval niet plaats vanuit een feitelijk voertuig van de vervoerder, maar vanaf een passagier (i.e. vanuit een virtueel vervoermiddel) buiten het feitelijke voertuig.

We hebben gekozen voor het afdekken van zulke mogelijkheden via de expliciet in deze toelichting duidelijk gemaakte mogelijkheid om het begrip voertuig resp. vervoermiddel extra ruim te interpreteren. Deze keus is zo gemaakt, omdat het niet makkelijk is om zulke mogelijkheden expliciet op te nemen in de formuleringen zonder deze weer wat ingewikkelder, onduidelijker en/of minder begrijpelijk te maken. Ter nadere illustratie schetsen we onze beste poging. In plaats van voertuig(en) moet in de formuleringen (zeker in conclusie 1, maar ook in een aantal andere conclusies) dan overal het ruimere begrip verkeersdeelnemer(s) gebruikt worden. Onder dit begrip moeten dan wel tenminste zowel personen als voertuigen vallen.

Bij punt c van conclusie 1 komt dan dus 'personen en/of verkeersdeelnemers' te staan. Merk op dat alleen 'verkeersdeelnemers' bij punt c onjuist zou zijn, want dan zou de essentie worden gemist zodra de verkeersdeelnemers niet staan voor personen, maar voor b.v. voertuigen, zoals o.a. het geval is bij wegverkeer. De eerder genoemde, wel juiste formulering van punt c heeft echter toch een merkwaardig trekje. Immers, de verkeersdeelnemers kunnen, zoals in het hierboven beschreven voorbeeld in de context van openbaar vervoer,

soms staan voor personen. Derhalve omvat de formulering van punt c dan in feite de op zich correcte, maar toch wat vreemde zinsnede 'personen en/of personen'. Hoe dan ook, we hopen met bovenstaande de grote reikwijdte van de formulering van conclusie 1 voldoende te hebben toegelicht.

5 Onder *in voertuigen aanwezige* middelen verstaan we o.a. middelen die alleen tijdens gebruik van het betreffende voertuig aanwezig zijn (bv. omdat een persoon die gebruik maakt van dat voertuig, het middel bij zich heeft), en natuurlijk ook middelen die in of aan het betreffende voertuig zijn aangebracht.

10 Onder *middelen ter verstrekking* van informatie verstaan we niet alleen de middelen (zoals bv. een zender) die direct betrokken zijn bij de verstrekking, maar ook middelen die daar indirect bij betrokken zijn, zoals m.n. middelen nodig voor het verzamelen en/of registreren van alle informatie die nodig is om de te verstrekken informatie te verkrijgen. Bijvoorbeeld kan hieronder ook een ontvanger vallen. Immers, stel dat een agent (zie hieronder) gebruikt wordt voor het aan een instantie verstrekken van betrouwbare informatie over, zeg, de kilometerstand, en dat de agent bij tijd en wijle de precisie van de bijgehouden kilometerstanden controleert m.b.v. vanuit de buitenwereld via een zender verstrekte betrouwbare informatie over, zeg, de snelheid van het betreffende voertuig op een zeker moment. (Zie de sectie over controle op de kilometerteller m.b.v. betrouwbare informatie over snelheid in het hoofdstuk over de aanpak m.b.v. agenten.) Dan behoort de benodigde ontvanger in dat voertuig tot de bedoelde middelen. In ieder geval kunnen alle middelen die genoemd worden in de in het hoofdstuk over apparatuur gegeven opsomming van mogelijk benodigde apparaten en/of  
20 elementen, behoren tot de in een voertuig aanwezige middelen ter verstrekking.

Onder de te verstrekken *informatie* valt in ieder geval alle informatie waaruit direct of indirect verkeersinformatie in de meest ruime zin (zie hierboven) afgeleid kan worden. Natuurlijk zal de vanuit een individueel voertuig verstrekte informatie in onze context i.h.a. betrekking hebben op dat ene voertuig en/of zijn directe  
25 omgeving en zal deze informatie vaak zelf al een vorm van individuele verkeersinformatie zijn. Denk bv. aan informatie over dat voertuig, over het gebruik van dat voertuig en/of over omstandigheden bij het gebruik van dat voertuig. Hoe dan ook, in principe kan het gaan om alle informatie die in een individueel voertuig verzameld (en dus vanuit dat voertuig verstrekt) kan worden.

30 De verkeersinformatie kan afgeleid worden uit *de inhoud* van de vanuit voertuigen verzonden berichten zelf of uit *de ontvangst*. Met de formulering '... uit (de ontvangst van) ...' willen we dit benadrukken. Onder de direct of indirect afleidbare verkeersinformatie valt dus o.a. ook informatie die af te leiden valt uit één of meer van de volgende constatering: 1) dat er überhaupt een bericht of een bepaald bericht ontvangen is, 2) dat een (bepaald) bericht op een bepaalde plaats ontvangen is, 3) dat een (bepaald) bericht vanaf een bepaalde  
35 plaats verzonden is, en/of 4) dat een (bepaald) bericht op een bepaald tijdstip ontvangen is.

Het begrip *onrechtmatige tracering* is in dit inleidende hoofdstuk al genoemd en wordt in het hoofdstuk over tracering uitgebreid behandeld. Het gaat hier dus om privacybescherming m.b.t. bewegingspatronen. Merk op dat de beperkende kwalificatie 'onrechtmatige' impliceert dat niet geëist wordt dat rechtmatige tracering van  
40 personen en/of voertuigen wordt voorkomen. Het (in beperkte mate) traceren van personen en/of voertuigen

waarvan de identiteit niet achterhaald kan worden, beschouwen wij als rechtmatig. Dus tracering kan bij een verkeersinformatiesysteem dat gebruik maakt van de werkwijze omschreven in deze conclusie, wel degelijk worden toegestaan, zolang de betreffende identiteit(en) maar niet te achterhalen zijn. Tracering buiten het verkeersinformatiesysteem om kan natuurlijk niet voorkomen worden. Het woord 'voorkomen' moet hier dus

5

m.n. gelezen worden als 'niet praktisch uitvoerbaar maken' of als 'in hoge mate tegengaan'.

De formulering 'in of vanuit voertuigen verstrekte informatie' is gekozen omdat de controle op de betrouwbaarheid niet alleen op afstand, i.e. buiten de voertuigen, kan plaatsvinden, maar evt. ook (geheel of gedeeltelijk) in het voertuig uitgevoerd kan worden door een agent. (Verderop wordt meer gezegd over het begrip agent.) De in het voertuig aan de agent verstrekte informatie wordt dan (geheel of gedeeltelijk) gecontroleerd en de agent zorgt dan voor verstrekking van betrouwbare informatie vanuit het voertuig aan (de rest van) de instantie in de buitenwereld.

10

Bij de controle op de betrouwbaarheid van informatie is de beperking 'voor zover nodig' aangebracht, m.n. omdat het voor (voldoende) fraudebestendigheid niet nodig is om alle informatie te controleren. Met dit laatste doelen we niet alleen op het feit dat controles meestal steekproefsgewijs worden uitgevoerd, maar m.n. ook op het feit dat het niet essentieel hoeft te zijn dat alle informatie correct is. Ter illustratie en verduidelijking van deze laatste opmerking wijzen we hier op de (in het hoofdstuk over gebruik van een zender genoemde) mogelijkheid om vanuit (een deel van) de voertuigen alleen (semi-)identificaties uit te laten zenden om op basis daarvan informatie over filevertragingen te kunnen afleiden. In dit voorbeeld is controle op de juistheid van de uitgezonden (semi-)identificatie van elk voertuig i.h.a. niet nodig. Immers, de gewenste file-informatie kan, zelfs als het percentage onjuiste verstrekkingen substantieel is, meestal toch verkregen worden. Bovendien zullen de meeste verkeersdeelnemers er dan i.h.a. geen belang bij hebben om verkeerde informatie te verstrekken.

15

20

25

Voor een nadere toelichting op de *fraudebestendigheid van individuele componenten*, verwijzen we naar het hoofdstuk over fraudebestendigheid. Middelen in het voertuig, zoals b.v. zenders, ontvangers, sensoren, meters, tellers en verbindingen, hoeven dus (wat de instantie betreft) niet fysiek tegen fraude beveiligd te worden, i.e. hoeven als individuele component niet fraudebestendig te zijn.

30

Voor het begrip *agent* verwijzen we primair naar de eerder in dit inleidende hoofdstuk gegeven omschrijving. Merk op dat een vanuit het oogpunt van de instantie fraudebestendige component alleen een agent wordt genoemd als die component bij tijd en wijle in een voertuig actief een taak uitvoert t.b.v. de instantie. Dus een passieve component, zoals bv. een magneetstrip of een ingeslagen chassisnummer, kan hier niet onder vallen. Ook niet als b.v. het chassisnummer zodanig op de carrosserie is aangebracht dat het door de instantie wel degelijk voldoende fraudebestendig wordt geacht. Voor een nadere verduidelijking van het begrip agent verwijzen we naar dit inleidende hoofdstuk en naar de drie hoofdstukken over de aanpak met agenten, over voorbereiding op 'groei' van het systeem en over TIP-systemen.

35



Met 'een klein aantal' zijn we bewust enigszins vaag, want men kan eventueel ook onnodig veel agenten gebruiken. De meest prominente aantallen die hieronder vallen, zijn 0, 1 en 2. Deze drie mogelijke aantallen worden in respectievelijk de conclusies 8, 9 en 10 expliciet tot uitdrukking gebracht.

5 Het woord 'eventueel' is bedoeld extra tot uitdrukking te brengen dat ook de afwezigheid van agenten (i.e. nul agenten) binnen de omschrijving valt.

In een voorkeursuitvoeringsvorm van een werkwijze volgens de uitvinding kan betrouwbare informatie worden verzameld over één of meerdere aspecten, waaronder begrepen individuele informatie over o.a. de afgelegde  
10 afstand, de plaats, de datum, het tijdstip, het merk, het model, het bouwjaar, het versnellingsbaktype, het motor-  
type, de ingeschakelde versnelling, het toerental, de snelheid, de snelheidsveranderingen, de gebruikte brandstof-  
soort, het brandstofverbruik, de geluidsproductie en/of de veroorzaakte milieuvuiling, en collectieve informa-  
tie over o.a. verkeersdrukke, files, het brandstofverbruik, de geluidsproductie en/of de veroorzaakte milieuv-  
vuiling. (Dit is conclusie 2.)

15

*Toelichting:*

Met deze conclusie proberen we de grote reikwijdte van het TIP-systeem aan te geven wat betreft de soorten  
informatie die verzameld en, voor zover nodig, op betrouwbaarheid gecontroleerd kunnen worden. Let wel,  
het gaat steeds om informatie die *in principe* verzameld kan worden. Het is dus niet zo dat elk TIP-systeem  
20 alle genoemde soorten informatie ook daadwerkelijk hoeft te (kunnen) verzamelen en controleren. De hier  
gebruikte begrippen individuele en collectieve informatie zijn geïntroduceerd in de toelichting bij conclusie 1.  
De preciezere betekenis van de beknopt geformuleerde opsomming is al eerder in dit inleidende hoofdstuk  
duidelijk(er) gemaakt d.m.v. een uitgebreider geformuleerde opsomming met enige bijbehorende toelichting.  
Voor alle zekerheid merken we hier nog eens expliciet op, dat de opsomming niet uitputtend is. Merk op dat  
25 de collectieve informatie desgewenst uitgesplitst kan worden naar één of meerdere van de (al dan niet ge-  
noemde) aspecten.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding kan het volgen van de  
loop van verkeersstromen en het bepalen van filevertragingen automatisch en op een privacy vriendelijke wijze  
30 worden uitgevoerd. (Dit is conclusie 3.)

*Toelichting:*

Met het volgen van de loop van verkeersstromen bedoelen we m.n. ook het inzicht krijgen in hoe verkeers-  
stromen zich splitsen en samenvoegen. Het is dus nodig om individuele voertuigen in de verkeersstroom te  
35 kunnen volgen. Beide genoemde taken kunnen uitgevoerd worden m.b.v. vanuit voertuigen uitgezonden semi-  
identificaties. (Zie ook de volgende conclusie.) Merk op dat het aspect van privacy vriendelijkheid in feite  
ook al opgenomen is in conclusie 1.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt gebruik ge-  
40 maakt van semi-identificatie(s). (Dit is conclusie 4.)

1011501

*Toelichting:*

De term *semi-identificatie* staat hier zowel voor een semi-identificatieproces als voor een semi-identificerend gegeven (resp. een semi-identificerende gegevenscombinatie). Deze begrippen worden behandeld in het hoofdstuk over semi-identificatie. Semi-identificaties kunnen o.a. gebruikt worden voor het privacy vriendelijk uitvoeren van trajectsnelheidscontroles, van controles op de precisie van tellers en van bepaalde taken vallend onder de noemer verkeersbeheer, zoals b.v. het doen van verkeerstellingen, het volgen van de loop van verkeersstromen, het bepalen van de gemiddelde snelheid van verkeersstromen, het bepalen van snelheidsverschillen tussen individuele voertuigen in een verkeersstroom, het bepalen van de onderlinge afstand tussen voertuigen, het detecteren van beginnende filevorming, het detecteren van files en/of het bepalen van filevertragingen. Indirect is dit o.a. ook nuttig voor verkeersregulering en voor het bepalen en/of plannen van de behoefte aan uitbreiding van de infrastructuur.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt onrechtmatige tractering voorkomen door gebruik te maken van tenminste één organisatie die onafhankelijk is van de instantie. (Dit is conclusie 5.)

*Toelichting:*

Deze conclusie dekt niet alleen het gebruik van een jager en/of een intermediair af, maar b.v. ook het gebruik van een organisatie die ervoor zorgt dat een bepaalde indirecte identificatie gebruikt kan worden voor de privacy bescherming. De indirecte identificatie betreft dan dus een identificatie die semi-anoniem is verstrekt. (Zie het hoofdstuk over privacybescherming. Het woord identificatie staat hier voor een identificerende combinatie van gegevens, zoals bv. een identificatienummer.) Voor alle zekerheid wordt het gebruik van een jager en/of een intermediair ook nog afgedekt door twee aparte, specifieke conclusies, nl. de conclusies 6 en 7.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt voor althans een deel van de communicatie tussen voertuigen en de instantie gebruik gemaakt van één of meerdere jagers. (Dit is conclusie 6.)

30 *Toelichting:*

Het begrip *jager* wordt beschreven in het hoofdstuk over privacybescherming (en m.n. aan het eind van dat hoofdstuk). Een jager is een organisatie die althans een deel van de zend- en/of ontvangmiddelen in de buitenwereld (i.e. buiten de voertuigen) t.b.v. de communicatie tussen voertuigen en (de rest van) het verkeersinformatiesysteem beheert en een bijdrage levert aan het zoveel mogelijk geheim houden van de positie van een persoon of voertuig m.n. op het moment van ontvangst van een bericht vanuit dat voertuig. Primair doelen we hier op een 'zuivere' jager (zie het hoofdstuk over privacybescherming), maar secundair ook op een jager die ook althans een deel van de taken van een intermediair uitvoert.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt voor althans een deel van de communicatie tussen voertuigen en de instantie gebruik gemaakt van één of meerdere intermediairs, die bij die communicatie fungeren als tussenpersoon. (Dit is conclusie 7.)

5 *Toelichting:*

Het begrip *intermediair* wordt beschreven in het hoofdstuk over privacybescherming (en m.n. aan het eind van dat hoofdstuk). Een intermediair is een organisatie die onafhankelijk is van de instantie en die t.b.v. de privacybescherming bij de communicatie vanuit voertuigen met de instantie fungeert als tussenpersoon.

10 In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding is in althans een deel van de voertuigen ook tijdens gebruik geen agent nodig. (Dit is conclusie 8.)

*Toelichting:*

15 De eventueel benodigde controles moeten dan voor de voertuigen zonder agent op afstand, i.e. buiten de betreffende voertuigen, worden uitgevoerd. Deze conclusie dekt dus het geval dat voor (een deel van) de voertuigen de aanpak met uitsluitend controles op afstand wordt gebruikt.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding is in althans een deel van de voertuigen tijdens gebruik één agent nodig. (Dit is conclusie 9.)

20

*Toelichting:*

Zie het hoofdstuk over de aanpak met agenten en m.n. de sectie over algemene en gespecialiseerde agenten en de sectie over het gebruik van één of meerdere agenten. Merk op dat hier b.v. niet is vastgelegd dat de agent controles moet uitvoeren. Als de agent wel controles uitvoert, dan hoeft de agent nog niet per sé alle controles uit te voeren. (Zie ook de toelichting bij conclusie 11.)

25

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding zijn in althans een deel van de voertuigen tijdens gebruik twee agenten nodig. (Dit is conclusie 10.)

30 *Toelichting:*

Zie de toelichting bij conclusie 9.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding worden alle of een deel van de controles op de betrouwbaarheid van de vanuit een bepaald voertuig verstrekte informatie geheel of gedeeltelijk buiten dat voertuig, i.e. op afstand, uitgevoerd. (Dit is conclusie 11.)

35

*Toelichting:*

40 Deze conclusie is m.n. bedoeld om *expliciet* alle mogelijkheden af te dekken waarbij controles voorkomen die geheel of gedeeltelijk op afstand worden uitgevoerd. *Impliciet* waren op z'n minst een aantal van die mogelijkheden al gedekt. Voor alle duidelijkheid sommen we hier expliciet vier van het totale aantal mogelijke si-

tuaties op: 1) de mogelijkheid dat *alle* controles m.b.t. een bepaald voertuig volledig op afstand worden uitgevoerd (deze mogelijkheid werd eigenlijk door conclusie 8 al indirect resp. impliciet gedekt), 2) de mogelijkheid dat *alle* controles volledig door één of meerdere agenten uitgevoerd worden (deze mogelijkheid werd door de conclusies 1, 9 en 10 al afgedekt, maar merk op dat de conclusies 9 en 10 ook gevallen afdekken waarin agenten voor een bepaalde controle slechts een deel van die controle verzorgen), 3) de mogelijkheid dat bij één bepaald voertuig een bepaalde controle *geheel* op afstand en een bepaalde controle *volledig* door één of meerdere agenten wordt uitgevoerd, en 4) de mogelijkheid dat een bepaalde controle *deels* op afstand en *deels* door een agent wordt uitgevoerd. Zie voor een voorbeeld van de laatstgenoemde mogelijkheid het hoofdstuk over de aanpak m.b.v. agenten, en wel i.h.b. de sectie over toezicht van een agent op de tellermonotonie en een aantal daarop volgende secties. Deze conclusie is bedoeld om mogelijkheid 1 en m.n. ook de mogelijkheden 3 en 4 expliciet af te dekken.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt informatie verzameld over het brandstofverbruik van individuele voertuigen. (Dit is conclusie 12.)

*Toelichting:*

Informatie over brandstofverbruik omvat zowel informatie over de toevoersnelheid van brandstof (i.e. over de aangeduide waarde van een brandstofverbruiksmeter) als over de stand van een brandstofmeter (i.e. van een brandstofverbruiksteller). De bedoelde informatie kan b.v. verzameld worden om praktijkgegevens te kunnen afleiden over het brandstofverbruik van voertuigen, al dan niet uitgesplitst naar b.v. merk, model, bouwjaar, versnellingsbaktype, motortype, snelheid, snelheidsverandering, ingeschakelde versnelling, toerental, motortemperatuur, luchtvochtigheid, buitentemperatuur, e.d. Of kan b.v. verzameld worden om (mede) gebruikt te worden voor het opleggen van een verkeersheffing (zie conclusie 18). Merk op dat de verzamelde informatie evt. kan worden gecontroleerd op betrouwbaarheid.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt informatie verzameld over door individuele voertuigen veroorzaakte milieuvervuiling. (Dit is conclusie 13.)

*Toelichting:*

Dit soort informatie kan verzameld worden b.v. om een beter beeld te krijgen van de totale milieuvervuiling veroorzaakt door motorvoertuigen of b.v. om deze informatie (mede) te gebruiken voor het opleggen van een verkeersheffing (zie conclusie 18). Merk op dat de verzamelde informatie evt. kan worden gecontroleerd op betrouwbaarheid.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt informatie verzameld over door individuele voertuigen veroorzaakt geluid. (Dit is conclusie 14.)

*Toelichting:*

Dit soort informatie kan verzameld worden b.v. om een beter beeld te krijgen van de geluidsbelasting resp. het verkeerslawaai op bepaalde weggedeelten of b.v. om deze informatie (mede) te gebruiken voor het opleg-

gen van een verkeersheffing (zie conclusie 18). Zie o.a. de voorlaatste sectie van het hoofdstuk over semi-identificatie, i.e. de sectie over eventueel geïntegreerde verkeersboetes in dat hoofdstuk, en de laatste sectie van het hoofdstuk over TIP-systemen, i.e. de sectie over TIP-systemen voor ander verkeer. Merk op dat de verzamelde informatie evt. kan worden gecontroleerd op betrouwbaarheid.

5

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt informatie verzameld over de bij individuele voertuigen ingeschakelde versnelling. (Dit is conclusie 15.)

*Toelichting:*

10 Merk op dat de verzamelde informatie evt. kan worden gecontroleerd op betrouwbaarheid. Zie ook conclusie 28. Dit soort informatie kan b.v. verzameld worden om deze informatie (mede) te gebruiken voor het opleggen van een verkeersheffing (zie conclusie 18).

15 In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt informatie verzameld over het motortoerental van individuele voertuigen. (Dit is conclusie 16.)

*Toelichting:*

20 Merk op dat de verzamelde informatie evt. kan worden gecontroleerd op betrouwbaarheid. Zie ook conclusie 28. Dit soort informatie kan b.v. verzameld worden om deze informatie (mede) te gebruiken voor het opleggen van een verkeersheffing (zie conclusie 18).

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt informatie verzameld over bepaalde, bij individuele voertuigen of personen horende tellers. (Dit is conclusie 17.)

25 *Toelichting:*

De *tellers* kunnen van allerlei aard zijn. Denk bv. aan kilometertellers, toerentellers, e.d., maar ook aan tellers m.b.t. brandstofverbruik, geluidsproductie, milieuvervuiling, verbruiksrechten, heffingspunten, e.d. Dit soort informatie kan verzameld worden b.v. om een beter beeld te krijgen van de totale omvang van het verkeer met bepaalde soorten motorvoertuigen of b.v. om deze informatie te gebruiken voor het opleggen van een ver-

30 keersheffing (zie conclusie 18).

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt de verzamelde informatie (mede) gebruikt voor het opleggen van een verkeersheffing. (Dit is conclusie 18.)

35 *Toelichting:*

De ruime betekenis van het begrip *verkeersheffing* is al beschreven in dit inleidende hoofdstuk. Merk op dat de in het hoofdstuk over soorten heffingen en tariefsystemen genoemde grens-, traject- en totaalheffingen hier allemaal bij inbegrepen zijn. Voor een aantal voorbeelden van tarieffuncties verwijzen we naar het hoofdstuk over administratie. Zie conclusie 2 en de eerdere tekst in dit inleidende hoofdstuk voor (controleerbare)

40 grootheden die o.a. gebruikt kunnen worden als argumenten (in de wiskundige betekenis) van een tarieffunctie. Zie ook conclusies 19 en 20.

N.B. Met tarief functie bedoelen we hetzelfde als met prijsfunctie (zie b.v. het hoofdstuk over administratie).

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding kan het gehanteerde tarief worden gerelateerd aan één of meerdere van de volgende aspecten: de afgelegde afstand, de plaats, de datum, het tijdstip, de verkeersdruk, het merk, model, bouwjaar, versnellingsbaktype, motortype, de ingescha-  
 5 kelde versnelling, het toerental, de snelheid, de snelheidsveranderingen, de brandstofsoort, het brandstofverbruik, de geluidsproductie en de veroorzaakte milieuvervuiling. (Dit is conclusie 19.)

*Toelichting:*

10 Deze conclusie ligt op basis van conclusies 2 en 18 tamelijk voor de hand. Er is voor gekozen om deze conclusie voor alle zekerheid ook expliciet te formuleren. Zie o.a. de tekst eerder in dit inleidende hoofdstuk voor een iets uitgebreider geformuleerde opsomming met (een deel van) de bijbehorende toelichting. Voor alle zekerheid wordt hier nog eens expliciet benadrukt, dat de opsomming niet uitputtend is. (Zie evt. ook de toelichting bij conclusie 2.) Bovenstaande geldt voor zowel een grens-, een traject- als een totaalheffing.

15

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt de verzamelde informatie (mede) gebruikt voor het opleggen van een totaalheffing. (Dit is conclusie 20.)

*Toelichting:*

20 Een *totaalheffing* is een specifieke vorm van verkeersheffing. Het begrip totaalheffing wordt behandeld in het hoofdstuk over soorten heffingen en tariefsystemen. De totaalheffing kan b.v. gebaseerd zijn op een kilometer teller, een brandstofverbruiksteller, een geluidsproductieteller, een milieuvervuilings(equivalenten)teller en/of enige andere verkeersheffingsteller. Op deze wijze kunnen dus b.v. alle afgelegde afstanden, al het brandstofverbruik, alle veroorzaakte lawaai, alle veroorzaakte milieuvervuiling e.d. in rekening worden ge-  
 25 bracht. Voor een aantal voorbeelden van tarief functies (prijsfuncties) verwijzen we naar het hoofdstuk over administratie.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding vindt althans een deel van de communicatie vanuit een bepaald voertuig met een verkeersinformatie verzamelende, controlerende en/of  
 30 verspreidende instantie plaats via een in dat voertuig aanwezig en/of aan dat voertuig bevestigd zendmiddel en een zich buiten dat voertuig bevindend ontvangmiddel. (Dit is conclusie 21.)

*Toelichting:*

35 Deze conclusie beschrijft dat alle of een deel van de communicatie tussen voertuig en een instantie in de buitenwereld kan plaatsvinden m.b.v. zend- en ontvangmiddelen. De zinsnede 'althans een deel' heeft een dubbele functie, want het benadrukt: 1) dat het hier gaat over de communicatie in één richting, nl. van voertuig naar buitenwereld, en 2) dat niet alle communicatie via de zend- en ontvangmiddelen hoeft te geschieden.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding vindt althans een deel van de communicatie vanuit een bepaald voertuig met een verkeersinformatie verzamelende, controlerende en/of verspreidende instantie plaats via een zich buiten dat voertuig bevindend zendmiddel en een in dat voertuig aanwezig en/of aan dat voertuig bevestigd ontvangmiddel. (Dit is conclusie 22.)

5

*Toelichting:*

Voor deze conclusie geldt hetzelfde als de vorige, zij het dat het nu de communicatie betreft vanuit de buitenwereld naar het voertuig.

10 In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding zijn althans een deel van de zich buiten de voertuigen bevindende zend- en/of ontvangmiddelen mobiel. (Dit is conclusie 23.)

*Toelichting:*

15 Deze conclusie spreekt voor zich, zij het dat de betekenis van mobiel tweeledig moet worden opgevat, nl. zowel in de betekenis van verplaatsbaar, als in de betekenis van in beweging zijnd (zeg maar, verplaatsend). Deze conclusie dekt dus o.a. het 'uitlezen' van voertuigen vanuit een rijdende patrouillewagen af. Het controleren vanuit een rijdende patrouillewagen wordt nog expliciet afgedekt in conclusie 30.

20 In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding is (ook) sprake van het verspreiden van verkeersinformatie door een instantie. (Dit is conclusie 24.)

*Toelichting:*

25 Deze conclusie beschrijft dat het betreffende verkeersinformatiesysteem ook geschikt is voor het verspreiden van verkeersinformatie. Merk op dat verkeersinformatie ook informatie over de infrastructuur omvat. Denk bv. aan inrijverboden, snelheidsbeperkingen en tijdelijk verplichte alternatieve routes (i.e. omleidingen). De informatie die naar een voertuig wordt gestuurd voor b.v. navigatie of t.b.v. controles in het voertuig door een agent (denk aan de eerder behandelde positie- en/of snelheidsgegevens), vallen ook onder ons ruime begrip verkeersinformatie.

30 In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt gebruik gemaakt van semi-identificaties die zijn afgeleid van een tellerstand. (Dit is conclusie 25.)

*Toelichting:*

35 De betreffende teller kan b.v. een kilometerteller, een verbruiksteller of een verkeersheffingsteller zijn. Het enige wat essentieel is, is dat het juiste verloop van de betreffende tellerstand extern (i.e. op enige afstand buiten het voertuig) voldoende nauwkeurig kan worden bepaald of voorspeld. De bedoelde teller kan bij het betreffende voertuig horen of bij de betreffende gebruiker of betaler. Zie ook het hoofdstuk over semi-identificatie.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt gebruik gemaakt van semi-identificaties die zijn afgeleid van het kenteken van het betreffende voertuig. (Dit is conclusie 26.)

5 *Toelichting:*

Zie ook het hoofdstuk over semi-identificatie en i.h.b. de sectie over kunstmatige semi-identificatienummers in dat hoofdstuk.

10 In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt gebruik gemaakt van semi-identificaties die voor elk voertuig lukraak gekozen zijn uit een verzameling elementen. (Dit is conclusie 27.)

*Toelichting:*

15 Zie ook het hoofdstuk over semi-identificatie en i.h.b. de sectie over kunstmatige semi-identificatienummers in dat hoofdstuk.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt de in of vanuit een voertuig verstrekte informatie gecontroleerd op betrouwbaarheid en betreft de (verstrekte en) gecontroleerde informatie tenminste informatie over één van de volgende aspecten: de kilometertellerstand, de snelheid, de ingeschakelde versnelling, het toerental, het brandstofverbruik, de geluidsproductie en/of de veroorzaakte milieuvervuiling. (Dit is conclusie 28.)

20

*Toelichting:*

25 Voor controle is externe bepaling van de juiste informatie nodig. Merk op dat kilometerstand en snelheidsaanduiding met elkaar te maken hebben en dus in zekere zin uitwisselbare gegevens zijn. (Zie ook de sectie over controles op basis van differentie- en differentiaalquotiënten in het hoofdstuk over controles.) Iets soortgelijks geldt natuurlijk voor een brandstofverbruiksmeter en -teller, een geluidsproductiemeter en -teller en een milieuvervuilingsmeter en -teller. Toerenteller staat i.h.a. zowel voor 'toerentalmeter' als voor 'toerental-teller'. Hoe de kilometerstand en/of de snelheidsmeteraanduiding kunnen worden gecontroleerd is uitgelegd in

30 de hoofdstukken over controles en over de aanpak m.b.v. agenten. Anders gezegd, externe bepaling van de lengte van een bepaald traject of van de snelheid op een bepaald moment is eenvoudig en bekend. De ingeschakelde versnelling kan extern worden bepaald (en dus gecontroleerd) via snelheidsmeting, acceleratiemeting en gerichte geluidsproductiemeting, waarbij tevens gebruik moet worden gemaakt van betrouwbare informatie over het type voertuig. Hoe het toerental en het brandstofverbruik extern kunnen worden bepaald

35 staat beschreven in de sectie over gegevens geschikt voor controle op afstand. In de daarop volgende sectie (over nog een voorbeeld van het nut van afgeleide informatie) wordt uitgelegd hoe de geluidsproductie kan worden bepaald. Het gebruik van afgeleide informatie werd al eerder in dit inleidende hoofdstuk toegelicht.



In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding voert een agent controles in het voertuig uit m.b.v. extern bepaalde, aan hem verstrekte, betrouwbare informatie. (Dit is conclusie 29.)

5 *Toelichting:*

Zie het hoofdstuk over de aanpak m.b.v. agenten. Hoe de benodigde betrouwbare, i.e. juiste, informatie extern kan worden bepaald, is voor een aantal soorten informatie al toegelicht bij conclusie 28. Voor o.a. plaats, datum en tijdstip behoeft de externe bepaling geen nadere toelichting. Hoe voor controles op kilometerstanden en snelheidsaanduiding gebruik kan worden gemaakt van toegestuurde, betrouwbare positie- of snelheidsgegevens, is beschreven in het hoofdstuk over de aanpak m.b.v. agenten. Controles op snelheidsveranderingen gaan soortgelijk. (Zie ook de sectie over controles op basis van differentie- en differentiaalquotiënten in het hoofdstuk over controles.) Ook controles op b.v. toerental, geluidsproductie, brandstofverbruik e.d. zijn in de tekst voldoende beschreven. De aan de agent verstrekte, extern bepaalde en betrouwbare informatie kan ook een berekeningswijze voor afgeleide informatie omvatten. Voor nadere toelichting op het gebruik van afgeleide informatie verwijzen we naar de betreffende sectie eerder in dit inleidende hoofdstuk.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding worden controles uitgevoerd vanuit mobiele controleposten. (Dit is conclusie 30.)

20 *Toelichting:*

Hier wordt met mobiel naast verplaatsbaar m.n. ook in beweging zijnd bedoeld. Deze conclusie dekt dus o.a. controles vanuit rijdende patrouillewagens af.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding worden trajectsnelheidscontroles uitgevoerd op een privacy vriendelijke wijze. (Dit is conclusie 31.)

*Toelichting:*

Met privacy vriendelijk bedoelen we dat alleen bij voertuigen waarmee de snelheidslimiet is overschreden, identificatie van de betreffende persoon (resp. betaler) en/of het betreffende voertuig plaatsvindt. De betekenis van betaler is behandeld in het hoofdstuk over apparatuur.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt de juiste tijd verspreid en wordt in althans een deel van de voertuigen tenminste één klok automatisch aangepast bij een tijdswisseling, waarvan b.v. sprake is bij het passeren van een tijdszonegrens of bij de overgang van zomertijd op wintertijd of andersom. (Dit is conclusie 32.)

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding is sprake van quoting van al dan niet verhandelbare verbruiksrechten. (Dit is conclusie 33.)

*Toelichting:*

Verbruiksrechten staat ook voor gebruiksrechten en 'vervuilingsrechten'. Gebruiksrechten kunnen b.v. in kilometers worden uitgedrukt en 'vervuilingsrechten' in een of andere milieuvervuilingseenheid.

- 5 In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding is sprake van opsporing van afwijkende, mogelijk niet (meer) juist functionerende voertuigen en/of voertuigapparatuur. (Dit is conclusie 34.)

*Toelichting:*

- 10 Voor het begrip voertuigapparatuur zie het hoofdstuk over apparatuur. De afwijking kan b.v. veroorzaakt zijn door een defect, door slijtage, door slechte afstelling of door een poging tot fraude.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding kunnen voertuigen op geautoriseerd verzoek worden opgespoord. (Dit is conclusie 35.)

15

*Toelichting:*

Zie het hoofdstuk over gebruik van een ontvanger.

- 20 In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding kan software via het verkeersinformatiesysteem verspreid en/of in werking gesteld worden. (Dit is conclusie 36.)

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding controleert een agent de betrouwbaarheid van een meetinstrument of teller in het betreffende voertuig geheel of gedeeltelijk. (Dit is conclusie 37.)

25

*Toelichting:*

Zie het hoofdstuk over de aanpak m.b.v. agenten. We laten daar zien dat controle op b.v. een kilometerteller ook gedeeltelijk door een agent kan worden uitgevoerd.

- 30 In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding is sprake van het gebruik van een agent bestaande uit een chip met een processor en geheugen dat althans voor een deel voldoende beveiligd is tegen het lezen van daarin opgeslagen gegevens en tegen het wijzigen van zulke gegevens en/of tegen het wijzigen van de door die chip gebruikte software. (Dit is conclusie 38.)

- 35 *Toelichting:*

Hoewel software in principe ook tot de gegevens gerekend kan worden, is het hier apart genoemd, omdat de software niet beveiligd hoeft te worden tegen lezen. Denk bij de tegen lezen en wijzigen (en dus ook tegen schrijven) beveiligde gegevens o.a. aan tellerstanden en/of cryptografische sleutels.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding worden praktijkgegevens verzameld over bepaalde prestaties van voertuigen bij bepaalde gebruiksomstandigheden en worden deze verzamelde gegevens al dan niet verwerkt tot informatie over bepaalde prestaties van bepaalde groepen voertuigen bij bepaalde gebruiksomstandigheden. (Dit is conclusie 39.)

5

*Toelichting:*

Onder gebruiksomstandigheden bedoelen we hier o.a. alle aspecten thuishorend bij gebruiksinformatie en bij omstandighedeninformatie, welke beide categorieën zijn beschreven in de toelichting op conclusie 1. Denk b.v. aan het verzamelen van gegevens m.b.t. brandstofverbruik en het verwerken tot informatie over de hoogte van het brandstofverbruik onder bepaalde gebruiksomstandigheden, zoals b.v. bij bepaalde snelheid, ingeschakelde versnelling, acceleratie, buitentemperatuur, e.d.

10

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding worden de verzamelde praktijkgegevens gebruikt voor het vinden/vaststellen van een berekeningswijze voor afgeleide informatie. (Dit is conclusie 40.)

15

*Toelichting:*

Een berekeningswijze kan b.v. worden vastgelegd als een algoritme of als één of meerdere tabellen. Een berekeningswijze kan b.v. gebruikt worden voor controles of voor gebruik in nieuwe 'meet'instrumenten.

20

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt gebruik gemaakt van een berekeningswijze voor afgeleide informatie voor het bepalen van het brandstofverbruik en/of de geluidsproductie van een individueel voertuig, al dan niet om gebruikt te gaan worden bij controles. (Dit is conclusie 41.)

25

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt gebruik gemaakt van een berekeningswijze voor afgeleide informatie voor het bepalen van de hoeveelheid (van een bepaalde vorm van) milieuvervuiling veroorzaakt door een individueel voertuig. (Dit is conclusie 42.)

30

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding maakt apparatuur voor cruise control in een voertuig gebruik van buiten het voertuig verspreide en door apparatuur in het voertuig ontvangen informatie over toegestane maximum snelheden. (Dit is conclusie 43.)

*Toelichting:*

35

De over snelheidslimieten verspreide informatie kan bestaan uit absolute aanduidingen van de snelheidslimieten of uit de relatieve verandering van de nieuwe snelheidslimiet t.o.v. de vorige. (In het laatste geval gaat het dus om het verschil op de grens van twee aaneengesloten gebieden met ieder hun eigen snelheidslimiet.) Een cruise control kan de informatie over de ter plekke geldende officiële snelheidslimiet (op verzoek van de bestuurder) gebruiken voor het automatisch respecteren van snelheidslimieten.

40

1011501

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt d.m.v. het verkeersinformatiesysteem verzamelde en/of verspreide informatie gebruikt voor ijking van een meetinstrument. (Dit is conclusie 44.)

5 *Toelichting:*

Zie de sectie over automatische ijking in het hoofdstuk over gebruik van een ontvanger. Deze conclusie dekt niet alleen ijking van instrumenten in een voertuig dan wel buiten de voertuigen af, maar ook het geval van wederzijdse ijking. Denk o.a. aan ijking van klokken, buitentemperatuurmeters, luchtvochtigheidsmeters, geluids(produktie)meters, snelheidsmeters en kilometertellers. Bij de twee laatstgenoemde voorbeelden kan op  
10 deze wijze de onnauwkeurigheid t.g.v. bandenslijtage uitgebannen worden.

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt een agent (ook) gebruikt voor fraudebestendige identificatie van het voertuig waarin die agent, al dan niet fraudebestendig gekoppeld, is aangebracht. (Dit is conclusie 45.)

15

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt de juistheid van verstrekte tellerstand(en) geheel of gedeeltelijk op afstand steekproefsgewijs gecontroleerd. (Dit is conclusie 46.)

20 *Toelichting:*

Dat tellers evt. geheel op afstand kunnen worden gecontroleerd, is geïllustreerd in het hoofdstuk over controles. Dat tellers evt. gedeeltelijk op afstand kunnen worden gecontroleerd, is aan de hand van kilometertellers geïllustreerd in het hoofdstuk over de aanpak m.b.v. agenten. Denk m.n. aan verschillende controle-aspecten, zoals controle op precisie en controle op monotonie.

25

In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding zijn in een voertuig audiovisuele middelen aangebracht welke tenminste een deel van de informatie kunnen weergeven. (Dit is conclusie 47.)

30 In een verdere voorkeursuitvoeringsvorm van een werkwijze overeenkomstig de uitvinding wordt althans een deel van de verspreide informatie (mede) gebruikt voor navigatie. (Dit is conclusie 48.)

De uitvinding refereert tevens aan een verkeersinformatiesysteem met een werkwijze volgens de uitvinding. (Dit is conclusie 49.)

35

De uitvinding is eveneens gerelateerd aan een verkeersinformatiesysteem volgens conclusie 49 dat is voorbereid op aanpassingen en uitbreidingen. (Dit is conclusie 50.)

40 De uitvinding heeft ook betrekking op een voertuig geschikt voor (gebruik bij) een werkwijze volgens de uitvinding. (Dit is conclusie 51.)

1011501

De uitvinding refereert tevens aan een agent geschikt voor (gebruik bij) een werkwijze volgens de uitvinding. (Dit is conclusie 52.)

*Toelichting:*

5 Een agent is een uit apparatuur en/of programmatuur bestaande, vanuit het oogpunt van de instantie fraudebestendige component.

De uitvinding is eveneens gerelateerd aan een uit apparatuur en programmatuur bestaande component, geschikt voor gebruik als voertuigprocessor voor een werkwijze volgens de uitvinding. (Dit is conclusie 53.)

10

*Toelichting:*

De component zal (zeer waarschijnlijk) een uit een processor met geheugen en software bestaand gegevensverwerkend middel zijn dat niet fraudebestendig hoeft te zijn. De voertuigprocessor is primair bedoeld om taken namens de houder (en evt. ook namens de gebruiker) van het voertuig te verrichten. De voertuigprocessor kan evt. (ook) bepaalde taken uitvoeren t.b.v. de instantie, tenminste als de instantie toestaat dat die taken namens haar worden uitgevoerd door een niet fraudebestendige component, i.e. als de instantie niet hecht aan werkelijk goede beveiliging tegen fraude. Zie o.a. de hoofdstukken over apparatuur en over voorbereiding op 'groei' van het systeem.

20 De uitvinding heeft ook betrekking op een gebruikerskaart geschikt voor (gebruik bij) een werkwijze volgens de uitvinding. (Dit is conclusie 54.)

*Toelichting:*

25 Het begrip gebruikerskaart heeft hier een ruime betekenis. Onder een gebruikerskaart wordt dus o.a. ook verstaan een verbruikspas. Zie het hoofdstuk over apparatuur.

De uitvinding heeft ook betrekking op een rollenbank voor het nader inspecteren van de werking van voertuigapparatuur (mede) t.b.v. een werkwijze volgens de uitvinding resp. (mede) t.b.v. een verkeersinformatiesysteem volgens de uitvinding. (Dit is conclusie 55.)

30

De uitvinding refereert tevens aan een betrouwbare taximeter waarbij gebruik gemaakt wordt van een werkwijze volgens de uitvinding. (Dit is conclusie 56.)

*Toelichting:*

35 Het adjectief 'betrouwbare' betreft hier, naast de fraudebestendigheid van het betreffende apparaat zelf, m.n. ook het controleren van de juistheid van (een deel van) de aangeleverde gegevens. (Zie het hoofdstuk over TIP-systemen.)

40 De uitvinding is tevens gerelateerd aan een betrouwbare tachograaf waarbij gebruik gemaakt wordt van een werkwijze volgens de uitvinding. (Dit is conclusie 57.)

1011501

*Toelichting:*

Het adjectief 'betrouwbare' betreft hier, naast de fraudebestendigheid van het betreffende apparaat zelf, m.n. ook het controleren van de juistheid van (een deel van) de aangeleverde gegevens. (Zie het hoofdstuk over TIP-systemen.)

5

De uitvinding heeft ook betrekking op een betrouwbare 'zwarte doos' (i.e. 'black box') waarbij gebruik gemaakt wordt van een werkwijze volgens de uitvinding. (Dit is conclusie 58.)

*Toelichting:*

10 Het adjectief 'betrouwbare' betreft hier, naast de fraudebestendigheid van het betreffende apparaat zelf, m.n. ook het controleren van de juistheid van (een deel van) de aangeleverde gegevens. (Zie het hoofdstuk over TIP-systemen.)

**Toelichting op en overzicht van verdere inhoud**

15

In het volgende zullen we stapsgewijs allerlei aspecten van het TIP-systeem behandelen en m.n. ook uitleggen hoe een en ander werkt. Bij de behandeling concentreren we ons voornamelijk op het gebruik van een TIP-systeem voor verkeersheffingen in het geval van wegverkeer en meer i.h.b. voor rekeningrijden. Dit doen we niet alleen omdat dit een belangrijke toepassing is, maar ook omdat daarbij de voor TIP-systemen kenmerkende wijzen van controle en van privacybescherming goed uit de verf kunnen komen. Immers, privacybescherming en fraudebestrijding zijn bij rekeningrijden, en bij verkeersheffingen meer in het algemeen, overduidelijk van groot belang. Zo nu en dan komen dan tussendoor aspecten en toepassingen aan bod die niet of niet direct met rekeningrijden of, algemener, verkeersheffingen van doen hebben.

20

25 We gebruiken zo nu en dan een concreet voorbeeld en noemen soms een aantal mogelijke varianten. De gegeven voorbeelden en varianten dienen, zoals al eerder opgemerkt, alleen ter illustratie en mogen niet begrepen worden als opgelegde beperkingen. Ook spreken we vaak, zoals al eerder in een voetnoot is opgemerkt, van *het* TIP-systeem, hoewel het feitelijk gaat om een klasse van vele systemen met bepaalde kenmerken.

30

Onze uitleg geschiedt min of meer in twee fases door in eerste instantie een aanpak te beschrijven zonder en daarna (bijna aan het eind pas) één met gebruik van agenten. Onbedoeld verhult onze uitleg (al dan niet mede daardoor) misschien in enige mate dat er een heel scala van mogelijkheden is om een TIP-systeem te realiseren m.b.v. de beschreven technieken en dat bij de diverse realisaties eventueel elementen uit beide meer expliciet beschreven aanpakken gecombineerd kunnen worden.

35

Ter nadere oriëntatie op de rest van de tekst geven we hier alleen de titels van de resterende hoofdstukken in de gebruikte volgorde:

- Soorten heffingen en tariefssystemen
- Tracering

40

- Fraudebestendigheid

- Apparatuur
- Cryptografie
- Administratie
- Gebruik van een zender
- 5 • Beveiliging van berichten
- Identificatienummers in berichten
- Controles
- Gebruik van een ontvanger
- Privacybescherming
- 10 • Identificatie
- Semi-identificatie en toepassingen ervan
- De aanpak m.b.v. agenten
- Voorbereiding op 'groei' van het systeem
- TIP-systemen
- 15 • Conclusies

## Soorten heffingen en tariefsystemen

Men kan diverse soorten heffingen resp. tariefsystemen onderscheiden. In dit stuk gebruiken we een classificatie waarbij (in ieder geval) onderscheid wordt gemaakt tussen grens-, traject- en totaalheffingen.

5

Bij *grensheffingen* wordt de heffing opgelegd op basis van het passeren van bepaalde grenzen, al dan niet in de directe omgeving van een bepaald (tol)punt. Hieronder vallen bijvoorbeeld de in- en uitvoerheffing op goederenverkeer bij het passeren van landsgrenzen, het sluis- en bruggeld in de scheepvaart en de tolheffing bij toltunnels en tolbruggen in geval van wegverkeer. Ook is er sprake van grensheffingen bij bepaalde zone-systemen, die b.v. voorkomen bij diverse vormen van openbaar vervoer. Het tarief bij de bedoelde zone-systemen is afhankelijk van het aantal zonegrenzen dat men passeert, zodat duidelijk van grensheffingen gesproken kan worden. Normaliter betaalt men echter ook voor het vervoer binnen één zone, waarbij dus geen enkele zonegrens gepasseerd wordt. Maar hierbij wordt toch wel degelijk een grens gepasseerd, nl. bij het betreden van het transportsysteem, i.h.b. bij het betreden van het voertuig of het perron.

15

*Trajectheffingen* worden opgelegd voor het afleggen van een of ander traject tussen een bepaald beginpunt en een bepaald eindpunt, waarbij het precieze traject, als dat überhaupt gekozen kan worden, geen rol speelt. Bekende voorbeelden van zulke tariefsystemen treft men aan bij post- en telefoonverkeer. Ook vallen hieronder bepaalde voor openbaar vervoer gehanteerde tariefsystemen en bepaalde tolsystemen waarbij van elke passagier resp. van elk voertuig zowel de plaats van toegang tot het vervoersysteem resp. tot een weg of wegnnet, als de plaats van verlaten ervan worden gebruikt voor het vaststellen van het juiste bedrag. Als er tussen het begin- en eindpunt meerdere routes kunnen worden gekozen, dan mag deze keuze geen invloed op de hoogte van het tarief hebben. Is dit laatste wel het geval, dan is er meestal sprake van een vorm van grensheffingen of soms van een vorm van totaalheffing.

25

Bij *totaalheffingen* wordt het totale 'verbruik' of de totale 'omzet', uitgedrukt in b.v. kilometers, liters brandstof, minuten, guldens of een of andere milieuvervuilingseenheid, in rekening gebracht. Hieronder vallen o.a. inkomstenbelasting, omzetbelasting en brandstofaccijnzen.

30

In bovenstaande kwam al enigszins naar voren dat het niet altijd even makkelijk is om een tariefstelsel juist te duiden als een systeem met grens-, traject- of totaalheffingen. Desalniettemin gaan we er vanuit dat e.e.a. duidelijk genoeg is voor ons doel, nl. het beschrijven en toelichten van allerlei aspecten van het TIP-systeem.



## Tracering

Zoals in de inleiding is opgemerkt, wordt het TIP-systeem o.a. gekenmerkt door de wijze waarop gezorgd kan worden voor de eigenschap dat (bij het verzamelen en/of controleren van informatie over personen en/of voertuigen) onrechtmatige tracering van individuele, uniek identificeerbare personen of voertuigen niet praktisch uitvoerbaar wordt gemaakt. Hiermee bedoelen we dat de informatie verzamelende en/of controlerende instantie i.h.a. geen toegang hoeft te krijgen, of redelijkerwijs zelfs kan krijgen, tot (privacy gevoelig beschouwde) informatie over het bewegingspatroon van een bepaald voertuig of een bepaalde persoon waarvan de identiteit achterhaald kan worden.

10

Het laatste deel van de voorgaande zin is van belang, omdat tracering van blijvend anonieme, i.e. niet identificeerbare, voertuigen en/of personen geen gevaar voor de privacy oplevert. De formulering dekt niet alleen het geval af dat de identiteit via het verkeersinformatiesysteem kan worden vastgesteld, maar ook het geval dat de identiteit (al dan niet later) op een andere wijze achterhaald kan worden. Merk op dat onbeperkte, volledige tracering van een vooralsnog niet identificeerbare persoon of voertuig een aanzienlijk gevaar oplevert, omdat er dan een reële kans is op latere identificatie. De bedreiging van de privacy door een vooralsnog anonieme tracering wordt kleiner naarmate de maximale duur en/of afstand waartoe zo'n tracering beperkt wordt, kleiner is. Als er sprake is van een voldoende beperking van de bedoelde duur en afstand, is er geen wezenlijk gevaar voor de privacy of, beter gezegd, kan het gevaar voor de privacy acceptabel worden gevonden.

20

In zo'n geval spreken wij van rechtmatige tracering. Het moge duidelijk zijn dat dit met het oog op de huidige praktijk alleszins gerechtvaardigd is. Immers, als een willekeurige burger een auto langs ziet rijden (i.e. het voertuig voor een tamelijk beperkte duur en afstand traceert) en vervolgens de identiteit van het voertuig (meestal juist) vaststelt door het lezen van de kentekenplaat, wordt algemeen geaccepteerd dat er geen sprake is van onrechtmatige tracering.

25

De toevoeging van het woord 'onrechtmatig' in de formulering van de genoemde eigenschap heeft nog een tweede reden. Vaak wil men voorkomen dat tracering onbeperkt kan plaatsvinden, maar wil men wel degelijk dat in bepaalde (bij voorkeur wettelijk vastgelegde) omstandigheden en onder bepaalde (bij voorkeur wettelijk vastgelegde) voorwaarden tracering mogelijk wordt. Denk enerzijds b.v. aan *trajectsnelheidscontroles*, waarbij de gemiddelde snelheid van een voertuig op een bepaald traject van, zeg, enkele kilometers wordt bepaald door een persoon of voertuig aan het begin en aan het eind van dat traject te identificeren en door de tijd vast te stellen die tussen beide identificaties verlopen is. Bij dit voorbeeld is de grootte van het traject meestal beperkt, zodat dit voorbeeld misschien niet voldoende overtuigend is. Denk daarom anderzijds b.v. ook aan de eventuele opsporing van gestolen voertuigen of zelfs aan de eventuele tracering van zware criminelen.

35

In het hoofdstuk over semi-identificaties zullen we laten zien dat voertuigen m.b.v. semi-identificaties voldoende goed getraceerd kunnen worden om b.v. trajectsnelheidscontroles uit te kunnen voeren of zelfs filevertragingen te meten zonder dat de privacy wezenlijk in gevaar komt. Deze vorm van tracering willen wij dus als rechtmatig betitelen. (Het moge duidelijk zijn dat, ten eerste, het hierbij gaat om een afweging van het praktisch nut en het

40

gevaar, en dat, ten tweede, wij denken dat het gevaar voldoende klein is om de balans door te mogen laten slaan ten gunste van het praktisch nut. Hoe klein het gevaar is, kan men zelf inschatten na lezing van dat hoofdstuk.)

5 Tenslotte herhalen we hier ten overvloede nog de eerder in een voetnoot gegeven opmerkingen over ons gebruik van diverse formuleringen. 'Privacybescherming m.b.t. bewegingspatronen' en 'niet praktisch uitvoerbaar maken van onrechtmatige tracering' betekenen bij ons hetzelfde. De toevoeging 'm.b.t. bewegingspatronen' laten we vaak en de toevoeging 'onrechtmatige' laten we soms voor het gemak achterwege. Ook spreken we vaak kortweg van 'voorkomen' of 'tegengaan' i.p.v. 'niet praktisch uitvoerbaar maken'. Wat precies bedoeld wordt, zal i.h.a. blijken uit de context. De omslachtige formulering 'niet praktisch uitvoerbaar maken' is al eerder en ook hier weer ge-  
10 noemd vanwege de grotere nauwkeurigheid t.o.v. 'voorkomen'. Immers, zoals uit een hierboven gegeven voorbeeld blijkt, is tracering in bepaalde mate sowieso al mogelijk en een verkeersinformatiesysteem kan zo'n tracering buiten zichzelf om natuurlijk niet voorkomen.

## Fraudebestendigheid

Strikt genomen is er pas sprake van (absolute) fraudebestendigheid als er geen enkele vorm van fraude mogelijk is. In de praktijk spreekt men vaak al van (voldoende) *fraudebestendigheid* als er sprake is van bestandheid tegen elke bekende, praktisch uitvoerbare en lonende vorm van fraude waartegen de belanghebbende zich wenst te wapenen. Immers, het is i.h.a. moeilijk zich te wapenen tegen alle nog onbekende vormen van fraude. En soms wenst men zich niet te bewapenen tegen bepaalde bekende vormen van fraude, omdat de kans op onaanvaardbare schade te klein wordt geacht (al dan niet in verhouding tot de kosten van beveiliging ertegen).

10 Wij gebruiken de term m.n. in de tweede betekenis. In dit stuk is de belanghebbende, i.e. degene die zich tegen fraude wil wapenen, meestal de instantie en bij ons wordt fraudebestendigheid dus meestal beschouwd vanuit het oogpunt van de verdediging van de belangen van (het verkeersinformatiesysteem resp.) de instantie. Dat belang behelst m.n. de juistheid van bepaalde informatie die verzameld wordt. M.b.v. controles op de betrouwbaarheid van die informatie kunnen we dus zorgen voor (tenminste een deel van de) fraudebestendigheid.

15 Met bovenstaande denken we voldoende duidelijk te hebben gemaakt wat *fraudebestendig* betekent. Met name moet nu voldoende duidelijk zijn wat we verstaan onder een fraudebestendig verkeersinformatiesysteem<sup>14</sup>. Het lijkt ons echter nuttig nog wat nader in te gaan op de toepassing van de term op een individuele component. We doen een poging tot het scheppen van extra duidelijkheid door hieronder een aanvullende, meer gedetailleerde en informatieve omschrijving te geven van het begrip fraudebestendigheid toegepast op een individuele component.

Een individuele *component* (in een voertuig) noemen we in deze tekst i.h.a. *fraudebestendig* als die component van zichzelf (!) zodanig beveiligd is dat deze redelijkerwijs niet vervalst kan worden, i.e. als die van zichzelf zodanig beveiligd is dat het niet lonend of niet praktisch uitvoerbaar is om die component te vervalsen. Onder vervalsen wordt niet alleen het maken van een (bedrieglijke) nabootsing verstaan, maar ook het manipuleren van die component (ten nadele van de instantie als belanghebbende). Denk bij dit laatste b.v. aan het in (voor de instantie) ongunstige zin beïnvloeden van het functioneren van de component (exclusief vernielen) of aan het aan de component ontfutselen van cruciale informatie (zoals b.v. van een cryptografische sleutel).

30 Bijvoorbeeld is een magneetkaart dus niet fraudebestendig, ook niet als de erin opgeslagen informatie m.b.v. cryptografische technieken beveiligd is. Immers, het maken van een nabootsing is bij een magneetkaart vrij makkelijk, omdat de bitpatronen op een magneetkaart zonder veel problemen gelezen kunnen worden. Bovendien geldt dat een magneetkaart niet van zichzelf beveiligd is tegen manipulatie, want het lezen, schrijven en/of wijzigen van het bitpatroon is tamelijk eenvoudig. Het doet dus niet ter zake dat het totale systeem (dat gebruik maakt van de bedoelde magneetkaarten) zich eventueel m.b.v. cryptografische technieken wel degelijk kan wapenen tegen bepaalde vormen van fraude met magneetkaarten, zoals b.v. tegen het begrijpend lezen of het zinvol veranderen van het bitpatroon dat erop staat. Voor andere passieve middelen voor gegevensopslag geldt natuurlijk iets soortgelijks.

<sup>14</sup> Wij concentreren onze aandacht (bijna vanzelfsprekend) op de fraudebestendigheid van componenten in het voertuig en van de communicatie via zenders.

Merk op dat er bij bepaalde electromagnetische (hulp)middelen, zoals b.v. magneet- en chipkaarten, i.h.a. alleen sprake kan zijn van nabootsing als men bepaalde cruciale bitpatronen (die b.v. een representatie zijn van software of gegevens, waaronder m.n. ook begrepen cryptografische sleutels) weet te kopiëren of produceren. Om zulke cruciale bitpatronen te kunnen kopiëren of produceren, is het gewoonlijk nodig om die of andere cruciale bitpatronen eerst aan één of meerdere niet vervalste exemplaren te ontfutselen. Maar dan is er dus eerst sprake van manipulatie van een ècht exemplaar ten nadele van de instantie. Kortom, manipulatie ten nadele van de belanghebbende is bij electromagnetische middelen i.h.a. de van overheersend belang zijnde vorm van vervalsing.

10 Merk ook op dat bij de fraudebestendigheid van een individuele component fysieke beveiliging i.h.a. een overheersende rol speelt en doorslaggevend is. Bij een groter geheel, zoals het totale verkeersinformatiesysteem, spelen logische beveiligingen (zoals b.v. toepassing van cryptografie, controles en organisatorische maatregelen) juist een grote rol. Bij de beoordeling van individuele componenten op hun eigen fraudebestendigheid, telt de logische beveiliging in het grotere geheel niet mee. Dit draagt in zekere zin bij aan de overheersende rol die fysieke beveiliging speelt bij de beschouwing van individuele componenten.

Verder willen we nog enigszins toelichten dat de keuze van het oogpunt, i.e. van wie de belanghebbende is, een rol speelt. Stel dat gebruikers van een bepaald systeem zich moeten identificeren m.b.v. digitale handtekeningen en dat ze daarbij gebruik maken van hulpmiddelen, b.v. in de vorm van magneet- of chipkaarten. (Zie ook de hoofdstukken over cryptografie en over identificatie.) Vanuit het oogpunt van iedere eigenaar van een identificatiehulpmiddel moet zijn eigen hulpmiddel dan bij voorkeur fraudebestendig zijn om te voorkomen dat iemand anders op enigerlei wijze misbruik kan maken van zijn digitale handtekening. Maar vanuit het oogpunt van de instantie (van het systeem) hoeven de hulpmiddelen helemaal niet fraudebestendig te zijn, omdat in principe elke juiste handtekening geaccepteerd kan worden. De wijze waarop de handtekening tot stand is gekomen (al dan niet m.b.v. een hulpmiddel, ècht of vals), speelt bij de geldigheid van digitale handtekeningen geen rol.

Er is nog een ander, minstens zo belangrijk aspect (m.b.t. de keuze van het oogpunt) dat aandacht verdient. Stel even dat het identificatiehulpmiddel niet beveiligd is tegen b.v. manipuleren of kopiëren. Vanuit het oogpunt van de eigenaar is het hulpmiddel dan niet fraudebestendig, want zijn belangen kunnen worden geschaad (m.n. door kopiëren). De eigenaar zal er dan dus heel voorzichtig mee moeten omspringen. In ons voorbeeld is het uitsluitend de verantwoordelijkheid van de eigenaar om misbruik van zijn identificatiehulpmiddel te voorkomen en worden de belangen van de instantie niet geschaad door vervalsingen. Vanuit het oogpunt van de instantie is het bedoelde identificatiehulpmiddel in zekere zin dus wel 'fraudebestendig', want er kan geen fraude ten nadele van de instantie mee worden gepleegd. (Althans niet direct ten nadele van de instantie, want wellicht wel indirect; zie ook het slot van deze sectie.)

I.h.a. zal men een component waarvan de fraudebestendigheid er niet toe doet, niet fraudebestendig noemen. In de bovengegeven omschrijving speelt onze toevoeging 'van zichzelf' hierbij een rol. Ondanks alle moeite die we ons hebben getroost voor het vinden van een zo sluitend mogelijke formulering, is ook onze formulering waarschijnlijk niet volledig sluitend. Het vinden van een volledig sluitende formulering is gewoonlijk op z'n minst

moeilijk of zelfs onmogelijk. Maar met de gegeven toelichting wordt e.e.a. geacht voldoende duidelijk te zijn. (Deze opmerking is natuurlijk niet alleen geldig voor het in ons geval belangrijke begrip fraudebestendigheid, maar ook voor alle andere begrippen die we gebruiken en van belang zijn, zoals m.n. tracering, agent, semi-identificatie, e.d.)

5

Tenslotte maken we nog een twee opmerkingen over bovenstaand voorbeeld. Het leek in bovenstaand voorbeeld misschien zo te zijn dat alleen de betreffende kaarthouder en de instantie betiteld konden worden als belanghebbende. Die eventuele indruk is onjuist. Ook alle andere kaarthouders zijn in zekere mate belanghebbend. Want alle kaarthouders hebben er belang bij dat de echte kaart van een ander niet zodanig gemanipuleerd (i.e. vervalst) kan worden dat daarmee hun eigen digitale handtekening kan worden gezet. Dus ook fraudebestendigheid vanuit het oogpunt van andere kaarthouders kan van belang zijn.

10

Daarnaast kan het (en zal het meestal ook) zo zijn dat de instantie er (zelfs als een andere instantie verantwoordelijk is voor de betreffende identificatiehulpmiddelen) wel degelijk (indirect) belang bij heeft dat kaarthouders elkaar niet al te gemakkelijk kunnen beduvelen. Immers, dit kan er toe leiden dat de gebruikers zich van het systeem van de instantie af (willen) keren, i.e. het niet (meer) willen gebruiken.

15

## Apparatuur

### Overzicht van de taken van de voertuigapparatuur

5 In eerste instantie beperken we ons (even) tot taken gerelateerd aan het heffen van verkeersbelasting. We gaan er vanuit dat in elk deelnemend voertuig tijdens verkeersdeelname apparatuur aanwezig is om de benodigde taken uit te voeren. Deze *voertuigapparatuur* (VA) zal bij het TIP-systeem dan veelal de volgende taken uitvoeren: 1) het vasthouden, meten en/of lezen van bepaalde voor de werking van de betreffende TIP-variant benodigde gegevens m.b.t. het voertuig, zijn beweging, brandstofverbruik, uitlaatgassen of wat dies meer zij, 2) het volgens  
10 een voorgeschreven berekeningswijze op basis van de benodigde gegevens bijhouden van één of meerdere tellers, 3) het uitzenden van bepaalde, voorgeschreven gegevens, zoals b.v. snelheid of tellerstand, die nodig zijn voor de belastingheffing en/of de controle op het juist functioneren. Als de voertuigapparatuur een ontvanger omvat i.h.a. ook nog: 4) het adequaat reageren op verzoeken resp. commando's die van de instantie (i.e. van geautoriseerde instanties) ontvangen worden.

15

### Benodigde voertuigapparatuur

Voor een TIP-systeem moet in elk deelnemend voertuig bepaalde apparatuur aanwezig zijn. Gewoonlijk is slechts een deel van de hieronder genoemde apparaten en/of elementen nodig.

20

- 1) een klein aantal processors met bijbehorend geheugen, waaronder ook een hoeveelheid niet-vluchtig geheugen (i.e. geheugen dat beschermd is tegen, of waarvan de inhoud sowieso intact blijft bij, stroomuitval) voor het bewaren van essentiële software en gegevens, zoals b.v. berekeningswijze(n) voor afgeleide informatie, tellerstanden en/of cryptografische sleutel(s).
- 25 2) (een verbinding met) een zender en/of een ontvanger voor communicatie met de buitenwereld.
- 3) een aantal (verbindingen met) sensoren en/of meetinstrumenten in het voertuig om allerlei gegevens, zoals b.v. toerental en/of kilometerstand, te kunnen bepalen of uitlezen.
- 4) (een aantal verbindingen met) andere apparatuur in het voertuig waarmee gecommuniceerd en/of samengewerkt kan worden, zoals b.v. een cruise control.
- 30 5) (een aantal verbindingen met) apparatuur voor communicatie met gebruikers, zoals b.v. een display en/of een luidspreker voor het geven van informatie aan gebruikers van het voertuig en b.v. een microfoon voor het ontvangen van informatie (voice-input).
- 6) een aantal (bij voorkeur gestandaardiseerde) aansluitpunten, zoals b.v. magneet- of chipkaartlezers, voor het leggen van een verbinding met losse, aan te koppelen apparatuur, zoals b.v. een door of namens de betaler  
35 aan te brengen verbruikspas en/of gebruikerskaart, die b.v. een tellerstand en/of een identificatiemiddel omvatten;
- 7) een (bij voorkeur gestandaardiseerd en centraal) aansluitpunt voor de juiste onderlinge aansluiting van alle apparatuur<sup>15</sup>;

<sup>15</sup> Dit aansluitpunt zal wellicht ook gebruikt worden voor de aansluiting van (een deel van) de apparatuur op een stroomvoorziening. Vanwege de vanzelfsprekendheid van de behoefte aan stroomvoorziening hebben we een al

Figuur 1 geeft een schematische weergave van een mogelijke situatie. In welke gevallen de bovengenoemde onderdelen van de apparatuur wel of niet aanwezig moeten resp. hoeven te zijn en waarvoor ze o.a. gebruikt kunnen worden, zal in de loop van de verdere uitleg beetje bij beetje duidelijker worden. Hieronder geven we alvast enige toelichting. Alle genoemde apparatuur is in velerlei vormen verkrijgbaar en/of bekend en daarom zullen we niet uitweiden over de apparatuur zelf. Echter, als in bepaalde gevallen of om bepaalde redenen speciale eisen (moeten) worden gesteld aan de onderdelen, zullen we (proberen) dat expliciet (te) vermelden.

We gaan er bij onze verdere uitleg van het TIP-systeem vanuit dat alle processing uitgevoerd wordt door maximaal drie processors, hoewel het werk natuurlijk ook verdeeld kan worden over meerdere processors. Eventueel kunnen ook processors gebruikt worden die voorkomen in andere genoemde onderdelen. Dat we wel expliciet de mogelijkheid van twee of drie processors noemen heeft alleen te maken met het mogelijk strikt gescheiden willen houden van enerzijds de eventuele processing namens 1) de instantie (i.e. de processing t.b.v. het toezicht houden door een eventuele agent) en anderzijds de processing namens 2) de houder van het voertuig en/of namens 3) de gebruiker of de betaler. (De twee laatstgenoemde processors dienen b.v. voor het namens de houder resp. de gebruiker of betaler toezicht houden op de agent en/of het zetten van digitale handtekeningen.)

Een reële mogelijkheid is b.v.: 1) een (al dan niet aan het voertuig bevestigde) fraudebestendige processor die fungeert als agent, 2) een (al dan niet fraudebestendige) processor bevestigd aan het voertuig voor toezicht namens de houder van het voertuig en 3) een processor op een chipkaart van de gebruiker van het voertuig zelf, dan wel van de *betaler*, i.e. van de persoon of organisatie die zich verantwoordelijk stelt voor het gebruik van het voertuig en dus m.n. ook voor de betaling van de kosten ten gevolge van het gebruik van het voertuig<sup>16</sup>. (Denk o.a. aan verkeersheffingen en verkeersboetes.) Deze derde processor is in het voorbeeld van figuur 1 niet weergegeven, maar de daarvoor benodigde chipkaartlezer wel (zie hieronder).

Een vet gedrukte omlijsting geeft in figuur 1 aan dat de betreffende component fraudebestendig is resp. dat de instantie moet vertrouwen op voldoende fraudebestendigheid van die component. Als er geen agent gebruikt wordt, zal de linker processor van figuur 1 vervallen. Als er een agent gebruikt wordt en gezamenlijk gebruik van één processor acceptabel is voor beide partijen (b.v. omdat er een fabrikant van fraudebestendige processors is die door beide partijen voldoende vertrouwd wordt), kan de rechter processor van figuur 1 weggelaten worden.

---

dan niet centrale stroomvoorziening, zoals b.v. de accu van het voertuig of aparte batterijen, niet genoemd bij de eventueel benodigde voertuigapparatuur. We zullen ook verder (vrijwel) geen aandacht meer besteden aan dit tamelijk triviale aspect.

<sup>16</sup> Juist vanwege deze mogelijkheid werd eerder in de tekst al een aantal keren rekening gehouden met dit onderscheid tussen gebruiker en betaler. In de verdere tekst zullen we vaak (proberen te) kiezen voor de meest geschikte term in de betreffende context. Dat neemt niet weg dat zowel het woord 'gebruiker' als het woord 'betaler' soms kan staan voor 'betaler en/of gebruiker'. Merk ook nog op dat de gebruiker niet per sé de bestuurder hoeft te zijn. Er kan dus (een misschien wat subtiel) onderscheid zijn tussen bestuurder, gebruiker en betaler. Omdat de context i.h.a. voldoende houvast geeft, hoeven wij in deze tekst niet altijd even precies te zijn in ons woordgebruik.

We benadrukken hier alvast dat het heel goed mogelijk is om per voertuig slechts één processor te gebruiken i.p.v. twee of drie (of eventueel zelfs nog meer).

Overigens is het zelfs mogelijk dat er helemaal geen sprake is van een 'echte' processor in strikte zin. Als bij-  
 5 voorbeeld continu slechts het kenteken en/of (een bepaald deel van) de kilometerstand van het voertuig uitgezon-  
 den wordt, dan is er niet of nauwelijks sprake van 'echte' processing uitsluitend t.b.v. het TIP-systeem. Het moge  
 duidelijk zijn dat in dit laatste geval ook de meeste andere (soorten) componenten weergegeven in figuur 1 zullen  
 vervallen.

10 Voor het gebruikte niet-vluchtige geheugen geldt i.h.a. dat (slechts) een kleine hoeveelheid ervan naast leesbaar  
 ook schrijfbaar moet zijn.

Vaak zullen de bedoelde sensoren en/of meetinstrumenten al in het voertuig aanwezig zijn en hoeven er, indien  
 gewenst, alleen nog adequate verbindingen met die apparatuur tot stand te worden aangebracht. Denk b.v. aan  
 15 verbindingen met al aanwezige sensoren op krukas en aandrijf-as of (in plaats daarvan) met eventueel aanwezige  
 elektronische toerenteller en kilometerteller. Maar natuurlijk kan men ook apparatuur speciaal voor gebruik door  
 het TIP-systeem aanbrengen. In figuur 1 is slechts één sensor of meetinstrument, zeg de kilometerteller, met  
 bijbehorende verbinding expliciet weergegeven.

20 Tot de categorie verbindingen met overige apparatuur in het voertuig zouden in principe ook gerekend kunnen  
 worden de eventuele verbinding(en) met aparte apparatuur t.b.v. fraudebestendige identificatie en/of voor het  
 fraudebestendig vasthouden van en toegang verlenen tot gegevens betreffende de typering van het voertuig, zoals  
 b.v. bouwjaar, merk, model, versnellingsbak- en motortype. Dit geldt ook voor een eventuele verbinding met  
 aparte apparatuur voor het bijhouden van de tijd (i.e. een klok) en het zetten van digitale handtekeningen namens  
 25 het voertuig resp. de houder van het voertuig. Later komen we nog uitgebreid terug op de onderwerpen identifi-  
 catie, typering en digitale handtekeningen. We zullen dan o.a. laten zien dat digitale handtekeningen gebruikt  
 kunnen worden voor uitstekende fraudebestendigheid van identificatie en typering.

Echter, als (resp. voor zover) de in de vorige alinea genoemde taken processing vereisen, gaan wij er voor het  
 30 gemak vanuit dat dergelijke functies vallen onder (resp. gecombineerd worden met) de taken van één van de  
 bovengenoemde processors. Deze aanname leidt niet tot een wezenlijke beperking van de algemeenheid van onze  
 uitleg, maar helpt wel figuur 1 eenvoudig te houden en te voorkomen dat we nader in zouden (moeten) gaan op  
 allerlei details resp. haken en ogen, die te maken hebben met beveiligingsaspecten, die niet specifiek zijn voor  
 onze vinding en waar we hier niet verder over willen uitweiden. De in figuur 1 weergegeven (verbinding met)  
 35 overige apparatuur betreft b.v. de cruise control van het voertuig.

De zender of de ontvanger is niet voor alle varianten van het TIP-systeem strikt noodzakelijk, maar gewoonlijk  
 toch op z'n minst handig. Een en ander wordt later vanzelf duidelijker. In figuur 1 is er sprake van een gecombi-  
 neerde zender plus ontvanger.



Toepassing van voice-input is misschien een aspect voor op wat langere termijn, hoewel de techniek op dit gebied al flink gevorderd is. In figuur 1 is slechts één component voor communicatie met een gebruiker expliciet weergegeven, zeg een display. Verwacht mag worden dat voor uitvoer gewoonlijk tenminste ook een luidspreker aanwezig zal zijn.

5

M.b.t. de aansluitpunten t.b.v. koppelbare apparatuur merken we op dat een (althans bij bepaalde varianten van het TIP-systeem) toezicht houdende agent zich op een losneembare chipkaart kan bevinden. (Later zullen we ook nog laten zien dat zo'n agent uitgevoerd als losse voertuigapparatuur evt. ook de taak van verbruikspas op zich kan nemen.) Ook kan de processor die namens een gebruiker of betaler bepaalde taken uitvoert, zoals b.v. het  
 10 zetten van digitale handtekeningen en/of het toezicht houden op de eventuele agent, zich op een losse chipkaart bevinden. Kortom, beide zojuist genoemde processors kunnen dus eventueel met de overige apparatuur verbonden worden d.m.v. een *chipkaartlezer*<sup>17</sup>. Het ligt het meest voor de hand dat in ieder geval de eventuele processor van (de houder van) het voertuig aan het voertuig is bevestigd. In figuur 1 zijn de processors t.b.v. de agent resp. (de houder van) het voertuig met elkaar verbonden via het centrale aansluitpunt en is de kaartlezer bedoeld voor  
 15 een gebruikerskaart.

Een *gebruikerskaart* is (primair) een hulpmiddel om te kunnen bepalen welke persoon of organisatie zich verantwoordelijk wil stellen voor (de kosten van) het gebruik van een voertuig. Het is dus primair een (hulp)middel voor de identificatie van de betaler. Een *verbruikspas* heeft (primair) als taak het bijhouden van een tellerstand  
 20 t.b.v. de gebruiker en evt. ook t.b.v. het verkeersinformatiesysteem. De tellerstand kan b.v. het gebruik van een bepaalde persoon betreffen, waarbij dat gebruik wellicht kan plaatsvinden verspreid over meerdere voertuigen en waarbij dat gebruik voor eigen rekening kan zijn of op rekening kan komen van een bepaalde organisatie, zoals b.v. de werkgever. Als de bijgehouden tellerstand van essentieel belang is voor het verkeersinformatiesysteem, dan maakt de verbruikspas dus deel uit van het verkeersinformatiesysteem. Als de verbruikspas ter beveiliging  
 25 van de tellerstand(en) vanuit het oogpunt van het verkeersinformatiesysteem (resp. de instantie) fraudebestendig moet zijn, is deze tevens een agent. (N.B. De tellerstanden opgeslagen in of op niet-fraudebestendige middelen, zoals b.v. magneetkaarten, kunnen ook op andere wijze tegen bepaalde vormen van misbruik beveiligd worden.)

Bovenstaande omschrijvingen maken het in principe mogelijk een duidelijk onderscheid te maken tussen gebruikerskaarten en verbruikspassen. Echter, voor het gemak en omdat beide functies ook gecombineerd op één kaart  
 30 kunnen voorkomen, zullen we in het vervolg de term *gebruikerskaart* vaak hanteren voor beide begrippen. Later komen we nog terug op het geval dat de gebruikerskaart (ook) een agent bevat resp. zelf tevens agent is. (Of, nog eens anders gezegd, het geval dat de agent ook de taak van gebruikerskaart op zich neemt.) Ten overvloede merken we hier nog op dat als voor het gebruik van een voertuig een gebruikerskaart en/of een agent op een losse  
 35 chipkaart nodig is, dan de gebruiker van het voertuig zo'n kaart moet 'aanbieden', i.e. die kaart(en) in verbinding moet brengen met de overige voertuigapparatuur. (B.v. door hem in de gleuf van een kaartlezer te steken.)

<sup>17</sup> Ondanks de misleidende naam gaan we er i.h.a. vanuit dat een kaartlezer communicatie in beide richtingen, i.e. ook 'schrijven', mogelijk maakt.

Een centraal aansluitpunt is allerm minst noodzakelijk. Aansluiting van alle apparatuur kan ook op vele andere manieren geschieden. Echter, een centraal aansluitpunt leidt wel tot een vereenvoudiging van de fysieke organisatie van de apparatuur en van onze weergave van een voorbeeld daarvan in figuur 1.

- 5 Een nadeel van figuur 1 is dat het lijkt of beide processors gelijkkelijk toegang hebben tot alle andere componenten. Dat hoeft echter beslist niet zo te zijn. Het is b.v. goed denkbaar dat alleen een processor van de houder of van de betaler directe toegang heeft tot de zender en ontvanger in het voertuig en dat de processor namens de instantie, i.e. de agent, dat beslist niet heeft. De agent kan dan dus niet onbeperkt en vrijelijk allerlei (geheime) berichten naar de instantie sturen, maar moet dat doen via een andere processor die (de communicatie van) de agent dus in de gaten kan houden.

- 10 In figuur 2 hebben we de situatie van figuur 1 op een iets andere wijze weergegeven om zo'n aspect van de 'logische' organisatie van de apparatuur beter tot zijn recht te laten komen<sup>18</sup>. Dus ook als de fysieke verbindingen tot stand worden gebracht als gesuggereerd in figuur 1, kan de logische organisatie zo zijn als gesuggereerd in figuur 2.
- 15 2. Figuur 2 is bedoeld tot uitdrukking te brengen dat de weergegeven processors met elkaar kunnen communiceren en beide directe toegang hebben tot alle andere voertuigapparatuur m.u.v. de zender en ontvanger. De processor namens de instantie, i.e. de agent, kan in dit voorbeeld alleen met de medewerking van de andere processor, dus indirect, toegang krijgen tot de zender en de ontvanger.

## 20 **Beveiliging tegen fraude**

- Bij gebruik van een verkeersinformatiesysteem voor b.v. verkeersheffingen is de behoefte aan voldoende beveiliging tegen fraude evident. Het ligt dus voor de hand dat (tenminste een deel van) de door het verkeersinformatiesysteem gebruikte apparatuur in voertuigen zelf fraudebestendig moet zijn en misschien ook nog op fraudebestendige wijze aan één specifiek voertuig gekoppeld moet worden, zodat gewaarborgd wordt dat bepaalde delen niet verwijderd kunnen worden voor (onrechtmatig) gebruik bij een ander voertuig.

- Hoe bij TIP-systemen gezorgd kan worden voor een goede of zelfs uitstekende bestendigheid tegen (pogingen tot) fraude, zal in de loop van de verdere uitleg duidelijk worden gemaakt. Hier merken we alvast op dat de beveiliging van apparatuur in voertuigen bij het TIP-systeem relatief eenvoudig en goedkoop is, omdat de fysieke beveiliging i.h.a. beperkt kan worden tot de gebruikte agenten. Bij een TIP-systeem zonder agenten hoeft de betrokken apparatuur in elk voertuig dus helemaal niet fysiek beveiligd te worden! Ook bij een TIP-systeem met agenten is de fysieke beveiliging allerm minst kostbaar, omdat chips goedkoop fysiek te beveiligen zijn en omdat voor elke agent volstaan kan worden met één chip met bijbehorende software. Bovendien kan het aantal agenten in elk voertuig beperkt worden tot één.

<sup>18</sup> Het feit dat de verbindingen in beide figuren niet alleen geïnterpreteerd kunnen worden als fysieke verbindingen, maar ook als communicatieverbindingen, was voor ons een extra reden om de (fysieke verbinding met) stroomvoorziening(en) uit de figuren weg te laten.

In bepaalde gevallen moet een agent ook nog fraudebestendig gekoppeld zijn aan één specifiek voertuig. Dit kan b.v. het geval zijn als een agent (ook) gebruikt wordt voor fraudebestendige identificatie en/of typering van het voertuig en als daarbij een zeer hoog niveau van fraudebestendigheid vereist is. Vaak kan volstaan worden met andere maatregelen, zoals eenvoudige en snelle opsporing van verwijdering of vernieling. Hier komen we later  
5 nog op terug. (Zie de hoofdstukken over identificatie en over voorbereiding op 'groei' van het systeem.)

Als men het desondanks verstandig acht om de overige voertuigapparatuur (ook) enige fysieke beveiliging mee te geven om pogingen tot fraude te ontmoedigen, kan men zich daarbij beperken tot zeer goedkope maatregelen, omdat die extra beveiliging niet van essentieel belang is, i.e. geen volledige bescherming hoeft te bieden.

10

### Het minimaliseren van het gebruik van fysieke beveiliging

Bij beveiliging is er altijd sprake van een soort van wapenwedloop. Met name bij fysieke beveiliging is er bij elke beveiligingsmaatregel wel weer een manier te vinden om die te omzeilen, wat verdergaande beveiligings-  
15 maatregelen noodzakelijk maakt, wat uitnodigt tot nieuwe tegenmaatregelen, etc., etc. Een hoog fysiek beveiligingsniveau gaat daarom i.h.a. gepaard met hoge kosten. Dit geldt te meer vanwege de noodzaak regelmatig fysieke inspectie uit te voeren, wat omslachtig en duur is i.v.m. de personeelskosten van controleurs. Dit alles verklaart waarom wij de fraudebestendigheid van een systeem i.h.a. niet graag willen laten afhangen van allerlei vormen van fysieke beveiliging.

20

Bij de door ons te beschrijven TIP-systemen kan een zeer hoog niveau van beveiliging en ook van privacybescherming worden bereikt. Hiertoe kan men, zoals we zullen schetsen, gebruik maken van organisatorische maatregelen en m.n. ook van cryptografie<sup>19</sup>. Bij gebruik van cryptografische technieken is er weliswaar ook sprake van een wapenwedloop, maar kan het beveiligingsniveau i.h.a. eenvoudig verhoogd worden door grotere getal-  
25 len, i.e. bitpatronen, te gaan gebruiken. De toenemende rekenkracht door de voortgaande ontwikkeling van steeds snellere chips vormt geen wezenlijke bedreiging voor de veiligheid van cryptografische technieken. Weliswaar wordt door grotere rekenkracht ontcijferen steeds gemakkelijker gemaakt, maar dat geldt ook voor het vercijferen. De veiligheid is bij cryptografische technieken veeleer gebaseerd op een essentieel verschil in complexiteit tussen bepaalde bewerkingen op getallen. Een zeer hoog beveiligingsniveau kan dus gewaarborgd blijven worden,  
30 den, zolang er maar een duidelijk verschil in complexiteit blijft bestaan tussen de onderliggende bewerkingen.

Omdat bij gebruik van cryptografische technieken het beveiligingsniveau o.a. afhangt van de mate waarin de gebruikte cryptografische sleutels beveiligd worden, is er bij gebruik van cryptografie i.h.a. wel degelijk sprake van een of andere vorm van fysieke beveiliging. Als, bijvoorbeeld, de gebruikte sleutels opgeslagen liggen in  
35 chips, is voor de beveiliging van deze chips tegen het ontfutselen van hun inhoud ook een vorm van fysieke beveiliging nodig. Echter, deze vorm van fysieke beveiliging, die o.a. gebruikt wordt bij chipkaarten, heeft in de praktijk bewezen een hoge mate van beveiliging te kunnen bieden tegen lage kosten, zodat wij het gebruik hiervan niet bezwaarlijk achten. Sterker nog, wij zien het als een voordeel dat bij de door ons ontwikkelde systemen

<sup>19</sup> Eigenlijk cryptologie. Zie ook het hoofdstuk over cryptografie.

de fysieke beveiliging (van m.n. de voertuigapparatuur) beperkt kan worden tot deze specifieke, goedkope vorm, waarvan de betrouwbaarheid zich heeft bewezen.

### **Al aanwezige apparatuur**

5

Het is te verwachten dat binnen afzienbare tijd nieuwe auto's standaard uitgerust zullen zijn met de meeste hierboven genoemde apparatuur. Deze apparatuur kan of zal een veelheid van taken kunnen uitvoeren, zoals b.v. toezicht houden op het juist functioneren van (delen van) het voertuig, administratie voeren t.b.v. geautomatiseerde diagnostiek (evt. op afstand), ondersteunen van navigatie, voldoende fraudebestendig vasthouden van en  
10 toegang verlenen tot een identificatienummer van het voertuig t.b.v. service- en garantieverlening, het onthouden van de gewenste instelling van b.v. stuur, bestuurdersstoel en spiegels voor diverse bestuurders, vergemakkelijken van opsporing na diefstal, implementeren van een tachograaf of black box, communiceren met parkeerautomaten voor het automatisch vaststellen en eventueel ook direct of indirect automatisch betalen van parkeerheffingen, communiceren met allerlei andere voorzieningen langs de weg, met andere voertuigen en/of met de rest van  
15 de buitenwereld, etc., etc.

Van de genoemde apparatuur zal in de toekomst dus slechts een fractie aanwezig (hoeven te) zijn uitsluitend voor het opleggen van verkeersheffingen m.b.v. het TIP-systeem. Immers, alleen de niet-vluchtige geheugenplaats(en) voor de (heffings)tellerstand(en) lijken uitsluitend daarvoor bestemd. Alle andere onderdelen kunnen ook nuttig  
20 en/of nodig zijn voor andere taken.

Bijvoorbeeld kan het aansluitpunt voor b.v. een chipkaart al aanwezig zijn (of ook gebruikt gaan worden) voor taken zoals b.v. het vaststellen door of namens wie het voertuig gebruikt gaat worden om te kunnen bepalen of dat gebruik toegestaan zal worden en/of om bestuurdersstoel, stuur, spiegels, e.d. automatisch in te stellen naar de  
25 op een chipkaart vastgelegde wensen van de gebruiker. De ontvanger kan o.a. gebruikt worden om gegevens over de infrastructuur te ontvangen, zoals bijvoorbeeld de ter plaatse geldende maximum snelheid of informatie over vertragingen t.g.v. files. Kortom, er zijn legio andere nuttige toepassingen mogelijk, zelfs te veel om op te noemen.

### **30 Eventuele integratie met andere toepassingen**

Omdat de in voertuigen door (het verkeersheffingendeel van) het TIP-systeem gebruikte apparatuur niet of nauwelijks fysiek beveiligd hoeft te worden om fraude tegen te gaan, kan het verkeersheffingendeel probleemloos geïntegreerd worden of samenwerken met allerlei andere toepassingen. Indien gewenst, kunnen bepaalde andere  
35 toepassingen daarom ook deel uit (gaan) maken van het totale TIP-systeem. De voor het verkeersheffingendeel van het TIP-systeem resp. de voor het totale TIP-systeem benodigde apparatuur kan dus gezamenlijk gebruikt worden met andere toepassingen binnen resp. buiten het totale TIP-systeem, zodat de kosten die per voertuig gemaakt moeten worden voor (het verkeersheffingendeel van) het TIP-systeem, (uitermate) gering kunnen zijn.

40

### Vaste en losse voertuigapparatuur (VVA en LVA)

Niet alle genoemde apparatuur hoeft vast bevestigd te worden (of zijn) aan het voertuig. De apparatuur of belangrijke delen ervan kunnen los<sup>20</sup> zijn en kunnen, in het geval dat er sprake is van een aansluitpunt, eventueel in verbinding worden gebracht met (i.e. gekoppeld worden aan) vaste voertuigapparatuur, zoals b.v. sensoren en/of de accu. De losse, koppelbare apparatuur kan b.v. bestaan uit een chipkaart, die zorg kan dragen voor een deel van de, of zelfs alle, processing en/of die (een deel van) het niet-vluchtige geheugen bevat. Ook is het b.v. mogelijk dat de zender en/of de ontvanger deel uitmaken van de losse apparatuur.

10 Met de term vaste voertuigapparatuur (VVA) doelen we in het vervolg op alle vast aan het voertuig bevestigde apparatuur die informatie levert aan resp. (direct of indirect) gebruikt wordt door het TIP-systeem en met de term losse voertuigapparatuur (LVA) op alle andere tijdens de verkeersdeelname in het voertuig aanwezige (en eventueel aan de VVA gekoppelde) apparatuur t.b.v. het TIP-systeem. We blijven de term voertuigapparatuur (VA) gebruiken voor de vereniging van VVA en LVA.

15 Het is enerzijds mogelijk dat er alleen sprake is van VVA, i.e. dat alle apparatuur vast aan het voertuig bevestigd is en dat er geen gebruik wordt gemaakt van losse, koppelbare apparatuur. Anderzijds is het in bepaalde gevallen mogelijk dat er alleen sprake is van LVA. Dit laatste kan alleen als er (nog) geen gebruik wordt gemaakt van aan het voertuig bevestigde sensoren (om b.v. de kilometerstand te kunnen bepalen) of fraudebestendig aan het voertuig gekoppelde identificatiemiddelen, zoals b.v. een chip met identificatienummer en/of type aanduiding. 20 Want anders zou er ook sprake zijn van VVA. Tussen beide extremen is er vanzelfsprekend nog een scala aan andere mogelijkheden.

25 Normaliter zal een TIP-systeem dat gebruikt wordt voor verkeersheffingen en m.n. 'rekeningtransport', ook toetaalheffingen ondersteunen, waarvoor het i.h.a. nodig is om gebruik te maken van gegevens die verkregen worden via sensoren aan het betreffende voertuig. In het algemeen zal er dus sprake zijn van VVA, waaraan al dan niet LVA gekoppeld kan worden. Echter, bij invoering van rekeningrijden m.b.v. het TIP-systeem kan men zich ook (eventueel alleen in eerste instantie) beperken tot grens- en trajectheffingen. (Zie ook het hoofdstuk over voorbereiding op 'groei' van het systeem.) Daarbij kan men zich dan b.v. beperken tot het uitzenden van een identificatienummer van de betaler of van zijn betaalrekening. Gegevens over het voertuig zijn dan dus niet noodzakelijk, 30 zodat in dit geval volstaan kan worden met alleen LVA.

### Ruime interpretatie van de gebruikte begrippen

35 Wellicht ten overvloede merken we voor alle zekerheid expliciet op dat de gebruikte begrippen i.h.a. ruim moeten worden geïnterpreteerd. Niet alleen de begrippen behandeld in dit hoofdstuk, maar alle begrippen in de hele

<sup>20</sup> We zijn ons ervan bewust dat er i.h.a. geen duidelijke grens is tussen wat los en wat vast genoemd kan worden. Bijvoorbeeld is de accu van een voertuig in zekere zin ook tamelijk eenvoudig losneembaar, zodat deze misschien ook, tegen onze bedoeling, als een los deel van het voertuig beschouwd zou kunnen worden. Voor ons doel lijkt een nauwkeuriger afbakening echter niet noodzakelijk.

tekst. Bijvoorbeeld zullen we het begrip zender gebruiken voor elke voorziening waarmee een bericht kan worden gegeven of beschikbaar gesteld aan de ontvanger(s) van andere objecten of personen in de omgeving. De term wordt meestal gebruikt als er geen sprake is van fysiek contact en berichten worden overgedragen door b.v. geluids- of radiogolven, licht, infrarood, of wat dan ook<sup>21</sup>. Maar de term dekt in onze context vanzelfsprekend ook die gevallen af waarin de overdracht van berichten via fysiek contact geschiedt, bijvoorbeeld d.m.v. elektrische geleiding. Zo hadden we het eventueel aanwezige aansluitpunt t.b.v. het koppelen van apparatuur van/namens de betaler dus ook als een zender plus ontvanger kunnen betitelen. Deze laatste opmerking illustreert dat de eerder gebruikte term aansluitpunt, zonder dat dat expliciet gezegd werd, wel degelijk bedoeld was om ruim geïnterpreteerd te worden, zodat het ook gevallen zonder fysiek contact omvat. Kortom, de communicatie tussen LVA en VVA kan ook plaatsvinden via zend- en ontvangmiddelen.

---

<sup>21</sup> Dus een display en een luidspreker vallen ook onder het ruime begrip zender.

## Cryptografie<sup>22</sup>

In het algemeen wordt bij de gesuggereerde TIP-systemen voor diverse doeleinden dankbaar gebruik gemaakt van reeds bekende cryptografische technieken.

5

Het is m.b.v. cryptografische technieken bijvoorbeeld mogelijk om de inhoud van een bericht geheim te houden voor ieder ander dan de bedoelde ontvanger. In het vervolg noemen we een bericht *geheim* als dat bericht zodanig vercijferd is dat alleen de bedoelde ontvanger het bericht kan ontcijferen, oftewel het bericht kan ontdoen van de 'verpakking' die zorgt voor de geheimhouding. Deze situatie is enigszins vergelijkbaar met een verzegelde envelop om een brief heen, zij het met dit verschil dat iedereen een verzegelde envelop wèl wederrechtelijk kan openmaken, maar een geheim bericht niet. (De vergelijking met een verzegelde envelop is niet ongebruikelijk, hoewel een kluis waarvan alleen de zender en de ontvanger een sleutel hebben, qua eigenschappen meer overeenkomsten biedt.)

10

15 Daarnaast kan m.b.v. cryptografische technieken de authenticiteit van de inhoud en/of van de afzender van een bericht gewaarborgd worden. Als beide aspecten gewaarborgd worden spreekt men van een digitale handtekening op dat bericht. In het vervolg noemen wij een bericht voorzien van een digitale handtekening *ondertekend*.

Om fraude tegen te gaan, moet elk bericht niet alleen ondertekend worden, maar moet er ook voor gezorgd worden dat van elk ondertekend bericht alleen het eerst ontvangen exemplaar telt, i.e. dat alle later en waar dan ook (eventueel) opduikende exemplaren geen enkel effect kunnen krijgen bovenop het (bedoelde) effect van het eerst ontvangen exemplaar. Hiertoe moet het origineel van elk ondertekend bericht in ieder geval uniek zijn. Meestal wordt voor de gewenste uniciteit gezorgd door aan elk bericht een tijdstempel of een volgnummer toe te voegen. Bovendien moet hiertoe van elk bericht het bedoelde effect duidelijk zijn. Het bedoelde effect wordt vaak duidelijk gemaakt door o.a. de geadresseerde en/of het onderwerp expliciet in het bericht te vermelden. Daarnaast is het voor een goede ondertekening i.h.a. nodig om in het bericht ook nog een bekend (of een uit de rest van het bericht afleidbaar) bitpatroon op te nemen.

20

25

Op al dit soort cryptografische details gaan wij niet dieper in en we zullen er verder geen (of nauwelijks nog) aandacht aan besteden. Sterker nog, wij zullen (misschien) soms niet eens expliciet aangeven of geheimhouding en/of ondertekening gewenst dan wel noodzakelijk is voor een juiste werking van de diverse protocollen die de revue zullen passeren. Een ter zake kundige wordt geacht zelf in staat te zijn om (verder) te bepalen welke beveiliging(en) nodig zijn en hoe die m.b.v. cryptografische technieken aangebracht kunnen worden.

30

35 Desalniettemin zullen wij toch flink wat aandacht schenken aan een aantal beveiligingsaspecten. Niet alleen om hier en daar te laten zien wat toepassing van cryptografie te bieden heeft, maar ook om de uitleg van een aantal

---

<sup>22</sup> Cryptografie staat strikt genomen alleen voor geheimschrift. Eigenlijk is de juiste term voor de leer van zowel vercijferen als ontcijferen (zeg maar, van zowel produceren als lezen van geheimschrift) cryptologie. In de rest van deze tekst zullen we desalniettemin de wat meer bekende en ingeburgerde term cryptografie blijven gebruiken.

aspecten van de protocollen en van de werking van de TIP-systemen helder(der) te krijgen. Daarbij zullen we ons (proberen te) beperken tot de twee eigenschappen *geheim* en *ondertekend*. Dus in onze beschrijving wordt soms het zwaardere middel van de digitale handtekening genoemd, terwijl b.v. volstaan zou kunnen worden met waarborging van de authenticiteit van alleen de afzender of van alleen de inhoud van het bericht. Ook geven wij hier en daar aan dat geheimhouding of ondertekening plaatsvindt of moet plaatsvinden, terwijl men zich ook tevreden zou kunnen stellen met een soortgelijke aanpak zonder deze cryptografische toevoegingen. Kortom, de gegeven beschrijvingen dienen alleen ter illustratie en mogen niet begrepen worden als opgelegde beperkingen.



## Administratie

### Bij te houden gegevens

5 Zoals eerder gezegd, concentreren we ons in eerste instantie op de heffing van verkeersbelasting. De gegevens die door de voertuigapparatuur actief moeten worden bijgehouden, betreffen dan i.h.a. alles wat bij (de hoogte van) die belasting een rol speelt (zeg, als parameter gebruikt wordt). Deze gegevens kunnen van allerlei aard zijn. Bijvoorbeeld zou, althans in principe, in een voertuig met verbrandingsmotor continu de hoeveelheid en hoedanigheid van de geproduceerde uitlaatgassen gemeten en bijgehouden kunnen worden. Veelal zal het echter gaan om goedkoper vast te stellen gegevens, zoals b.v. afgelegde weg, snelheid, tijdstip, toerental, voertuigtype, mo-  
10 tortype, ingeschakelde versnelling, positie van het gaspedaal, e.d.

### De kilometerteller als odometer

15 Hieronder geven we een aantal voorbeelden, waarbij tenminste de kilometerstand wordt bijgehouden. Eigenlijk zouden we i.p.v. kilometerstand misschien het minder bekende woord odometerstand moeten gaan gebruiken, want bij de door ons bedoelde kilometerteller kan, en zal i.v.m. de gewenste nauwkeurigheid i.h.a. ook, de eenheid (respectievelijk de kleinste eenheid) een andere zijn dan de kilometer. Toch zullen we voor de odometer steeds het ingeburgerde woord kilometerteller blijven gebruiken. In de verdere tekst gaan we er vanuit dat de  
20 kilometerteller in een voldoende aantal decimalen bijgehouden wordt en afgelezen kan worden.

### Een aantal voorbeelden

Ter illustratie geven we een aantal concrete voorbeelden. Bij het eerste voorbeeld wordt alleen de kilometerstand  
25 (voldoende nauwkeurig) bijgehouden. De bijbehorende verkeersbelasting zal in dit geval kunnen bestaan uit een vast bedrag per afgelegde afstandseenheid.

Bij het tweede voorbeeld wordt naast de kilometerstand ook de tijd, de snelheid en de cumulatief betaalde en/of verschuldigde belasting bijgehouden. Elk van de vier genoemde gegevens moet natuurlijk worden uitgedrukt in  
30 een of andere voorgeschreven eenheid. De verschuldigde belasting kan uitgedrukt worden in een geldbedrag, maar ook in een aantal heffingspunten o.i.d. De wijze waarop de verschuldigde belasting moet worden berekend uit de andere gegevens, wordt natuurlijk voorgeschreven (waarschijnlijk door de overheid).

De voorgeschreven bijdrage van elke afgelegde afstandseenheid aan het cumulatieve aantal heffingspunten kan  
35 bij dit tweede voorbeeld dus afhangen van de tijdsduur waarin (i.e. de snelheid waarmee) deze afstand is afgelegd en van de precieze periode waarin (i.e. de datum en tijd waarop) deze eenheid is afgelegd. Anders geformuleerd, de prijs die voor een afgelegde afstandseenheid moet worden betaald, kan in dit voorbeeld bepaald worden door een willekeurig te kiezen functie van snelheid en tijdstip. In dit geval kunnen dus bijvoorbeeld kilometers afge-  
40 legd met een snelheid hoger dan, zeg, 90 km/u progressief (dus hoe hoger de snelheid, des te zwaarder) worden belast, evenals kilometers afgelegd gedurende bepaalde spitsuren op bepaalde dagen. Ook kan een U-vormige

functie van de snelheid gebruikt worden, waarbij de kosten voor een afstandseenheid ook nog eens steeds hoger worden naarmate de snelheid waarmee die is afgelegd, lager is dan, zeg, 60 km/u. De gedachte hierachter is dat bij zowel hoge als hele lage snelheden het brandstofverbruik en/of de veroorzaakte vervuiling per afstandseenheid groter is.

5

In ons derde voorbeeld wordt, naast de in het tweede voorbeeld genoemde gegevens, ook nog gebruik gemaakt van het kenteken (of een ander registratienummer) van het voertuig. In de kentekenregistratie die door of namens de overheid al wordt (of gaat worden) bijgehouden, kan b.v. nauwkeurig omschreven staan (of gaan worden) om wat voor voertuig het gaat, wat voor motor er in zit, en wat dies meer zij. Daarom kan voor elk type voertuig, i.e. voor elke combinatie van merk, model, bouwjaar, versnellingsbak- en motortype e.d., de prijsfunctie nu zodanig gekozen worden, dat de prijs van een afgelegde afstandseenheid vrij nauwkeurig gerelateerd wordt aan het brandstofverbruik en/of de veroorzaakte milieuvervuiling, zonder dat de uitlaatgassen van elk voertuig continu gemeten en/of geanalyseerd hoeven te worden. Merk op dat men ervoor kan kiezen de prijs van een afgelegde kilometer niet alleen te laten afhangen van de gemiddelde snelheid waarmee deze afstandseenheid is afgelegd, maar ook van de gemiddelde snelheid op de vorige afstandseenheid. Dus extra vervuiling (en/of brandstofverbruik) t.g.v. variaties in snelheid, i.e. acceleratie en deceleratie, kan ook vrij nauwkeurig in rekening worden gebracht zonder de uitlaatgassen van het betreffende voertuig tijdens verkeersdeelname continu te analyseren en te meten.

#### **Het empirisch vaststellen van een berekeningswijze**

20

Om een voldoende nauwkeurige berekening van de vervuiling door een voertuig mogelijk te maken op basis van een aantal relevante gegevens (zoals b.v. snelheid, acceleratie, temperatuur, brandstofverbruik, toerental, e.d.) is het gewenst om van tenminste één exemplaar van elk type voertuig onder allerlei omstandigheden de aard en hoeveelheid van de geproduceerde milieuvervuiling daadwerkelijk te analyseren en te meten en de bijbehorende combinatie van relevante gegevens vast te stellen. Eén exemplaar kan al voldoende zijn, omdat van alle andere exemplaren via het verkeersinformatiesysteem informatie kan worden verzameld en kan worden gecontroleerd of ze dezelfde karakteristieke combinaties van deze voor de berekening relevante gegevens vertonen. Men kan de aldus verzamelde informatie ook gebruiken om ogenschijnlijk afwijkende exemplaren op te roepen voor een nadere inspectie. Op deze wijze kunnen ook voertuigen, die b.v. door slechte afstelling of ouderdom niet meer voldoen aan de (milieu)normen, opgespoord worden. (Iets soortgelijks als hier beschreven is van toepassing op het voorbeeld van de totale geluidsproductie van een voertuig. In het hoofdstuk over controles komt dit laatstgenoemde voorbeeld van het gebruik van afgeleide, i.e. berekende, informatie ter sprake.)

Als men de heffing wil baseren op het brandstofverbruik, is vaak zelfs geen enkel exemplaar nodig voor het vooraf uitvoeren van experimenten. Immers, men kan alle informatie over brandstofverbruik van elk type voertuigen in allerlei gebruiksomstandigheden verzamelen via het TIP-systeem, eventueel te ver afwijkende waarden (b.v. t.g.v. pogingen tot fraude) eruit filteren en vervolgens per type voertuig nauwkeurige informatie afleiden over het brandstofverbruik in de praktijk. De verkregen waardes kunnen gebruikt worden voor het bepalen van een voldoende nauwkeurige berekeningswijze (b.v. in de vorm van een functie of een meerdimensionale tabel) voor het brandstofverbruik op basis van een geschikt (b.v. zo klein mogelijk) aantal input-parameters. Zo'n berekeningswijze kan dan op zijn beurt gebruikt worden voor controle op het door een individueel voertuig opgege-

ven brandstofverbruik. (Iets soortgelijks als hier beschreven geldt voor het eventueel via het verkeersinformatie-systeem verzamelen van meetgegevens over de geluidsproductie in de motorruimte van voertuigen.)

Het op één van de twee hierboven beschreven, empirische manieren vinden van een berekeningswijze voor afgeleide informatie is evt. ook toepasbaar voor andere gegevens dan brandstofverbruik (en geluidsproductie). Meer in het algemeen kan men dus, zolang met de overgrote meerderheid van de voertuigen van een bepaald type niet gefraudeerd wordt, de informatie die nodig is ter bestrijding van fraude met voertuigen van dat type, automatisch verzamelen.

## 10 Nog meer voorbeelden

Eventueel kan men de voor een bepaalde verkeersheffing gebruikte prijsfunctie ook nog variëren per gebied of weggedeelte. Dan moet vanzelfsprekend bijgehouden worden in welk tariefgebied het voertuig zich bevindt. Bijvoorbeeld kan men, als de voertuigapparatuur ook een ontvanger omvat, de voertuigapparatuur op de hoogte houden van welk tarief, i.e. welke prijsfunctie, gehanteerd moet worden door via een zendertje bij elke grensovergang tussen verschillende tariefgebieden bekend te maken wat voor soort tariefgebied nu betreden wordt. Ook zou men het te betalen tarief (mede) af kunnen laten hangen van de verkeersdrukte ter plaatse. Een aantal andere voordelen van het gebruik van ontvangers behandelen we later nog apart.

Uit bovenstaande moet duidelijk zijn geworden dat er legio mogelijkheden zijn, zelfs te veel om op te noemen. Min of meer toevallig speelde bij alle zojuist gegeven voorbeelden de kilometerteller een rol. Toevallig in die zin, dat er maar al te goed ook situaties denkbaar zijn waarbij de grootte van de afgelegde afstanden geen rol speelt bij de (bepaling van de hoogte van de) heffing. Anderzijds allerm minst toevallig, omdat we verwachten dat in de praktijk uiteindelijk in veel gevallen wel degelijk gebruik zal worden gemaakt van een kilometerteller. Immers, een belangrijk kenmerk van het TIP-systeem is dat het totaalheffingen mogelijk maakt. Dit verklaart ook waarom we ons bij de verdere uitleg voor een belangrijk deel zullen concentreren op het gebruik van tellers. In onze voorbeelden beperken we ons vaak tot het noemen van tellers (tellers i.h.a. of kilometertellers i.h.b.).

We merken nu alvast op dat als parameters van de prijsfunctie alle mogelijke soorten gegevens gebruikt kunnen worden waarvoor geldt dat ze voldoende gemakkelijk op afstand op betrouwbaarheid te controleren zijn, dan wel op andere wijze voldoende beveiligd worden tegen pogingen tot fraude. We komen hierop terug in het hoofdstuk over controles.

### Een heffingstellerstand per persoon en/of per voertuig

Alle parameters die een rol spelen bij de hoogte van de verkeersheffing, worden op een voorgeschreven wijze gebruikt om de stand van een heffingsteller bij te houden. Vaak zal het hierbij gaan om een cumulatieve, oftewel monotoon stijgende, heffingsteller, maar het kan ook gaan om een monotoon dalende teller. Om de uitleg te vereenvoudigen wordt in onze uitleg vaak gesproken over 'de teller', waarbij bewust verzwegen wordt dat er eventueel ook meer dan één teller kan worden bijgehouden en waarbij ook in het midden gelaten wordt waar die tel-

ler(s) bij horen. De heffingsteller, i.e. de teller die ten grondslag ligt aan het betalingsproces<sup>23</sup>, kan bijvoorbeeld gekoppeld zijn aan het voertuig of aan de betaler. Nog een interessante mogelijkheid is het bijhouden van twee tellers, één gekoppeld aan het voertuig en één gekoppeld aan de betaler.

- 5 Een teller gekoppeld aan het voertuig (en dus indirect aan de houder van dat voertuig) is een voor de hand liggende mogelijkheid, die nauw aansluit bij de (eind)verantwoordelijkheid van de kentekenhouder voor de betaling van de voor gebruik van het voertuig verschuldigde verkeersheffingen. Deze mogelijkheid sluit ook goed aan bij de traditionele koppeling van kilometertellers en kilometer(teller)standen aan voertuigen.
- 10 Het direct koppelen van tellers aan betalers heeft als voordeel dat wisselende gebruikers het voertuig kunnen benutten, terwijl ze ieder toch zelf direct door de instantie, in dit geval de heffingsinner, aangesproken kunnen worden op betaling van de op grond van hun eigen gebruik verschuldigde verkeersbelasting.

Het eventueel aan de feitelijke gebruikers doorberekenen van de met een voertuig opgelopen verkeersheffingen kan beschouwd worden als een eigen verantwoordelijkheid van de houder van het voertuig. In zo'n geval is de verkeersheffingsteller dus gekoppeld aan het voertuig en staat het de houder vrij om zelf (eventueel m.b.v. LVA) de heffingsbedragen voor individuele gebruikers bij te (laten) houden. In dit geval is de houder dus verantwoordelijk voor het eventuele gebruik van een tweede type teller.

20 Maar het is natuurlijk ook mogelijk dat de instantie, i.e. de heffingsinner, geïnteresseerd is in beide tellers<sup>24</sup> en ze beide gebruikt voor het controle- en/of betalingsproces. De redundantie in tellers geeft de instantie dan een extra controlemogelijkheid (op consistentie), want b.v. moet het totaal aan verschuldigde verkeersbelasting volgens de tellers gekoppeld aan voertuigen in principe gelijk zijn aan de totale verkeersbelasting verschuldigd volgens de tellers gekoppeld aan betalers.

25

Hoe dan ook, in de verdere tekst blijven we i.h.a. voor het gemak over één teller spreken.

<sup>23</sup> Het kan dus eventueel gewoon een kilometerteller zijn.

<sup>24</sup> Bijvoorbeeld als er sprake is van al dan niet verhandelbare vervuilingrechten per persoon.

## Gebruik van een zender

Een realisatie van een TIP-systeem waarbij geen zender wordt gebruikt, lijkt onwaarschijnlijk. In principe is het bij een aanpak m.b.v. agenten (die we pas in één van de laatste hoofdstukken zullen behandelen) wel degelijk goed mogelijk om de agenten via b.v. een elektrisch contact alleen rapport uit te laten brengen tijdens een perio-

5 dieke controle. Maar het gebruik van zenders is dermate goedkoop en handig, dat we in het vervolg het gebruik van een zender zullen veronderstellen. Er is geen reden om de wat 'klassiekere' mogelijkheden zonder zender nog apart in meer detail te behandelen, want alle relevante aspecten liggen al opgesloten in de verdere uitleg van het geval met zender. (Merk op dat communicatie via fysiek contact ook onder ons begrip zender in ruime zin valt.)

10

### Het continu of op verzoek uitzenden van gegevens

Als (resp. voor zover) de voertuigapparatuur in elk deelnemend voertuig de administratie op eigen houtje bijhoudt, moet de instantie om effectieve controle te kunnen uitoefenen op elk gewenst moment inzage kunnen krijgen in die administratie van iedere deelnemer. Bij de door ons als eerste te beschrijven aanpak met uitsluitend

15 controles op afstand moet elk deelnemend voertuig hiertoe via een zender cruciale gegevens aan de instantie in de buitenwereld beschikbaar stellen. In een later hoofdstuk zullen we een soortgelijke aanpak beschrijven, waarbij deze gegevens worden verstrekt aan een in het voertuig aanwezige agent, i.e. vertegenwoordiger, van de instantie. Deze agent communiceert dan via een zender met (de rest van) de bedoelde instantie in de buitenwereld.

20

Het uitzenden van berichten met de vereiste gegevens kan (vrijwel) continu gebeuren, d.w.z. dat de berichten tenminste met een voorgeschreven, hoge frequentie moeten worden uitgezonden, òf alleen op geautoriseerd verzoek (beter gezegd, na een geautoriseerde opdracht). Als men kiest voor uitsluitend inzage op verzoek, dan wordt het op afstand uitvoeren van goede controle moeilijker en dus kostbaarder, zodat een aangepaste aanpak, zoals

25 die m.b.v. in het voertuig aanwezige agenten, op z'n minst gewenst lijkt. De aanpak m.b.v. agenten wordt, zoals ook in de vorige alinea al gezegd, behandeld in een later hoofdstuk. Tot aan dat hoofdstuk beperken we ons bij onze verdere uitleg (zoveel mogelijk) tot het geval waarbij de vereiste gegevens vrijwel continu via de zender beschikbaar worden gesteld.

### 30 Op afstand lezen

De door voertuigen (of beter gezegd, door voertuigapparatuur) uitgezonden berichten kunnen d.m.v. ontvangers gelezen worden, zonder dat het verkeer enige hinder ondervindt. Ontvangers kunnen in principe op een willekeurige afstand worden opgesteld, zolang dat maar binnen het voorgeschreven bereik van de zenders van de 'uit te

35 lezen' voertuigen is. De benodigde ontvangers kunnen b.v. langs of boven de weg staan opgesteld, maar geen enkele andere mogelijkheid wordt uitgesloten!

40

**Eventueel alleen uitzenden van (semi-)identificaties**

Als het TIP-systeem alleen wordt gebruikt voor b.v. het verzamelen van verkeersinformatie in striktere zin, dus o.a. voor het meten van de omvang en/of gemiddelde snelheid van bepaalde verkeersstromen en/of het bepalen van filevertragingen en/of het bepalen van de (gemiddelde) snelheden van individuele voertuigen op bepaalde weggedeelten, dan kan volstaan worden met het vanuit elk voertuig uitzenden van identificaties of semi-identificaties. Het begrip semi-identificatie wordt pas later duidelijk gemaakt en komt uitgebreid aan de orde in het hoofdstuk over semi-identificatie. Ook bij het opleggen van grens- en trajectheffingen kan men zich eventueel beperken tot het uitzenden van (semi-)identificaties. (Zoals al eerder werd opgemerkt in de op één na laatste alinea van het hoofdstuk over apparatuur. Een voorbeeld hiervan wordt gegeven in het hoofdstuk over voorbereiding op 'groei' van het systeem.)

## Beveiliging van berichten

### Handtekening op berichten

5 Het uitzenden van berichten naar de instantie met relevante gegevens over de eigen administratie kan gezien worden als het doen van een geautomatiseerde, elektronische aangifte. Als er in zo'n aangifte al dan niet doelbewust gemaakte fouten blijken voor te komen, zal men de verantwoordelijke afzender daarop aan willen spreken. Het is dus prettig als: 1) de verantwoordelijke afzender onomstotelijk kan worden vastgesteld, en 2) deze dan kan worden aangesproken op de precieze inhoud van de aangifte. Voor dit laatste is het nodig dat niemand onopge-  
10 merkt de inhoud van andermans aangifte kan veranderen.

Als men beide zojuist genoemde eigenschappen wil hebben, moet men eisen dat elke aangifte voorzien wordt van een (niet te vervalsen) digitale handtekening. Een digitale handtekening zorgt namelijk voor de authenticiteit van zowel de identiteit van de afzender als van de inhoud van het ondertekende bericht. Met andere woorden, zo'n  
15 handtekening zorgt ervoor dat bewijsbaar is dat het bericht niet door iemand anders is verstuurd en dat de inhoud ervan ook niet door iemand anders stiekem kan zijn aangepast. Digitale handtekeningen kunnen dus een valse aangifte door iemand anders onmogelijk maken, evenals kans op succes bij latere ontkenning van een zelf ingediende verkeerde aangifte.

20 De door een digitale handtekening verzekerde authenticiteit van zowel inhoud als afzender hoeft vanzelfsprekend niet alleen van belang te zijn voor elektronische aangiften, maar kan ook nuttig en/of nodig zijn voor meer, of zelfs alle, berichten.

### Alleen geautoriseerde inzage

25 Door toepassing van cryptografie kan men er voor zorgen dat elk bericht geheim blijft voor ieder ander dan de bedoelde ontvanger. Men kan er dus bijvoorbeeld voor zorgen dat een bepaald uitgezonden bericht, zoals b.v. een aangifte, alleen leesbaar is voor de geadresseerde. Later zullen we nader op de behoefte aan privacybescherming en de geheimhouding tegenover bepaalde personen of instanties ingaan. Nu kan volstaan worden met de  
30 opmerking dat de uitgezonden berichten versleuteld kunnen worden ter beveiliging tegen ongeoorloofde inzage.

## Identificatienummers in berichten

### De behoefte aan identificaties

- 5 Vaak geldt dat er in een door voertuigapparatuur uit te zenden bericht ook een aantal identificaties moet voorkomen. Hiervoor zijn een aantal redenen te noemen.

Allereerst moet, zoals later uitgebreid zal worden uitgelegd, gecontroleerd kunnen worden of de tellerstand(en) alleen toenemen en niet af en toe (tijdens verkeersdeelname of stilstand) stiekem worden teruggedraaid. Daartoe  
10 moet van op verschillende tijdstippen verstrekte tellerstanden bepaald kunnen worden of ze bij dezelfde VVA resp. dezelfde LVA horen, of niet. Dus moet, bij de door ons eerst beschreven aanpak met uitsluitend controles op afstand, met elke tellerstand een bijbehorend identificatienummer meegezonden worden.

Daarnaast moeten de geadmistreerde verkeersheffingen regelmatig in rekening kunnen worden gebracht bij de  
15 juiste betaler. Daartoe is het gewenst om een of ander identificatienummer van de betaler te administreren bij of mee te sturen met elke tellerstand en/of telleridentificatie. Betaling kan, als men dat wil, eventueel ook op een anonieme of semi-anonieme wijze verricht worden *in* het voertuig. Vanwege de behoefte aan privacybescherming lijkt het misschien aantrekkelijk om dit te doen en dan samen met de tellerstand(en) slechts een betalingsbewijs mee te zenden. Toch is men dan nog niet per sé verlost van de behoefte aan identificatienummers. Want bijvoorbeeld zal de heffingsinner normaliter willen dat op/in het betalingsbewijs vermeld wordt voor welke teller betaald  
20 is. Aan het gebruik van een of ander identificatienummer bij het in rekening brengen lijkt dus niet zo makkelijk te ontkomen.

Ten derde geldt dat het op zijn minst gewenst is dat bepaalde berichten, zoals aangiften, voorzien worden van een  
25 (digitale) handtekening. Maar iemand kan een handtekening op een bericht alleen controleren als hij kan bepalen wiens handtekening het geacht wordt te zijn. Kortom, als een bericht getekend is, moet de bedoelde ontvanger de eigenaar van de handtekening kunnen identificeren.

Kortom, enige vorm van identificatie lijkt onontbeerlijk. Hoe bij gebruik van identificatie(s) toch voor voldoende  
30 privacybescherming gezorgd kan worden, zullen we later in het hoofdstuk over privacybescherming behandelen. Nog later zullen we in de hoofdstukken over semi-identificaties en over de aanpak m.b.v. agenten laten zien dat en hoe het gebruik van identificaties van personen en/of voertuigen geminimaliseerd kan worden.

### Aantal identificaties

35 Er kunnen meerdere identificatienummers nodig zijn en er kunnen diverse soorten gebruikt worden. Op het laatste komen we terug in het hoofdstuk over privacybescherming. Als men bepaalde tellerstanden associeert met voertuigen dan moet in de berichten bij zulke tellerstanden een voertuigidentificatie vermeld worden. Feitelijk zal de teller in zo'n geval gebonden zijn aan de VVA en kan in dit geval dus eventueel gekozen worden voor een  
40 VVA-identificatienummer i.p.v. een voertuigidentificatienummer. Wat handiger is hangt onder meer af van de



gewenste gang van zaken bij b.v. vervanging van de apparatuur in geval van defecten e.d. Ook kan men er voor kiezen om elke persoon te verbinden met één of meer eigen tellers. Dan moet het identificatienummer de persoon of zijn teller, i.e. zijn LVA, betreffen. Denk bij deze laatste afweging o.a. aan wat er gebeuren moet bij b.v. verlies en/of diefstal van de persoonlijke LVA. Ook kan men evt. tijdens verkeersdeelname twee tellers laten bijhouden: één horend bij de VVA en één bij de LVA. Dan moeten in berichten dus tenminste de twee hierbij horende identificatienummers meegezonden worden.

Er zijn een aantal voordelen verbonden aan het bijhouden van een teller per persoon. Ten eerste kunnen meerdere gebruikers/betalers dan om beurten gebruik maken van één en hetzelfde voertuig ('sharing') en toch ieder individueel opdraaien voor de door eigen toedoen verschuldigde verkeersheffingen. Ten tweede maakt dit het mogelijk om een quoteringssysteem in te voeren, waarbij elke burger b.v. een quotum aan kilometers gemotoriseerd mag afleggen of een bepaald quotum aan (een zekere vorm van) milieuvervuiling mag veroorzaken. Eventueel wordt verhandeling van (delen van) zulke verbruiks- resp. vervuilingsrechten toegestaan of geregeld.

In de rest van de tekst zullen we voor het gemak (bijna) steeds spreken over één teller en in het midden laten om wat voor teller het gaat. Dus in de verdere beschrijving maken we i.h.a. geen onderscheid tussen de diverse mogelijke gevallen met één of meerdere tellers en met al dan niet persoonlijke tellers. Een ter zake kundige wordt geacht in staat te zijn de voor elk geval benodigde details zelf aan te vullen.

## Controles

Om een verkeersinformatiesysteem voldoende fraudebestendig te maken en te houden, zullen er i.h.a. allerlei controles nodig zijn. Natuurlijk is er m.n. controle nodig op de betrouwbaarheid van gegevens waarbij direct of indirect een economisch belang (zeg maar, geld) in het geding is, zoals b.v. in het geval van prijsberekening of verkeersheffing. Een bij controle vastgestelde onjuistheid of niet acceptabele afwijking kan b.v. het gevolg zijn van een poging tot fraude, een defect of een onjuiste afstelling. De tegenactie kan b.v. bestaan uit aanhouding van het voertuig of het toesturen van een oproep aan de houder om het voertuig aan te bieden ter nadere inspectie.

### 10 De heffingsinner als controleur

Hoewel de overheid resp. de heffingsinner bepaalde controles zou kunnen uitbesteden aan diverse met elkaar concurrerende organisaties, gaan we er voor ons gemak in de rest van deze beschrijving vaak vanuit dat controleur en heffingsinner één en dezelfde zijn, i.e. dat er sprake is van één heffingsinner die zelf zorg draagt voor de uitvoering van de benodigde controles. We kunnen ons dus beperken tot de term *heffingsinner* als we de instantie specifiek willen aanduiden. (Vaak zullen we echter gewoon de abstractere term instantie blijven gebruiken.)

### Op afstand controleren

Een belangrijk aspect is dat de instantie ook op enige afstand, i.e. zonder het verkeer te hinderen, kan controleren of in een voertuig de administratie *juist* wordt bijgehouden. In eerste instantie behandelen we e.e.a. voor het geval dat de administratie alleen de kilometerstand betreft. Voor een goede controle op juiste kilometerstanden moet er i.h.a. op twee aspecten gelet worden, nl. 1) of de kilometerteller steeds correct wordt opgehoogd, i.e. of de teller *precies* is, en 2) of de kilometerteller niet af en toe stiekem wordt teruggezet, i.e. of de teller *monotoon* stijgend (preciezer geformuleerd: monotoon niet-dalend) is.

### Controle op precisie van kilometertellers

Voor het controleren op het eerstgenoemde aspect kan men op willekeurige, wisselende (en evt. ook op een aantal vaste) plaatsen een *controleval* inrichten. Als de controleval bestaat uit een weggedeelte zonder mogelijkheid om de weg tussen het begin en het einde van de val te verlaten, dan heeft hij één ingang en één uitgang. Als er na het begin van de controleval b.v. een aantal splitsingen en/of afritten voorkomen, dan kan de controleval gezien worden als een boomstructuur met één ingang als wortel en vele uitgangen als bladeren. Nog ingewikkelder controlevallen met meerdere ingangen zijn denkbaar. Hoe dan ook, het is de bedoeling dat men een controleval alleen kan binnenkomen via één van zijn ingangen en alleen verlaten via één van zijn uitgangen. Daarnaast is het voor controle op kilometertellers van belang dat de lengte van elk controletraject, i.e. van elk traject van een ingang naar een uitgang, voldoende nauwkeurig bekend is. (Een controle val kan ook gebruikt worden voor verkeersbeheer, nl. voor het waarnemen van en inzicht verkrijgen in de loop van verkeersstromen. Hierbij spelen de lengtes van de trajecten binnen de controlevallen geen rol.)

40

Van elk deelnemend voertuig dat (oftewel, van elke VA die) een controletraject aflegt, wordt tweemaal de kilometerstand uitgelezen. Eénmaal op het moment dat het voertuig het begin van het controletraject passeert, i.e. de val binnenkomt, en éénmaal op het moment dat hetzelfde voertuig het eind van dat traject passeert, i.e. de val verlaat. M.b.v. een processor kan elk tweetal bij elkaar horende kilometerstanden van elkaar afgetrokken worden en vergeleken worden met de bekende lengte van het controletraject.

Als de beide lengtes voldoende nauwkeurig overeenkomen, wordt de kilometerteller in het voertuig blijkbaar naar behoren bijgehouden. Maar als het verschil te groot gevonden wordt, zal er vanzelfsprekend een bepaalde actie in gang worden gezet. Die actie kan b.v. bestaan uit het iets verderop aanhouden van het betreffende voertuig. Of b.v. uit het maken van een video-opname van het kenteken van het betreffende voertuig om de verantwoordelijke houder later op te sporen en hem of haar vervolgens te sommeren spoedig langs te komen met het voertuig voor een nader onderzoek. (N.B. We merken hier alvast op dat manipulatie met kentekenplaten i.h.a. eenvoudig is en dat men dus beter kan zorgen voor een wel goed fraudebestendig identificatiemiddel.)

Of twee tellerstanden bij elkaar horen, i.e. bij hetzelfde voertuig dan wel bij dezelfde betaler horen, kan bepaald worden door ervoor te zorgen dat bij elke tellerstand in een uitgezonden bericht een bijbehorend identificatienummer of een semi-identificatienummer wordt vermeld. Het begrip semi-identificatienummer komt later uitgebreid aan de orde in het hoofdstuk over semi-identificatie.

## 20 Controle tegen stiekem terugdraaien

Om ervoor te zorgen dat de tellerstanden alleen monotoon stijgen, i.e. dat ze niet op enig moment zonder reële kans op ontdekking kunnen worden teruggedraaid<sup>25</sup>, moeten er voldoende controles gehouden worden op tellermonotonie. Deze controles vinden plaats door op willekeurige momenten, dus ook op de meest 'wilde' momenten, tellerstanden met bijbehorende identificatie uit te lezen, i.e. aangiften op te vangen. Bij ontvangst van een aangifte wordt in een door de controleur bij te houden administratie opgezocht welke tellerstand tot nu toe als meest recent ontvangen genoteerd stond bij de betreffende identificatie. Als de nu ontvangen tellerstand hoger is, wordt deze in de administratie opgenomen als meest recente en als deze lager is moet er een tegenactie worden ondernomen, want dan is er sprake van een ongeoorloofde situatie.

De voor controles op monotonie benodigde administratie bestaat dus uit één meest recent opgevangen tellerstand per identificatie. Het moge duidelijk zijn dat elke tellerstand steeds uniek geïdentificeerd moet worden door één en dezelfde identificatie en dat het gebruik van echte identificatienummers voor deze controles onontbeerlijk is. Semi-identificatienummers zijn hiervoor dus niet geschikt. Dit laatste aspect wordt geacht de lezer duidelijk te worden na lezing van het latere hoofdstuk over semi-identificatie.

Merk op dat het voor controle op monotonie voldoende is om vanuit voertuigen uitgezonden berichten op te vangen. Het is bij deze controles dus niet nodig om de plaats van het voertuig op het moment van ontvangst te bepalen, wat wel nodig is bij de controles op precisie.

<sup>25</sup> Met name moet ook beveiligd worden tegen terugdraaien van een teller tijdens stilstand!

Als de tellerstand(en) in elk bericht worden geïdentificeerd door identificatie-nummers, dan kan in elke controleval de controle op precisie eventueel gecombineerd worden met een controle op monotonie. Het is dus niet altijd noodzakelijk om 'aparte' controles uit te voeren op tellermonotonie.

5

### Controle op tellers in het algemeen

De hierboven beschreven wijze van controle op monotonie kan niet alleen gebruikt worden voor kilometertellers, maar ook voor alle andere soorten tellers. Bovendien kan ze niet alleen toegepast worden in geval van stijgende (oplopende) tellers, maar vanzelfsprekend ook in geval van dalende (aflopende) tellers<sup>26</sup>. Kortom, de monotonie mag ook best dalend i.p.v. stijgend zijn. Voor volledige controle is ook nog controle op precisie vereist. Maar ook controle op precisie is mogelijk voor veel meer tellers dan alleen kilometertellers.

10

Stel bijvoorbeeld dat er sprake is van een heffingsteller en dat de hoeveelheid heffingspunten voor een afgelegde afstandseenheid een functie is van meerdere variabelen, zoals b.v. snelheid, toerental, voertuigtype, lengte, breedte, e.d. Zolang de juiste waarde van alle gebruikte variabelen betrouwbaar kan worden bepaald, kan de heffingsteller volledig worden gecontroleerd. De waarde van betrokken variabelen kan op twee manieren betrouwbaar worden vastgesteld, namelijk ofwel 1) door ze extern, i.e. (op afstand en) onafhankelijk van de opgave vanuit het voertuig, te bepalen, ofwel 2) ervoor te zorgen dat de opgave vanuit het voertuig wel degelijk vertrouwd kan worden. In de volgende twee secties gaan we hier nog wat nader op in.

20

We merken hier nog even op dat voor extern te bepalen gegevens de aanwezigheid in elke aangifte strikt genomen niet vereist hoeft te worden. Het is echter meestal handiger om dat wel te doen. Immers, controleren of een opgegeven waarde klopt kan gemakkelijker (en dus goedkoper) zijn dan onafhankelijke vaststelling, maar nooit moeilijker (resp. duurder). Bijvoorbeeld is het controleren of een opgegeven kenteken overeenkomt met dat op de kentekenplaat gemakkelijker dan het geheel zelfstandig (i.e. zonder hint te hebben) lezen van het kenteken op de kentekenplaat.

25

Tenslotte wordt nog opgemerkt dat er bij aparte controles op precisie en monotonie voorkomen moet worden dat een bepaalde teller in een voertuig aan volledige controle kan ontsnappen, doordat de schijn gewekt wordt van twee verschillende tellers. Met andere woorden, er moet voor gezorgd worden dat beide soorten controles voor elke individuele teller correct 'aan elkaar gekoppeld' kunnen worden.

30

### Gegevens geschikt voor controle op afstand

35

De detectie van onjuistheden of afwijkingen is in ieder geval mogelijk voor alle soorten door de voertuigapparatuur te leveren gegevens waarvan de juiste waarde (liefst automatisch) op afstand kan worden vastgesteld bij passerende voertuigen. Dit kan gebeuren door *directe* bepaling, zoals b.v. bij snelheid, snelheidsverandering,

<sup>26</sup> Aflopende tellers kunnen b.v. de nog beschikbare kilometers of 'vervuilingsrechten' bijhouden.

lengte, breedte, kleur, carrosserievorm, kenteken op kentekenplaat, e.d. Het kan soms ook *indirect* via afleiding uit andere gegevens.

5 Een al eerder gegeven voorbeeld daarvan is het brandstofverbruik. Hoewel het brandstofverbruik van een passerend voertuig niet op afstand direct gemeten kan worden, is het vaak wel mogelijk om het brandstofverbruik tamelijk nauwkeurig af te leiden uit een aantal andere gegevens die in belangrijke mate bepalend blijken te zijn voor het brandstofverbruik van het passerende voertuig. Denk hierbij aan de volledige typering van het voertuig en aan bepaalde gegevens over het gebruik (incl. de gebruiksomstandigheden) van het voertuig, i.e. bepaalde gegevens verband houdende met zijn beweging. Zoals al eerder gezegd kan een volledige typering b.v. bestaan uit merk, model, bouwjaar, versnellingsbak- en motortype. Gegevens over het gebruik die een rol kunnen spelen, zijn enerzijds b.v. snelheid, acceleratie, toerental, e.d., en anderzijds b.v. de luchtvochtigheid, luchtdruk, buiten-temperatuur, windsnelheid en windrichting. Als er een voldoende nauwkeurig verband bekend is en m.b.t. de daarvoor benodigde gegevens (i.e. de input-parameters) wel betrouwbare waarden beschikbaar zijn, kan het juiste brandstofverbruik dus toch afgeleid worden. Een vanuit het voertuig opgegeven waarde kan dan dus wel degelijk  
15 gecontroleerd worden op geloofwaardigheid.

Een ander voorbeeld van een afleidbaar gegeven is b.v. het toerental. Als een volledige typering (merk, model, bouwjaar, versnellingsbak- en motortype, e.d.) van het passerende voertuig bekend is, kan men d.m.v. een snelheidsmeting, een snelheidsveranderingsmeting (zeg maar, acceleratiemetings) en een gerichte geluidsmeting indirect controleren in welke versnelling gereden wordt. Op basis van de snelheid en door de fabrikant beschikbaar gestelde (en wellicht door de instantie gecontroleerde) gegevens over overbrengingsverhoudingen, kan men dan veel preciezer het toerental afleiden en dit gebruiken voor de controle op juistheid van het opgegeven toerental.

25 We hebben al eerder beschreven dat en hoe diverse tellers steekproefsgewijs op afstand gecontroleerd kunnen worden. Het moge nu duidelijk zijn dat ook toerentellers en brandstoftellers tot die categorie (kunnen) behoren.

#### **Nog een voorbeeld van het nut van afgeleide informatie**

30 Ter illustratie van de mogelijkheden die afleidingen kunnen bieden, beschrijven we hier in het voorbijgaan nog één specifiek voorbeeld. Dit voorbeeld betreft de mogelijkheid om de totale hoeveelheid lawaai veroorzaakt door een voertuig (dus incl. geluid door luchtstroming langs het voertuig) tamelijk nauwkeurig af te leiden uit een aantal andere gegevens. Het aardige van dit voorbeeld is, dat afleiding zelfs geboden kan zijn, omdat het in bepaalde gevallen ondoenlijk of onmogelijk lijkt om dit gegeven voldoende nauwkeurig daadwerkelijk te meten.

35 Immers, in geval van wegverkeer geldt dat men, zowel bij meting vanuit het voertuig zelf als bij meting op een zekere afstand langs of boven de weg, veel last zal hebben van het lawaai voortgebracht door eventueel volop aanwezig ander verkeer. Daarnaast lijkt het onmogelijk om vanuit een snel voortbewegend voertuig het geluid als gevolg van de zelf veroorzaakte luchtwervelingen te meten. Dit laatste speelt m.n. ook een rol in het geval van vliegverkeer. Hierbij lijkt voldoende nauwkeurige geluidsmeting overigens alleen ondoenlijk vanuit de betreffen-  
40 de vliegtuigen zelf.

Merk op dat het verschil met het eerder genoemde voorbeeld van veroorzaakte milieuvervuiling is dat het, althans bij wegverkeer, in principe wel degelijk mogelijk is om in het voertuig de uitlaatgassen daadwerkelijk te meten en te analyseren. We gingen er bij dat voorbeeld alleen vanuit dat daadwerkelijke meting en analyse te kostbaar was.

5

### **Gegevens niet geschikt voor controle op afstand**

Natuurlijk kan men de voertuigapparatuur eventueel ook gegevens laten gebruiken en laten uitzenden, waarvan men (nog) niet weet hoe die voldoende gemakkelijk, en dus voldoende goedkoop, op afstand bij aan het verkeer deelnemende voertuigen direct of indirect gecontroleerd kunnen worden. Denk hierbij bijvoorbeeld aan het type motor dat in het voertuig aanwezig is, de stand van het gaspedaal en/of of op LPG dan wel benzine gereden wordt. (Overigens is het wel degelijk denkbaar dat de stand van het gaspedaal indirect gecontroleerd kan worden als voldoende andere factoren bekend zijn. Ook kan de uitlaat van een voertuig evt. op enige afstand voldoende goed 'besnuffeld' worden om een verschil tussen gebruik van LPG en benzine te constateren zonder het verkeer te hinderen.)

15

Als de juistheid van dergelijke gegevens van voldoende hoog belang is, moet er dan wel voor gezorgd worden dat deze gegevens op voldoende fraudebestendige wijze worden verkregen, verzameld en verzonden. Om b.v. valse input voor de processor (van de VA) te voorkomen, moeten de bij het verzamelen van dat soort informatie betrokken componenten, vaak sensoren en hun verbindingen naar de processor, voldoende fraudebestendig worden uitgevoerd<sup>27</sup>.

20

Kortom, voor elke gebruikte gegevenssoort die niet of niet makkelijk genoeg steekproefsgewijs (en bij onze eerste aanpak: op afstand) gecontroleerd kan worden bij voortbewegend verkeer, lijkt een voldoende garantie op betrouwbaarheid d.m.v. fysieke beveiliging vereist!<sup>28</sup> Als bijvoorbeeld een betrouwbare opgave vanuit het voertuig van het kenteken van het voertuig en/of van de volledige typering van het voertuig, nodig wordt geacht voor het gewenste systeem van verkeersheffing, dan kunnen deze gegevens door een (b.v. verzegeld aangebrachte) component op voldoende fraudebestendige wijze worden vastgehouden en verstrekt. Het kan gaan om een aparte, speciale component alleen voor dit doel (i.e. wat we in het hoofdstuk over de aanpak met agenten een gespecialiseerde agent zullen noemen), maar deze taak kan ook worden verricht door een (algemene) agent die op fraudebestendige wijze aan het voertuig bevestigd is. We komen nog op e.e.a. terug in de hoofdstukken over identificatie en over de aanpak met agenten.

30

<sup>27</sup> Omdat dan het hele traject t/m verzending moet worden beveiligd tegen fraude, zal de processor vrijwel zeker ook fraudebestendig moeten zijn. Hoe dan ook, we lopen hier in feite even vooruit op de latere behandeling van het gebruik van agenten.

<sup>28</sup> Zoals we al eerder hebben laten blijken, zijn we van mening dat het i.h.a. verstandig is om zo min mogelijk te vertrouwen op (alleen) fysieke beveiliging, o.a. omdat een hoog fysiek beveiligingsniveau vaak gepaard gaat met hoge kosten.

### Controles op basis van differentie- of differentiaalquotienten

We hebben met het voorgaande geïllustreerd dat het meer in het algemeen mogelijk is om controles op precisie uit te voeren door op elk van twee opeenvolgend te passeren punten een waarde te ontvangen en te kijken of het verschil tussen de opgegeven waarden klopt met een op andere, betrouwbare wijze verkregen referentie- of ijk-  
5 waarde. Waarschijnlijk heeft de lezer de suggestie geproefd (en niet ten onrechte) dat deze twee punten op een zekere afstand van elkaar moeten liggen. Echter, nu lijkt het moment gekomen om nadrukkelijk te wijzen op de mogelijkheid om controles uit te voeren m.b.v. differentie- of differentiaalquotienten. Anders gezegd, in principe kan men de afstand tussen de meetpunten eventueel heel klein kiezen en eventueel kan men vanuit het voertuig  
10 differentie- of differentiaalquotienten laten uitzenden. In het hoofdstuk over de aanpak met agenten zullen we deze mogelijkheid illustreren door te laten zien dat controle op een kilometerteller ook kan plaatsvinden door de juiste snelheid op een bepaald moment (i.p.v. de juiste lengte van een controletraject) als referentie- of ijkwaarde te gebruiken.

### 15 Rollenbank voor nadere inspectie

Als op basis van een controle blijkt dat er iets niet klopt, moet het betreffende voertuig en m.n. de betreffende voertuigapparatuur nader geïnspecteerd en gecontroleerd worden. Ook kan eventueel wettelijk de verplichting worden vastgelegd om elk voertuig periodiek, b.v. minstens eenmaal per jaar, zo'n nadere controle te laten ondergaan. Naast een visuele inspectie op (pogingen tot) fraude zal de nadere controle kunnen bestaan uit het testen  
20 van de juiste werking van de voertuigapparatuur op een daartoe ingerichte rollenbank. Met de rollenbank kunnen allerlei situaties worden gesimuleerd en kan juiste functionering van de voertuigapparatuur in die situaties worden gecontroleerd resp. de oorzaak van onjuist functioneren worden opgespoord.

## Gebruik van een ontvanger

Als elk deelnemend voertuig ook wordt uitgerust met een ontvanger, dan geeft dit een groot aantal mogelijkheden en voordelen, waarvan we hier slechts een klein aantal noemen.

5

### Automatische ijking

Bijvoorbeeld kan door zenders langs of boven de weg informatie worden uitgezonden (b.v. over de snelheid van het voertuig òf over de juiste afstand tussen twee te passeren punten), die het na ontvangst in het voertuig mogelijk maakt om bepaalde apparatuur (in ons voorbeeld de kilometerteller en de snelheidsmeter) automatisch te ijken.

10

Eén voordeel is dus dat kilometertellers en snelheidsmeters tijdens het rijden op bepaalde weggedeelten volautomatisch geijkt kunnen worden, zodat ze steeds nauwkeurig blijven werken. Zo kan eventueel zelfs de invloed van bandenslijtage op de nauwkeurigheid van kilometertellers en snelheidsmeters weggenomen worden. Op soortgelijke wijze kan b.v. ook een thermometer die aan het voertuig bevestigd is voor het bepalen van de buitentemperatuur, zelfijkend worden gemaakt, i.e. zichzelf automatisch controleren en/of aanpassen op basis van een toegestuurde betrouwbare temperatuur van de plek waar het voertuig zich bevindt. Door ervoor te zorgen dat de thermometer in een voertuig de buitentemperatuur nauwkeuriger kan weergeven, kan b.v. nauwkeuriger gewaarschuwd worden voor eventuele gladheid t.g.v. bevriezing.

15

20

Vanzelfsprekend kan op soortgelijke wijze ook andere meetapparatuur in voertuigen automatisch geijkt worden. Ook het omgekeerde is mogelijk, nl. dat meetapparatuur langs de weg zichzelf ijkt, i.e. zichzelf controleert op juiste werking en/of zichzelf automatisch aanpast, op basis van door passerende voertuigen verstrekte meetwaarden. Immers, eventueel kan men een waarde, zoals bijvoorbeeld de temperatuur, op een bepaalde plaats tamelijk nauwkeurig berekenen op basis van een voldoende aantal door passerende voertuigen gemeten en verstrekte waarden. Dus de automatische ijking van meetapparatuur, zoals b.v. snelheidsmeters en thermometers, kan zowel meetapparatuur in voertuigen als meetapparatuur langs de weg betreffen en kan eventueel zelfs wederzijds geschieden.

25

30

### Enkele andere voordelen

Ook kan door gebruik van een ontvanger voorkomen worden dat de klok op den duur te veel gaat afwijken en kunnen tijdswisselingen (bij overschrijding van een tijdszonegrens en bij overgang van zomer- naar wintertijd of v.v.) automatisch verwerkt worden. Omdat snelheid een afgeleide grootheid is van afgelegde weg en tijd, zal de snelheidsmeting in een voertuig ook extra nauwkeurig kunnen geschieden als bekend wordt in welke mate zijn kloksnelheid afwijkt.

35

Verder is het mogelijk om per tariefgebied, bestaande uit een bepaald weggedeelte of uit alle wegen in een bepaald gebied, een verschillende berekeningswijze te hanteren. Daartoe moeten dan wel bij *alle* overgangen tussen

40



tariefgebieden zenders staan om de passerende voertuigen op de hoogte te stellen van de tariefovergang. Een ander voordeel is dat ook een nieuwe berekeningswijze, i.e. tarieffunctie, kan worden ontvangen. Dit kan bijvoorbeeld gebruikt worden om een tariefverhoging door te voeren of om de geldende spitstijden aan te passen.

- 5 De zenders van de infrastructuur (veelal langs of boven de weg) en de ontvangers in de voertuigen zouden ook gebruikt kunnen worden voor de distributie van nieuwe programmatuur in het algemeen en van nieuwe programmatuur t.b.v. het verkeersinformatiesysteem in het bijzonder. Door ervoor te zorgen dat programmatuur voorzien van een juiste handtekening automatisch geïnstalleerd en in werking gesteld kan worden ter vervanging van een eerdere versie, kunnen bepaalde wijzigingen of aanpassingen eventueel zelfs zonder tussenkomst van de gebruiker of houder van het voertuig worden aangebracht.
- 10

- De ontvanger kan ook worden gebruikt om het zenden vanuit een voertuig te beperken tot een korte periode na elk geautoriseerd verzoek. Het waarschijnlijk belangrijkste voordeel hiervan is dat er minder bandbreedte nodig is voor de communicatie met alle voertuigen. Voor de privacybescherming heeft dit het voordeel dat het voor derden iets moeilijker wordt om het berichtenverkeer af te luisteren. Daarnaast zullen evt. pogingen tot misbruik door de overheid (b.v. een poging om toch al het verkeer te traceren door op elke hoek een zender/ontvanger te plaatsen) dan sneller opvallen resp. makkelijker gedetecteerd kunnen worden. Anderzijds het is vanuit het oogpunt van fraudebestrijding een nadeel als men in elk voertuig te weten kan komen op welke momenten en/of plaatsen er door controleurs om gegevens gevraagd wordt. Immers, zonder extra tegenmaatregelen wordt de steekproefsgewijze beveiliging tegen fraude dan i.h.a. zwakker, want men kan dan beter inspelen of gokken op momenten waarop manipulatie met de teller waarschijnlijk niet ontdekt zal worden. (Zie voor verdere details het hoofdstuk over de aanpak m.b.v. agenten.)
- 15
- 20

- Men lijkt dus in geval van uitsluitend controles op afstand een afweging te moeten maken tussen ofwel 1) een simpeler fraudebestrijding en meer (behoefte aan) gebruik van cryptografie om tegen afluisteren te beschermen, ofwel 2) lastiger fraudebestrijding maar minder of misschien zelfs geen (behoefte aan) gebruik van cryptografie voor de privacybescherming. Omdat cryptografie veelal sowieso gewenst zal zijn voor b.v. geheimhouding van en/of digitale handtekeningen op berichten, zal de balans bij deze keuze kunnen door slaan naar (vrijwel) continu uitzenden. De in een later hoofdstuk beschreven aanpak zonder continu uitzenden vanuit het voertuig, maar met controles door agenten in het voertuig, biedt echter een zeer aantrekkelijk alternatief. Overigens wordt bij deze laatste aanpak normaal gesproken wel degelijk gebruik gemaakt van een ontvanger.
- 25
- 30

- Natuurlijk kan de ontvanger nog voor vele andere doeleinden worden gebruikt. Bijvoorbeeld zou bij ontvangst van een bepaalde code of van een passend en (mede) door de houder of eigenaar ondertekend bericht overgeschakeld kunnen worden op het toevoegen van een volledige identificatie aan elk uitgezonden bericht en eventueel ook overgeschakeld kunnen worden naar het continu uitzenden van identificaties. Een dergelijke voorziening kan o.a. gebruikt worden ter opsporing van voertuigen na b.v. diefstal. Ook is het bijvoorbeeld mogelijk om passerende voertuigen via zenders langs de weg frequent te informeren over b.v. filevertragingen of over de ter plaatse geldende maximum snelheid. Dit laatste gegeven kan b.v. gebruikt worden om de bestuurder te waar-
- 35

schuwen als hij te hard rijdt. In het navolgende wordt beschreven hoe de verkeersveiligheid verhoogd kan worden door maximum snelheden automatisch te laten respecteren.

### **Automatisch respecteren van officiële snelheidsbeperkingen**

5

Wij stellen voor om apparatuur voor cruise control zodanig uit te gaan voeren dat deze gebruik kan gaan maken van door het verkeersinformatiesysteem verspreide berichten over snelheidsbeperkingen. Op deze wijze kan de bestuurder ontlast worden van een deel van zijn taak, want de maximum te rijden snelheid kan dan automatisch aangepast en gerespecteerd worden. Aanpassing aan een hogere maximum snelheid zal dan normaliter alleen

10

gebeuren als deze maximaal toegestane snelheid lager ligt dan de door de bestuurder aan de cruise control opgegeven gewenste snelheid.

Zo'n voorziening zal de verkeersveiligheid ongetwijfeld ten goede komen. Alleen de taakverlichting van de bestuurder kan al zorgen voor een positief effect. Ook wordt nog eens voorkomen dat de officiële maximum snelheid per ongeluk overschreden wordt, b.v. doordat de bestuurder een verkeersbord met een snelheidsbeperking over het hoofd ziet. Tevens kan op deze wijze de snelheid van voertuigen bij het naderen van een file geleidelijk aangepast worden en in een file de snelheid van de voertuigen tamelijk homogeen en gelijkmatig worden gemaakt.

15

20

Als op den duur alle voertuigen (tegen een aanvaardbare prijs) voorzien (kunnen) worden van dergelijke apparatuur, ontstaat er bovendien een betere basis voor strenge handhaving van maximum snelheden, omdat er dan geen redelijk excuus meer is voor per ongeluk te hard rijden. Door strenge handhaving, hetgeen met de door ons voorgestelde verkeersinformatiesystemen zeer wel mogelijk wordt, kan de verkeersveiligheid nog verder toenemen. Denk o.a. aan het handhaven van de snelheidsbeperkingen in woonbuurten resp. op woonerven.

25

Tenslotte levert het ook nog een aanzienlijke kostenbesparing op, als blijkt dat dan minder (aanleg en daarna onderhoud van) verkeersdrempels en andere snelheidsontmoedigende voorzieningen nodig zijn. Denk daarnaast ook aan de besparingen ten gevolge van verminderde slijtage aan b.v. vering en schokbrekers en aan besparing op brandstofverbruik. (De huidige praktijk van remmen voor en weer optrekken na een verkeersdrempel is ook nog eens extra belastend voor het milieu.)

30

Merk op dat zulke apparatuur voor cruise control bestuurders ook de mogelijkheid biedt om, indien gewenst, zo hard mogelijk te rijden zonder ergens de maximum snelheid te overschrijden. Op het eerste gezicht lijkt dit misschien een verkeersveiligheidonvriendelijke toepassing, maar het kan de verkeersveiligheid toch wel degelijk ten goede komen! Immers, het komt in de praktijk maar al te vaak voor dat men zo snel mogelijk ergens naar toe wil. Als bestuurders zonder hulpmiddel zelf proberen om zoveel mogelijk de maximum snelheden aan te houden, kost dat een hoge mate van aandacht en concentratie, terwijl ze toch zo nu en dan de maximum snelheid zullen overschrijden, zelfs zonder dat te willen. Bij massaal gebruik van deze mogelijkheid op autosnelwegen zullen de snelheidsvariaties en -verschillen afnemen, wat de verkeersveiligheid ook nog eens ten goede komt.

40

**Ondersteuning bij het invoegen op snelwegen**

5 De samenwerking tussen het TIP-systeem en de cruise control kan op termijn evt. ook verder gaan. Bijvoorbeeld zou er ondersteuning geboden kunnen worden bij het invoegen op een autosnelweg. Het verkeersinformatiesysteem kan dan b.v. een invoegpositie bepalen tussen de al op de snelweg rijdende voertuigen en, als dat nodig is, de snelheid van die voertuigen en van het invoegende voertuig zodanig beïnvloeden dat er veilig, soepel en probleemloos wordt ingevoegd. We gaan hier verder niet in op de details hiervan.

## Privacybescherming

In dit hoofdstuk gaan we in op hoe betaling en controles geregeld kunnen worden en hoe daarbij voldoende privacybescherming kan worden geboden. We baseren onze uitleg primair op de situatie waarbij de verkeersheffingen per giro- of bankrekening worden voldaan, b.v. via automatische betalingen op basis van een machtiging.  
 5 Later zullen we nog een keer de mogelijkheid aanstippen van directe betaling in de auto m.b.v. een chipkaart.

Zoals hierboven gemeld, gaan we er vanuit dat de heffingsinner tevens fungeert als controleur. In het geval dat controles wel zouden worden uitbesteed aan meerdere onafhankelijke organisaties, wordt de privacy van de verkeersdeelnemers minder bedreigd, zodat het dan makkelijker wordt om de privacy te beschermen. Wij beperken  
 10 onze uitleg hier dus tot het moeilijkere geval waarbij de heffingsinner zelf de enige controleur is.

### Directe en indirecte identificaties

15 Voor de identificatie van een betaler zijn verschillende mogelijkheden. Voor de betaling is het niet vereist dat de instantie, in dit geval de heffingsinner, precies weet wie de betaler is. Dus een *directe* persoonsidentificatie, waarvan o.a. sprake is bij gebruik van een rijbewijs-, paspoort- of sofinummer, is niet per sé nodig en kan zelfs ongewenst zijn. Uit oogpunt van privacybescherming is het i.h.a. beter om een geschikte *indirecte* identificatie (denk hierbij b.v. aan een bankrekeningnummer) te gebruiken, zodat de heffingsinner wel weet waar de rekening  
 20 heen moet, maar niet ook meteen weet wie daar achter schuil gaat.

Normaliter zal de organisatie die een bepaald indirecte identificatienummer voor dit doel heeft uitgegeven, geheim (moeten) houden welke persoon er achter dat indirecte identificatienummer schuil gaat. Natuurlijk zijn dan wetten nodig, waarin ook vastgelegd wordt in welke omstandigheden de betreffende organisatie de identiteit van de  
 25 bijbehorende persoon wel mag resp. moet prijsgeven.

Merk op dat niet elke indirecte identificatie geschikt is. Bijvoorbeeld wordt, als elk voertuig één bijbehorende houder heeft, de houder van een voertuig indirect geïdentificeerd door het kenteken van het voertuig. Desalniettemin bieden kentekens een onvoldoende waarborg voor de privacybescherming van de houders als de kentekenregistratie, zoals gebruikelijk is, volledig toegankelijk is voor de overheid. (Men zou natuurlijk ook kunnen overwegen om de koppeling tussen voertuigen en houders uit de kentekenregistratie van de overheid te halen en die ter bescherming van de privacy onder te brengen bij één of meerdere aparte organisaties.)  
 30

### Fraudebestendige componenten, zoals b.v. chipkaarten

35 Het toevoegen van een of ander identificatienummer lijkt misschien op het eerste gezicht onaanvaardbaar voor de gewenste bescherming van de privacy. Echter, er zijn diverse mogelijkheden om de privacy voldoende te beschermen, terwijl toch gebruik wordt gemaakt van identificatienummers. Eén interessante mogelijkheid betreft het gebruik van chipkaarten, of andersoortige combinaties van apparatuur en/of programmatuur, op de fraudebe-

stendigheid waarvan de instantie wil vertrouwen<sup>29</sup>. Wij zullen in het vervolg alleen spreken over chipkaarten, maar de uitleg gaat ook op voor allerlei andere verschijningsvormen, waaronder b.v. ook chipsleutels.

Bij de beveiliging van chipkaarten tegen allerlei vormen van fraude is altijd sprake van een vorm van fysieke  
 5 beveiliging. Als, zoals gebruikelijk is, voor de beveiliging van de chipkaart en zijn functioneren gebruik wordt  
 maakt van cryptografie, geldt bijvoorbeeld dat er tenminste één sleutel (i.e. één bitpatroon) op de kaart aanwezig  
 zal zijn waarvan de geheimhouding alleen gewaarborgd wordt door fysieke beveiliging. Dus als er bij een sys-  
 teem gebruik wordt gemaakt van chipkaarten, is de veiligheid van het totale systeem mede afhankelijk van (de  
 kwaliteit van) deze fysieke beveiliging. In de praktijk blijkt dat geen bezwaar, omdat bij chipkaarten blijkbaar  
 10 gezorgd kan worden voor een prima fysieke beveiliging tegen diefstal van een (cryptografische) sleutel.

Hoe dan ook, de organisatie die de chipkaart uitgeeft, kan voldoende waarborgen inbouwen dat ze durft te garan-  
 deren dat de chipkaart alleen op de bedoelde wijze functioneert en gebruikt kan worden. Daardoor is het b.v.  
 mogelijk om anonieme betalingen uit te laten voeren m.b.v. zo'n chipkaart. We gaan er vanuit dat het gebruik van  
 15 zulke chipkaarten voor anonieme of semi-anonieme betalingen al voldoende bekend is en dat het niet nodig is om  
 in meer detail te beschrijven hoe zulke (semi-)anonieme betalingen kunnen bijdragen aan een sluitend TIP-  
 systeem, waarbij de privacy voldoende wordt beschermd. Wel zullen we nu toch even iets verder ingaan op een  
 aantal relevante aspecten van de mogelijkheid om chipkaarten voor andere doeleinden dan betaling in te schake-  
 len. De verdere behandeling van de mogelijkheid om chips i.h.a. en chipkaarten i.h.b. te gebruiken voor b.v. het  
 20 (meer) vertrouwenswaardig verstrekken van gegevens vanuit een voertuig, vindt plaats in het hoofdstuk over de  
 aanpak met agenten.

#### **Anonieme, anoniem verstrekte of semi-anoniem verstrekte chipkaarten**

Chipkaarten kunnen anoniem zijn of anoniem dan wel semi-anoniem worden verstrekt. Een chipkaart noemen wij  
 25 *anoniem* als hij niet (voldoende uniek) identificeerbaar is. De houders van zo'n chipkaart en/of voertuigen waarin  
 zo'n chipkaart gebruikt wordt, kunnen vanzelfsprekend niet uitsluitend op basis van de door hun gebruikte kaart  
 geïdentificeerd worden als de gebruikte kaart anoniem is. Maar ook als elke chipkaart zelf wel geïdentificeerd  
 wordt m.b.v. een uniek identificatienummer, i.e. niet anoniem is, kan identificatie van de houder van de kaart  
 30 en/of van het bijbehorende voertuig vermeden worden. Dit kan door zulke identificeerbare chipkaarten anoniem  
 of semi-anoniem te verstrekken. Er is sprake van *anonieme verstrekking* als niet geregistreerd wordt voor wie of  
 voor welk voertuig een bepaalde chipkaart, al dan niet tegen betaling, is verstrekt. Bij *semi-anonieme verstrek-*  
*king* wordt dit wel geregistreerd, maar door aparte organisatie(s) die fungeren als privacybeschermer(s). De kop-  
 peling tussen chipkaart en houder en/of voertuig mag in dit geval alleen onder in de wet duidelijk omschreven  
 35 condities prijsgegeven worden en dan nog alleen aan de overheid. (Dit is in zekere mate vergelijkbaar met de  
 uitgifte van b.v. geheime bankrekeningnummers of geheime telefoonnummers.) In geval van semi-anonieme  
 verstrekking is er dus sprake van een vorm van indirecte identificatie.

<sup>29</sup> In deze sectie en de twee volgende secties lopen we even een beetje vooruit op de latere behandeling van het gebruik van agenten.

### Privacybescherming bij gebruik van chipkaarten of chipsleutels

Het voert te ver om uitputtend alle mogelijkheden te behandelen waarop m.b.v. (semi-)anoniem verstrekte en/of anonieme chipkaarten een sluitend TIP-systeem verkregen kan worden waarbij de privacy voldoende wordt beschermd. We wijzen nu alleen op de mogelijkheid om (bepaalde vormen van) fraude onmogelijk te maken door een chipkaart in te schakelen bij het (gecontroleerd) verstrekken van gegevens, zoals b.v. kilometerstanden, vanuit een voertuig. In feite hebben we het hier al over een aanpak m.b.v. agenten, waaraan we verderop een heel hoofdstuk wijden. Omdat, zoals later duidelijk zal worden, o.a. chipkaarten kunnen fungeren als agent, wordt in dat hoofdstuk in feite ook een nadere illustratie gegeven van deze mogelijkheid om chipkaarten te gebruiken. Die latere illustratie wordt geacht voor ter zake kundigen voldoende te zijn.

Op dit moment is het eigenlijk alleen van belang dat de lezer al inziet dat het met gebruik van anonieme, anoniem verstrekte of semi-anoniem verstrekte chipkaarten makkelijker is om de privacy te beschermen dan zonder. Wij geven nu in het navolgende een uitgebreide uitleg van het moeilijkere geval waarbij géén gebruik wordt gemaakt van (semi-)anoniem verstrekte of anonieme chipkaarten om personen en/of voertuigen te representeren.

### Privacybescherming bij gebruik van identificatienummers van persoon of voertuig

Zoals al eerder opgemerkt, lijkt misschien op het eerste gezicht het toevoegen van een identificatienummer onaanvaardbaar voor de gewenste bescherming van de privacy. Hierboven hebben we al gesuggereerd dat de privacy vrij makkelijk beschermd kan worden als het identificatienummer een (semi-)anoniem verstrekte chipkaart identificeert. In het navolgende zullen we laten zien dat ook voldoende privacybescherming geboden kan worden als het identificatienummer wel degelijk een persoon of voertuig identificeert.

Het is namelijk goed mogelijk te voorkomen dat men de bewegingen van het voertuig en/of van de betaler stelsmatig kan volgen. Wij zullen laten zien dat dit m.n. gedaan kan worden door een keten van organisaties te creëren, waarbij we onderscheid zullen maken tussen jagers, intermediairs (gespecialiseerde privacybeschermers) en de uiteindelijke geadresseerde(n) resp. berichtontvanger(s), die we ook wel *eindontvanger(s)* zullen noemen. (Zoals eerder gezegd, maken we geen onderscheid tussen controleurs en heffingsinners, zodat in ons voorbeeld van verkeersbelasting de heffingsinners de eindontvanger is.) Berichten worden hierbij alleen afgeleverd bij de eindontvanger na tussenkomst van een jager en één of meerdere intermediairs. Natuurlijk zijn er ook allerlei andere oplossingen/varianties mogelijk, waarbij dan b.v. één of meerdere van de gedachten die schuil gaan achter wat hier expliciet geschetst wordt, op een andere wijze worden gecombineerd tot een sluitend systeem.

#### 35 Jagers

De idee is dat de instantie (resp. de heffingsinners) niet te weten mag komen op welke plaatsen de afzenders van de berichten zich bevonden ten tijde van de ontvangst van de betreffende berichten. We gaan er vanuit, en in de praktijk zal dit meestal ook het geval zal zijn, dat bij de ontvangst van een bericht vrij goed bepaald kan worden waar de afzender zich bevindt. Het lijkt dus op het eerste gezicht vereist dat de instantie (resp. de heffingsinners

of, algemener, de overheid) geen directe toegang mag worden verschaft tot de door het verkeer uitgezonden berichten.

Voor de volledigheid merken we nu alvast op dat dit niet per sé betekent dat de betreffende instantie, b.v. de heffingsinner, de berichten niet zelf mag inzamelen. Want dat kan weinig kwaad als er intermediairs (zie verder-  
 5 op) gebruikt worden en de inhoud van elk bericht op het moment van inzamelen niet leesbaar is voor die instantie (resp. de heffingsinner). Hoewel het ons hier primair gaat om de geheimhouding van de verzendplaats van een bericht, is de geheimhouding van de inhoud van een bericht dus ook wel degelijk een belangrijk aspect. Een en ander wordt straks wel duidelijk(er).

10

Hoe dan ook, voor het ontvangen van berichten van zoveel mogelijk deelnemende voertuigen zonder het verkeer te hinderen kunnen onafhankelijke, met elkaar concurrerende organisaties in het leven geroepen worden, die zich bij de overheid aanbieden als jagers. In het geval dat de eindontvanger b.v. een controlerende instantie of heffingsinner is, betaalt deze de jagers waarschijnlijk om o.a. berichten van zoveel mogelijk deelnemende voertuigen op te pikken en/of dat te doen op de meest 'wilde' plaatsen.

15

Hiertoe kan ieder van deze jagers bijvoorbeeld op diverse vaste locaties ontvangers plaatsen voor continu gebruik. Daarnaast kan elke jager ook tijdelijk ontvangers opstellen op wisselende plaatsen en tijdstippen. Deze ontvangers worden dus regelmatig verplaatst. Tenslotte kan een jager ook nog met ontvangers werken die continu van plaats veranderen (b.v. doordat ze rondgereden worden), om ervoor te zorgen dat (door pogingen tot fraude of anderszins) niet goed functionerende voertuigapparatuur zoveel mogelijk kans heeft om 'betrap't te worden.

20

Het fanatisme waarmee op berichten gejaagd wordt, is voor goede controle nadrukkelijk van belang. Het lijkt in eerste instantie verstandig deze taak niet door de betreffende controlerende instantie zelf te laten verrichten, maar deze te privatiseren en door invoering van concurrentie ervoor te zorgen dat de 'scherpte' van de jagers op peil  
 25 gehouden wordt. Door de hoogte van het jaagloon afhankelijk te stellen van het succes van de jager, kan dit eventueel extra gestimuleerd worden.

25

Via regelgeving kan ervoor gezorgd worden dat iedere jager zich moet beperken tot een 'lichte bewapening', i.e. dat hij zich moet beperken tot een voldoende klein netwerk van ontvangers met een bepaalde geografische spreiding. Het totale netwerk van alle jagers kan natuurlijk wel heel uitgebreid zijn. De opzet met onafhankelijke jagers heeft daardoor een aantal voordelen m.b.t. de bescherming van burgers tegen hun eigen overheid: 1) de overheid heeft geen directe toegang tot enige ontvanger in dit netwerk en heeft dus de toestemming van een jager nodig om een bepaalde ontvanger legaal te kunnen benutten, en 2) de overheid kan alleen op een normale wijze  
 30 toegang krijgen tot een aanzienlijk deel van dit netwerk met medewerking van meerdere jagers, zodat zelfs samsenpannen met één of enkele jagers niet of nauwelijks loont.

35

De beschreven opzet geeft al met al een zekere bescherming tegen eventuele pogingen van de overheid om, desnoods op illegale wijze, d.m.v. een zeer dicht netwerk van ontvangers het verkeer toch vrij goed te kunnen  
 40 traceren. Immers, men kan het netwerk van de jagers niet zomaar gebruiken en moet dus ofwel 'inbreken' bij een

zeer groot aantal ontvangers van dat netwerk, ofwel apart voor dit doel een eigen netwerk van ontvangers creëren. Beide mogelijkheden lijken nogal kostbaar en lijken ook nauwelijks onopgemerkt uitgevoerd te kunnen worden.

- 5 Tenslotte zij opgemerkt dat voor alle zekerheid de jagers verplicht kunnen worden om de plaats van ontvangst (beter gezegd, elke mogelijke indicatie van de plaats van de verzender op het moment van de ontvangst) van ieder door hen opgevangen bericht geheim te houden. Verder zou eventueel ook nog voorgeschreven kunnen worden dat voor bepaalde soorten berichten het precieze tijdstip van ontvangst ook geheim moet worden gehou-  
10 den. Op deze verplichtingen kunnen (en zullen i.h.a.) natuurlijk een aantal precies omschreven uitzonderingen worden gemaakt.

Een extreem geval is dat het jagers wettelijk verboden wordt om de plaats (en evt. het precieze tijdstip van ont-  
15 vangst) van berichten zelfs maar te administreren<sup>30</sup>. Het kan b.v. echter ook dat voorgeschreven wordt dat jagers van elk bericht alleen gedurende een bepaalde beperkte tijd na ontvangst mogen en moeten administreren waar de afzender zich op het betreffende moment moet hebben bevonden, terwijl alleen in bepaalde door de wet duidelijk omschreven omstandigheden voor specifieke gevallen op voorgeschreven wijze mag worden afgeweken van volstrekte geheimhouding. We komen later nog terug op het gebruik van zo'n administratie t.b.v. ingrepen, zoals b.v. video-opnames, op de juiste plaats.

## 20 **Intermediairs als privacybeschermers**

Hoewel op bovenstaande wijze op zich al een redelijke bescherming geboden kan worden, hoeven we nog niet tevreden te zijn. Het primaire belang van de jagers hoeft immers niet altijd bij de privacybescherming van de burgers te liggen, zeker niet als ze worden betaald door b.v. de heffingsinnehmer of, algemener, de overheid. Boven-  
25 dien willen we een betere beveiliging tegen de mogelijkheid dat de overheid via een eigen netwerk van ontvangers meer te weten kan komen dan sommigen lief is.

We zullen nu laten zien dat er een belangrijke bijdrage aan de totale beveiliging kan worden geleverd door alle berichten afkomstig van het verkeer zodanig te laten vercijferen, dat noch de overheid, noch anderen de inhoud  
30 ervan kunnen lezen zonder eerst hulp te krijgen van een of meerdere onafhankelijke, privacy beschermende organisaties, die we verder intermediairs zullen noemen. Het doel van de inschakeling van intermediairs is ongewenste tracering van voertuigen en/of verantwoordelijke betalers zoveel mogelijk te belemmeren.

De idee is dat de houder van elk voertuig en/of elke betaler, verder *verzender* te noemen, zelf tenminste één in-  
35 termediair kiest, die dan de gewenste dienst zal leveren. (We gaan hier verder niet in op de wijze waarop de intermediair betaald krijgt voor het leveren van deze diensten.) De verplichte, vanuit een voertuig te versturen berichten worden dan door de verzender m.b.v. cryptografische technieken vóór verzending zodanig vercijferd, dat ze alleen door de gekozen intermediair(s) ontcijferd kunnen worden. Bijna het enige wat intermediairs hoe-

<sup>30</sup> Later zal blijken dat het zuiverder is om jagers niet tevens (deels) als intermediair te laten fungeren. In het geval van zulke 'zuivere' jagers lijkt zo'n wettelijk verbod allerminst extreem. Zie verderop in dit hoofdstuk.



ven te doen is de voor hen bestemde berichten, die via jagers aan hen geleverd worden, te ontcijferen en deze daarna ontcijferd door te sturen naar de eindontvanger (b.v. de heffingsinner) of de volgende geadresseerde op weg naar de eindontvanger.

- 5 Een essentieel punt is dat er m.b.v. cryptografische technieken voor gezorgd kan worden, dat alleen de door de verzender uitgekozen intermediair in staat is het betreffende bericht te ontcijferen. Bovendien is het voor buitenstaanders, zelfs als ze de berichtenstroom naar en van een bepaalde intermediair afluisteren/onderscheppen, niet mogelijk om te bepalen welk ingaand bericht hoort bij welk uitgaand bericht van die intermediair.
- 10 In het volgende beperken we ons bij onze nadere uitleg tot het geval dat het hele bericht wordt geanonimiseerd. Het is natuurlijk ook mogelijk om de beschreven technieken alleen toe te passen op een deel van het oorspronkelijke bericht.

- 15 Meer in detail bestaat de dienst die intermediairs moeten leveren i.h.a. uit: 1) het ontcijferen van elk bericht dat ze ontvangen via een jager en evt. andere intermediairs, i.e. het verwijderen van de beveiliging tegen het lezen (door ieder ander dan de intermediair) van het betreffende bericht, 2) het doorsturen van het ontcijferde bericht naar de volgende geadresseerde (b.v. de eindontvanger) en 3) het geheim houden van de relatie tussen inkomende en uitgaande berichten. In latere secties zullen we uitleggen dat intermediairs zo nodig ook 4) een zekere administratie zullen bijhouden over de relatie tussen inkomende en uitgaande berichten om een eventuele reactie van de
- 20 eindontvanger op een door hem ontvangen bericht via de omgekeerde weg toe te kunnen sturen naar de jager via welke het bericht binnengekomen was. Later zullen we laten zien dat, als het bericht van een 'zuivere' jager komt, de (eerste) intermediair allereerst nog de plaats en het tijdstip moet verwijderen.

- 25 Het derde genoemde punt stelt dat deze administratie geheim moet worden gehouden. Eventueel kan in de wet duidelijk worden omschreven in welke specifieke gevallen en omstandigheden er op voorgeschreven wijze mag worden afgeweken van volstrekte geheimhouding. Ook kan wettelijk vastgelegd worden dat intermediairs van elk bericht deze relatie alleen gedurende een bepaalde beperkte tijd na ontvangst mogen of moeten administreren.

- 30 Door, zoals hierboven geschetst, intermediairs in het leven te roepen wordt er op een tamelijk eenvoudige wijze voor gezorgd dat de privacy (althans voor zover het bewegingspatronen betreft) niet geschonden wordt, zelfs niet als we er vanuit gaan dat de jagers de verzender van een bericht kunnen lokaliseren. Dit laatste zal i.h.a. het geval zijn als de ontvangers langs of boven de weg zijn opgesteld.

#### **Per bericht wisselende intermediair**

- 35 We wijzen er op dat men niet hoeft te kiezen voor één vaste intermediair om dan voor zijn privacy afhankelijk te zijn van de onkreukbaarheid van die ene organisatie. Want men kan ook meerdere, en evt. zelfs alle, intermediairs kiezen uit de beschikbare en dan bij elk uit te zenden bericht een random keuze maken uit de gemaakte voorselectie. De berichten lopen dan via steeds wisselende intermediairs. Met andere woorden, de stroom berichten
- 40 van zo'n random kiezende klant wordt 'in stukjes geknipt' en verspreid over diverse intermediairs, wat de privacybescherming zeker ten goede komt. Immers, zelfs als een bepaalde intermediair samenspannt met een jager om

illegaal het een en ander over het bewegingspatroon van een dergelijke klant te weten te komen, dan kunnen zij toch slechts een klein, willekeurig deel van zijn berichtenstroom bemachtigen.

#### **Berichten alleen leesbaar voor de eindontvanger**

5

Men kan er overigens voor zorgen dat elke intermediair en/of jager de inhoud van de berichten niet kan lezen en dus niet of nauwelijks informatie kan krijgen over bewegingspatronen. Immers, de berichten kunnen ook nog eens zodanig versluierd zijn dat ze na ontcijfering door de intermediair alleen gelezen kunnen worden door de volgende geadresseerde (b.v. de eindontvanger). De jagers en intermediairs ontvangen dan dus domweg berichten en bewerken die dan zonder verder iets van de inhoud van de berichten te kunnen begrijpen.

10

In dit geval worden berichten (of een deel daarvan, maar dat geval zouden we niet expliciet behandelen) dus (tenminste) dubbel gecijferd. Eenmaal om het bericht alleen leesbaar te maken voor de feitelijke, zeg tweede, geadresseerde en daarna nog eenmaal om het bericht zodanig te verpakken dat deze tweede geadresseerde het pas kan lezen met hulp van (i.e. na ontcijfering door) de intermediair, i.e. de eerste geadresseerde. Kortom, zolang een intermediair niet samenspannt met de tweede geadresseerde (zeg, de eindontvanger), kan die intermediair geen informatie destilleren uit de inhoud van de ontvangen en doorgestuurde berichten.

15

Op de beschreven wijze, waarbij altijd het hele bericht versluierd wordt voor ieder ander dan de eindontvanger (resp. de volgende geadresseerde), is er geen enkel gevaar te duchten van de intermediairs en/of de jagers.

20

#### **Meerdere intermediairs voor één bericht**

Natuurlijk kan de privacy van een random kiezende klant nu nog voor een klein deel worden geschonden als een intermediair samenspannt met zowel een jager als de eindontvanger, tenminste als deze laatste de tweede geadresseerde is. Maar door een reeks van geadresseerden te gebruiken en op een bericht de bijbehorende reeks van gecijferingen uit te voeren, kan men er ook nog eens voor zorgen dat een bericht via een aantal opeenvolgende intermediairs moet lopen. Bijvoorbeeld kan de privacy in geval van 3 intermediairs tussen de jager en de eindontvanger alleen geschonden worden als alle 5 genoemde organisaties samenspannen. Als men steeds bij elk bericht de te gebruiken intermediairs opnieuw en willekeurig kiest, betreft zo'n eventuele schending toch nog maar een klein, willekeurig deel van de door een bepaalde afzender uitgezonden stroom berichten.

25

30

Overigens zij opgemerkt dat gebruik van één intermediair voor een bericht al voldoende bescherming lijkt te bieden en dat er waarschijnlijk in de praktijk voorlopig weinig behoefte zal zijn om meer dan één intermediair voor een bericht te gebruiken.

35

#### **Retourzendingen, zoals verzoeken om een ingreep**

In sommige gevallen is het nodig om b.v. een video-opname te (laten) maken van het voertuig behorende bij een uitgezonden bericht. Als er iets mis is met het uitgezonden bericht, zeg een aangifte, maar het is wel correct ondertekend, dan kan de eindontvanger, zeg de heffingsinnehmer, de verantwoordelijke identificeren en gewoonlijk dus

40

ook achterhalen. Een tegenactie in de vorm van b.v. aanhouding of een video-opname lijkt dan dus niet noodzakelijk. Maar als er sprake is van een aangifte resp. een bericht zonder correcte handtekening, dan moet er een tegenactie, zoals b.v. een aanhouding of het maken van een video-opname, in gang worden gezet op de plaats waar het voertuig zich bevindt.

- 5 Dit is mogelijk zonder dat de eindontvanger de plaats van het voertuig te weten komt. Eén relatief simpele mogelijkheid schetsen we expliciet en gaat als volgt. Volgens wettelijk voorschrift kent elke jager bij ontvangst van een bericht er een uniek nummer aan toe en administreert/bewaart dan dat nummer voor een korte termijn samen met (een indicatie van) de plaats van ontvangst (resp. de plaats waar vandaan het bericht verzonden is). Het bericht zelf hoeft of mag door de jager niet bewaard gaan worden, maar moet wel met dit nummer eraan gehecht  
10 doorgestuurd worden naar de opgegeven intermediair.

- Elke intermediair haalt van elk binnenkomend bericht dat nummer af, zorgt voor het 'uitpakken' van het bericht en zendt het dan door naar de volgende geadresseerde met aangehecht een ander uniek nummer. Elke intermediair bewaart gedurende een bepaalde termijn de bij elkaar horende combinaties ingekomen en uitgaande bericht-  
15 nummers en van wie het inkomende bericht ontvangen werd.

- Als de eindontvanger b.v. een video-opname wil laten maken van het betreffende voertuig, dan zendt hij aan de intermediair van wie hij het gewraakte bericht ontving een getekend verzoek om zo'n tegenactie met vermelding van het door deze intermediair eerder aan het bericht gehechte berichtnummer. (Dat het verzoek getekend moet  
20 zijn heeft te maken met voorkoming van misbruik van deze mogelijkheid.) De intermediair zoekt in zijn administratie op welk inkomend nummer hoorde bij dit door hem ooit gekozen uitgaande nummer. Vervolgens stuurt hij het verzoek met het gevonden inkomende nummer door naar de daarbij horende en geregistreerde afzender.

- Uiteindelijk krijgt de juiste jager zo het verzoek. De jager zoekt de juiste, bijbehorende plek op in zijn administratie en zorgt voor de tegenactie, zeg de video-opname, op die plek. Jagers worden dus niet alleen betaald voor de jacht op vanaf of vanuit voertuigen verzonden berichten, maar ook voor het op geautoriseerd verzoek uitvoeren van tegenacties, i.e. (een deel van) de 'jacht' op mogelijke overtredders.  
25

### **'Openzetten' van lokaties t.b.v. controles**

- 30 Voor het uitvoeren van bepaalde controles, met name voor controles op het juist functioneren van kilometertellers, kan het gewenst zijn dat de controleur weet wat de afstand is tussen twee plaatsen die een voertuig achtereenvolgens passeert. Hiertoe kan men eventueel tijdelijk de geheimhouding van een aantal plaatsen opheffen. De controleur krijgt ook dan dus zeker geen onbeperkte toegang tot de informatie over de plaatsen van ontvangst,  
35 maar moet elke keer zulke toegang voor een aantal controlepunten vooraf aanvragen. Vanzelfsprekend wordt dan alleen toegang verleend voor een beperkte tijd en m.b.t. een beperkt aantal wisselende plaatsen.

### **Jager liever niet als 'halve' intermediair**

- 40 Bij de inrichting van het hele traject zoals hierboven beschreven, zorgen de jagers al voor (een deel van) de privacybescherming door deels ook te opereren als een intermediair. Het enige verschil van een jager t.o.v. een

'gewone' intermediair is eigenlijk dat de klant hem niet zelf kiest. Dus kunnen er, als er sprake is van meerdere jagers, ook geen geheime berichten naar de jagers worden toegestuurd, omdat de klant niet vooraf weet door welke jager het bericht zal worden opgevangen.

5 Bij een iets andere en eigenlijk ook zuiverdere en betere benadering fungeert een jager niet tevens als 'halve' intermediair. De jager voegt dan aan elk ontvangen bericht de plaats en de datum plus het tijdstip van ontvangst toe en ondertekent het aldus ontstane bericht. Het is dan niet meer noodzakelijk dat elke jager administratie bijhoudt om later aan te kunnen geven op welke plaats het bericht ontvangen was, respectievelijk op welke plek het voertuig zich bevond tijdens het uitzenden van het bericht. (Sterker nog, dit kan dan zelfs verboden worden.) De  
10 eerste intermediair in de keten bewaart het totale, door de jager ondertekende bericht, maar zendt alleen het oorspronkelijke, vanuit het voertuig verzonden bericht door naar de volgende in de keten. Het bewaarde bericht administreert dus de plaats van het voertuig ten tijde van het uitzenden, respectievelijk de plaats van ontvangst door de jager, en kan zo nodig later worden opgevoerd als bewijsstuk. Dit laatste is een voordeel t.o.v. de eerder geschetste variant.

15

Merk op dat een eindontvanger, zoals b.v. een overheidsinstantie, nu eventueel zelf kan optreden als 'berichtenjager' zonder dat de privacybescherming in het gedrang hoeft te komen. Voor een echt goede privacybescherming blijft het wel nodig om de overheid onbelemmerde toegang tot bepaalde zaken, zoals b.v. videocamera's langs de weg, te onthouden. Bepaalde tegenacties, zoals b.v. het maken van video-opnames, moeten dus bij voorkeur  
20 ondergebracht worden bij onafhankelijke 'verdachtenjagers'.

### Een omschrijving van jagers en van intermediairs

Het voert te ver om alle mogelijke variaties op de taken van en de taakverdeling tussen jagers en intermediairs te behandelen. De voorafgaande uitleg wordt geacht de achterliggende gedachte voldoende te hebben geïllustreerd.  
25 Nu deze gedachte duidelijk is gemaakt, doen we een poging tot het geven van een beknopte omschrijving van de begrippen jager en intermediair.

Een *jager* is een organisatie die althans een deel van de zend- en/of ontvangmiddelen in de buitenwereld (i.e. buiten voertuigen) t.b.v. de communicatie tussen voertuigen en (de rest van) het verkeersinformatiesysteem (resp. de instantie) beheert en een bijdrage levert aan het zoveel mogelijk geheim houden van de positie van een persoon of voertuig m.n. op het moment van ontvangst van een bericht vanuit dat voertuig.  
30

Primair doelen we hier op de 'zuivere' jager als beschreven in de vorige sectie. Een 'zuivere' jager voert geen administratie en zendt elk ontvangen bericht door naar een intermediair, echter uitsluitend na 1) aan het bericht de datum plus het tijdstip van ontvangst, de plaats van ontvangst en/of de plaats van de persoon of het voertuig op het moment van ontvangst te hebben toegevoegd en 2) het aldus ontstane bericht te hebben ondertekend. (Als men genoeg wil nemen met een zwakker systeem, dan kan men b.v. de laatste eis laten vervallen.) Een 'zuivere' jager kan dus alleen fungeren als er ook sprake is van tenminste één intermediair. Ook het uitvoeren van bepaalde  
40 tegenacties, i.e. de taak van 'verdachtenjager' (zie vorige sectie), kan gerekend worden tot de taken van een 'zuivere' jager.

Secundair gebruiken we de term jager tevens voor een jager die ook (alle of althans een deel van de) taken van een intermediair uitvoert. (M.a.w. voor een jager die tevens als 'hele' of 'halve' intermediair fungeert.)

- 5 Een *intermediair* is een organisatie die onafhankelijk is van de instantie en die t.b.v. de privacybescherming bij de communicatie vanuit voertuigen met de instantie fungeert als tussenpersoon. Een intermediair, althans de eerste intermediair in een eventuele keten van intermediairs, scheidt de handtekening van de jager en de door de jager toegevoegde gegevens (i.e., plaats en tijdstip) van het bericht en bewaart deze voor een bepaalde termijn op een privacy veilige wijze. De rest van het binnengekomen bericht wordt ontcijferd en doorgestuurd naar de volgende geadresseerde, i.e. de eindontvanger of de volgende intermediair in de keten. Als een intermediair niet als eerste intermediair in een keten een bepaald bericht ontvangt, dan hoeft alleen de in de vorige zin geschetste taak op dat bericht te worden uitgevoerd. Daarnaast zullen alle intermediairs op een of andere wijze zorg dragen voor de mogelijkheid van retourzendingen.

#### 15 **Toepassingen van de geschetste aanpak voor privacybescherming**

- Het voert te ver om alle mogelijke variaties uitputtend te behandelen. Op basis van de eerst beschreven aanpak en de zojuist beschreven variatie met jagers en/of intermediairs, worden de achterliggende gedachten geacht voldoende duidelijk te zijn geworden. Een ter zake kundige heeft hieraan genoeg om de beveiliging tegen onrechtmatige tracersing in een TIP-systeem (dus inclusief allerlei daaronder begrepen variaties) te kunnen toepassen.

- We hebben laten zien hoe de privacy beschermd kan worden, zelfs als vanuit elk voertuig continu berichten met een identificatie worden uitgezonden. De vermelde identificatie kan niet alleen worden gebruikt voor verkeersheffingen, maar, indien gewenst, ook voor andere toepassingen, zoals b.v. snelheidsmetingen op bepaalde plaatsen. In het volgende hoofdstuk gaan we eerst nog even wat nader in op (problemen bij) de identificatie van personen en objecten, alvorens in de twee daarop volgende hoofdstukken te laten zien dat het gebruik van jagers en/of intermediairs ook vermeden kan worden.

- In het hoofdstuk over semi-identificatie laten we zien dat voor een aantal toepassingen semi-identificatienummers i.p.v. identificatienummers gebruikt kunnen worden. De 'omweg' via jagers en/of intermediairs is dan niet meer nodig voor de privacybescherming. In het hoofdstuk over de aanpak m.b.v. agenten laten we zien dat het gebruik van identificaties nog verder kan worden teruggedrongen, en wel zover dat gebruik van jagers en/of intermediairs niet of nauwelijks meer nodig is. Het gebruik van agenten en semi-identificaties zal dus een zeer aantrekkelijke optie blijken te zijn.

## Identificatie

We hebben de term identificatie al vele keren een beetje slordig gebruikt, nl. ter aanduiding van een identificerend gegeven of een identificerende combinatie van gegevens. We zullen dat ongetwijfeld nog vaker doen, hoewel de term identificatie strikt genomen (het proces van) het vaststellen van de identiteit van een persoon of zaak betreft. In dit hoofdstuk gaan we juist op dit laatste wat nader in.

### Problemen met identificatie van voertuigen

Momenteel wordt in Nederland bij het opnemen van een voertuig in de centrale kentekenregistratie een kentekenbewijs, bestaande uit een aantal documenten, afgegeven. Deze officiële papieren staan bloot aan allerlei vormen van fraude. Bovendien wordt er niet alleen met deze papieren geknoeid, maar juist ook met de bijbehorende voertuigen. Het rijden met valse kentekenplaten (wat schrikbarend makkelijk te doen is en al jaren een te lage pakkans lijkt op te leveren), maar ook het (moeilijker) knoeien met identificatienummers op chassis en motor (zoals wijzigen, verwijderen en/of opnieuw aanbrengen) schijnt volgens kranteberichten maar al te vaak plaats te vinden. Er is daarom behoefte aan een fraudebestendiger manier om kentekens, chassisnummers e.d. aan voertuigen te koppelen.

Eén mogelijke gedachte is om het voertuig te voorzien van een component die het chassisnummer (of het kenteken) bevat en die dit nummer beschikbaar kan stellen aan de buitenwereld. Echter, het beschikbaar stellen van een vast bitpatroon kan leiden tot ongewenste problemen. Immers, het nadeel is dat het betreffende bitpatroon onderschept kan worden. (En dat is des te meer een reële mogelijkheid als het bitpatroon via een zender wordt verstuurd.) Dus is het mogelijk om vervalste componenten te maken die precies hetzelfde doen als het origineel. Anders gezegd, het probleem is dat de authenticiteit van het bitpatroon en van de afzender niet (op afstand) door de ontvanger van het bitpatroon kan worden vastgesteld. Kortom, bij gebruik van zulke componenten lijkt fraude i.h.a. eenvoudig te zijn.

### Géén uitwisseling van vaste gegevens ter identificatie

Dit bezwaar tegen gebruik van (passieve) componenten die een vast bitpatroon ter beschikking stellen, is enigszins vergelijkbaar met het bezwaar tegen het gebruik van wachtwoorden (passwords) of pincodes ter beveiliging van het gebruik van identificatiehulpmiddelen, zoals pinpassen, die toegepast worden bij vele systemen, zoals b.v. betaalsystemen en gelduitgifte-automaten. Het bezwaar is in beide gevallen dat in het normale gebruik een vast gegeven uitgewisseld moet worden en dat dit vaste gegeven juist tijdens die uitwisseling extra het gevaar loopt van onderschepping. Denk b.v. aan onderschepping door ongemerkt meekijken op het betreffende toetsenbord (b.v. via spiegels en/of verborgen videocamera of via gebruik van een onopvallende substantie op de toetsen) of aan het afluisteren van de (tele-)communicatie bij het verzenden van de pincode of het password. Na onderschepping kan een kopie van het vaste gegeven gebruikt worden als echt, omdat er bij bitpatronen geen verschil is tussen origineel en kopie.

40

## Het probleem van fraudebestendige identificatie in het algemeen

In het algemeen geldt dan ook dat voor goede beveiliging tegen fraude (directe) uitwisseling van cruciale informatie zoveel mogelijk moet worden voorkomen. Het is daarom beter om (indirect) te bewijzen dat men over  
 5 bepaalde cruciale informatie beschikt, zonder die informatie zelf prijs te geven<sup>31</sup>. Deze aanpak staat bekend als het gebruiken van *challenges*, i.e. uitdagingen waarbij men moet laten zien dat men tot iets unieks in staat is.

Een goed voorbeeld van deze aanpak is unieke identificatie d.m.v. het zetten van een digitale handtekening. Men laat daarbij zien in staat te zijn een handtekening te zetten op een bepaald bericht zonder het bitpatroon dat (i.e.  
 10 de sleutel die) ten grondslag ligt aan die handtekening, prijs te geven<sup>32</sup>.

De boodschap waarop de gevraagde handtekening wordt gezet, moet natuurlijk slechts eenmalig gebruikt kunnen worden (kopietjes mogen immers geen waarde hebben) en moet dus elke keer weer een andere zijn. Bovendien moet het een beslist onschuldige boodschap zijn, d.w.z. het ondertekenen ervan mag geen ongewenste implicaties  
 15 kunnen hebben. Het mag b.v. beslist niet zo zijn dat men door ondertekening de andere partij direct of indirect in staat stelt om een valse ondertekening te verkrijgen van een bericht (b.v. een contract) met ongewenste gevolgen.

Zonder in te willen gaan op alle verdere haken en ogen doen we één suggestie voor zulke 'onschuldige alleen-ter-identificatie berichten' en een bijbehorend identificatie protocol. Om tegemoet te komen aan de eis van uniciteit  
 20 en veranderlijkheid eisen we dat elk zo'n bericht het betreffende tijdstip bevat in een bepaald en vast voorgescreven formaat. Om te voorkomen dat iemand een kopie van andermans identificatie elders (vrijwel) tegeliktijd kan gebruiken om zich valselijk voor te doen als die ander, moet elk zo'n bericht ook nog toegespitst worden op het ene onderhavige identificatieproces. Dit kan b.v. door af te spreken dat de identificatievrager altijd  
 25 eerst een ondertekend identificatieverzoek<sup>33</sup> met daarin het tijdstip van dit verzoek moet doen toekomen aan de te identificeren persoon of het te identificeren object en dat de geïdentificeerde (als hij of zij überhaupt aan dat verzoek tegemoet wil komen) daarna dat identificatieverzoek ondertekent, bij voorkeur na er zelf het tijdstip van ondertekening aan te hebben toegevoegd.

Overigens merken we nog op dat het in bepaalde gevallen mogelijk is om identificatiemiddelen te gebruiken met  
 30 een (deels) gemeenschappelijke handtekening. Als een bepaalde organisatie de zorg voor de verstrekking en de juiste werking van de identificatiemiddelen toevertrouwd wordt, is het b.v. mogelijk om meerdere, en evt. zelfs alle, identificatiemiddelen gebruik te laten maken van dezelfde 'basis'-handtekening. De 'basis'-handtekening

<sup>31</sup> Een alternatief is ervoor te zorgen dat cruciale informatie na de eerste de beste uitwisseling al niet meer cruciaal is, i.e. om elke keer een ander bitpatroon te gebruiken. Er kan dus evt. toch gebruik worden gemaakt van een passief geheugenmiddel, zoals b.v. een magneetkaart. Echter, vanwege het eenvoudige lezen, veranderen en schrijven van het bitpatroon op b.v. een magneetkaart zitten aan dit alternatief nog wel allerlei haken en ogen. Hoe dan ook, we gaan hier niet verder in op dit alternatief en zijn beperkingen.

<sup>32</sup> Ter zake kundigen zal duidelijk zijn dat hier m.n. gedacht wordt aan het gebruik van asymmetrische cryptografie, oftewel public key cryptografie. De genoemde sleutel die niet prijsgegeven wordt, betreft dan de private key.

<sup>33</sup> Hiermee wordt gelijk het probleem van nabootsingen, zoals b.v. valse gelduitgifte-automaten, opgelost.

dient dan om te bewijzen dat het betreffende identificatiemiddel ècht is, i.e. uitgegeven is door de daartoe geautoriseerde organisatie.

Die organisatie zal er dan wel voor moeten zorgen dat elk identificatiemiddel ook nog beschikt over een uniek  
 5 identificatienummer en dat dat nummer altijd deel zal uitmaken van iedere ondertekening van enig identificatie-  
 verzoek m.b.v. de 'basis'-handtekening, b.v. door het unieke nummer voor de ondertekening toe te voegen aan het  
 te tekenen identificatieverzoek. Dit unieke identificatienummer moet dus altijd samen met de 'basis'-handtekening  
 gebruikt worden voor het vormen van de complete identificerende handtekening. Het moet dan ook net zo goed  
 10 beveiligd worden tegen diefstal als de sleutel van de 'basis'-handtekening. Anders gezegd, de unieke sleutel die  
 ten grondslag ligt aan de complete handtekening, bestaat in dit geval uit het unieke identificatienummer en de  
 gemeenschappelijke sleutel gebruikt voor de 'basis'-handtekening.

Al met al hopen we met bovenstaande voldoende duidelijk te hebben gemaakt dat voor een goede identificatie bij  
 voorkeur een middel nodig is dat in staat is de vereiste processing uit te voeren, zeg, een apparaatje dat digitale  
 15 handtekeningen kan zetten. Als elk zo'n apparaatje voldoende fysiek beveiligd is tegen diefstal van zijn sleutel,  
 i.e. van de sleutel die ten grondslag ligt aan de ermee te zetten digitale handtekeningen, dan is dat apparaatje  
 voldoende beveiligd tegen impersonatie door een valse kopie.

Als we in staat zijn om apparaatjes te maken die zich uniek en fraudebestendig kunnen identificeren, hebben we  
 20 strikt genomen nog geen oplossing gevonden voor de identificatie van willekeurige objecten (hieronder mede  
 begrepen personen). Want om zulke apparaatjes te kunnen gebruiken voor fraudebestendige identificatie van  
 objecten (incl. personen), moeten ze ook nog op adequate wijze gekoppeld kunnen worden aan de betreffende  
 objecten. In de volgende twee secties gaan we iets dieper in op het koppelen van identificatiemiddelen aan perso-  
 nen respectievelijk voertuigen.

25

### **Persoonsidentificatie**

Als we aan elke persoon één uniek en fraudebestendig identificatiemiddel uitreiken, bereiken we daarmee (nog)  
 niet dat elke eigenaar van zo'n middel zich fraudebestendig kan identificeren. Immers, het identificatiemiddel kan  
 30 b.v. verloren of gestolen worden. Er moet dus o.a. voor gezorgd worden dat het identificatiemiddel niet gebruikt  
 kan worden zonder toestemming van de rechtmatige eigenaar. Dit laatste is voldoende voor b.v. betalingsverkeer,  
 maar niet voor persoonsidentificatie. Voor betrouwbare persoonsidentificatie moet het middel fraudebestendig  
 gekoppeld worden aan één juiste persoon, d.w.z. moet zelfs voorkomen worden dat het identificatiemiddel met  
 hulp van de eigenaar gebruikt kan gaan worden voor resp. door een ander.

35

Voor zowel betalingsverkeer als persoonsidentificatie hebben we een oplossing gevonden die veel betere beveili-  
 ging tegen fraude biedt dan de ons bekende, bestaande oplossingen. Onze oplossing is m.n. geschikt voor beta-  
 lingsverkeer, omdat deze niet alleen een uitstekende beveiliging biedt tegen de eerder genoemde risico's (zoals  
 b.v. het uitlekken van de pincode door meekijken of afluisteren, dan wel door fouten of fraude binnen de pincode  
 40 verstreckende organisatie), maar ook heel simpel in het gebruik is. Er wordt dus voldaan aan de belangrijke eis



van praktisch bruikbaarheid voor een breed publiek. We hebben echter besloten de bedoelde oplossing bij nader inzien niet prijs te geven in de huidige context, i.e. in deze aanvraag voor octrooi op het TIP-systeem.

### Voertuigidentificatie

5

Twee secties terug hebben we beschreven hoe een identificatiemiddel zich uniek kan identificeren. Door aan elk voertuig zo'n identificatiemiddel te bevestigen wordt al een beduidend fraudebestendiger manier van identificatie verkregen dan bij de huidige aanpak.

10

Immers, er wordt nu voorkomen dat de identificatiefunctie kan worden overgenomen door een falsificatie. En het alleen buitenwerking stellen van het authentieke identificatiemiddel heeft geen zin. Want de afwezigheid van een goed werkend identificatiemiddel kan (m.n. tijdens gebruik van het voertuig) voldoende makkelijk ontdekt worden.

15

Dus, hoewel het beveiligen van het identificatiemiddel tegen daadwerkelijke vernieling of verwijdering op zich nog steeds even moeilijk is, kan er, door sancties te zetten op het ontbreken van een correct functionerend identificatiemiddel, toch voldoende voor gezorgd worden dat het slechts buiten werking stellen van het originele identificatiemiddel door vernieling of verwijdering allerminst lonend is.

20

De enige overblijvende mogelijkheid tot fraude waartegen nog beveiligd moet worden, lijkt derhalve het onderling verwisselen van authentieke identificatiemiddelen van een aantal voertuigen te zijn. Hoewel het voordeel dat met verwisseling te behalen valt in veel gevallen (al) beperkt(er) zal zijn, moet men zich daar in bepaalde gevallen wel degelijk tegen wapenen. Dit laatste is het geval als de identificatie en/of de typering van het voertuig zeer fraudebestendig, i.e. ook tegen verwisselingen bestand, moeten zijn, b.v. omdat bij een verkeersheffing verschillende tarieven gehanteerd worden voor verschillende types voertuigen.

25

Eén mogelijkheid daartoe is het zodanig bevestigen van elk identificatiemiddel aan het bijbehorende voertuig dat dit (vrijwel) onmogelijk verwijderd kan worden zonder fatale beschadiging, i.e. zonder het correct functioneren van het identificatiemiddel teniet te doen.

30

Als voertuigen voorzien zijn van fraudebestendige identificatiemiddelen, biedt dat een aantal voordelen. Eén voordeel is dat verkeersovertredingen dan efficiënter en nauwkeuriger kunnen worden afgehandeld. Door de volautomatische identificatie hoeven geen kentekens meer afgelezen te worden van kentekenplaten op van de overtredingen gemaakte foto's, zoals momenteel gebruikelijk is. Bovendien verdwijnen bepaalde problemen t.g.v. het gebruik van valse (of, misschien beter gezegd, misleidende) kentekenplaten. Voor deze voordelen is het vaak nog niet eens noodzakelijk dat het identificatiemiddel fraudebestendig aan de voertuigen gekoppeld is, omdat op andere wijze voorkomen wordt dat verwisseling profijt oplevert. (Voor meer details m.b.t. dit laatste verwijzen we naar het voorbeeld in het hoofdstuk over voorbereiding op 'groei' van het systeem.)

35

## Semi-identificatie en toepassingen ervan

Alvorens verder te gaan met de behandeling van een belangrijke variant, nl. de aanpak met agenten, introduceren we eerst nog het begrip semi-identificatie en laten we zien waarvoor semi-identificatie(nummer)s zoal gebruikt  
 5 kunnen worden. Eén toepassing betreft anonieme controle op de precisie van tellers. Een andere toepassing is b.v. het op privacy vriendelijke wijze automatisch vaststellen van de vertragingen t.g.v. files.

### De kilometerstand als semi-identificerend gegeven

10 Voor controles op het juist bijhouden van de tellerstanden is het van essentieel belang dat twee berichten die ontvangen worden van een bepaald voertuig dat twee opeenvolgende ontvangers passeert, met hoge kans herkend kunnen worden als bij elkaar horend. Hiertoe kan men aan elk uitgezonden bericht een identificatienummer (van het voertuig of van de voertuigapparatuur o.i.d.) toevoegen. Het aardige is dat voor de controle op bepaalde tel-  
 15 lers, zoals b.v. kilometertellers, toevoeging van een unieke identificatie niet strikt noodzakelijk is. Want de kilometerstand van een voertuig kan zelf al een, wat wij zullen noemen, semi-identificerend gegeven zijn met voldoende uniciteit. (Eigenlijk zelfs met teveel uniciteit, maar daar komen we later op terug.)

Op het onderwerp semi-identificatie gaan we straks nader in. Maar om een en ander beter te kunnen begrijpen, leggen we eerst uit dat we bij elkaar horende kilometerstanden bijna altijd terug kunnen vinden. Immers, omdat  
 20 de kilometerstanden van een niet al te groot aantal voertuigen i.h.a. voldoende van elkaar zullen verschillen, zullen twee berichten zeer waarschijnlijk bij elkaar horen, i.e. van dezelfde voertuigapparatuur afkomstig zijn, als het verschil tussen de twee erin vermelde kilometerstanden niet of weinig afwijkt van de lengte van het controle-  
 25 traject. (N.B. De grootte van toegestane afwijkingen wordt niet alleen bepaald door de vereiste nauwkeurigheid van de afstandsmeter in het voertuig, maar b.v. ook door rekening te houden met het effect van een slingerende koers van het voertuig, b.v. als gevolg van het meermalen wisselen van rijstrook. Kortom, de nauwkeurigheid van de controle speelt een belangrijke rol bij de grootte van toegestane afwijkingen.)

Als er toevallig eens meerdere mogelijkheden zijn om berichten te koppelen, zoals b.v. in geval van twee auto's die kort na elkaar dezelfde controleval betreden hebben met (vrijwel) dezelfde kilometerstand, dan is er de keus  
 30 om ofwel 1) een actie op gang te brengen tegen de betreffende voertuigen om ze nader te laten inspecteren, ofwel 2) de betreffende voertuigen gewoon buiten de controle te laten vallen. Omdat de kans dat zoiets gebeurt, voldoende klein is, zullen zulke ontsnappingen aan één specifieke controle i.h.a. geen probleem opleveren.

Maar in het geval dat zulke voertuigen buiten de controle gehouden worden, moet men dan wel op een of andere  
 35 wijze voorkomen dat hier stelselmatig misbruik van gemaakt kan worden. Iemand zou b.v. kunnen proberen gedurende een bepaalde tijdsduur aan controles te ontsnappen door gedurende die tijd zijn voertuig zich continu te laten voordoen als twee voertuigen met dezelfde kilometerstand. Zo'n situatie is te detecteren en er kunnen dus tegenmaatregelen genomen worden. Hier gaat het ons er alleen maar om aan te geven dat men goed moet uitkij-  
 40 ken voor allerlei pogingen tot fraude.

Hoe dan ook, het achterliggende principe van het *koppelen*, i.e. het uitvinden welke kilometerstanden bij elkaar horen, wordt nu geacht een ter zake kundige lezer voldoende duidelijk te zijn geworden om concrete voorbeelden zelf (verder) uit te kunnen werken en om de (gedachte achter) onderstaande beknopte formulering van het door ons geïntroduceerde begrip semi-identificatie(nummer) voldoende te kunnen begrijpen. De zojuist beschreven wijze van koppelen noemen we wel de *koppelingstruc*.

### Semi-identificatie

Met de door ons geïntroduceerde term *semi-identificatie* (in de betekenis van semi-identificerend gegeven<sup>34</sup>) bedoelen we een gegeven<sup>35</sup> dat niet uniek en/of voorspelbaar genoeg is om het bijbehorende object (resp. persoon) door de tijd heen uniek te kunnen representeren in de verzameling van alle relevante objecten (resp. personen), maar wel voldoende uniek en voorspelbaar om het bijbehorende object (resp. persoon) met voldoende hoge kans uniek te kunnen representeren in een relatief kort tijdsbestek of in een relatief kleine deelverzameling van alle relevante objecten.

In ons voorbeeld waren de kilometerstanden uniek genoeg om vrijwel alle voertuigen die het begin resp. het einde van een controletraject passeren in een bepaalde beperkte periode, met hoge kans van elkaar te kunnen onderscheiden en ook nog voorspelbaar genoeg (althans op het betreffende controletraject) om bijna alle bij elkaar horende tweetallen te kunnen terugvinden. De grootte van de bedoelde periode wordt in dit voorbeeld grofweg begrensd door de maximale tijdsduur die één van de bedoelde voertuigen nodig heeft om het controletraject af te leggen.

Kilometerstanden zijn echter nog niet goed genoeg voor praktisch gebruik als privacy beschermend semi-identificatienummer, omdat voor kilometerstanden o.a. grofweg geldt: hoe hoger de stand, des te meer selectief hij is, i.e. des te meer hij unieke identificatie benadert. Daarnaast speelt ook het totale aantal deelnemende voertuigen een rol bij de mate van uniciteit, evenals de door de kilometerteller aangegeven kleinste afstandseenheid. Dit alles bij elkaar maakt dat kilometerstanden, en met name hoge, vaak een voor ons doel te hoge uniciteit zullen hebben of zelfs identificerend zullen zijn i.p.v. semi-identificerend.

Let wel, dit is allerminst een probleem voor de zojuist geschetste controles op zich, maar moet wel als een probleem worden gezien als we rekening houden met de wens tot privacybescherming. Ter vergoelijking moet overigens wel worden opgemerkt dat kilometerstanden, omdat ze steeds veranderen en de veranderingen tussen twee waarnemingen niet (altijd) volledig voorspelbaar zijn, altijd nog veel veiliger zijn voor de privacy dan kentekens of andere voertuigidentificatienummers. Hoe dan ook, we zullen uitleggen hoe we betere semi-identificatienummers kunnen verkrijgen.

<sup>34</sup> Het woord semi-identificatie hoort misschien alleen gebruikt te worden voor het semi-identificatieproces. Door ons wordt het dus, net als het woord identificatie, enigszins slordig gebruikt. (Zie onze eerdere opmerking daarover aan het begin van het hoofdstuk over identificatie.)

<sup>35</sup> Of een combinatie van gegevens.

### Kunstmatige semi-identificatienummers

Men kan ook een kunstmatig gegeven creëren dat geschikt is voor gebruik als semi-identificatie(nummer). En wel m.n. door voor elk voertuig eenmalig een willekeurige keuze te maken uit een verzameling met een geschikt  
 5 aantal verschillende elementen en dan dat gekozen element te gebruiken als vaste semi-identificatie voor dat voertuig. Dus bijvoorbeeld kan men voor elk voertuig eenmalig een willekeurig getal uit een beperkt bereik kiezen en dan dat getal gebruiken als vast semi-identificatienummer.

Stel dat voor elk voertuig een random getal van 4 cijfers wordt gekozen. Dan zal, bij een totaal aantal van b.v. 5  
 10 miljoen voertuigen, elk semi-identificatienummer gemiddeld door 500 voertuigen gebruikt worden. (N.B. Dit is overigens, vanuit het oogpunt van privacybescherming, nog wat weinig.) Echter, binnen een willekeurige deelverzameling van, zeg, 1000 voertuigen zal het overgrote deel<sup>36</sup> van de voertuigen wel degelijk uniek geïdentificeerd worden door hun semi-identificatienummer. Dus zolang zich bij dit voorbeeld op ieder moment minder  
 15 dan, pakweg, 1000 voertuigen binnen een controleval bevinden, kan zo'n kunstmatig ontwikkeld gegeven prima gebruikt worden om bij elkaar horende kilometerstanden te 'identificeren'.

Ondanks deze lokale 'identificatie' wordt de privacy dan toch in een zekere mate beschermd, omdat het betreffende voertuig niet volledig gevolgd kan worden in het verkeer. Immers, zelfs bij een tamelijk dicht netwerk van  
 20 ontvangers langs de wegen, blijft volledig traceren vrijwel onmogelijk, o.a. vanwege de kans op 'ontmoetingen' met andere voertuigen met hetzelfde semi-identificatienummer. Merk overigens op dat iets soortgelijks geldt als men voor de semi-identificatie gebruik zou maken van een deel van het kenteken, zoals b.v. de laatste 3 of 4 cijfers en/of letters.

De mate van privacybescherming hangt bij dit soort semi-identificatienummers o.a. af van: 1) de grootte van de  
 25 verzameling waaruit de semi-identificaties lukraak gekozen worden, 2) het totaal aantal voertuigen in het betreffende gebied, 3) de grootte van het betreffende gebied, en 4) de intensiteit waarmee de betreffende voertuigen gebruikt worden. Kortom, het is niet altijd even makkelijk een geschikt (i.e. niet te groot en niet te klein) getalbereik te kiezen.

### 30 Semi-identificatienummers op basis van een tellerstand

De zojuist uitgelegde aanpak kan eenvoudig gecombineerd worden met het gebruik van tellerstanden met voldoende voorspelbaarheid, zoals b.v. kilometerstanden, wat leidt tot een aanzienlijke verbetering t.o.v. apart gebruik van één van de beide methoden. Hiertoe kan men simpelweg een deel van de cijfers, zeg 4 stuks, kiezen uit  
 35 de tellerstand. Bijvoorbeeld kan men, als de kilometerteller tot op tenminste één decimaal nauwkeurig is, kiezen voor de laatste 3 cijfers voor de komma en het eerste cijfer achter de komma van de kilometerstand.

---

<sup>36</sup> Voor een precieze berekening verwijzen we naar het in de wiskunde bekende 'birthday problem' dat hier nauw aan verwant is.

Voor het selecteren van een deelbereik hoeft niet per sé een aantal cijfers uit de tellerstand gekozen te worden, maar kan men ook gebruik maken van allerlei berekeningen, zoals b.v. berekeningen m.b.v. de modulo-operator en/of de delingsoperator met afronding naar beneden. In de rest van dit verhaal worden semi-identificatienummers meestal geacht van het op een (controleerbare of voldoende voorspelbare) tellerstand gebaseerde type te zijn.

### Controle op tellers m.b.v. semi-identificatie

Zoals aan het begin van dit hoofdstuk al werd aangegeven, kan het zojuist genoemde type semi-identificatienummers gebruikt worden voor controles op het juist bijhouden van tellerstanden. Niet alleen voor controles op de teller gebruikt voor het semi-identificatienummer, maar natuurlijk ook voor die van andere tellers. Het zal sommigen misschien verbazen dat tellerstanden gebruikt kunnen worden voor de controle op tellerstanden, maar het is wel degelijk zo. Hoewel nu eigenlijk al duidelijk moet zijn hoe dit in zijn werk gaat, geven we voor alle duidelijkheid toch nog maar een expliciete uitleg.

Voor de controle op de precisie van een willekeurige teller moeten vanuit het voertuig steeds het semi-identificatienummer en de laatste zoveel cijfers (i.e. een i.h.a. klein aantal van de minst significante cijfers) van de te controleren tellerstand worden uitgezonden. (Als dit laatste getal ook als semi-identificatie wordt gebruikt, hoeft dus alleen het semi-identificatienummer uitgezonden te worden om de teller die ten grondslag ligt aan dat semi-identificatienummer, te kunnen controleren op precisie.) Controles kunnen dan worden uitgevoerd door op twee opeenvolgend te passeren punten de bijpassende, uitgezonden berichten op te vangen. M.b.v. de koppelingstruc kan men dan van elk voertuig bepalen hoeveel zijn tellerstand is verhoogd (of verlaagd) op het controletraject. Er vanuit gaande dat men extern (i.e. in de buitenwereld) bepaalt of bepaald heeft hoeveel de te controleren teller zou moeten veranderen, kan men de vanuit het voertuig bekend geworden verandering van de tellerstand vergelijken met de correcte, vereiste verandering.

Als b.v. de semi-identificatienummers bestaan uit de laatste 4 cijfers van kilometertellers met één decimaal, i.e. met hectometeraanduiding, dan hoeven alleen deze semi-identificatienummers uitgezonden te worden en kan de precisie van de kilometertellers worden gecontroleerd door de betreffende semi-identificatienummers op te vangen op twee op bekende afstand van elkaar verwijderde punten langs de weg.

Kortom, voor de controle op de precisie van kilometertellers en andere tellers zijn echte identificaties dus niet noodzakelijk en kunnen semi-identificatie(nummer)s gebruikt worden om de privacybescherming gemakkelijker te maken. Merk echter op dat bij de tot nu toe beschreven aanpak (met uitsluitend controles op afstand) dan even goed nog echte identificaties gebruikt moeten worden, omdat die niet gemist kunnen worden bij de controles op teller-monotonie.

### Volautomatische bepaling van filevertragingen

De koppelingstruc waarbij een deel van een voldoende voorspelbare teller(stand) wordt gebruikt voor semi-identificatie, kan ook voor andere doeleinden gebruikt worden. Op grond van bovenstaande zal duidelijk zijn dat

voor voertuigen die beide ontvangers passeren, m.b.v. semi-identificatie i.h.a. nauwkeurig kan worden bepaald hoe lang ze gedaan hebben over het traject tussen de twee ontvangers.

Als men op basis van een voldoende aantal van zulke voertuigen het gemiddelde van de over het traject gerealiseerde reistijden berekent (en daarbij al te ver afwijkende waarden eventueel buiten beschouwing laat), kan men van deze gemiddelde reistijd de gemiddelde tijd aftrekken die normaliter nodig is voor het traject als er geen files zijn, en zodoende de feitelijke filevertraging tot op de minuut nauwkeurig bepalen. Kortom, de uitgezonden semi-identificatienummers kunnen gebruikt worden om continu en volautomatisch de filevertraging op een privacy vriendelijke manier te meten.

Overigens zij aanvullend nog opgemerkt dat filevertragingen uitgedrukt in tijd (zeg, minuten) vaak veel betere informatie geven dan filelengtes uitgedrukt in afstand (zeg, kilometers). Immers, een file van 1 km met een gemiddelde rijsnelheid van 5 km/u levert meer vertraging op dan een file van 5 km met een gemiddelde snelheid van 30 km/u.

### **Trajecetsnelheidscontroles**

Natuurlijk kan de koppelingstruc voor nog meer toepassingen worden gebruikt, zoals b.v. voor het op zeer eenvoudige en privacy vriendelijke wijze uitvoeren van trajecetsnelheidscontroles. Bij een trajecetsnelheidscontrole wordt van elk voertuig dat een bepaald traject met bekende lengte aflegt, (of van een persoon in dat voertuig) vastgesteld hoeveel tijd verstrijkt tussen het passeren van het begin- en het eind van dat traject. Zodoende kan vastgesteld worden met welke gemiddelde snelheid dat traject is afgelegd door elk individueel voertuig.

### **Eventueel geïntegreerde verkeersboetes**

Nu we het toch over snelheidscontroles hebben, stippen we hier ook maar meteen even de mogelijkheid aan om i.p.v. het opleggen van aparte boetes de 'prijs' van snelheidsoverschrijdingen eventueel op te nemen in de tarief-functie van rekeningrijden, zodat automatisch een extra hoog bedrag in rekening wordt gebracht voor elke afstandseenheid die sneller is afgelegd dan ter plaatse is toegestaan. Zulke geïntegreerde, i.e. in het tarief verwerkte, verkeersboetes kunnen natuurlijk niet alleen toegepast worden voor snelheidsoverschrijdingen, maar ook voor andere overtredingen, zoals b.v. het produceren van teveel lawaai.

Denk bij dit laatste voorbeeld m.n. ook aan toepassing in de context van vliegverkeer. Men kan (al dan niet geïntegreerde) boetes eventueel gebruiken voor het beperken van de geluidshinder door vliegtuigen. Het ligt voor de hand dat de hinder op de grond als uitgangspunt genomen wordt en dat een vliegtuig dus meer geluid zal mogen produceren op grotere dan op lagere hoogte. Ongetwijfeld zal de functie voor het bepalen van de toegestane geluidsproductie dan niet alleen afhankelijk gemaakt worden van de hoogte, maar b.v. ook van de afstand tot en

liefst zelfs de positie t.o.v. een luchthaven<sup>37</sup>, zodat rekening kan worden gehouden met starts, landingen en voorgeschreven aan- en uitvliegroutes.

Voor alle duidelijkheid benadrukken we dat het opleggen van al dan niet geïntegreerde<sup>38</sup> verkeersboetes een mogelijke toepassing van het TIP-systeem is die los staat van het al dan niet gebruiken van semi-identificaties. De lezer moet zich dus niet laten misleiden door het feit dat geïntegreerde boetes in dit hoofdstuk even tussendoor aan de orde zijn gesteld. (Overigens, dit soort zijsprongen maken we in deze tekst wel vaker. Meestal zelfs zonder er expliciet bij te vermelden dat er sprake is van een zijsprong.)

## 10 Het nut van semi-identificatie

We hebben in het hoofdstuk over privacybescherming al laten zien dat de privacy met enige moeite (nl. door jagers en/of intermediairs te gebruiken) beschermd kan worden, zelfs als er gebruik wordt gemaakt van echte identificatie(s). Echter, het is simpeler en dus ook goedkoper om, waar mogelijk, semi-identificatie(s) toe te passen. De privacy is dan voldoende gewaarborgd, terwijl de beheerder van de infrastructuur (zeg, de overheid) dan toch direct toegang kan krijgen tot bepaalde benodigde of gewenste informatie. Want alle voor verkeersbeheer in de inleiding gegeven voorbeelden kunnen privacy veilig uitgevoerd worden m.b.v. semi-identificaties.

We nemen als voorbeeld een geïntegreerd verkeersinformatiesysteem t.b.v. verkeersheffingen en verkeersbeheer, waarbij de voertuigen berichten ontvangen (over maximum snelheden, files, e.d.) en zelf berichten uitzenden. Zeg, zelf berichten uitzenden met semi-identificaties t.b.v. snelheidscontroles en verkeersbeheer, en berichten met identificaties t.b.v. de verkeersheffing. In dit voorbeeld kan de verkeersbeheerder (zeg, de overheid) dan uit de direct toegankelijke semi-identificaties de nodige informatie afleiden, terwijl alleen voor de berichten met identificaties een omweg nodig is (althans bij de tot nu toe beschreven aanpak met jagers en/of intermediairs) op weg naar de bedoelde ontvanger (i.e. de overheid).

We zullen in het volgende hoofdstuk laten zien dat m.b.v. agenten de bedreiging van de privacy ten gevolge van het gebruik van identificaties nog verder kan worden teruggedrongen, en wel zover dat gebruik van jagers en/of intermediairs niet of nauwelijks meer nodig is. Er zal blijken dat het een zeer aantrekkelijke optie is om agenten en semi-identificaties te gebruiken.

<sup>37</sup> Merk op dat de geografische positie van een verkeersvliegtuig gewoonlijk niet als privacy gevoelig wordt bestempeld.

<sup>38</sup> Waarschijnlijk is het meestal verstandiger boetes niet te integreren in het tarief, maar apart bij te houden.

## Een aanpak m.b.v. agenten

Het is ondoenlijk om alle mogelijke variaties van het TIP-systeem expliciet te beschrijven. Om toch duidelijk te maken wat voor mogelijkheden er zoal zijn bij de implementatie van een TIP-systeem, geven we in dit hoofdstuk een voorbeeld waarbij twee wel eerder genoemde, maar niet in detail uitgelegde aspecten aan bod komen. De twee aspecten betreffen het alleen uitzenden op verzoek en het gebruik maken van een fraudebestendige component. Aan de hand van dit voorbeeld zullen deze beide aspecten ongetwijfeld wat duidelijker uit de verf komen.

### Alleen zenden op verzoek

Als niet continu berichten worden uitgezonden met de vereiste gegevens, wordt de controle aanmerkelijk bemoeilijkt. Want kennis van de momenten waarop gegevens worden verstrekt aan de controleur schept een ruimere mogelijkheid tot fraude. Dit kan het beste met een concreet voorbeeld geïllustreerd worden.

Stel dat op een zeker moment op plaats X de kilometerstand van een bepaald voertuig is verstrekt. Als het eerstvolgende verzoek (of, beter gezegd, de eerstvolgende opdracht) dat voertuig bereikt op plaats Y, dan moet de kilometerstand tenminste opgehoogd zijn met de lengte van de kortst mogelijke route van X naar Y. Zolang dit principe niet geschonden wordt, kan de controleur niets onoorbaars constateren. Dat betekent dus dat als een grotere afstand is afgelegd, b.v. omdat in de tijd tussen beide controles ook plaats Z ver van de route tussen X en Y is bezocht, de extra afgelegde afstand of een deel ervan verzwegen kan worden.

Eén mogelijkheid om dit tegen te gaan is het zo dicht maken van het netwerk van controlepunten en het daarmee zo vaak opdracht geven gegevens te verstrekken, dat deze vorm van fraude niet meer lonend is. Deze optie lijkt niet erg aantrekkelijk vanwege de eraan verbonden kosten.

### Gebruik van agenten

Een andere, veel aantrekkelijker mogelijkheid is om (een deel van) de controle in het voertuig te laten uitvoeren door wat wij een agent hebben genoemd. Een agent moet enerzijds de informatie verzamelende en/of controlerende instantie bepaalde zekerheden bieden en mag anderzijds geen inbreuk kunnen plegen op de gewenste privacy. Zoals al eerder gezegd is, bestaat een agent uit programmatuur en/of apparatuur die vertrouwd wordt door (minstens) de instantie.

We laten in het volgende zo veel mogelijk in het midden of een agent uitgevoerd wordt als vaste of als losse voertuigapparatuur, maar beide kan, ook tegelijkertijd! (Aan het eind van dit hoofdstuk wordt hierover nog iets meer gezegd.) Ook gaan we zo min mogelijk in op details van allerlei andere variaties, zoals b.v. die ten gevolge van het wel of niet uniek identificeerbaar zijn van iedere agent of van het eventueel (semi-)anoniem verstrekken van identificeerbare agenten. Desalniettemin zal een ter zake kundige lezer duidelijk worden dat, als de agent bestaat uit een chipkaart, ons voorbeeld ook gezien kan worden als een nadere illustratie van het mogelijke ge-



bruik van al dan niet anonieme of (semi-)anoniem verstrekte chipkaarten, zoals eerder in de tekst al gesuggereerd werd. (Zie het hoofdstuk over privacybescherming.)

5 Een agent houdt in een voertuig tijdens verkeersdeelname i.h.a. toezicht op bepaalde zaken. Op geautoriseerd verzoek (en/of zo nu en dan op eigen initiatief) zorgt de agent voor een door hem ondertekend verslag van zijn bevindingen. Zo'n verslag kan via de zender toegestuurd worden aan de instantie (b.v. de beheerder van het verkeersinformatiesysteem of een aparte op de agenten toezicht houdende instantie).

10 De zender en/of ontvanger hoeven niet vertrouwd te worden door de agent en/of de betreffende instantie. Wij gaan er daarom bij onze uitleg voor het gemak vanuit dat de zender en de ontvanger geen onderdeel uitmaken van de agent. Er wordt natuurlijk voor gezorgd dat men niet onopgemerkt fraude kan plegen door de communicatie te belemmeren. Dit kan voorkomen worden door expliciet of impliciet gebruik te maken van acknowledgements, i.e. ontvangstbevestigingen. Als er bijvoorbeeld een verzoek om een verslag van de agent wordt gedaan, is het de taak van de overige voertuigapparatuur om te zorgen voor een adequate respons. Omdat het bedoelde  
15 verslag nodig is voor een adequate respons, is het invoeren van de hulp van de agent onontbeerlijk en kan uitzending van het verslag niet onopgemerkt voorkomen worden. In dit voorbeeld zijn expliciete acknowledgements dus niet nodig.

20 Het door de agent opgestelde en ondertekende verslag wordt (bij voorkeur) altijd eerst overhandigd aan de overige voertuigapparatuur. Immers, dan hoeft de houder en/of de gebruiker van het voertuig niet te vertrouwen op de correctheid en integriteit van de agent. De voertuigapparatuur kan vóór uitzending van het verslag van de agent o.a. controleren of de agent zich in het verslag inderdaad beperkt tot de precies voorgeschreven gegevens en 'formattering'. Er kan dus vermeden worden dat de agent stiekem ongeoorloofde, privacy gevoelige informatie  
25 mee stuurt of dat de agent ongeoorloofd vaak berichten stuurt naar de instantie, wat de privacy in gevaar kan brengen. Ook kan de juistheid van het verslag van de agent in twijfel worden getrokken. Als dit zo is, moet naast het verslag ook een aantekening worden opgenomen in de te leveren respons.

30 Als alle controles zijn uitgevoerd en de te leveren respons (bestaande uit het verslag van de agent en eventuele toevoegingen) is samengesteld en ondertekend, moet de ondertekende respons via de zender overhandigd worden aan de controlerende instantie. Er kan afgesproken worden dat de controlerende instantie na ontvangst van een adequate respons een bewijs van ontvangst moet verstrekken. Als de respons een aantekening van onenigheid of twijfel over de juistheid van het verslag van de agent bevatte, volgt er binnen een bepaalde termijn een afgesproken procedure, zoals b.v. het aanbieden van het voertuig met die agent ter nadere inspectie en controle.

### 35 **Toezicht van agent op tellermonotonie**

40 Zoals al geschetst heeft een agent in ieder geval als taak om desgewenst een ondertekend verslag te verstrekken van zijn bevindingen bij het houden van toezicht. Een agent kan er o.a. op toezien dat hij, in ieder geval tijdens het rijden, voortdurend wordt geïnformeerd over de tellerstand(en), dan wel de toename ervan. De agent kan dus ter plekke controle uitoefenen op de monotonie van tellerstand(en), dan wel de doorgegeven informatie gebruiken om zelf tellerstand(en) monotoon stijgend bij te houden. Beide gevallen komen op hetzelfde neer, maar wij

zullen voor het gemak uitgaan van het geval dat er alleen (pulsen of andere) ophogingen worden doorgegeven en de agent zelf de tellerstand(en) bijhoudt. Merk op dat er bij gebruik van een agent dus géén identificatie van het voertuig nodig is voor de controle van de tellerstand(en) op monotonie, wat wèl nodig was in geval van controle op afstand.

5

### Een bijdrage van de agent aan de controle op tellerprecisie

De agent kan, en moet i.h.a., er ook op toezien dat de tellerstand niet te vlug wordt opgehoogd. Dus een plotselinge ophoging met een te grote afstand wordt niet toegestaan. Anders gezegd, een ophoging die overeenkomt met een te hoge snelheid<sup>39</sup> hoeft niet geloofd te worden en een te plotselinge snelheidstoename, i.e. een onmogelijk hoge acceleratie, eventueel ook niet. Op deze wijze kan de aan het begin van dit hoofdstuk (in de sectie over alleen zenden op verzoek) geschetste vorm van fraude worden tegengegaan. We lichten dit nu even toe.

Stel dat de agent op plaats X verslag heeft gedaan van een bepaalde tellerstand. Dan kan men de agent misleiden door tijdens het rijden geen ophogingen van de tellerstand door te geven en dus tegenover de agent te doen alsof men niet rijdt. Of men kan te lage of te weinig ophogingen doorgeven. Maar dergelijk bedrog komt uit zodra bij het passeren van plaats Y een verzoek om respons binnenkomt. Immers, men kan dan niet meer in korte tijd alsnog de agent zijn tellerstand voldoende laten ophogen, opdat tenminste de kortste afstand tussen X en Y in zijn tellerstand verdisconteerd wordt. Dus zal de tellerstand van de agent dan mogelijk te laag zijn en zal bij verzending van zijn verslag de fraude ontdekt worden. Het enige alternatief is geen adequate respons leveren, maar dat betekent dat toch gedetecteerd wordt dat er iets aan de hand is en dat er actie kan worden ondernomen. Kortom, doordat elke agent zelf de tellerstand bijhoudt en hij dat alleen doet op basis van beperkte ophogingen, is zulke fraude met tellerstanden niet meer mogelijk of niet meer lonend.

We hebben nu behandeld hoe een agent monotonie kan garanderen en dat een agent ongeloofwaardige ophogingen van de tellerstand kan en moet detecteren. Als er iets niet correct lijkt te verlopen, moet de agent daarover op enig tijdstip, b.v. zodra hij daartoe de kans krijgt, verslag uitbrengen. Het niet accepteren van ongeloofwaardige ophogingen is nodig als bijdrage aan de controle op precisie.

Als de agent niet meer doet dan tot nu toe beschreven, moet de rest van de controle op precisie van de teller nog op afstand uitgevoerd worden door de controlerende instantie. Een agent kan echter nog meer controle uitoefenen. In het navolgende zullen we laten zien dat een agent ook zelf de rest van de controles op precisie kan uitvoeren.

35

---

<sup>39</sup> B.v. hoger dan de maximaal haalbare snelheid met dat voertuig, rekening houdend met een bepaalde marge i.v.m. bijzondere omstandigheden.

### Controle op tellerprecisie volledig door de agent

Om een agent zelfstandig de precisie te kunnen laten controleren, i.e. te laten controleren of hij door de overige voertuigapparatuur steeds correct op de hoogte wordt gehouden van de juiste ophogingen van de tellerstand, moet hij wel af en toe kunnen beschikken over betrouwbare informatie.

We illustreren nu e.e.a. voor het geval van kilometertellers. In dit geval moet de agent bij tijd en wijle betrouwbare informatie krijgen over de juiste snelheid of over de juiste lengte van een bepaald afgelegd traject. Dit laatste zou bijvoorbeeld kunnen doordat de agent zelf zijn geografische positie kan bepalen, dan wel af en toe informatie toegestuurd krijgt over zijn positie, respectievelijk de positie van het voertuig waarin hij zich bevindt. Zoals we nu eerst zullen laten zien, kan dit laatste eventueel ook op zodanig wijze gebeuren, dat de agent niet eens te weten komt waar hij zich bevindt.

### Controle op kilometerteller m.b.v. al dan niet (semi-)anonieme posities

De controle op precisie van kilometertellers kan bijvoorbeeld als volgt bewerkstelligd worden. Op bepaalde plaatsen worden denkbeeldige meetlijnen over de weg getrokken. In het simpelste geval gaat het om paren meetlijnen, waarbij de eerste meetlijn het begin van een controle markeert en de tweede het eind.

Als een agent de eerste meetlijn passeert wordt hem een geheim en ondertekend bericht toegezonden met een tijdstempel en met de boodschap dat hier een kilometertellercontrole begint. Bij passeren van de tweede meetlijn krijgt de agent weer een geheim en ondertekend bericht met een tijdstempel, maar nu met de afstand tot de eerste meetlijn. De agent kan op basis van de geleverde informatie bepalen of de hem vanuit het voertuig verstrekte informatie over de tellerstand op dit meettraject juist is geweest.

De berichten aan de agent moeten geheim zijn, omdat bij deze aanpak i.v.m. de fraudebestendigheid alleen de agent mag zien waar controles beginnen en eindigen. Daarom zal het in dit geval ook verstandig zijn om niet alleen paren meetlijnen te gebruiken, maar eventueel ook controletrajecten met drie of meer meetlijnen. Dit laatste zorgt er b.v. voor dat het risico om gepakt te worden voor (een poging tot) fraude d.m.v. het 'slim gokken' op juist geschatte begin- en eindpunten van controletrajecten aanzienlijk toeneemt.

De ondertekening is nodig om te voorkomen dat er (b.v. via manipulatie met de rest van de voertuigapparatuur) geknoeid kan worden met deze berichten, i.e. dat ze vervalst of onopgemerkt gewijzigd kunnen worden.

Om te voorkomen dat de berichten vertraagd of eventueel zelfs helemaal niet doorgegeven worden aan de agent, kan geëist worden dat een door de agent ondertekende ontvangstbevestiging teruggestuurd moet worden als respons. De tijdstempels helpen voorkomen dat men kan frauderen m.b.v. gekopieerde berichten. Merk op dat er in dit geval bij de tellercontroles dus in zekere zin (nog steeds) sprake is van 'opdrachten/verzoeken' met bijbehorende responsen.

40

Bij de bovenbedoelde controles kan nuttig gebruik worden gemaakt van semi-identificaties. Bij het passeren van elke meetlijn wordt een agent dan een 'positiebericht' toegezonden met een semi-identificatie van deze meetlijn (b.v. in de vorm van een getal van twee cijfers) en de semi-identificatie(s) van één of meerdere, mogelijk door hem eerder gepasseerde meetlijnen met hun kortste afstand tot deze meetlijn.

5

Eén voordeel van deze alternatieve aanpak is dat er geen onderscheid meer is tussen begin- en eindpunten van controles en dat de berichten aan de agenten nu dus ook niet meer geheim gehouden hoeven te worden. Een ander, hier nauw aan verbonden voordeel is dat dezelfde berichten nu eventueel in het voertuig gebruikt kunnen worden voor het nader bepalen van de geografische positie, bijvoorbeeld ter ondersteuning van al dan niet geautomatiseerde navigatie.

10

Let wel, bij elke meetlijn wordt in het 'positiebericht' alleen een semi-identificatie van de plek uitgezonden, zodat de agent niet te weten komt waar hij zich bevindt en dus zeker geen informatie aan de rest van de controlerende instantie (of anderen) kan verstrekken over zijn geografische positie, ook niet via een of ander verborgen kanaal<sup>40</sup>. Maar b.v. de bestuurder van het voertuig kan wel degelijk weten waar hij zich ongeveer bevindt en kan de semi-identificatie van een meetlijn, tenminste als die meetlijn zich op een vaste en bekende plek bevindt, gebruiken om nu zijn precieze geografische positie te bepalen.

15

Voor goede controle is het vanzelfsprekend nodig dat niet van alle meetlijnen de positie bekend is. Voor de benodigde 'verrassingscontroles' kan men o.a. gebruik maken van mobiele meetlijnen, i.e. mobiele apparatuur voor het leggen van een meetlijn en het uitzenden van 'positieberichten' m.b.t. deze meetlijn. Voor alle zekerheid merken we tenslotte nog op dat het vanzelfsprekend ook mogelijk is om in de bedoelde (positie)berichten de afstand tot de betreffende meetlijn te melden i.p.v. alleen het exacte passeren van de betreffende meetlijn.

20

## 25 **Controle op kilometerteller m.b.v. betrouwbare informatie over snelheid**

Afgelegde weg en snelheid zijn aan elkaar gerelateerd. Als men wordt geïnformeerd over de toename van de kilometerteller en beschikt over voldoende nauwkeurige tijdmeting, kan men de bijbehorende snelheid bepalen. Maar 'het omgekeerde' geldt ook, zodat men op basis van betrouwbare snelheidsgegevens en nauwkeurige tijdsmeting dus ook de juistheid van gemelde tellerophogingen kan controleren. Kortom, een alternatieve aanpak voor controle maakt gebruik van snelheidsgegevens.

30

Bijvoorbeeld kan de snelheid van passerende voertuigen m.b.v. radar onafhankelijk worden bepaald. De controle kan nu op twee manieren geschieden. Ofwel de extern bepaalde snelheid wordt aan de agent bekend gemaakt en de agent controleert of de snelheid op basis van de in het voertuig verstrekte informatie inderdaad klopt, of de agent zendt de intern bepaalde snelheid uit en de controle vindt plaats buiten het voertuig.

35

<sup>40</sup> Als men zich niet wil beveiligen tegen deze mogelijkheid, kunnen de posities van de meetlijnen ook aangeduid worden met unieke identificaties. De agent kan dan wel zijn positie te weten komen, maar kan die kennis toch niet zomaar uitzenden via de zender in het voertuig zonder reële kans op ontdekking.

Vanzelfsprekend moeten de twee vergeleken snelheden wel het zelfde tijdstip betreffen. Voor alle zekerheid vestigen we hier nog de aandacht op een tamelijk subtiel punt, nl. dat dit een tijdstip moet zijn vóór het moment waarop men in het voertuig met enige reden kan gaan vermoeden dat er een verhoogde kans is dat binnenkort controle gaat plaatsvinden. Dus een tijdstip vóór het begin van enige communicatie, welke dan ook, m.b.t. deze  
 5 controle tussen voertuig en infrastructuur. Immers, om fraude tegen te gaan moet geen enkele informatie prijsgegeven worden op grond waarvan men enig nader vermoeden over dit tijdstip zou kunnen verkrijgen. Bij deze aanpak van controles moet de agent recente snelheidsgegevens dus altijd korte tijd bewaren.

Als de apparatuur benodigd voor onafhankelijke snelheidsmeting duurder is dan een extra zender, zal de aanpak  
 10 van de controles m.b.v. snelheidsgegevens i.h.a. minder aantrekkelijk zijn dan die m.b.v. positiegegevens. Wel kan deze aanpak dan toch nog voordeliger zijn voor verplaatsbare controlepunten t.b.v. verrassingscontroles. Bovendien biedt deze aanpak de mogelijkheid van controles vanuit rijdende patrouillewagens. Kortom, deze aanpak is zeker interessant voor mobiele controles in beide betekenissen, i.e. verplaatsbaar en rijdend.

15 Het in deze sectie gegeven voorbeeld kan beschouwd worden als een specifieke illustratie van de eerder genoemde, meer algemene mogelijkheid om controles uit te voeren m.b.v. differentie- of differentiaalquotiënten. (Zie ook het hoofdstuk over controles. We gebruiken de toch wat voorzichtige formulering 'kan beschouwd worden als', omdat bij externe snelheidsmeting de snelheid meestal 'direct' bepaald wordt m.b.v. radargolven en het dopplereffect en dus niet expliciet bepaald wordt als afgeleide grootte van afgelegde afstand, i.e. niet expliciet  
 20 gemeten wordt als een in zeer korte tijd afgelegd afstandsverschil.)

#### Ook andere controles door agent

Zojuist hebben we beschreven dat het bijhouden van de kilometer(teller)stand en de controle erop geheel door de  
 25 agent kan geschieden als hem voldoende geschikte en betrouwbare informatie wordt toegezonden. Zoals eerder al gesuggereerd is en nu duidelijk moet zijn, kan een agent ook controle uitoefenen op allerlei andere tellerstanden en gegevens, zoals b.v. toerental, benzineverbruik en/of in de motorruimte geproduceerd lawaai.

We hebben in de voorgaande sectie al beschreven dat een agent de precisie van de snelheidsmeter kan controle-  
 30 ren. Echter, omdat de agent in het voertuig zit en daardoor vrijwel continu toezicht kan houden, kan hij ook constateren of de ter plekke geldende maximum snelheid overschreden wordt, tenminste als hem vanuit de buitenwereld betrouwbare informatie over de maximaal toegestane snelheid wordt toegestuurd.

Ook bij andere verkeersovertredingen, zoals b.v. door rood rijden, kan de agent een rol spelen. Bijvoorbeeld  
 35 door op geautoriseerd verzoek de identiteit van het voertuig of van de betaler prijs te geven, als hij daar tenminste over beschikt. Of door de overtreding in samenwerking met de verkeerslichtinstallatie te constateren en deze constatering vast te leggen.

Bij constatering van een verkeersovertreding heeft een agent een aantal mogelijkheden. Hij kan de overtreding  
 40 t.z.t. ter verdere afhandeling doorgeven aan de rest van het verkeersinformatiesysteem of hij kan de verschuldigde boete zelf vaststellen en evt. optellen bij het reeds verschuldigde bedrag aan verkeersheffingen. Als de betref-

fende boete geïntegreerd is, i.e. opgenomen in de tariefstructuur van de verkeersheffing, hoeft hij zelfs niets bijzonders te doen. Deze mogelijkheid is er b.v. bij snelheidsovertredingen. Men kan de boete dan b.v. zodanig opnemen in de tariefstructuur, dat de feitelijk extra in rekening gebrachte boete afhangt van de mate waarin de toegestane snelheid is overschreden en van het aantal afstandseenheden waarin dat is gebeurd. Voor deze afhankelijkheid kan natuurlijk ook gezorgd worden zonder de boetes in de tarieven te integreren.

Hoe dan ook, volautomatische en efficiënte afhandeling van verkeersovertredingen en -boetes wordt in veel gevallen mogelijk. Als de agent zorg draagt voor het fraudebestendig beschikbaar stellen van een identificatie, dan kunnen verkeersovertredingen veel efficiënter afgehandeld worden, doordat het lezen van kentekens vanaf foto's dan niet meer nodig is. In bepaalde gevallen kunnen de foto's zelfs geheel achterwege blijven, wat ook een aanzienlijke besparing oplevert.

Tenslotte merken we nog even op dat het afhandelen van boetes tamelijk goed vergelijkbaar is met het opleggen en innen van grensheffingen, zoals b.v. bij tolheffing voor bruggen of tunnels. Aan dit laatste hebben we tot nu toe nauwelijks aandacht besteed, o.a. omdat grensheffingen veel meer ingeburgerd zijn dan totaalheffingen. Hoewel gebruik van een TIP-systeem voor uitsluitend grensheffingen misschien wat minder opmerkelijk is, moge duidelijk zijn dat onze aanpak ook bij grensheffingen bepaalde voordelen biedt.

#### **Privacybescherming door beperking van uitzenden van identificaties**

Als de agent alle controles zoveel mogelijk voor zijn rekening neemt, hoeven er nauwelijks nog andere berichten uitgezonden te worden dan de berichten voor het bevestigen van de ontvangst van toegezonden betrouwbare informatie, zoals b.v. positiegegevens, extern gemeten snelheid, lawaai of wat dies meer zij. Het enige wat daarnaast uitgezonden hoeft te worden, is meldingen van de agent over een goede of verkeerde gang van zaken en in geval van verkeersheffingen zo nu en dan, zeg eens per maand, een bericht met de tellerstand en met een identificatienummer waarmee indirect een verantwoordelijke betaler kan worden geïdentificeerd. Dit laatste is nodig voor het automatisch innen van de verkeersheffingen. Misschien zal een heel enkele keer ook nog een klein aantal berichten extra uitgewisseld worden, b.v. omdat men het nodig acht om de juiste werking van de agent bij tijd en wijle op afstand (extra) te controleren.

Strikt genomen hoeft een agent de meldingen van tellerstanden en (in)correct functioneren natuurlijk niet per sé 1) automatisch, 2) zo spoedig mogelijk en/of 3) tijdens het rijden te verstrekken. In principe is het b.v. ook mogelijk om de agent periodiek door of namens de instantie te laten 'uitlezen'. Dit uitlezen, i.e. het vragen om en krijgen van een rapportage, hoeft niet via de zender van het voertuig te gebeuren, maar kan evt. ook geschieden via fysiek (b.v. elektrisch) contact. Het uitlezen zou b.v. gecombineerd kunnen worden met (evt. andere) periodieke keuringen of inspecties. Ook als uitlezing slechts eenmaal per jaar zou geschieden, kan de betaling natuurlijk even goed gespreid plaatsvinden, net als momenteel in Nederland gebruikelijk is bij b.v. de betaling voor gas en electriciteit.

Desalniettemin verwachten wij dat men meestal zal kiezen voor uitlezen via de zender van het voertuig tijdens normaal gebruik vanwege de voordelen die dat biedt. Immers, het kost de klant geen tijd en men kan daardoor

zonder al te veel bezwaar de agent ook vaker 'uitlezen'. Bovendien komen (pogingen tot) fraude (en onjuist functioneren meer in het algemeen) dan sneller aan het licht, zodat sneller kan worden ingegrepen.

Als de agenten niet uniek identificeerbaar zijn, i.e. als ze niet ieder een eigen handtekening hebben, of als de agenten wel uniek identificeerbaar zijn, maar niet bekend is door welke persoon of in welk voertuig een agent gebruikt wordt, i.e. als de agenten anoniem verstrekt worden, dan wordt er bij de door agenten ondertekende ontvangstbevestigingen geen enkele privacy gevoelige informatie prijs gegeven. Dus de enige berichten die de privacy dan nog zouden kunnen bedreigen, zijn de meldingen van de tellerstanden met bijbehorende identificaties ten behoeve van het betalingsproces. Als deze laatste berichten slechts een enkele keer, bijvoorbeeld eens per maand, worden uitgezonden, is er nauwelijks sprake van een bedreiging van de privacy, zelfs niet als van elk zo'n tellerstandmelding precies vastgesteld zou kunnen worden waar vandaan dat bericht verzonden is. (Men zou voor zulke berichten evt. een communicatiekanaal kunnen gebruiken, waarbij localisatie van de zender niet eenvoudig is.)

Iets soortgelijks als hierboven beschreven geldt als de agenten identificeerbaar zijn, maar semi-anoniem worden verstrekt. Kortom, de privacybescherming m.b.v. jagers en/of intermediairs kan in de genoemde gevallen deels, of eventueel zelfs geheel, achterwege worden gelaten! Eventueel zou men de betaling ook nog in het voertuig kunnen laten plaatsvinden. Hierover wordt in de volgende sectie nog iets meer gezegd.

## 20 Verschillen met de eerdere aanpak

De aanpak m.b.v. agenten verschilt niet zo heel veel van de eerder beschreven aanpak met uitsluitend controles op afstand. Een verschil is dat de controlerende instantie via vooruitgeschoven posten, nl. agenten, dichter op de te controleren objecten zit en dat controles (alle controles of evt. slechts een deel ervan) in het voertuig plaatsvinden. De communicatie tussen de (veelal niet tegen fraude beveiligde) objecten (denk m.n. aan sensoren en/of meetinstrumenten) in het voertuig en de informatie verzamelende en/of controlerende instantie vindt nu hoofdzakelijk of geheel plaats in het voertuig (nl. tussen object en agent), zodat voor deze communicatie nu niet meer steeds de wat grotere afstanden tussen de zender (resp. ontvanger) van het voertuig en de ontvangers (resp. zenders) in de buitenwereld overbrugd hoeven te worden. Het communicatiekanaal tussen voertuig en buitenwereld wordt dus niet meer (direct) gebruikt voor de communicatie tussen de gecontroleerde objecten (zeg, meetinstrumenten) in het voertuig en de controleur in de buitenwereld, maar wordt nu in plaats daarvan gebruikt voor de communicatie tussen de agent (als vooruitgeschoven post en evt. als volwaardig controleur) en de rest van de informatie verzamelende en/of controlerende instantie.

Een en ander wordt geïllustreerd in de figuren 3 en 4. In die figuren behoort de rechts weergegeven zender plus ontvanger toe aan de jager (weergegeven door hokje 8) en is er in beide gevallen één intermediair (hokje 9), hoewel die in de situatie van figuur 4 waarschijnlijk niet of nauwelijks meer nodig is. In figuur 3 zorgt de instantie, i.e. de eindontvanger (hokjes 10 en 11), zowel voor de controles (hokje 10) als voor de rest van zijn taken (hokje 11), zoals b.v. inning van de verschuldigde heffingen. In figuur 4 worden de controletaken namens de instantie uitgevoerd door de agent in het voertuig.

Eén verschil is dus dat (tenminste een deel van) de controle 'verschoven' is, i.e. op een andere plaats in de totale keten van activiteiten en/of deelnemers plaats vindt. Dit in abstractie niet zo grote verschil heeft wel degelijk wezenlijke gevolgen. Immers, omdat de feitelijke controleur nu zelf in het voertuig zit, is er geen identificatie meer nodig om van verschillende berichten aan de controleur (met b.v. ophogingen van tellerstanden of andere metingen) te kunnen bepalen of ze uit hetzelfde voertuig afkomstig zijn. Sterker nog, er hoeven nauwelijks nog berichten over gecontroleerde objecten (meetinstrumenten) met daarin identificaties van die objecten uitgewisseld te worden met de buitenwereld. Zoals al eerder gezegd is, hoeft alleen nog zo nu en dan een (evt. indirecte) identificatie in een bericht met de resulterende rekening naar de instantie in de buitenwereld te worden verstuurd. En zelfs dit laatste is niet strikt noodzakelijk, omdat de agent ook bij periodieke controles 'uitgelezen' kan worden.

Ook als de betaling in het voertuig plaats vindt, hoeft de communicatie met de buitenwereld niet per sé berichten aan de instantie betreffende de rekeningen te omvatten. Maar die communicatie zal (in plaats daarvan) dan i.h.a. wel uitgebreid worden met een uitwisseling van berichten t.b.v. het betalingsproces. Dit laatstgenoemde berichtenverkeer betreft de communicatie tussen een bankagent, i.e. programmatuur en apparatuur van of namens de bank, in het voertuig en (de rest van) de bankorganisatie in de buitenwereld. Merk wel op dat in het extreme geval dat agenten alleen berichten naar de buitenwereld, i.e. naar de instantie, zenden in de trant van 'alles gaat OK, ook de betaling', de instantie (zeg, de heffingsinner) geen of een minder goed overzicht heeft. Dit laatste wordt mogelijk niet op prijs gesteld.

Een ander verschil is dat bij de beveiliging van de agent tegen fraude sprake is van een fysiek aspect. Als de agent bijvoorbeeld wordt geïmplementeerd (uitgevoerd) m.b.v. een chip of chipkaart, hangt de totale beveiliging af van de fysieke beveiliging van (de opslag van) de programmatuur en sleutel(s) van de agent in de chip. Omdat chipkaarten in de praktijk voldoende beveiligd blijken te kunnen worden en omdat er verder geen fysieke beveiliging noodzakelijk is, lijkt dit geen serieus bezwaar.

### **'Vaste' of 'losse' agenten**

Het gebruik van agenten lijkt een aantrekkelijke mogelijkheid voor het uitvoeren van taken, zoals m.n. het in rekening brengen van allerlei verkeersheffingen, en voor het uitoefenen van de daarvoor benodigde controles. De betreffende agenten kunnen bijvoorbeeld in elk voertuig worden aangebracht als vaste voertuigapparatuur (VVA), zeg, in de vorm van een chip met programmatuur in een behuizing. Maar een agent kan, zoals al vaker gesuggereerd, eventueel ook uitgevoerd worden als losse voertuigapparatuur (LVA), b.v. in de vorm van een chipkaart die, in ieder geval tijdens gebruik, via een aansluitpunt (b.v. een stekker of een kaartlezer) verbonden is met de overige voertuigapparatuur van het betreffende voertuig, zoals b.v. de zender, de ontvanger, de accu en een aantal sensoren en/of meetinstrumenten.

Als elke gebruiker zijn eigen 'losse' agent heeft, b.v. op een chipkaart (die wellicht tevens fungeert als identificatiemiddel en/of verbruikspas), en deze vóór elke rit via een kaartlezer in het betreffende voertuig in verbinding brengt met de overige voertuigapparatuur in dat voertuig, dan is zo'n agent natuurlijk niet zo geschikt voor de



taak van voertuigidentificatie. In zo'n geval kan desgewenst een tweede, vaste agent zorg dragen voor fraudebestendige identificatie en/of typering van het voertuig. (Zie ook verderop de sectie over één of meerdere agenten.)

### Algemene en gespecialiseerde agenten

5

Soms maken we voor ons gemak onderscheid tussen algemene en gespecialiseerde agenten. Met de term *gespecialiseerde* agent doelen we dan op een agent met een specifieke functie beperkt tot slechts een klein deel van alle agententaken horende bij het betreffende verkeersinformatiesysteem. Denk b.v. aan een fraudebestendige verbruikspas die een voor het verkeersinformatiesysteem *essentiële* teller bijhoudt en verder geen andere bij het betreffende verkeersinformatiesysteem horende agententaken vervult. (We noemen een teller slechts *informatief* als deze alleen ten genoegen van de gebruiker wordt gebruikt en niet van doorslaggevend belang is voor het bijhouden van de juiste tellerstand door het verkeersinformatiesysteem.) Een ander voorbeeld is een agent die uitsluitend dient voor de fraudebestendige identificatie en/of typering van een voertuig. Een *algemene* agent daarentegen verricht (bijna) alle agententaken die horen bij het betreffende verkeersinformatiesysteem.

15

Tot nu toe werd in de tekst de term agent voornamelijk gebruikt voor algemene agenten en moest (resp. mocht) men bij lezing van de term agent primair denken aan de spil in het voertuig waar alles m.b.t. controles in het voertuig om draait. Anders gezegd, de nadruk heeft steeds gelegen op m.n. de controletaak van de agent, i.e. op zijn taak als vertegenwoordiger van de instantie in een voertuig die zorg draagt voor (een deel van de) controles op de betrouwbaarheid van de in voertuigen verstrekte informatie en via welke informatie wordt verstrekt aan de rest van het verkeersinformatiesysteem. Ook in de rest van de tekst wordt met het woord agent primair een algemene agent aangeduid. Slechts een enkele keer gebruiken we daarnaast voor ons gemak de term gespecialiseerde agent. Het verschil tussen beide termen speelt dus nauwelijks een rol van betekenis. Terecht, want het verschil is toch wat vaag.

25

### Iets meer over uitvoeringsmogelijkheden

Net als bij de aanpak met uitsluitend controles op afstand zijn er bij het gebruik van agenten legio (vaak voor de hand liggende) uitvoeringen en/of variaties mogelijk. Het is daarom te veel van het goede om alle mogelijkheden expliciet op te sommen. Op basis van de gegeven beschrijving is het voor een ter zake kundige makkelijk om allerlei verschillende variaties en uitvoeringen te verzinnen. Hier stippen we, eigenlijk al ten overvloede, slechts een klein aantal mogelijkheden aan.

35

Eén voor de hand liggende en al veel vaker gesuggereerde mogelijkheid is om de agenten uit te voeren als een chip, eventueel aangebracht in een chipsleutel of op een chipkaart. Zeker als b.v. chipkaarten of chipsleutels worden gebruikt, kan men de uit te geven chips desgewenst ook voorzien van een (zeg, aflopende) teller, waarbij die verbruiksteller vanaf een bepaalde beginstand wordt bijgehouden door de agent. De agent zorgt dan dus tevens voor de functie van verbruikspas, waarbij het verbruik van het tegoed kan plaatsvinden verspreid over een willekeurig aantal verschillende voertuigen. Het voordeel van zo'n agent met verbruikspasfunctie is, dat de tracing van identificeerbare gebruikers van zulke chipkaarten dan onmogelijk is, simpelweg doordat er dan helemaal geen identificaties van gebruikers meer in het spel zijn. Door restricties op te leggen aan de verkoop van zulke

40

chipkaarten, kan eventueel een systeem met verhandelbare gebruiks- en/of vervuiliingsrechten (per persoon per jaar) worden verkregen.

5 Verder noemen we nog de mogelijkheid om alle genoemde functionaliteit evt. op één chip te combineren met andere toepassingen, zoals b.v. met elektronisch betalingsverkeer m.b.v. een chipkaart of met elektronische toegang m.b.v. een chipsleutel. Wel kan het dan gewenst zijn om goede waarborgen in te bouwen tegen ongewenste uitwisseling van informatie tussen de diverse toepassingen. Ook wijzen we nog op de mogelijkheid om de functionaliteit van een agent uit te breiden. B.v. tot die van een '*betrouwbare black box*', i.e. een black box die niet alleen toegeleverde gegevens registreert en gedurende een bepaalde tijd onthoudt (zoals gebruikelijk is), maar 10 m.n. ook (een deel van) de aangeleverde gegevens *controleert* op betrouwbaarheid. Andere voorbeelden zijn het evt. gebruik van een agent als *betrouwbare* taximeter of tachograaf.

### **Eén of meerdere agenten per voertuig**

15 Tot nu toe hebben we de mogelijkheid van meerdere agenten per voertuig voor ons gemak zoveel mogelijk buiten schot gehouden. Dat was wat ons betreft om meerdere redenen terecht. Allereerst hielp dat onnodige complexiteit bij de uitleg te voorkomen. Bovendien hebben we al in het hoofdstuk over de benodigde apparatuur expliciet opgemerkt dat we wilden abstraheren van de mogelijkheid om de processing te verdelen over meerdere processors, zodat we in feite deze mogelijkheid wel degelijk hebben afgedekt. Het enige bijzondere dat nu ter 20 sprake zal komen is de eventuele spreiding van het agentenwerk over een 'vaste' en een 'losse' processor, i.e. een vaste en een losse agent.

In geval van een vaste agent, gaan we er vaak vanuit dat deze alle gewenste taken verricht. De eventuele gebruikerskaarten dienen dan alleen voor de identificatie van een individuele teller behorend bij een bepaalde kaart of 25 persoon. De agent in het voertuig kan het verbruik behorend bij die teller bijhouden en op geschikte momenten doorgeven aan de rest van het verkeersinformatiesysteem in de buitenwereld. Als men prijs stelt op de mogelijkheid dat tellerstanden ook op gebruikerskaarten worden vermeld, b.v. omdat gebruikers dan op elk gewenst moment die tellerstanden uit kunnen lezen, dan moeten de agenten in voertuigen er simpelweg voor zorgen dat een tellerstand na wijziging ook op de gekoppelde gebruikerskaart wordt teruggeschreven.

30 Manipulatie met een tellerstand op een gebruikerskaart heeft geen zin als die tellerstand alleen informatief (i.e. alleen ten genoegen van de gebruiker) wordt gebruikt en niet van doorslaggevend belang is voor het juist bijhouden van de juiste tellerstand door het verkeersinformatiesysteem. Als de tellerstanden op de gebruikerskaarten wel essentieel zijn voor het verkeersinformatiesysteem, moeten ze beveiligd worden. Dit kan b.v. m.b.v. cryptografische technieken en aanvullende maatregelen, maar kan in plaats daarvan evt. ook door (mede) te vertrouwen 35 op de fraudebestendigheid van de gebruikerskaart, die in dit laatste geval dan wel een chipkaart zal zijn (en geen magneetkaart). Alleen in dit laatstgenoemde geval van (vanuit het oogpunt van de instantie) fraudebestendige chipkaarten met essentiële tellerstanden is er tijdens gebruik van een voertuig naast de vaste agent ook sprake van een tweede, losse agent in het voertuig.

40

Maar als de gebruikerskaart toch een agent omvat, dan ligt het voor de hand om die agent ook maar meteen alle agententaken op zich te laten nemen, zodat de vaste agent in het voertuig dan kan vervallen. Let op, dit laatste kan niet altijd. Alleen als de vaste agent fraudebestendig gekoppeld was aan het voertuig om ook de voertuig-identificatie- en/of voertuigtyperingstaak op zeer fraudebestendige wijze uit te voeren, kan deze laatstgenoemde taak niet worden overgenomen door de losse agent.

Kortom, we hebben laten zien dat meestal met één agent per voertuig kan worden volstaan. Er zijn, zoals hierboven geschetst, ook reële situaties waarin meerdere agenten per voertuig gebruikt worden. Stel dat men er toe neigt om aparte agenten te gebruiken 1) voor de voertuigidentificatie- en/of voertuigtyperingstaak, 2) voor de functie van verbruikspas met teller en 3) voor de functie van identificatiehulpmiddel, waarbij men de overige agententaken dan b.v. onderbrengt bij één van de gebruikte agenten, die dan dus de algemene agent wordt. Dan zouden er dus eigenlijk drie agenten nodig zijn, één algemene en twee gespecialiseerde. Maar voor de functie van identificatiehulpmiddel is niet altijd per sé een agent nodig, zoals in het hoofdstuk over fraudebestendigheid al is gesuggereerd. (B.v. niet als identificatie plaatsvindt door het laten zetten van een digitale handtekening.) Bovendien kan men (en zal men i.h.a. ook) de functies van identificatiehulpmiddel en van verbruikspas combineren in één gebruikerskaart. Kortom, in de geschetste situatie kan i.h.a. makkelijk volstaan worden met twee agenten.

Merk op dat voor de voertuigidentificatie- en/of voertuigtyperingstaak alleen een agent nodig is als fraudebestendige identificatie of typering van een voertuig van belang is voor het juist functioneren van het verkeersinformatiesysteem. Dit is b.v. het geval als de typering van een voertuig een rol speelt bij de hoogte van het tarief bij het opleggen van verkeersheffingen. Tenslotte wijzen we er nog eens op dat het gebruik van een losse agent een aantrekkelijke optie is vanuit het oogpunt van privacybescherming (zie ook de vorige sectie).

Samengevat komt ons betoog op het volgende neer. Er kan volstaan worden met één agent. In ieder geval met één vaste agent. Maar ook met één losse agent als zeer fraudebestendige voertuigidentificatie of -typering niet vereist is voor het juist functioneren van het verkeersinformatiesysteem. Bij gebruik van een losse agent zijn twee agenten nodig als ook zeer fraudebestendige voertuigidentificatie en/of -typering vereist is.

Hoewel er dus wel degelijk sprake kan zijn van meerdere agenten (b.v. omdat de te verrichten taken toch verdeeld worden over een vaste en een losse agent/processor), gingen en gaan wij er ter vereenvoudiging van de tekst i.h.a. vanuit dat dit niet het geval is. Dus veronderstellen we in deze tekst (i.e. deze toelichting op onze vinding) zonder beperking der algemeenheid (i.e. uitsluitend voor het gemak) meestal dat er sprake is van maximaal één agent (en soms dat er sprake is van maximaal twee agenten) per voertuig en dat het toezicht en de controle uitgevoerd wordt door deze ene agent (resp. deze twee agenten). Hoewel dat allerminst noodzakelijk is, gaan we er in het geval dat (toch) meerdere agenten gebruikt worden, vanuit dat er sprake is van één algemene agent en een aantal gespecialiseerde (hulp)agenten.

#### **Het gebruik van agenten als aantrekkelijke optie**

Zoals al meermalen opgemerkt, lijkt het gebruik van agenten een aantrekkelijke mogelijkheid voor het uitoefenen van controle en het in rekening brengen van allerlei verkeersheffingen. Het lijkt aantrekkelijk om een agent niet

alleen te gebruiken voor het bijhouden van de verschuldigde verkeersheffingen en/of verbruikte rechten per persoon en/of per voertuig, maar deze ook te gebruiken voor andere taken, zoals b.v. het op verzoek (of evt. vrijwel continu) uitzenden van semi-identificaties. Immers, het gebruik van semi-identificaties biedt als voordeel dat de beheerder van de infrastructuur op directe, maar toch privacy veilige wijze allerlei nuttige verkeersinformatie kan verzamelen, zoals b.v. informatie over verkeersstromen, filevertragingen, benuttingsgraad van wegen, e.d. In een  
5 volgend hoofdstuk komen we nog terug op de taken die een agent zoal kan verrichten.

## Vorbereiding op 'groei' van het systeem

Door aan elk bericht altijd een protocolnummer (en evt. daarin opgenomen of separaat een betaalwizzenummer) en/of een berichttypennummer toe te voegen, kunnen binnen één en hetzelfde systeem tegelijkertijd verschillende (sub)systemen, zoals b.v. versies, worden toegestaan en dus ook meerdere heffingsstructuren en/of betalingswijzen worden ondersteund. Op deze wijze kan men beginnen met een eenvoudige versie van het systeem en stap voor stap uitbreidingen en verfijningen aanbrengen.

Bijvoorbeeld kan men er voor kiezen dat men in het begin maar één tamelijk eenvoudig protocol ondersteunt met een bepaald protocolnummer (b.v. nummer 1). Stel dat men e.e.a. als volgt doet. In elk voertuig worden aangebracht: 1) een zender en een ontvanger, 2) een fraudebestendige component die als agent kan gaan fungeren, 3) een voertuigprocessor, i.e. een component voor o.a. het controleren van berichten van de agent en/of vercijferen van die berichten t.b.v. de privacy bescherming, en 4) een centraal aansluitpunt voor het aan elkaar verbinden van de genoemde en evt. toekomstige componenten. Men kiest één vaste jager die tevens als enige intermediair fungeert. Elke voertuigprocessor zendt dus bij dit protocol alle berichten van de agent bestemd voor eindontvangers uit, zij het verpakt in een geheim bericht aan de jager/intermediair, zodat eindontvangers alleen berichten kunnen lezen met hulp van die ene jager/intermediair.

Bij dit eerste protocol is het enige wat de agent in elk voertuig doet, het reageren op verzoeken om identificatie. Op elk geautoriseerd verzoek identificeert de agent zichzelf (en daarmee in zekere mate het voertuig) door zo'n verzoek te ondertekenen na toevoeging van het tijdstip en een identificatienummer, zeg het identificatienummer van de agent (of evt. het kenteken van het voertuig waarvoor de agent is verstrekt). Dit aldus ondertekende verzoek wordt overhandigd aan de voertuigprocessor, die het dan vercijfert tot een geheim bericht aan de jager en die dat geheime bericht via de zender van het voertuig verstuurt. We gaan er vanuit dat in eerste instantie alleen grensheffingen ingevoerd worden. Bij de betreffende tolpunten wordt door de geautoriseerde jager aan elk passerend voertuig, i.e. aan elke passerende agent, gevraagd om identificatie. Elke ontvangen respons wordt door de jager ontdaan van de voor geheimhouding toegevoegde verpakking en vervolgens doorgestuurd naar de heffingsinnehmer, die de tol in rekening brengt bij de houder van de agent (resp. van het kenteken).

Merk op dat we in ons voorbeeld niet hebben geeist dat de agent fraudebestendig aan het voertuig moet worden bevestigd. Ook zonder fraudebestendige koppeling is e.e.a. wel degelijk voldoende fraudebestendig. Immers, verwisseling van authentieke agenten lijkt niet aantrekkelijk. Zolang passage van een tolpunt voor elk voertuig leidt tot een zelfde bedrag aan tol, lijkt verwisseling met instemming van de geregistreerde houders van de agenten (resp. van de bijbehorende voertuigen) geen zin te hebben. Verwisseling met een gestolen exemplaar lijkt op het eerste gezicht misschien wel aantrekkelijk, omdat de rekening dan bij een ander, nl. de bestolene, terecht komt. Echter, het opsporen van een gestolen agent is voldoende eenvoudig (tenminste, als het daadwerkelijk gebruikt wordt om een ander voor de tol op te laten draaien) om de aantrekkingskracht van zulke pogingen tot fraude te minimaliseren. Natuurlijk is het van het begin af aan fraudebestendig bevestigen van agenten aan voertuigen, tenminste als men beschikt over een voldoende goedkope techniek daarvoor, ook een aantrekkelijke optie, omdat men dan ook voorbereid is op toepassingen waarbij fraudebestendige koppeling van agenten aan voertuigen wel gewenst of vereist is.

Vanaf een bepaald moment kan men eisen dat nieuwe voertuigen voorbereid zijn op het continu aan de agent kunnen leveren van gegevens over de kilometerstand. Zij moeten de vereiste informatie aan de agent leveren in de vorm van b.v. kilometerstanden (in b.v. twee decimalen), tellerophogingen of pulsen van een sensor op de aandrijf-  
 5 as. Men kan dan op enig moment bij nieuwe voertuigen overgaan op gebruik van een tweede protocol (zeg, met protocolnummer 2), waarbij voor de verkeersheffingen ook gebruik kan worden gemaakt van een to- taalheffing op alle afgelegde kilometers. Bestaande voertuigen kunnen hieraan ook meedoen na montage van een sensor op de aandrijf-  
 10 as. De aansluiting van de sensor op de rest van het systeem is eenvoudig te realiseren, omdat we er door het aanbrengen van een geschikt aansluitpunt van het begin af aan voor hebben gezorgd dat het sys- teem is voorbereid op aansluiting van overige voertuigapparatuur. Hoewel de software in de agent al van het begin af aan voorbereid kan zijn op deze uitbreiding/aanpassing, zal er waarschijnlijk toch het e.e.a. aangepast moeten worden. Bijvoorbeeld moet de software, als pulsen van een sensor op de aandrijf-  
 15 as worden gebruikt, mogelijk nog informatie krijgen over de afgelegde weg van dit voertuig die correspondeert met één puls. (Evt. kan er voor gezorgd worden dat deze informatie ook al van het begin af aan aanwezig is.) Natuurlijk worden nu ook de eerder (in het hoofdstuk over de aanpak m.b.v. agenten) beschreven controles op de correctheid van de door de agent bijgehouden kilometerteller ingevoerd.

De agent kan de bijgehouden kilometerstand, pas later of meteen in deze tweede fase, ook gebruiken voor het creëren en uitzenden van semi-identificaties op basis van de kilometerteller, bijvoorbeeld t.b.v. het verzamelen  
 20 van informatie over vertragingen t.g.v. files. (Bij het eerste protocol had de agent evt. ook al meteen een vaste semi-identificatie kunnen uitzenden, maar nog niet één van het soort waarbij de semi-identificatie gebaseerd is op de kilometerteller en dus steeds verandert.) Ook kan men, meteen of weer later en zonder verdere wijziging van de in voertuigen inmiddels aanwezige hardware, ervoor zorgen dat de processor programmatuur gaat gebruiken die het tarief van elke kilometer afhankelijk stelt van de snelheid waarmee die is afgelegd. (Zoals al eerder is  
 25 opgemerkt, zou die programmatuur eventueel ook verstrekt kunnen worden via de zenders van de infrastructuur, zeg langs of boven de weg, en eventueel ook automatisch in werking gesteld.) Ook kan men op enig moment de mogelijkheid tot gebruik van LVA toevoegen, zodat daarna de betaler iemand anders kan zijn dan de houder van het voertuig, en kan men eventueel een systeem van verhandelbare vervuiliingsrechten invoeren. Etcetera, etcete-  
 30 ra.

We merken ter aanvulling op bovenstaande voor alle duidelijkheid nog een keer op dat, zeker zolang de tarieven van de verkeersheffing gelijk zijn voor alle soorten deelnemende voertuigen (en de agent dus geen betrouwbare informatie over de typering hoeft te verschaffen), fraudebestendige koppeling van de agent aan het voertuig zon-  
 35 der al te veel bezwaar achterwege gelaten kan worden. Fraudebestendige koppeling, i.e. beveiliging tegen ver- wisseling, is pas noodzakelijk als een zeer hoge betrouwbaarheid van de typering en/of identificatie van voertui- gen middels de agenten vereist is.

Men kan afspreken dat er voor elke combinatie van protocol en betaalwijze een apart protocolnummer wordt gebruikt. Men kan ook (in plaats van het koppelen van de betaalwijze aan een protocolnummer) een apart be-

taalwijzenummer introduceren. Hiermee kan men aangeven hoe men wenst te betalen. B.v. automatisch via een bankrekening, per week of per maand, met of zonder kredietfaciliteit, etc.

## TIP-systemen

In het voorgaande hebben we allerlei mogelijkheden geschetst om een verkeersinformatiesysteem met bepaalde eigenschappen te verkrijgen. Om een verkeersinformatiesysteem met de door ons als gewenst beschouwde eigen-  
 5 schappen te kunnen verkrijgen zijn door ons een aantal technieken geïntroduceerd, zoals o.a. het creëren van *semi-identificatienummers* (al dan niet op basis van tellerstanden), het uitvoeren van *snelheidscontroles* en bepa-  
 len van *filevertragingen* m.b.v. zulke semi-identificatienummers, het op afstand en/of in het voertuig uitvoeren van *controles* op o.a. tellerstanden, toerental en benzineverbruik, het tamelijk nauwkeurig berekenen van veroor-  
 10 zaakte *milieuvervuiling*, het gebruik van *jagers* en/of *intermediairs* voor privacybescherming en het gebruik van *agenten* in voertuigen voor privacybescherming en/of controles.

In principe kan een TIP-systeem gebruik maken van alle beschreven technieken. Maar dat is, zoals we al eerder hebben laten blijken, niet noodzakelijk. Bijvoorbeeld is het mogelijk om een TIP-systeem te realiseren zonder agenten en zonder gebruikerskaarten, dus zonder enige fraudebestendige component in elk voertuig. Ook kan  
 15 men zodanig gebruik maken van agenten dat jagers en/of intermediairs overbodig zijn. Of men kan bijvoorbeeld besluiten geen gebruik te maken van semi-identificaties. Kortom, in het algemeen zal een TIP-systeem slechts een deel van de beschreven (en al dan niet kenmerkende) technieken gebruiken. Er zal i.h.a. al sprake zijn van een TIP-systeem als tenminste één van de door ons nieuw geïntroduceerde, i.e. TIP-systemen kenmerkende, technieken (deelvindingen) gebruikt wordt. Het is in ieder geval uitdrukkelijk de bedoeling dat elk gebruik van  
 20 één of meerdere van de kenmerkende technieken *de jure et de facto* een inbreuk betekent op onze vinding.

### Een TIP-systeem met agenten

Juist omdat er zoveel onderling verschillende mogelijkheden zijn om een TIP-systeem te realiseren, lijkt het ons  
 25 goed om ter illustratie één aantrekkelijke mogelijkheid eruit te lichten en als een samenhangend geheel te beschrijven. We doen dat voor het geval van wegverkeer en kiezen daarbij voor een aanpak met agenten in de voertuigen, omdat zo'n aanpak een aantal belangrijke voordelen biedt en geen serieuze nadelen lijkt te hebben.

Een duidelijk voordeel is dat met agenten veel meer informatie kan worden verzameld en gecontroleerd zonder  
 30 dat de kosten de pan uitrijzen. Immers, voor een agent in het voertuig is het een koud kunstje om *continu* toezicht te houden, terwijl bij de aanpak zonder agenten de nadruk toch wat meer (of duidelijker) ligt op het *steekproefsgewijs* opvangen van uitgezonden informatie t.b.v. controles. Bij de aanpak zonder agenten kan in principe weliswaar vrijwel even intensief informatie verzameld en gecontroleerd worden als bij de aanpak met agenten, maar dan toch alleen als het verkeersnetwerk wordt volgebouwd met zenders, ontvangers en computers om conti-  
 35 nu contact te kunnen hebben met alle voertuigen en om de enorme stroom aan informatie uitgezonden door de voertuigen te kunnen verwerken. Denk vooral ook aan de veel hogere behoefte aan rekenkracht die dan nodig is voor het veelvuldig gebruik van jagers en intermediairs voor de gewenste privacybescherming. Kortom, bij gebruik van agenten is intensieve controle mogelijk met een veel goedkopere infrastructuur, omdat er dan veel minder zenders, ontvangers en vooral ook computers nodig zijn dan bij de andere aanpak.

40



Vanuit een iets andere invalshoek komt men tot het hieraan verwante voordeel dat er minder communicatie nodig is tussen de voertuigen en de buitenwereld dan bij de aanpak met alle controles op afstand. Er zal dus veel minder kans zijn dat de communicatie met veel voertuigen tegelijk tot problemen leidt. Dat er voor de communicatie tussen de voertuigen en de buitenwereld bij gebruik van agenten inderdaad beduidend minder bandbreedte nodig is dan bij de aanpak zonder agenten, moge duidelijk zijn. Immers, elke agent verwerkt de gegevens lokaal en kan de informatie samenvatten en/of selectief oversturen, zodat voor de communicatie met de buitenwereld slechts een fractie nodig is van de bandbreedte die anders nodig zou zijn. (De bandbreedte die anders nodig zou zijn voor de communicatie met de buitenwereld, is gelijk aan de bandbreedte nodig voor de communicatie tussen de agent en de overige apparatuur in het voertuig, zoals sensoren en meetinstrumenten.)

10

Het enige nadeel van de aanpak met agenten t.o.v. de aanpak met uitsluitend controles op afstand is, dat voor elke agent een fraudebestendige component nodig is. Deze component zal i.h.a. een chip bevatten met daarop een processor en bijbehorend geheugen waarvan (een deel van) de inhoud niet ongeautoriseerd gewijzigd of zelfs maar gelezen kan worden. Dit nadeel legt echter vrijwel geen gewicht in de schaal. Niet alleen omdat zo'n component niet veel hoeft te kosten, maar ook omdat, vanwege de behoefte aan voldoende fraudebestendige voertuigidentificatie en/of -typering, het aan voertuigen moeten bevestigen van een fraudebestendige component met een chip sowieso onvermijdelijk lijkt.

15

Derhalve ligt het tamelijk voor de hand om te kiezen voor de aanpak met agenten en om elke agent wellicht tevens te gebruiken voor het fraudebestendig vasthouden en verstrekken van betrouwbare voertuiginformatie. Onder voertuiginformatie verstaan we: 1) voertuig (min of meer) identificerende gegevens, zoals het chassisnummer, motornummer, kenteken, e.d., 2) voertuig typerende gegevens, zoals b.v. merk, model, bouwjaar, versnellingsbak- en/of motortype, en 3) overige informatie over het voertuig, zoals bv. toegestane brandstofsoort(en), gewicht, kleur en/of informatie over de rechtmatige houder of eigenaar, zoals b.v. zijn of haar sofinummer of zijn of haar naam en adres.

25

Als de keus voor een aanpak met agenten eenmaal is gemaakt, moet daarna ook nog gekozen worden welke taken de agenten zullen verrichten. Een agent kan, indien gewenst, een veelheid aan taken verrichten, waarvan we hier een aantal opsommen in de context van wegverkeer:

30

1. Het *verzamelen* en/of *bijhouden* van allerlei relevant geachte informatie over het *gebruik* van het voertuig op basis van door apparatuur in het voertuig (m.n. sensoren en/of meetinstrumenten) geleverde informatie. Denk b.v. aan gegevens zoals snelheid, toerental, kilometertellerstand, brandstofverbruik, brandstoftellerstand, temperatuur, e.d. Merk op dat deze gegevens i.h.a. tamelijk dynamisch zijn, i.e. bij tijd en wijle tamelijk frequent aan verandering onderhevig zullen zijn.
2. Het (direct of indirect) *controleren* of die aangeleverde informatie voldoende geloofwaardig en/of juist is. Hierbij wordt veelal gebruik gemaakt van vanuit de buitenwereld verstrekte, betrouwbare informatie. Denk b.v. aan (directe) controle op snelheidsmeter, kilometerteller en buitentemperatuurmeter, en b.v. aan (indirecte) controle op toerenteller en brandstofverbruiksmeter.

35

3. Het op geëigende momenten aan een (bevoegde) controlerende instantie in de buitenwereld *rapporten* van de bevindingen bij de controlewerkzaamheden.

Denk b.v. aan het melden van eventuele onregelmatigheden of van (ogenschijnlijk) ongestoorde werking.

4. Het op basis van beschikbare informatie *berekenen* en/of *bijhouden van afgeleide informatie*.

5 Denk bij afgeleide informatie b.v. aan een tamelijk nauwkeurige berekening van het brandstofverbruik en/of van de op een zeker moment veroorzaakte vervuiling, in beide gevallen op basis van andere gegevens, zoals b.v. merk, model, bouwjaar, versnellingsbaktype, motortype, snelheid, toerental, acceleratie, brandstofverbruik<sup>41</sup>, buitentemperatuur, motortemperatuur, e.d. Denk ook aan een tamelijk nauwkeurige berekening van de geluidsproductie. Voor de berekening van afgeleide informatie uit andere gegevens moet de agent natuurlijk kunnen beschikken over een berekeningswijze, b.v. in de vorm van een formule of van één of meerdere tabellen.

Het afgeleide brandstofverbruik kan m.n. gebruikt worden om het door het voertuig opgegeven brandstofverbruik (indirect) op betrouwbaarheid te controleren. De afgeleide vervuiling kan gebruikt worden voor het bijhouden van een teller m.b.t. de in totaal veroorzaakte milieuvervuiling.

- 15 5. Het zo nu en dan op geëigende momenten *verstrekken* van bepaalde (betrouwbare) informatie over het *gebruik* van het voertuig aan een bepaalde bevoegde instantie in de buitenwereld.

Deze verstrekking kan b.v. plaatsvinden t.b.v. het opleggen en innen van verkeersheffingen en/of van verkeersboetes. Denk b.v. aan het verstrekken van bepaalde tellerstanden samen met identificerende gegevens van het bijbehorende voertuig (of van zijn gebruiker, betaler of eigenaar) t.b.v. het opleggen en innen van een totaalheffing en aan het verstrekken van gegevens over eventueel door de agent geconstateerde verkeersovertredingen. Bepaalde boetes kunnen evt. al in de tarieven van een verkeersheffing geïntegreerd zijn.

6. Het verzamelen en zo nu en dan verstrekken van bepaalde informatie aan een bepaalde (bevoegde) instantie in de buitenwereld t.b.v. het verkrijgen van *statistische praktijkgegevens*.

25 Denk b.v. aan het (al dan niet selectief) verstrekken van gegevens over het door het voertuig opgegeven brandstofverbruik in diverse omstandigheden (b.v. gekarakteriseerd door snelheid, acceleratie, toerental, buitentemperatuur, motortemperatuur, e.d.) met bijbehorende vermelding van het type van het voertuig, zodat de betreffende instantie een goed beeld kan krijgen van het brandstofverbruik van voertuigen van dat type (i.e. merk, model, bouwjaar, versnellingsbaktype, motortype e.d.) in de praktijk.

30 Zulke (statistische) praktijkgegevens kunnen o.a. gebruikt worden voor het vinden van berekeningswijzen t.b.v. het bepalen van afgeleide informatie.

7. Het fraudebestendig *opslaan* en *beschikbaar stellen van voertuiginformatie*.

35 Het beschikbaar stellen van voertuiginformatie moet, zeker als het houder/eigenaar of voertuig identificerende informatie betreft, natuurlijk alleen geschieden onder bepaalde, duidelijk omschreven voorwaarden en/of in bepaalde, duidelijk omschreven omstandigheden en dan liefst nog maar alleen aan bepaalde, relevant geachte instantie(s) in de buitenwereld. Merk ook op dat voertuiginformatie i.h.a. tamelijk statisch is, i.e. niet of tamelijk infrequent aan verandering onderhevig zal zijn.

---

<sup>41</sup> Dit gegeven hoort natuurlijk alleen in de opsomming thuis bij het voorbeeld van de berekening van veroorzaakte milieuvervuiling.

8. Het op verzoek van een bevoegde instantie (construeren en) toesturen van een *semi-identificatienummer*.

Dit nummer kan b.v. afgeleid zijn van de kilometertellerstand en kan door de bedoelde instantie b.v. gebruikt worden voor het bepalen van verkeersvertragingen ten gevolge van files, het controleren of de gemiddelde snelheid op een bepaald traject beneden de maximum snelheid is gebleven, het bestuderen van verkeersstromen, het uitvoeren van verkeerstellingen, etc.

9. Het *verifiëren* van de authenticiteit van ontvangen berichten over de infrastructuur en het *doorgeven van berichten* aan andere apparatuur in het voertuig.

Denk b.v. aan doorgifte van officiële berichten over snelheidsbeperkingen, filevertragingen, de buitentemperatuur, de positie, de snelheid, e.d.

10. Alleen als er bij gebruik van het voertuig gebruik kan of moet worden gemaakt van een (gebruikers)kaart, het verzorgen van de *communicatie met* de aangeboden gebruikerskaart *of*, als de agent zelf op die kaart zit, het zelf (tevens) *vervullen van* de functie van *gebruikerskaart* (verbruikspas).

De genoemde communicatie kan o.a. betrekking hebben op het over en weer op echtheid controleren, het (voor zover van toepassing en gewenst) uitwisselen van identificerende gegevens en/of het voldoende frequent (laten) bijwerken van de juiste tellerstand op de kaart.

Merk op dat de gebruikerskaart een anonieme of een persoonlijke tellerstand kan bevatten en dat het bijwerken van een tellerstand dus b.v. het steeds verlagen van de tellerstand op een anonieme of anoniem verkochte verbruikskaat kan betreffen of b.v. het steeds ophogen van een persoonlijke tellerstand op een identificeerbare betalings- of gebruikerskaart.

11. Het na ontvangst van een door de rechtmatige houder of eigenaar getekend verzoek daartoe (of na ontvangst van een door de rechtmatige houder/eigenaar eerder opgegeven wachtwoord) zorgen voor *frequente uitzending van identificerende gegevens*.

Hierdoor wordt het vaak relatief eenvoudig om het betreffende voertuig snel op te sporen, b.v. na diefstal.

12. Het fungeren als *betrouwbare taximeter, tachograaf en/of black box* e.d.

- Het adjectief 'betrouwbare' betreft hier (naast de fraudebestendigheid van het betreffende apparaat zelf) m.n. het controleren van de juistheid van (een deel van) de aangeleverde gegevens (i.e. de input).

Natuurlijk hoeft een agent niet per sé alle (al dan niet genoemde) taken te vervullen en kan gekozen worden voor een (eventueel kleine) deelverzameling. Wel illustreert bovenstaande nog eens de brede toepasbaarheid van het TIP-systeem, i.e. dat het TIP-systeem ook geschikt is voor gebruik als (al dan niet geïntegreerd) multifunctioneel verkeersinformatiesysteem.

Een agent is per definitie een fraudebestendige component. We benadrukken hier ten overvloede dat het voor bepaalde taken ook nog nodig is dat de agent *fraudebestendig gekoppeld* wordt (en dus blijft) aan het juiste, bijbehorende voertuig.

#### Componenten deel uitmakend van het TIP-systeem

Bij een TIP-systeem bestaat het verkeersinformatiesysteem o.a. uit een groot aantal met elkaar communicerende computers, waarvan bij gebruik van agenten een substantieel aantal (nl. iedere agent) zich (evt. alleen tijdens gebruik) in de betrokken voertuigen bevindt en derhalve mobiel is. Een agent maakt daarom in onze ogen deel uit

van het verkeersinformatiesysteem. Voor eventuele gebruikerskaarten (zeg, magneet- of chipkaarten) die gebruikers bij zich kunnen hebben en die niet vallen onder het begrip agent, ligt de keus wat minder duidelijk. Als ze hoofdzakelijk dienen voor het m.b.t. het TIP-systeem vast- en/of bijhouden van al dan niet persoonlijke gebruiksrechten, vervuilingrechten en/of andere tellerstanden, rekenen wij ze als een onderdeel van het totale systeem.

5 Alle overige voertuigapparatuur kan beschouwd worden geen deel uit te maken van het TIP-systeem. Het is dus niet nodig om de in voertuigen aanwezige componenten, zoals b.v. sensoren en/of meetinstrumenten, te beschouwen als onderdelen die deel uitmaken van het TIP-systeem, ook niet als ze informatie leveren die nuttig of zelfs nodig is voor het functioneren van het betreffende TIP-systeem.

## 10 TIP-agenten

Gezien de vele en diverse taken die het TIP-systeem kan verrichten, is het zeer wel denkbaar dat niet alle toepassingen onder dezelfde instantie vallen. In zo'n geval is wellicht één van de betrokken instanties of een aparte instantie die onafhankelijk is van de instanties betrokken bij de toepassingen, verantwoordelijk voor het functioneren van het TIP-systeem. Als dat zo is, dan kan een agent primair gezien worden als een vertegenwoordiger van de voor het TIP-systeem verantwoordelijke instantie, en pas secundair als vertegenwoordiger van de bij toepassingen betrokken instantie(s), die blijkbaar voldoende vertrouwen stellen in de agenten (en de rest van het TIP-systeem) om hen bepaalde taken toe te (durven) vertrouwen.

## 20 TIP-systemen voor ander verkeer

De opsomming van taken die een agent zoal kan verrichten, werd gegeven in de context van wegverkeer. Het is niet zo moeilijk om een vergelijkbare opsomming te maken voor een aantal andere vormen van verkeer. We willen hier wel benadrukken dat de afweging tussen een aanpak met of zonder agenten bij elke verkeersvorm anders kan komen te liggen. Bijvoorbeeld geldt dit voor het geval van vliegverkeer, waarbij tracering van verkeersvliegtuigen i.h.a. niet als een bedreiging van de privacy wordt beschouwd. Bij het eerder geschetste voorbeeld van beperking van geluidshinder kan men dus ook prima uit de voeten zonder agenten.

Men eist dan b.v. dat vliegtuigen binnen een bepaalde afstand tot een (bepaalde) luchthaven (vrijwel) continu informatie moeten uitzenden over hun positie en over het door hun geproduceerde geluid. De juistheid van de opgegeven positie kan regelmatig (via radiopeilingen en/of radarinstallaties of wat dies meer zij) gecontroleerd worden. De geluidsproductie kan steekproefsgewijs met een redelijke mate van nauwkeurigheid op juistheid of, beter gezegd, op geloofwaardigheid gecontroleerd worden door op diverse plaatsen in de nabijheid van aan- en uitvliegroutes (m.n. vanaf de grond) geluidsmetingen te verrichten. Door voldoende kennis te verzamelen over de voortplanting van geluid resp. geluidsterkte (beide afhankelijk van een aantal omstandigheden, zoals b.v. windrichting), kan men uit de vanuit het vliegtuig opgegeven geluidswaarden door berekening afleiden hoeveel lawaai er ter plekke van het meetpunt ongeveer waargenomen had moeten worden en dus controleren of de werkelijk gemeten waarde daar niet teveel van afwijkt.

40 Het is duidelijk dat men sowieso het correct volgen van de voorgeschreven aanvliegroute kan controleren. Daarnaast kan men dan controleren of het betreffende vliegtuig niet teveel geluid heeft geproduceerd. Door de aan-

vliegroutes eventueel te beschrijven als vaste 'toegestane geluidscontouren', kan men op efficiënte en flexibele wijze de geluidshinder beperken. 'Stillere' vliegtuigen zullen dan wat meer bewegingsvrijheid hebben binnen de vaste contouren dan meer lawaaiige. En ook minder gauw de gestelde geluidsgrenzen overschrijden als tijdens de landing b.v. tussentijds gas blijkt te moeten worden gegeven. Eventuele boetes kunnen dan natuurlijk afhankelijk gemaakt worden van de ernst (duur en mate) van de geluidsoverschrijding. Luchtvaartmaatschappijen hebben er dan belang bij om boetes te vermijden en zullen hun piloten stimuleren (b.v. via een bonus- en/of malusstelsel) om binnen de geluidscontouren te blijven. Juist met wat lawaaiiger toestellen zal de gewenste aan- resp. uitvlieg-route dan dus nauwkeuriger gevolgd worden. Dat is niet alleen gunstig voor degenen die de geluidshinder moeten ondergaan, maar ook voor een luchthaven. Want een luchthaven zal dan minder gauw gedwongen worden tot 'zwart/wit-beslissingen', i.e. het voordeel hebben dat het wat lawaaiiger toestellen (en wel m.n. de 'grensgevallen') niet meteen volledig hoeft te weren.

## Conclusies

### Conclusie 1:

Werkwijze voor het verzamelen van verkeersinformatie door een instantie

- 5 a) waarbij gebruik wordt gemaakt van in althans een deel van de voertuigen aanwezige middelen ter ver-  
strekking van informatie,
- b) waarbij uit (de ontvangst van) de vanuit voertuigen verstrekte informatie direct of indirect verkeersinfor-  
matie wordt afgeleid,
- c) waarbij onrechtmatige tracering van individuele personen en/of voertuigen wordt voorkomen,
- 10 d) waarbij de betrouwbaarheid van de in of vanuit voertuigen verstrekte informatie voor zover nodig wordt  
gecontroleerd,
- e) waarbij de instantie niet hoeft te vertrouwen op de fraudebestendigheid van individuele componenten in  
voertuigen anders dan eventueel een per voertuig klein aantal agenten, en
- f) waarbij geen gebruik hoeft te worden gemaakt van een GPS (Global Positioning System).

15

### Conclusie 2:

Werkwijze volgens conclusie 1, waarbij betrouwbare informatie kan worden verzameld over één of meerdere  
aspecten, waaronder tenminste begrepen individuele informatie over o.a. de afgelegde afstand, de plaats, de  
datum, het tijdstip, het merk, het model, het bouwjaar, het versnellingsbaktype, het motortype, de ingescha-  
kelde versnelling, het toerental, de snelheid, de snelheidsveranderingen, de gebruikte brandstofsoort, het  
20 brandstofverbruik, de geluidsproductie en/of de veroorzaakte milieuvervuiling, en collectieve informatie over  
o.a. verkeersdrukke, files, het brandstofverbruik, de geluidsproductie en/of de veroorzaakte milieuvervuiling.,  
en waarbij de collectieve informatie desgewenst uitgesplitst kan worden naar één of meerdere van de (al dan  
niet genoemde) aspecten.

25

### Conclusie 3:

Werkwijze volgens een voorgaande conclusie, waarbij het volgen van de loop van verkeersstromen en het be-  
palen van filevertragingen automatisch en op een privacy vriendelijke wijze kan worden uitgevoerd.

30

### Conclusie 4:

Werkwijze volgens een voorgaande conclusie, waarbij gebruik wordt gemaakt van semi-identificatie(s).

### Conclusie 5:

Werkwijze volgens een voorgaande conclusie, waarbij onrechtmatige tracering wordt voorkomen door ge-  
bruik te maken van tenminste één organisatie die onafhankelijk is van de instantie.

35

### Conclusie 6:

Werkwijze volgens een voorgaande conclusie, waarbij voor althans een deel van de communicatie tussen  
voertuigen en de instantie gebruik wordt gemaakt van één of meerdere jagers.

40

**Conclusie 7:**

Werkwijze volgens een voorgaande conclusie, waarbij voor althans een deel van de communicatie tussen voertuigen en de instantie gebruik wordt gemaakt van één of meerdere intermediairs, die bij die communicatie fungeren als tussenpersoon.

5

**Conclusie 8:**

Werkwijze volgens een voorgaande conclusie, waarbij in althans een deel van de voertuigen ook tijdens gebruik geen agent nodig is.

10 **Conclusie 9:**

Werkwijze volgens een voorgaande conclusie, waarbij in althans een deel van de voertuigen tijdens gebruik één agent nodig is.

**Conclusie 10:**

15 Werkwijze volgens een voorgaande conclusie, waarbij in althans een deel van de voertuigen tijdens gebruik twee agenten nodig zijn.

**Conclusie 11:**

20 Werkwijze volgens een voorgaande conclusie waarbij alle of een deel van de controles op de betrouwbaarheid van de vanuit een bepaald voertuig verstrekte informatie geheel of gedeeltelijk buiten dat voertuig, i.e. op afstand, worden uitgevoerd.

**Conclusie 12:**

25 Werkwijze volgens een voorgaande conclusie, waarbij informatie verzameld wordt over het brandstofverbruik van individuele voertuigen.

**Conclusie 13:**

30 Werkwijze volgens een voorgaande conclusie, waarbij informatie verzameld wordt over door individuele voertuigen veroorzaakte milieuvervuiling.

**Conclusie 14:**

Werkwijze volgens een voorgaande conclusie, waarbij informatie verzameld wordt over door individuele voertuigen veroorzaakt geluid.

35 **Conclusie 15:**

Werkwijze volgens een voorgaande conclusie, waarbij informatie verzameld wordt over de bij individuele voertuigen ingeschakelde versnelling.

**Conclusie 16:**

40 Werkwijze volgens een voorgaande conclusie, waarbij informatie verzameld wordt over het motortoerental van individuele voertuigen.

**1011501**

**Conclusie 17:**

Werkwijze volgens een voorgaande conclusie, waarbij informatie verzameld wordt over bepaalde, bij individuele voertuigen of personen horende tellers.

5

**Conclusie 18:**

Werkwijze volgens een voorgaande conclusie, waarbij de verzamelde informatie (mede) wordt gebruikt voor het opleggen van een verkeersheffing.

10

**Conclusie 19:**

Werkwijze volgens conclusie 18, waarbij het gehanteerde tarief kan worden gerelateerd aan één of meerdere van de volgende aspecten: de afgelegde afstand, de plaats, de datum, het tijdstip, de verkeersdruk, het merk, model, bouwjaar, versnellingsbaktype, motortype, de ingeschakelde versnelling, het toerental, de snelheid, de snelheidsveranderingen, de brandstofsoort, het brandstofverbruik, de geluidsproductie en de veroorzaakte milieuvervuiling.

15

**Conclusie 20:**

Werkwijze volgens een voorgaande conclusie, waarbij de verzamelde informatie (mede) wordt gebruikt voor het opleggen van een totaalheffing.

20

**Conclusie 21:**

Werkwijze volgens een voorgaande conclusie, waarbij althans een deel van de communicatie vanuit een bepaald voertuig met een verkeersinformatie verzamelende, controlerende en/of verspreidende instantie plaatsvindt via een in dat voertuig aanwezig en/of aan dat voertuig bevestigd zendmiddel en een zich buiten dat voertuig bevindend ontvangmiddel.

25

**Conclusie 22:**

Werkwijze volgens een voorgaande conclusie, waarbij althans een deel van de communicatie vanuit een bepaald voertuig met een verkeersinformatie verzamelende, controlerende en/of verspreidende instantie plaatsvindt via een zich buiten dat voertuig bevindend zendmiddel en een in dat voertuig aanwezig en/of aan dat voertuig bevestigd ontvangmiddel.

30

**Conclusie 23:**

Werkwijze volgens een voorgaande conclusie, waarbij althans een deel van de zich buiten de voertuigen bevindende zend- en/of ontvangmiddelen mobiel zijn.

35

**Conclusie 24:**

Werkwijze volgens een voorgaande conclusie, waarbij (ook) sprake is van het verspreiden van verkeersinformatie door een instantie.

40

1011501



**Conclusie 25:**

Werkwijze volgens een voorgaande conclusie, waarbij gebruik wordt gemaakt van semi-identificaties die zijn afgeleid van een tellerstand.

5 **Conclusie 26:**

Werkwijze volgens een voorgaande conclusie, waarbij gebruik wordt gemaakt van semi-identificaties die zijn afgeleid van het kenteken van het betreffende voertuig.

**Conclusie 27:**

10 Werkwijze volgens een voorgaande conclusie, waarbij gebruik wordt gemaakt van semi-identificaties die voor elk voertuig lukraak gekozen zijn uit een verzameling elementen.

**Conclusie 28:**

15 Werkwijze volgens een voorgaande conclusie, waarbij de in of vanuit een voertuig verstrekte informatie gecontroleerd wordt op betrouwbaarheid en waarbij de (verstrekte en) gecontroleerde informatie tenminste informatie over één van de volgende aspecten betreft: de kilometertellerstand, de snelheid, de ingeschakelde versnelling, het toerental, het brandstofverbruik, de geluidsproductie en/of de veroorzaakte milieuvervuiling.

**Conclusie 29:**

20 Werkwijze volgens een voorgaande conclusie, waarbij een agent controles in het voertuig uitvoert m.b.v. extern bepaalde, aan hem verstrekte, betrouwbare informatie.

**Conclusie 30:**

25 Werkwijze volgens een voorgaande conclusie, waarbij controles worden uitgevoerd vanuit mobiele controleposten.

**Conclusie 31:**

30 Werkwijze volgens een voorgaande conclusie, waarbij trajectnelheidscontroles worden uitgevoerd op een privacy vriendelijke wijze.

**Conclusie 32:**

35 Werkwijze volgens conclusie 24, waarbij de juiste tijd wordt verspreid en in althans een deel van de voertuigen tenminste één kloktijdsaanduiding automatisch wordt aangepast bij een tijdswisseling, waarvan b.v. sprake is bij het passeren van een tijdszonegrens of bij de overgang van zomertijd op wintertijd of andersom.

**Conclusie 33:**

40 Werkwijze volgens een voorgaande conclusie, waarbij sprake is van quotering van al dan niet verhandelbare verbruiksrechten.

**Conclusie 34:**

Werkwijze volgens een voorgaande conclusie, waarbij sprake is van opsporing van afwijkende, mogelijk niet (meer) juist functionerende voertuigen en/of voertuigapparatuur.

5 **Conclusie 35:**

Werkwijze volgens een voorgaande conclusie, waarbij voertuigen op geautoriseerd verzoek kunnen worden opgespoord.

**Conclusie 36:**

10 Werkwijze volgens een voorgaande conclusie, waarbij software via het verkeersinformatiesysteem verspreid en/of in werking gesteld kan worden.

**Conclusie 37:**

15 Werkwijze volgens een voorgaande conclusie, waarbij een agent de betrouwbaarheid van een meetinstrument of teller in het betreffende voertuig geheel of gedeeltelijk controleert.

**Conclusie 38:**

20 Werkwijze volgens een voorgaande conclusie, waarbij sprake is van het gebruik van een agent bestaande uit een chip met een processor en geheugen dat althans voor een deel voldoende beveiligd is tegen het lezen van daarin opgeslagen gegevens en tegen het wijzigen van zulke gegevens en/of tegen het wijzigen van de door die chip gebruikte software.

**Conclusie 39:**

25 Werkwijze volgens een voorgaande conclusie, waarbij praktijkgegevens worden verzameld over bepaalde prestaties van voertuigen bij bepaalde gebruiksomstandigheden en deze verzamelde gegevens al dan niet verwerkt worden tot informatie over bepaalde prestaties van bepaalde groepen voertuigen bij bepaalde gebruiksomstandigheden.

**Conclusie 40:**

30 Werkwijze volgens een voorgaande conclusie, waarbij de verzamelde praktijkgegevens worden gebruikt voor het vinden/vaststellen van een berekeningswijze voor afgeleide informatie.

**Conclusie 41:**

35 Werkwijze volgens een voorgaande conclusie, waarbij gebruik wordt gemaakt van een berekeningswijze voor afgeleide informatie voor het bepalen van het brandstofverbruik en/of de geluidsproductie van een individueel voertuig, al dan niet om gebruikt te gaan worden bij controles.

**Conclusie 42:**

40 Werkwijze volgens een voorgaande conclusie, waarbij gebruik wordt gemaakt van een berekeningswijze voor afgeleide informatie voor het bepalen van de hoeveelheid (van een bepaalde vorm van) milieuvuiling veroorzaakt door een individueel voertuig.

**Conclusie 43:**

5 Werkwijze volgens een voorgaande conclusie, waarbij apparatuur voor cruise control in een voertuig gebruik maakt van buiten het voertuig verspreide en door apparatuur in het voertuig ontvangen informatie over toegestane maximum snelheden.

**Conclusie 44:**

10 Werkwijze volgens een voorgaande conclusie, waarbij d.m.v. het verkeersinformatiesysteem verzamelde en/of verspreide informatie wordt gebruikt voor ijking van een meetinstrument.

**Conclusie 45:**

15 Werkwijze volgens een voorgaande conclusie, waarbij een agent (ook) gebruikt wordt voor fraudebestendige identificatie van het voertuig waarin die agent, al dan niet fraudebestendig gekoppeld, is aangebracht.

**Conclusie 46:**

20 Werkwijze volgens een voorgaande conclusie, waarbij de juistheid van verstrekte tellerstand(en) geheel of gedeeltelijk op afstand steekproefsgewijs wordt gecontroleerd.

**Conclusie 47:**

25 Werkwijze volgens een voorgaande conclusie, waarbij in een voertuig audiovisuele middelen zijn aangebracht welke tenminste een deel van de informatie kunnen weergeven.

**Conclusie 48:**

30 Werkwijze volgens conclusie 24, waarbij althans een deel van de verspreide informatie (mede) gebruikt wordt voor navigatie.

**Conclusie 49:**

Verkeersinformatiesysteem met een werkwijze volgens een voorgaande conclusie.

**Conclusie 50:**

35 Verkeersinformatiesysteem volgens conclusie 49 dat is voorbereid op aanpassingen en uitbreidingen.

**Conclusie 51:**

Voertuig geschikt voor (gebruik bij) een werkwijze volgens een voorgaande conclusie.

**Conclusie 52:**

Agent geschikt voor (gebruik bij) een werkwijze volgens een voorgaande conclusie.

**Conclusie 53:**

40 Een uit apparatuur en programmatuur bestaande component, geschikt voor gebruik als voertuigprocessor voor een werkwijze volgens een voorgaande conclusie.

**Conclusie 54:**

Een gebruikerskaart geschikt voor (gebruik bij) een werkwijze volgens een voorgaande conclusie.

5 **Conclusie 55:**

Rollenbank voor het nader inspecteren van de werking van voertuigapparatuur (mede) t.b.v. een werkwijze volgens een voorgaande conclusie resp. (mede) t.b.v. een verkeersinformatiesysteem volgens conclusies 49 en 50.

10 **Conclusie 56:**

Betrouwbare taximeter waarbij gebruik gemaakt wordt van een werkwijze volgens een voorgaande conclusie.

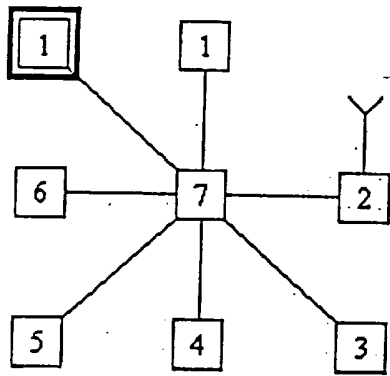
**Conclusie 57:**

15 Betrouwbare tachograaf waarbij gebruik gemaakt wordt van een werkwijze volgens een voorgaande conclusie.

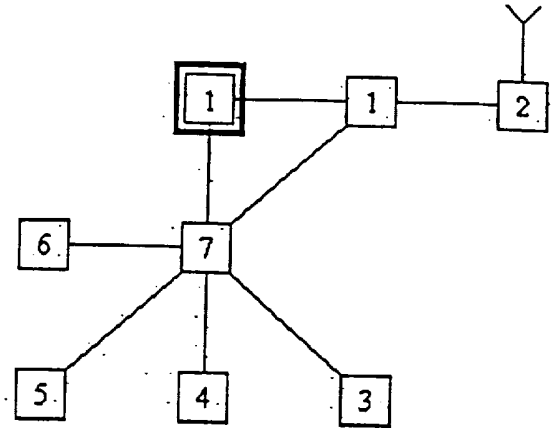
**Conclusie 58:**

20 Betrouwbare 'zwarte doos' (i.e. 'black box') waarbij gebruik gemaakt wordt van een werkwijze volgens een voorgaande conclusie.

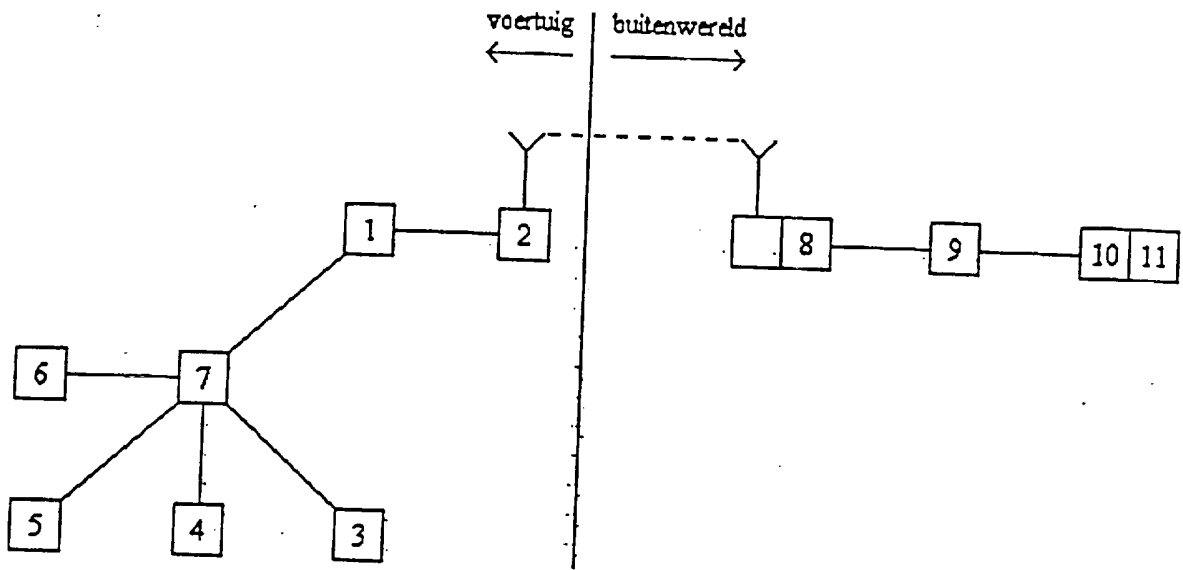
Figuur 1



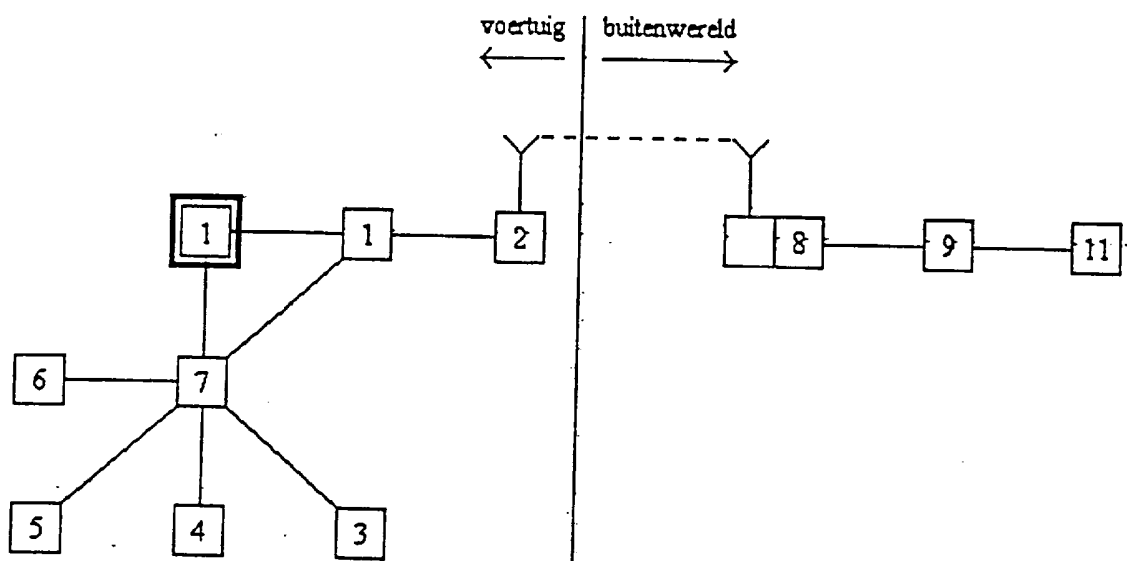
Figuur 2



Figuur 3



Figuur 4



SAMENWERKINGSVERDRAG (PCT)  
 RAPPORT BETREFFENDE  
 NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

IDENTIFIKATIE VAN DE NATIONALE AANVRAGE	Kenmerk van de aanvrager of van de gemachtigde  Q.UH73
Nederlandse aanvraag nr.  1011501	Indieningsdatum  9 maart 1999
	Ingeroepen voorrangsdatum
Aanvrager (Naam)  de Jonge, Wiebren	
Datum van het verzoek voor een onderzoek van internationaal type	Door de Instantie voor Internationaal Onderzoek (ISA) aan het verzoek voor een onderzoek van internationaal type toegekend nr.  SN 32901 NL
I. CLASSIFICATIE VAN HET ONDERWERP (bij toepassing van verschillende classificaties, alle classificatiesymbolen opgeven)	
Volgens de Internationale classificatie (IPC)  Int.Cl. <sup>6</sup> :G 08 G 1/01, G 08 G 1/09	
II. ONDERZOCHETE GEBIEDEN VAN DE TECHNIEK	
Onderzochte minimum documentatie	
Classificatiesysteem	Classificatiesymbolen
Int.Cl. <sup>6</sup> :	G 08 G
Onderzochte andere documentatie dan de minimum documentatie voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen	
III. <input type="checkbox"/> GEEN ONDERZOEK MOGELIJK VOOR BEPAALDE CONCLUSIES (opmerkingen op aanvullingsblad)	
IV. <input type="checkbox"/> GEBREK AAN EENHEID VAN UITVINDING (opmerkingen op aanvullingsblad)	



VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN  
INTERNATIONAAL TYPE

Nummer van het verzoek om een nieuwheidsonderzoek

NL 1011501

A. CLASSIFICATIE VAN HET ONDERWERP  
IPC 6 G08G1/01 G08G1/09

Volgens de Internationale Classificatie van octrooien (IPC) of zowel volgens de nationale classificatie als volgens de IPC.

B. ONDERZOCHE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie (classificatie gevolgd door classificatiesymbolen)  
IPC 6 G08G

Onderzochte andere documentatie dan de minimum documentatie, voor dergelijke documenten, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

Tijdens het internationaal nieuwheidsonderzoek geraadpleegde elektronische gegevensbestanden (naam van de gegevensbestanden en, waar uitvoerbaar, gebruikte trefwoorden)

C. VAN BELANG GEACHTE DOCUMENTEN

Categorie °	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
A	EP 0 884 708 A (MANNESMANN AG) 16 December 1998 (1998-12-16) figuur 4 ---	1-58
A	EP 0 715 285 A (MANNESMANN AG) 5 Juni 1996 (1996-06-05) kolom 5, regel 27 - regel 49 ---	1-58
A	US 5 812 069 A (HEIMANN JOSEF ET AL) 22 September 1998 (1998-09-22) kolom 1, regel 53 - kolom 2, regel 10 kolom 3, regel 51 - kolom 4, regel 2 kolom 6, regel 41 - regel 54 -----	1-58

Verdere documenten worden vermeld in het vervolg van vak C.

Leden van dezelfde octrooifamilie zijn vermeld in een bijlage

° Speciale categorieën van aangehaalde documenten

"A" document dat de algemene stand van de techniek weergeeft, maar niet beschouwd wordt als zijnde van bijzonder belang

"E" eerder document, maar gepubliceerd op de datum van indiening of daarna

"L" document dat het beroep op een recht van voorrang aan twijfel onderhevig maakt of dat aangehaald wordt om de publicatiedatum van een andere aanhaling vast te stellen of om een andere reden zoals aangegeven

"O" document dat betrekking heeft op een mondelinge uiteenzetting, een gebruik, een tentoonstelling of een ander middel

"P" document gepubliceerd voor de datum van indiening maar na de ingeroepen datum van voorrang

"T" later document, gepubliceerd na de datum van indiening of datum van voorrang en niet in strijd met de aanvraag, maar aangehaald ter verduidelijking van het principe of de theorie die aan de uitvinding ten grondslag ligt

"X" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet als nieuw worden beschouwd of kan niet worden beschouwd op inventiviteit te berusten

"Y" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet worden beschouwd als inventief wanneer het document beschouwd wordt in combinatie met één of meerdere soortgelijke documenten, en deze combinatie voor een deskundige voor de hand ligt

"&" document dat deel uitmaakt van dezelfde octrooifamilie

Datum waarop het nieuwheidsonderzoek van internationaal type werd voltooid

20 December 1999

Verzenddatum van het rapport van het nieuwheidsonderzoek van internationaal type

Naam en adres van de instantie

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx 31 651 epo nl,  
Fax: (+31-70) 340-3016

De bevoegde ambtenaar

Crechet, P

**VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN  
INTERNATIONAAL TYPE**

Informatie over leden van dezelfde octrooifamilie

Nummer van het verzoek om een nieuwheidsonderzoek  
NL 1011501

In het rapport genoemd octrooigeschrift		Datum van publicatie	Overeenkomend(e) geschrift(en)	Datum van publicatie
EP 0884708	A	16-12-1998	DE 19725556 A	24-12-1998
EP 0715285	A	05-06-1996	DE 19513640 A AT 181440 T DE 59506226 D ES 2132521 T	05-06-1996 15-07-1996 22-07-1999 16-08-1999
US 5812069	A	22-09-1998	DE 19526148 A EP 0755039 A	06-02-1997 22-01-1997