Systemen voor fraudebestendige en privacyvriendelijke kilometerheffing

Wiebren de Jonge

Divisie Wiskunde & Informatica

Vrije Universiteit, Amsterdam

1 Inleiding

Kilometerheffing is een belangrijk en doeltreffend beleidsinstrument dat momenteel volop in de belangstelling staat. Dat en waarom kilometerheffing rechtvaardiger èn effectiever is dan tolheffing m.b.v. electronische tolpoorten wordt hier niet meer uit de doeken gedaan[1]. Noch dat kilometerheffing ook een meer verfijnd beleidsinstrument is dan (verhoging van de) brandstofaccijns, althans als het tarief (ook) afhankelijk wordt gemaakt van de milieu(on)vriendelijkheid van het voertuig. Wel gaan we in dit stuk in op de mogelijkheden voor een goede technische invulling, waarbij we m.n. aandacht zullen besteden aan de belangrijke eisen fraudebestendigheid en privacybescherming.

In hoofdstuk 2 komen positie-gebaseerde systemen aan bod en ook een aantal voor- en nadelen. Mede omdat blijkens de berichtgeving van de afgelopen paar maanden in de media de angst voor aantasting van de privacy een belangrijke rol lijkt te spelen bij de discussie over eventuele invoering van kilometerheffing (KMH), leggen we in dat hoofdstuk de nadruk op de eis van privacybescherming. Bij positie-gebaseerde systemen en bij alle andere tot voor kort bekende (ontwerpen voor) KMH-systemen berust de fraudebestendigheid primair op allerlei vormen van fysieke beveiliging. In hoofdstuk 3 schetsen we een belangrijk deel van de problematiek van fysieke beveiliging in de context van KMH-systemen. Daarna presenteren we in hoofdstuk 4 een nieuwe, relatief simpele en goedkope aanpak, waarbij heel weinig of zelfs geen fysieke beveiliging nodig is. Deze aanpak is bij uitstek geschikt om tegemoet te komen aan de model- en systeemeisen uit het MobiMiles rapport[2]. Tenslotte eindigen we met het geven van een aantal conclusies in hoofdstuk 5.

2 Positie-gebaseerde KMH-systemen

Onder positie-gebaseerde KMH-systemen verstaan we KMH-systemen waarbij a) de KMH-instantie van *buiten* de voertuigen hun posities bepaalt en bijhoudt, of waarbij b) *in* de betrokken voertuigen een kastje van de KMH-instantie wordt geplaatst dat continu positiegegevens ontvangt of zelf continu zijn positie bepaalt[3]. In het eerste geval beschikt de KMH-instantie buiten de voertuigen dus over heel veel privacygevoelige positiegegevens en is er sprake van een ‘volgsysteem’. In het tweede geval is er sprake van een ‘potentieel traceersysteem’, omdat het in een betrokken voertuig aanwezige kastje van of namens de KMH-instantie over heel veel positiegegevens

---

[1] Op de homepage van de auteur (*www.cs.vu.nl/~wiebren*) is meer informatie te vinden over verkeersinformatie- en verkeersheffingssystemen i.h.a. en de voordelen van kilometerheffing t.o.v. tolpoortsystemen, zoals rekeningrijden, i.h.b.

[2] Prof.ir. R. Pieper, “MobiMiles - Bewust op weg”, 10 april 2001. (Zie ook voetnoot 7.)

[3] Met positie bedoelen we hier steeds een absolute positie. (Zie ook voetnoot 8.)

beschikt die in potentie terecht kunnen komen bij (het deel van) de KMH-instantie buiten de voertuigen (zie sectie 2.3). In dit tweede geval maakt een of ander positiebepalingssysteem onlosmakelijk deel uit van de in een betrokken voertuig benodigde apparatuur en behoort dit positiebepalingssysteem tot de tegen fraude te beveiligen componenten van die apparatuur in zo'n voertuig.

Bij positie-gebaseerde KMH-systemen kan de benodigde positiebepaling bijvoorbeeld geschieden m.b.v. GPS, GSM en/of een electronische wegenkaart. Wij gebruiken de tamelijk bekende term GPS (Global Positioning System) in de meer algemene betekenis van GNSS (Global Navigation Satellite System), hoewel strikt genomen het GPS, evenals het nog niet gerealiseerde Europese Galileo systeem, slechts één specifiek voorbeeld van een GNSS is. Omdat het principe van positiebepaling m.b.v. GSM (Global System for Mobile communication) hetzelfde is als m.b.v. één van zijn opvolgers, zoals GPRS (General Packet Radio Service) en UMTS (Universal Mobile Telecommunication System), staat in het navolgende de algemeen bekende term GSM in feite ook voor zulke modernere mobiele telefonie systemen.

In de rest van dit hoofdstuk geven we eerst wat meer informatie over diverse mogelijkheden m.b.t. positiebepaling, gaan we daarna vrij uitgebreid in op het gevaar voor de privacy en noemen we tenslotte nog enkele andere nadelen van positie-gebaseerde KMH-systemen.

2.1 Positiebepaling buiten het voertuig door een GSM netwerk

Bij één aanpak m.b.v. GSM worden de posities van in voertuigen aanwezige mobieltjes continu berekend en bijgehouden door (computers in) het GSM netwerk. Op basis van het verschil in aankomsttijd van een door een mobieltje uitgezonden bericht of signaal bij 3 verschillende *ontvang*masten van het GSM netwerk kan men namelijk vrij goed berekenen waar het mobieltje zich bevindt.

Dit betekent wel dat overal tenminste 3 GSM ontvangmasten binnen het bereik van een mobieltje moeten zijn. Er zijn t.b.v. plaatsbepaling dus veel meer ontvangmasten nodig dan t.b.v. telefoongesprekken, waarvoor één zend- en ontvangmast binnen het bereik al genoeg is. De kosten van de voor KMH extra benodigde infrastructuur zijn in dit geval dus hoog vanwege de extra ontvangmasten, vanwege de benodigde synchronisatie van de tijdklokken op alle ontvangmasten en vanwege het vele rekenwerk dat in het netwerk moet worden uitgevoerd.

2.2 Positiebepaling in het voertuig

Bij een andere, 'gespiegelde' aanpak m.b.v. GSM wordt in elk voertuig de positie bepaald door het mobieltje. Dit gebeurt dan op basis van het verschil in aankomsttijd van door tenminste 3 *zend*masten van het GSM netwerk gelijktijdig uitgezonden signalen.

Bij deze aanpak moet elke plek dus binnen het bereik van tenminste 3 GSM zendmasten vallen en moeten de klokken op de zendmasten gesynchroniseerd worden. In dit geval is er geen grote rekencapaciteit nodig in het netwerk, maar zijn er wel nieuwe mobieltjes nodig die in staat zijn het verschil in aankomsttijd voldoende nauwkeurig te meten en de verdere berekening uit te voeren. Kortom, de extra kosten voor KMH zijn ook bij deze 'gespiegelde' aanpak hoog.

Merk op dat dit gebruik van GSM in wezen hetzelfde is als gebruik van GPS. Alleen bevinden de zenders van de gesynchroniseerde signalen zich bij GPS in de ruimte en bij GSM op aarde. Ook wordt bij GPS met een klein

aantal zenders de hele wereld bestreken, terwijl bij GSM voor een veel kleiner gebied al heel veel zendmasten nodig zijn.

Gebruik van GPS voor KMH biedt t.o.v. gebruik van GSM twee belangrijke voordelen, namelijk dat 1) positiebepaling m.b.v. GPS vooralsnog nauwkeuriger is dan m.b.v. GSM, en dat 2) de voor positiebepaling m.b.v. GPS benodigde infrastructuur (i.e. het stelsel met satellieten) al volledig aanwezig is, terwijl voor positiebepaling m.b.v. GSM nog flink wat extra infrastructuur zou moeten worden aangebracht.

Tenslotte noemen we nog de mogelijkheid om een electronische wegenkaart, al dan niet in samenwerking met GPS of GSM, te gebruiken voor het in een voertuig bepalen van zijn positie. Zeker als hierbij CD-ROM's gebruikt worden, zijn zowel de initiële als de operationele kosten vrij aanzienlijk.

2.3 Het gevaar voor de privacy

Het is evident dat volgsystemen slecht zijn voor de privacybescherming en dat positiebepaling door een GSM netwerk daarom geen reële oplossing voor KMH kan bieden. Maar ook alle andere positie-gebaseerde KMH-systemen leveren wel degelijk een serieus gevaar op voor de privacy! Anders gezegd, als er in elk voertuig een kastje van de KMH-instantie zou komen dat continu positiegegevens ontvangt of zelf continu zijn positie bepaalt, is er alleszins reden voor bezorgdheid over de privacybescherming!

Want zo'n kastje krijgt in het voertuig de beschikking over een schat aan privacy bedreigende gegevens, die het zou kunnen gaan verzamelen en die het zo nu en dan zou kunnen overseinen naar een persoon of organisatie buiten het voertuig. En het heeft, zoals we in deze sectie nog nader zullen beargumenteren, weinig zin om in een wet vast te leggen dat zulke privacy gevoelige gegevens niet mogen worden verzameld en overgeseind naar buiten het voertuig, omdat niet goed te controleren valt of men zich aan zo'n wet houdt!

Immers, het kastje zal zeker een of ander communicatiekanaal moeten hebben voor contact met de buitenwereld. Bijvoorbeeld om een betalingsproces uit te kunnen voeren of om af en toe kilometerstanden over te kunnen sturen naar een bij de KMH betrokken instantie buiten het voertuig. Maar een toegestaan communicatiekanaal kan, zoals elke informaticus weet (of hoort te weten), altijd heimelijk misbruikt worden voor het ongeoorloofd overzenden van allerlei extra informatie.

Bijvoorbeeld kunnen twee gespreksdeelnemers bij het voeren van een publiek gesprek altijd zodanig gebruik maken van verborgen afspraken m.b.t. de timing van hun wederzijdse vragen en antwoorden, dat zij onderling stiekem extra informatie kunnen uitwisselen. Dus onderling toch informatie kunnen uitwisselen die toehoorders bij dat gesprek niet kunnen bemachtigen. Kortom, de privacy kan bij KMH alléén worden gewaarborgd als het kastje van de KMH-instantie helemaal géén positiegegevens of andere privacygevoelige gegevens verstrekt krijgt![4]

Dat er naast wetten ook controles nodig zijn, is recent maar al te duidelijk geworden n.a.v. de rampen in Volendam en Enschede. En dat wetten soms ook overtreden worden door de eigen overheid[5] is voldoende naar voren gekomen bij b.v. de IRT-affaire, het Pikmeer-arrest en recent nog bij het op ongeoorloofde wijze gebruik maken

---

[4] Hoe kilometerheffing dan toch kan worden gerealiseerd wordt later duidelijk gemaakt in hoofdstuk 4. Zie m.n. sectie 4.1.

[5] Zeg, door misschien wel goedwillende, maar soms toch 'wat al te enthousiaste' of juist lakse overheidsdienaren.

van DNA dat afgenomen werd van een officieel nog niet verdachte persoon via een door de politie aangeboden kopje koffie. Er is dus voldoende reden om niet volledig blind te varen op de eigen overheid[6].

Uit bovenstaande kan de conclusie getrokken worden dat positie-gebaseerde KMH-systemen géén goede oplossing bieden voor de gewenste privacybescherming. Eigenlijk zou dat al voldoende reden moeten zijn om voor een KMH-systeem op een andere grondslag te kiezen. Desalniettemin geven we hieronder ten overvloede een aantal andere nadelen kort weer.

2.4 Enkele andere nadelen

Ook op de kosten en de fraudebestendigheid van positie-gebaseerde KMH-systemen valt het nodige aan te merken. Bijvoorbeeld geldt dat het gebruikte positiebepalingssysteem i.h.a. vrij makkelijk misleid kan worden. Denk hierbij b.v. aan het afschermen van de antenne van het mobieltje of van de GPS ontvanger. Maar ook het naar de eigen antenne toesturen van valse signalen behoort tot de mogelijkheden tot fraude. Een ander belangrijk nadeel is dat de fraudebestendigheid van positie-gebaseerde KMH-systemen tot nu toe altijd primair gebaseerd is op fysieke beveiliging, wat leidt tot hoge kosten, matige fraudebestendigheid en minder flexibiliteit. Omdat de fraudebestendigheid ook bij alle andere tot voor kort bestaande (ontwerpen voor) KMH-systemen primair berust op fysieke beveiligingsmaatregelen, komt het onderwerp fysieke beveiliging in het volgende hoofdstuk wat uitgebreider aan bod.

3 Fysieke beveiliging

Voor het fraudebestendig maken van een KMH-systeem kan men gebruik maken van allerlei logische en fysieke beveiligingsmaatregelen. Bij alle tot voor kort bestaande (ontwerpen voor) KMH-systemen spelen vooral fysieke beveiligingsmaatregelen een grote rol. In dit hoofdstuk geven we eerst kort enige verduidelijking van de begrippen logische en fysieke beveiliging. Daarna komen een aantal aspecten van fysieke beveiliging aan bod die van belang zijn voor het onderling vergelijken van KMH-systemen en ook voor het maken van keuzen bij het ontwerpen van een geschikt KMH-systeem.

3.1 Logische en fysieke beveiliging

Voor het bereiken van een bepaalde mate van fraudebestendigheid moet men een systeem vanzelfsprekend beveiligen tegen allerlei fraudemogelijkheden. Zoals gezegd, kan dat met fysieke beveiligingsmaatregelen, maar ook met maatregelen op een logisch (i.e., niet-fysiek) niveau, zoals b.v. juridische, organisatorische en procedurele maatregelen.

Denk bij fysieke beveiliging aan het zodanig fysiek uitvoeren van (componenten van) het systeem dat (een serieuze poging tot) fraude moeilijker wordt. Bijvoorbeeld is een bankkluis fysiek zodanig uitgevoerd dat het moeilijker is om hem in z'n geheel mee te nemen en/of om er geld uit te halen dan in geval van een sigarenkistje of de eerste de beste kassa.

---

[6] Of wat explicieter en omslachtiger geformuleerd: er is in de praktijk gebleken dat een kritische, enigszins sceptische houding met misschien zelfs enig gezond wantrouwen t.o.v. (beloftes van) de eigen overheid niet onverstandig is. ☺

Alle andere beveiligingsmaatregelen scharen wij onder de noemer van logische beveiliging. De voor dit stuk belangrijkste vorm betreft de combinatie van fraudedetectie en juridische maatregelen (zeg maar, strafwetten). De kans op ontdekking en straf maken (pogingen tot) fraude minder aantrekkelijk. De genoemde combinatie draagt dus indirect bij aan de fraudebestendigheid, d.w.z. aan de verlaging van de kans op uiteindelijk succes bij een fraudepoging. Fysieke beveiligingsmaatregelen leveren een meer directe bijdrage.

3.2 Aanzienlijke kosten en nooit perfect

Elke fysieke beveiliging kan doorbroken worden. Er is bij fysieke beveiliging dan ook altijd sprake van een soort van wapenwedloop. Elke maatregel leidt tot een tegenmaatregel, die weer leidt tot een tegen-tegenmaatregel, wat weer leidt tot een tegen-tegen-tegenmaatregel, etcetera, etcetera. Dit alles leidt er toe dat de kosten van fysieke beveiliging i.h.a. aanzienlijk zijn. Ook de noodzaak om zo nu en dan d.m.v. een fysieke inspectie te controleren of een maatregel misschien doorbroken is, leidt tot hoge kosten (zie ook sectie 3.4).

Een systeem met meerdere te beveiligen componenten biedt i.h.a. meerdere aangrijpingspunten voor pogingen tot fraude en een slechtere fraudebestendigheid dan een systeem met slechts één te beveiligen component. Het per aparte component fysiek beveiligen van alle voor de fraudebestendigheid essentiële componenten maakt een systeem met meerdere componenten al gauw veel te duur. Bovendien wordt het bereikte beveiligingsniveau altijd bepaald door de zwakste schakel in het geheel.

3.3 Zoveel mogelijk in één kastje?

In een poging de beveiligingskosten in de hand te houden en het aantal aangrijpingspunten voor fraude te verkleinen kan men de te beveiligen componenten natuurlijk zoveel mogelijk concentreren in één fysiek beveiligd kastje. Dit is b.v. gedaan bij het Zwitserse KMH-systeem voor zware vrachtwagens. Echter, ook het opnemen van veel of zelfs alle componenten in één fysiek beveiligd kastje biedt i.h.a. weinig soelaas. Immers, de ‘wapenwedloop’ maakt ook dat ene kastje al gauw (te) duur, terwijl nieuwe problemen de kop op kunnen steken.

Eén zo’n probleem betreft fraudegevoeligheid en heeft te maken met het feit dat er dan op betrouwbaarheid geselecteerd en gecertificeerd personeel nodig is voor b.v. onderhoud en reparatie. Want juist dat personeel vormt een groot gevaar voor de fraudebestendigheid!

Een ander probleem is dat het systeem aanzienlijk verliest aan flexibiliteit. Want als men het later wil uitbreiden en er een component moet worden toegevoegd, kan dat weer allerlei problemen opleveren. Bijvoorbeeld wordt een later gewenste uitbreiding dan heel duur, omdat deze alleen door gecertificeerd personeel mag worden uitgevoerd. Of zelfs bijna onmogelijk, omdat de nieuwe component niet meer in het kastje past en men dan nieuwe kastjes zou moeten ontwerpen, produceren en plaatsen.

3.4 Benodigde inspecties kostbaar en/of ontoereikend

In geval van fysieke beveiliging zijn altijd fysieke inspecties nodig om te controleren of er mogelijk met de fysieke beveiliging is geknoeid. Zulke inspecties zijn bij KMH-systemen zeer kostbaar en/of ontoereikend. Als bijvoorbeeld de inspectie plaatsvindt tijdens de jaarlijkse APK, kunnen ‘handige jongens’ (m/v) zich de overige 364 dagen per jaar heerlijk uitleven, zolang ze maar bij de jaarlijkse APK ogenschijnlijk ongeschonden apparatuur kunnen laten zien. Maar het op willekeurige tijdstippen en plaatsen bij passerende voertuigen uitvoeren van

visuele inspecties op de KMH-apparatuur in die voertuigen is zeer kostbaar en ook nog eens slecht voor de doorstroming van het verkeer, omdat men de voertuigen dan eerst zal moeten aanhouden.

3.5 De les m.b.t. KMH-systemen

De lering die uit bovenstaande getrokken kan worden, is dat de noodzaak voor *fysieke beveiliging* het beste *geminimaliseerd* kan worden en dat *steekproefsgewijze controles* bij voorkeur *op efficiënte wijze* en dus o.a. *zonder enige hinder* voor het verkeer uitgevoerd moeten kunnen worden op willekeurig gekozen plaatsen en tijdstippen. Want des te goedkoper steekproefsgewijze controles kunnen worden uitgevoerd, des te beter intensieve fraudedetectie (i.e. logische beveiliging) in de plaats kan treden van dure fysieke beveiligingsmaatregelen.

3.6 Positie-gebaseerde vs. meer traditionele KMH-systemen

Zoals in de inleiding al is gezegd, berust de fraudebestendigheid van alle tot voor kort bekende (ontwerpen voor) KMH-systemen primair op allerlei vormen van fysieke beveiliging. Omdat positie-gebaseerde systemen geen goede oplossing bieden voor de gewenste privacybescherming, zou je misschien mogen verwachten dat juist de meer traditionele, aan tachografen en taximeters verwante KMH-systemen met fysiek beveiligde tellers in de belangstelling staan. Dat is echter niet het geval, want de laatstgenoemde systemen krijgen juist weinig aandacht, althans in de publiciteit.

Een mogelijke verklaring voor dit laatste is dat de praktijk al heeft uitgewezen dat tachografen en taximeters vooralsnog te fraudegevoelig en/of te duur zijn om soortgelijke apparatuur massaal te (willen) gaan gebruiken voor KMH. Maar als dat inderdaad zo is, dan komt dat waarschijnlijk juist doordat de fraudebestendigheid bij zulke systemen primair berust op fysieke beveiliging. Kortom, dan is dus wel de geringe aandacht voor meer traditionele KMH-systemen verklaard, maar nog allerminst waarom positie-gebaseerde KMH-systemen momenteel veel meer aandacht krijgen, want ook bij die systemen is de beveiliging primair van fysieke aard. Eén noemenswaardig punt is echter wel dat de montagekosten bij positie-gebaseerde systemen eventueel beduidend lager kunnen zijn, althans als de positiebepalingsapparatuur opgenomen kan worden in de On-Board Unit.

De enige andere verklaring die de auteur rest, is dat de materie vaak nog onvoldoende begrepen wordt. Ten eerste onderschat men bij positie-gebaseerde systemen vaak het gevaar voor de privacy, eenvoudigweg omdat men niet bekend is met de problematiek van verborgen communicatie (i.e. het gebruik van zogenoemde ‘covert channels’), zoals kort geschetst in sectie 2.3. Ten tweede is men i.h.a. vaak (te) enthousiast en (te) optimistisch over oplossingen waarbij nieuwe technologie gebruikt wordt, zoals b.v. een GPS. Bijvoorbeeld denkt men in dit geval misschien dat het opnemen van een GPS ontvanger in een beveiligd kastje de oplossing is voor b.v. de problemen die kleven aan het gebruik van een fysiek beveiligde sensor op de aandrijfas, en onderschat men eventueel de (vergelijkbare) mogelijkheden tot manipulatie in geval van gebruik van een GPS.

Hoe dan ook, het is de auteur niet helemaal duidelijk waarom de aan tachograaf en taximeter verwante KMH-systemen beduidend minder aandacht (lijken te) krijgen dan positie-gebaseerde KMH-systemen. Dat neemt niet weg dat de auteur hoopt dat dit artikel in ieder geval een nuttige bijdrage zal leveren aan het maken van betere afwegingen bij het kiezen en/of ontwerpen van een geschikt KMH-systeem.

4 Aangifte-gebaseerde KMH-systemen

De essentie van een nieuwe, in 1998 ontwikkelde en inmiddels aangifte-gebaseerd genoemde aanpak[7] is dat:

- de betrokken mobilisten *zelf verantwoordelijk* zijn voor en ook *zelf controle* hebben over het verzamelen, bijhouden en doorgeven van de voor KMH benodigde informatie, en
- die mobilisten *continu aangifte* moeten doen van elke relevante gebeurtenis en dus m.n. van elk stukje afgelegde afstand, en
- hun aangiften door of namens de KMH-instantie *steekproefsgewijs* op juistheid worden *gecontroleerd*, en
- deze steekproefsgewijze controles *tijdens hun verkeersdeelname* m.b.v. telecommunicatie *vanaf enige afstand* van hun voertuig (dus zonder het verkeer te hinderen) *efficiënt* kunnen worden uitgevoerd.

Bij deze aanpak kan de fysieke beveiliging in hoge mate worden geminimaliseerd, omdat de gewenste mate van fraudebestendigheid primair bereikt wordt d.m.v. efficiënte fraudedetectie (i.e. efficiënte logische beveiliging).

4.1 Electronische aangiften

Natuurlijk hoeven de mobilisten niet zelf bij elke afgelegde meter handmatig een formuliertje in te vullen, maar wordt het samenstellen en indienen van hun aangiften geautomatiseerd en doet bepaalde apparatuur dan steeds electronische aangifte namens de mobilist. In de aangiften moet b.v. melding worden gemaakt van de afgelegde afstand en het toe te passen tarief. Maar beslist *niet* van de absolute positie van het betreffende voertuig![8]

Voor het verkrijgen van de voor aangiften benodigde gegevens over afgelegde afstand kan een automobilist bijvoorbeeld gebruik laten maken van een signaal opgewekt door een sensor op de aandrijfas of door het ABS-systeem. Maar zulke afstandsgegevens kunnen desgewenst ook berekend en toegeleverd worden door een processor die verbonden is met of deel uitmaakt van een positiebepalingssysteem!

Om eventuele misverstanden zoveel mogelijk te voorkomen benadrukken we hier maar meteen dat er, ook als er bij de aangifte-gebaseerde aanpak wel degelijk gebruik wordt gemaakt van een positiebepalingssysteem, tenminste twee grote en belangrijke verschillen zijn met de eerder besproken positie-gebaseerde systemen.

Het eerste belangrijke verschil betreft het feit dat de mobilist bij een aangifte-gebaseerd KMH-systeem *zelf controle* heeft over het doorgeven van informatie aan de KMH-instantie en dat hij of zij er dus zelf op kan toezien dat de privacy *niet* in gevaar komt. Want natuurlijk mag de mobilist de hem of haar eventueel ter beschikking staande positiegegevens voor zichzelf houden en wordt hij of zij zeker niet verplicht om zulke (mogelijk) privacygevoelige gegevens stelselmatig door te geven aan de KMH-instantie. Dus zelfs àls voor het bepalen van afgelegde afstanden in het voertuig gebruik wordt gemaakt van positiegegevens, dan worden toch echt alléén de uit die positiegegevens afgeleide afstanden benut voor de aangiften aan de KMH-instantie! Met andere woorden, bij een aangifte-gebaseerd systeem is een positiebepalingssysteem nooit meer dan een hulpmiddel van en voor de mobilist, dat hij of zij eventueel kan (laten) gebruiken om de door hem of haar afgelegde afstanden en/of het

---

[7] Het MobiMiles rapport is in belangrijke mate gebaseerd op de hier (in dit hoofdstuk, maar ook in de rest van dit artikel) beschreven kennis. Door diverse omstandigheden is het MobiMiles rapport echter eerder verschenen (zie ook voetnoot 2).

[8] Melden van het *soort* tariefgebied waarin een stukje afstand is afgelegd (zeg maar, een 'relatieve positie'), kan eventueel wel. Maar zelfs als de tarieven plaatsafhankelijk zijn, is dat nog niet per se noodzakelijk! We gaan hier niet verder op in.

van toepassing zijnde soort tariefgebied te (laten) berekenen t.b.v. zijn of haar aangiften. (En natuurlijk ook voor andere doeleinden, zoals b.v. navigatie.)

Het tweede belangrijke verschil betreft enkele gevolgen van het feit dat bij een aangifte-gebaseerde aanpak elke aangifteplichtige natuurlijk *zelf verantwoordelijk* gesteld wordt en blijft voor het juist functioneren van de door hem of haar ingeschakelde hulpmiddelen, d.w.z. voor het juist functioneren van alle componenten behalve de chip(s) van de KMH-instantie.

Eén gevolg daarvan is dat alle door een aangifteplichtige ingeschakelde hulpmiddelen voor het geautomatiseerd samenstellen (en indienen) van zijn aangiften, zoals b.v. een GPS ontvanger of een sensor op de aandrijfas, niet per se beveiligd hoeven te worden tegen pogingen tot fraude. Want bij een aangifte zijn alleen de verantwoordelijke afzender en de juistheid van belang, terwijl i.h.a. de wijze waarop de aangifte al dan niet met hulpmiddelen tot stand gekomen is, er niet toe doet. Dus heeft bij een aangifte-gebaseerd KMH-systeem manipulatie met een hulpmiddel, zoals b.v. manipulatie met een positiebepalingssysteem door afscherming of door toesturen van valse signalen, weinig of geen zin. Want enerzijds blijft men hoe dan ook verantwoordelijk voor de inhoud van de aangiften en kan men ook nog steeds betrapt worden op een valse aangifte. En anderzijds zal er bovendien vaak een makkelijker manier zijn om een valse aangifte samen te stellen dan via manipulaties met facultatief te gebruiken hulpmiddelen. Kortom, alle facultatief te gebruiken hulpmiddelen kunnen buiten het beveiligde domein vallen, hetgeen gunstig is voor de flexibiliteit (en dus de ‘toekomstvastheid’) van het systeem en voor het laag houden van de initiële en operationele kosten. (Denk bij de operationele kosten nu ook aan het feit dat als er voor minder componenten fysieke beveiliging nodig is, er dan ook voor minder componenten fysieke inspecties nodig zullen zijn.)

Een tweede gevolg betreft een andere substantiële bijdrage aan het laag kunnen houden van de operationele kosten. Want de genoemde verantwoordelijkheid van de gebruiker maakt het niet alleen volkomen vanzelfsprekend dat hij of zij zelf moet opdraaien voor de onderhouds- en reparatiekosten van alle door hem of haar ingeschakelde hulpmiddelen, maar zorgt er vooral ook voor dat er veel minder problemen (denk b.v. aan juridische geschillen) zullen ontstaan in geval van onjuist functionerende componenten. Natuurlijk zal bij elk systeem de gebruiker verantwoordelijk worden gesteld voor het in de gaten houden van het correct functioneren van alle apparatuur in zijn voertuig en zal een gebruiker verplicht worden om zodra hij of zij een mogelijke afwijking ontdekt, daarvan op een voorgeschreven wijze melding te maken bij de KMH-instantie. Maar bij een aangifte-gebaseerd systeem is er veel minder kans op geschillen over de periode van verkeerd functioneren voorafgaande aan de melding. Want als een verkeerd werkend hulpmiddel inmiddels al geleid heeft tot zodanige aangiften dat een te hoog bedrag aan KMH is of nog moet worden betaald, dan kan men de KMH-instantie daar achteraf niet zomaar voor aansprakelijk stellen. Terwijl dat bij de andere systemen juist veel makkelijker wel lijkt te kunnen. Immers, bij die systemen maken de hulpmiddelen onlosmakelijk deel uit van de door de KMH-instantie verkochte of verstrekte apparatuur en/of lijken de fysiek beveiligde kastjes om de hulpmiddelen heen het onontkoombaar te maken dat de KMH-instantie op z’n minst mede aansprakelijk zal zijn voor het juist functioneren van hetgeen in zo’n beveiligd kastje verborgen zit.

Tenslotte merken we nog op dat de electronische aangiften behalve de eerder al genoemde afgelegde afstand en het toe te passen tarief eventueel ook informatie kunnen of moeten bevatten over allerlei andere variabelen die van belang zijn voor (de controle op) een juiste berekening van de verschuldigde heffing. Denk hierbij b.v. aan

voertuigtype (merk, bouwjaar, motortype, versnellingsbaktype, etc.), snelheid, acceleratie, toerental, aantal inzittenden, brandstofsoort, brandstofverbruik, tijdstip, e.d. Maar denk ook aan andere gegevens, zoals b.v. het laatst gepasseerde tolpunt en het daar verschuldigde tolbedrag of b.v. het nu toegepaste parkeertarief en het tijdstip waarop de nu lopende parkeerperiode begon (zie ook sectie 4.10).

4.2 Indiening van aangiften

De aangiften kunnen op twee manieren aan de KMH-instantie beschikbaar worden gesteld. Ofwel door de aangiften continu te verzenden via een zender met een mogelijk zelfs zeer beperkt bereik[9]. Ofwel door ze naar een tijdens verkeersdeelname in het voertuig aanwezige chip van de KMH-instantie te sturen, die op z'n minst fungeert als een soort van beveiligde brievenbus. Deze brievenbus hoeft eventueel alleen de laatste zoveel aangiften vast te houden, b.v. alleen de aangiften m.b.t. de laatste 5 kilometer.

Essentieel is dat men een eenmaal gedane aangifte niet uit deze brievenbus kan terugnemen, maar dat de KMH-instantie de laatste zoveel aangiften er wel m.b.v. telecommunicatie uit kan halen. Dus, als iemand merkt dat hij of zij gecontroleerd gaat worden, kan hij of zij niet gauw even een valse aangifte terugnemen om die nog snel even te corrigeren.

De genoemde chip met software kan gezien worden als een electronische vertegenwoordiger van de KMH-instantie, die naast het in ontvangst nemen van aangiften eventueel ook nog andere taken kan vervullen namens de KMH-instantie.

4.3 Steekproefsgewijze controles van aangiften

De KMH-instantie kan vrij makkelijk steekproefsgewijs controleren of de administratie in een voertuig correct wordt bijgehouden, d.w.z. of het beeld zoals weergegeven in aangiften overeenkomt met de werkelijkheid.

Stel bijvoorbeeld dat de bijgehouden administratie alleen de kilometerteller betreft en dat in aangiften alleen kilometerstanden worden vermeld. Dan kan de juistheid van aangiften steekproefsgewijs worden gecontroleerd door op twee opeenvolgende punten A en B langs een weg de kilometerstand op te vragen en te controleren of het verschil tussen de twee opgevraagde kilometerstanden overeenkomt met de afstand tussen A en B. (Zo ja, dan is de kilometerteller op het betreffende traject correct opgehoogd.) Of men kan de snelheid van passerende voertuigen meten en deze vergelijken met de snelheid die afgeleid kan worden uit de aangiften in hun brievenbus[10]. Een derde mogelijkheid is dat de chip van de KMH-instantie niet louter als brievenbus fungeert, maar zelf op basis van de binnenkomende aangiften steeds de bijbehorende snelheid uitrekent. Dan zal de chip dit gegeven bij controles ter beschikking stellen en wordt bij een controle de buiten het voertuig gemeten snelheid simpelweg vergeleken met de snelheid volgens de chip van de KMH-instantie.

In het algemene geval, waarin ook andere gegevens dan alleen de kilometerstand kunnen worden bijgehouden, bestaat een controle dus uit het doen van onafhankelijke metingen en/of waarnemingen m.b.t. het gecontroleerde

---

[9] B.v. kan het bereik slechts 100 meter zijn. De bijna continue stroom aangiften wordt dan lokaal 'rond gestrooid'. Hoewel deze variant m.n. vanuit het oogpunt van fraudebestendigheid heel interessant is, gaan we er hier niet verder op in.

[10] Snelheid en afgelegde weg staan met elkaar in verband en kunnen uit elkaar worden afgeleid. B.v. wordt dus gecontroleerd of de kilometerstand wel in het bij de werkelijke snelheid van het voertuig passende tempo wordt opgehoogd.

voertuig en het vergelijken van de verkregen resultaten met de corresponderende aangifte(n). Hieronder valt ook het vergelijken met door de chip van de KMH-instantie op basis van die aangiften berekende waarde(n). Voor de bedoelde controles is een of andere vorm van telecommunicatie nodig, omdat de buiten en de binnen het voertuig vastgestelde gegevens eerst bijeen moeten worden gebracht op de plaats van vergelijking, alvorens ze met elkaar vergeleken kunnen worden. Voor het gemak veronderstellen we hier dat dit de plaats is waarvandaan de onafhankelijke metingen en/of waarnemingen worden verricht.

Om de authenticiteit van zowel de afzender als de inhoud van de vanuit het voertuig verstrekte rapportage te kunnen controleren en bewijzen, moet de chip van de KMH-instantie de rapportage met de te verstrekken informatie (berekend op basis van of direct afkomstig uit binnengekomen aangiften) natuurlijk voorzien van een digitale handtekening. Deze handtekening hoeft slechts onderscheid tussen èchte en valse chips mogelijk te maken en hoeft dus niet per se uniek te zijn voor elke chip. Echter, het is niet voldoende om buiten het voertuig alleen te kunnen bepalen dat met een echte chip van de KMH-instantie werd gecommuniceerd. Bij een controle is het namelijk beslist ook nog van belang te weten (en later zelfs te kunnen bewijzen!) dat met zo'n chip in het juiste, aan controle onderworpen voertuig wordt (resp. werd) gecommuniceerd. Hiertoe kan men gebruik maken van gerichte communicatie.

Bijvoorbeeld kan het vanaf een controlepunt naar een bepaald voertuig te zenden verzoek om informatie overgedragen worden via een smalle bundel electromagnetische golven gericht op een passende ontvanger in of aan dat voertuig. Door in dit verzoek b.v. een random getal op te nemen en de chip van de KMH-instantie dit getal te laten vermelden in zijn (in reactie op dat verzoek) terug te sturen rapportage, kan worden vastgesteld dat deze rapportage inderdaad het met de smalle bundel 'aangewezen' voertuig betreft.

De bewijsvoering kan dus op een soortgelijke wijze plaatsvinden als bij de huidige snelheidscontroles. Bij de huidige snelheidscontroles worden een bundel electromagnetische golven (radar of laser) en een camera beiden langs dezelfde lijn gericht. Omdat alleen gebruik wordt gemaakt van zorgvuldig gecertificeerde en geijkte controle-apparatuur, strekt een foto van het gecontroleerde voertuig waarop de gemeten snelheid ook vermeld staat, tot bewijs. Op soortgelijke wijze kan m.b.v. gecertificeerde apparatuur een foto van een gecontroleerd voertuig gemaakt worden met daarop b.v. vermeld de onafhankelijk gemeten snelheid èn de vanuit het voertuig door de chip van de KMH-instantie gerapporteerde snelheid.

E.e.a. zou eventueel ook nog wat meer gevisualiseerd kunnen worden door op het door de bundel aangewezen voertuig één of meerdere lampjes op te laten lichten. Bijvoorbeeld zou het laten oplichten van een lampje de controleur een extra mogelijkheid geven om te zien of hij de bundel goed op het juiste voertuig heeft gericht en op de foto zichtbaar maken dat er maar één voertuig door de bundel werd bestreken. Meerdere voertuigen op dezelfde foto hoeft dan dus geen probleem te zijn.

Als bij een controle blijkt dat er iets mis is met de aangifte(n) òf als er niet gereageerd wordt op het verzoek (of beter gezegd, de opdracht) om informatie te verstrekken, dan wordt er natuurlijk overgegaan tot één van de welbekende tegenmaatregelen, zoals b.v. een aanhouding voor nadere inspectie of het vaststellen van de identiteit van het voertuig. Dit laatste kan eventueel 'ouderwets' gedaan worden door het maken van een foto van het kenteken, maar natuurlijk ook m.b.v. Electronische Voertuig Identificatie (EVI). De verkregen identiteit kan b.v. gebruikt worden voor het sturen van een opdracht om spoedig te verschijnen voor nadere inspectie of eventueel zelfs voor het direct sturen van een bon.

Merk op dat het bij de geschetste aanpak zelfs bij controles niet per se nodig is om meteen het kenteken of een andere identificatie te gebruiken. Pas bij verdenking van fraude wordt nadere identificatie noodzakelijk! Bij een aangifte-gebaseerde aanpak kan dus een uitstekende privacybescherming worden geboden.

Merk ook op dat men door manipulatie met hulpmiddelen, zoals b.v. sensor(s) en positiebepalingssysteem, altijd in staat is om bij een in het voertuig aanwezige chip van de KMH-instantie een vals beeld op te wekken. Dat geldt niet alleen voor aangifte-gebaseerde, maar ook voor alle andere systemen! Daarom kan een chip van de KMH-instantie nooit (dus bij geen enkel systeem!) geheel zelfstandig controleren of alle relevante apparatuur in het betreffende voertuig correct werkt en is er voor een werkelijk goede controle altijd onafhankelijk vastgestelde informatie van buiten het voertuig nodig[11]. Dit essentiële punt ligt mede ten grondslag aan de aangifte-gebaseerde aanpak. Want als men toch steekproefsgewijs moet controleren of het eindresultaat van alle gegevensverwerking door de chip van de KMH-instantie wel overeenstemt met de werkelijkheid, dan geldt: a) dat men dat dan maar beter op een efficiënte manier (zoals m.b.v. telecommunicatie) kan doen, en b) dat daarmee[12] dan ook meteen het belang afneemt van fysieke beveiligingsmaatregelen die bedoeld zijn om af (proberen!) te dwingen dat de chip van de KMH-instantie uitsluitend correcte invoer aangeleverd krijgt. Aldus vormt het zojuist genoemde essentiële punt in feite een kiem tot het kunnen bereiken van hoge fraudebestendigheid tegen relatief lage kosten.

Kortom, de mogelijkheid om steekproefsgewijs controles *op enige afstand* van passerende voertuigen uit te voeren m.b.v. telecommunicatie met de chip in het voertuig biedt een aantal belangrijke voordelen t.o.v. de meer gebruikelijke fysieke inspecties. Ten eerste zijn de bedoelde controles veel *efficiënter*, oftewel *goedkoper*, omdat ze makkelijk te automatiseren en dus veel minder bewerkelijk zijn. Controles op vaste plaatsen kunnen eventueel zelfs volledig geautomatiseerd worden! Door de lage kosten kunnen controles veel *intensiever* plaatsvinden, zodat elk voertuig makkelijk meerdere keren per jaar gecontroleerd kan worden i.p.v. slechts een enkele keer per jaar, zoals b.v. slechts één keer per jaar bij de Algemene Periodieke Keuring (APK). Ook kunnen de bedoelde controles veel beter *bij verrassing* worden uitgevoerd. Denk hierbij o.a. ook aan mobiele controles vanuit rijdende patrouillewagens of vanuit overvliegende patrouillevliegtuigen of -helicopters. En vanzelfsprekend geldt: hoe meer verrassing, hoe beter (i.e. effectiever). Bijvoorbeeld zijn verrassingscontroles veel *effectiever* tegen fraude dan controles op geplande momenten, zoals b.v. APK's[13]. Tenslotte benadrukken we nog eens dat zulke controles *zonder hinder* voor het verkeer uitgevoerd kunnen worden *tijdens verkeersdeelname*, dus terwijl de KMH-apparatuur in het voertuig gewoon *in werking* (!) is.

4.4 Informatieverstrekking t.b.v. het betalingsproces

Alleen bij betaling in het voertuig of bij overzending van informatie m.b.t. het totaal verschuldigde bedrag naar de KMH-instantie buiten het voertuig moet er natuurlijk een of andere directe of indirecte identificatie, zoals

---

[11] Bij een werkelijk goed controleproces kan men zich dus *nooit* beperken tot het aan de chip vragen of alles goed gaat!

[12] In dubbel opzicht, want punt b volgt enerzijds direct (d.w.z. ook los van punt a) uit het voorgaande en anderzijds ook nog eens indirect, omdat punt b natuurlijk juist door uitvoering van punt a in versterkte mate zal opgaan.

[13] Bijvoorbeeld is het mogelijk vóór een APK correcte banden te monteren en die banden direct ná de keuring weer te vervangen door ongeoorloofde exemplaren.

b.v. een persoonsnummer, bankrekeningnummer of kenteken, worden verstrekt om aan te geven welke persoon of organisatie zich verantwoordelijk heeft gesteld voor de betaling van het verschuldigde bedrag. Hoewel er technieken zijn om ook bij deze gegevensverstrekking te zorgen voor goede privacybescherming, lijkt dat bij de hier beschreven variant niet eens echt nodig. Want als de mobilist zelf invloed uit kan oefenen op het moment van verzending, zal het af en toe versturen van zo'n bericht, zeg eens per maand, nauwelijks enige inbreuk op de privacy met zich mee brengen.

Let wel, als de aangiften informatie over het gehanteerde tarief en/of het soort tariefgebied bevatten, dan is deze laatstgenoemde informatie in veel gevallen alleen nodig voor controles. Dus hoeft t.b.v. het betalingsproces in die gevallen alleen maar informatie over het totaalbedrag geleverd te worden aan de KMH-instantie en is uitsplitsing naar b.v. de soorten tariefgebieden beslist niet noodzakelijk!

Tenslotte merken we hier nog op dat het i.h.a. beter is om zoveel mogelijk gebruik te maken van monotone tellers, d.w.z. tellers die alléén kunnen stijgen of alléén kunnen dalen. We raden b.v. aan om een heffingsteller bij te houden die steeds dóórloopt (net zoals b.v. een electriciteitsmeter of kilometerteller) en die na betaling dus *niet* (zoals b.v. een zogeheten dagteller in een auto) teruggezet wordt op nul!

Als de heffingsteller wèl bij elke betaling teruggezet wordt op nul, gaat namelijk nuttige informatie verloren. Deze nuttige informatie kan behouden worden door in plaats van één op- en neergaande teller twee monotone tellers bij te houden. In ons voorbeeld dus één teller die cumulatief het totaal van alle verschuldigde bedragen bijhoudt, en één teller die cumulatief het totaal van alle betaalde bedragen bijhoudt. De daardoor behouden informatie is m.n. nuttig voor het bereiken van een betere fraudebestendigheid. Het is vanuit het oogpunt van fraudebestrijding nog beter om alléén de eerstgenoemde cumulatieve teller in het voertuig bij te houden! Want fraude door in het voertuig op slinkse wijze de tweede cumulatieve teller ten onrechte op te hogen is dan principieel onmogelijk. Merk op dat betaling in het voertuig i.h.a. dus onveiliger is dan betaling buiten het voertuig (zie ook de volgende sectie).

4.5 Betaling

Een simpele, goedkope en veilige oplossing is om de betaling buiten het voertuig plaats te laten vinden. De informatie t.b.v. het betalingsproces (nl. het cumulatieve bedrag en een identificatie) wordt dan af en toe[14] overgestuurd naar de KMH-instantie buiten het voertuig. De betaling kan dan via bestaande infrastructuur plaatsvinden. Denk hierbij b.v. aan automatische afschrijving van een bankrekening. Vanzelfsprekend kunnen t.b.v. de inning allerlei regelingen bedacht en toegepast worden. Bijvoorbeeld m.b.t. in zekere mate gespreide betaling, zoals b.v. gebruikelijk is bij de betaling voor water, gas en electriciteit of bij de betaling voor met een creditcard gedane uitgaven.

Natuurlijk kan men de betaling eventueel ook in het voertuig laten plaatsvinden m.b.v. bijvoorbeeld een pinpas, chipknip, creditcard, contactloze smartcard of een mobieltje. Daartoe moeten deze middelen in contact kunnen treden met de chip die namens de KMH-instantie het totaal verschuldigde bedrag in het voertuig bijhoudt.

Als de daartoe benodigde apparatuur, zoals b.v. een pinpas- of chipknipterminal, alléén voor betaling gebruikt zou worden, lijkt dit géén aantrekkelijke optie. Want dan worden niet alleen heel veel (n.l. in elk voertuig één)

---

[14] Bijvoorbeeld eens per maand of bij elk bezoek aan een benzinestation.

extra aangrijpingspunten voor pogingen tot fraude geïntroduceerd[15], maar wordt ook onnodig veel geld besteed aan deze apparatuur. Onnodig, want het kan immers prima zonder! Kortom, het lijkt in dit geval slimmer te kiezen voor het zo nu en dan naar de KMH-instantie sturen van een ondertekende boodschap met daarin het cumulatief verschuldigde bedrag en een passende identificatie.

Maar in bepaalde gevallen kan de extra uitgave voor zulke apparatuur wel degelijk verantwoord of zelfs aantrekkelijk zijn. Denk b.v. aan een draadloze (zeg, een Bluetooth of infrarood) verbinding voor het in contact kunnen treden met een mobieltje. Want dan kan o.a. de display en het toetsenbord (of fraaier nog, de spraakinterface) van het mobieltje benut worden als gebruikersinterface! Of denk b.v. aan apparatuur t.b.v. het gebruik van een contactloze smartcard. Want een smartcard kan, net als een mobieltje, eventueel ook geschikt gemaakt worden voor o.a.: 1) de betaling voor openbaar vervoer, en/of 2) het dienen als rijbewijs of als puntenrijbewijs, en/of 3) het dienen als sleutel voor toegang tot voertuigen, en/of 4) het leveren van bepaalde informatie over de gebruiker, zoals b.v. de door hem of haar gewenste instelling van stoel, stuur, spiegels, e.d. in een bepaalde auto.

In principe kan een draadloze (zeg, Bluetooth of infrarood) verbinding gebruikt worden voor het in contact komen met diverse andere apparatuur. Zo'n verbinding kan dus (eventueel later pas) gebruikt worden om in contact te komen met b.v. een smartcardlezer en/of een mobieltje, maar ook met b.v. de toerenteller en/of brandstofverbruiksmeter van het voertuig en/of een door de autofabrikant in het dashboard opgenomen gebruikersinterface. Daarom lijkt het verstandig te overwegen om de in elk voertuig benodigde apparatuur òfwel a) van het begin af aan zo'n draadloze verbinding te laten omvatten, òfwel b) in ieder geval zodanig te ontwerpen (en te laten produceren) dat later zo'n draadloze verbinding makkelijk kan worden toegevoegd.

4.6 Minimalisatie van de fysieke beveiliging

Bij de zojuist geschetste aanpak is er één component waar alles om draait, n.l. de chip die fungeert als electronische vertegenwoordiger van de KMH-instantie en die tenminste de aangiften namens de KMH-instantie in ontvangst neemt. Deze ene component[16] moet per se in voldoende mate fysiek beveiligd zijn tegen manipulatie. Andere componenten, zoals b.v. positiebepalingssysteem, display, toetsenbord, sensor(s), zender(s), ontvanger(s) en antenne(s), zijn slechts hulpmiddelen t.b.v. (het aangifteproces van) de mobilist. Omdat deze hulpmiddelen namens en onder verantwoordelijkheid van de aangifteplichtige functioneren, is fysieke beveiliging van deze hulpmiddelen (zoals ook eerder al is opgemerkt) niet per se noodzakelijk!

Echter, om de intensiviteit van de benodigde steekproefsgewijze controles te verlagen, kan het in bepaalde gevallen wel verstandig zijn toch enkele goedkope fysieke beveiligingsmaatregelen aan te brengen t.b.v. een enkel onderdeel, zoals b.v. een sensor op de aandrijfas. Omdat zulke maatregelen alleen bedoeld zijn als eerste barrière om aldus het aantal fraudepogingen te verminderen en ze dus niet essentieel zijn voor de fraudebestendigheid[17], kan men zich hierbij probleemloos beperken tot simpele, goedkope maatregelen.

---

[15] Zie ook de laatste alinea van sectie 4.4.

[16] Bij de eerste variant is zelfs geen enkele fraudebestendige component in de voertuigen noodzakelijk! Zie ook voetnoot 9.

[17] Want de steekproefsgewijze controles vormen het ultieme vangnet, waarbij voldoende intensieve controles mogelijk zijn om de bedoelde maatregelen overbodig te maken.

Zoals al eerder is gesuggereerd, levert minimalisatie van de fysieke beveiliging niet alleen een belangrijke bijdrage aan het laag houden van de initiële en operationele kosten, maar ook aan het kunnen bereiken van een grotere flexibiliteit en een betere fraudebestendigheid.

4.7 Snel te realiseren tegen lage kosten

Omdat een voldoende mate van fysieke beveiliging van programmatuur en gegevens in chips[18] relatief goedkoop te realiseren is èn omdat voor gebruikte hulpmiddelen geen fysieke beveiliging noodzakelijk is en dus hooguit enkele goedkope fysieke beveiligingsmaatregelen zullen worden toegepast, kan een aangifte-gebaseerd KMH-systeem relatief goedkoop gehouden worden. Bovendien kan bij een aangifte-gebaseerde aanpak volstaan worden met bestaande technologie. Er hoeven geen nieuwe componenten ontwikkeld te worden en er is niet of nauwelijks nieuwe infrastructuur nodig. Dit is niet alleen gunstig voor de kosten, maar ook voor de snelheid van eventuele invoering.

Omdat behalve de chip van de KMH-instantie alles buiten het fysiek beveiligde domein kan vallen, is relatief weinig tijd en geld nodig voor het selecteren van geschikte fabrikanten en het toezicht houden op hun produktieproces, hetgeen m.b.t. noodzakelijkerwijs fraudebestendige componenten altijd van belang is. Voor de ene fraudebestendige component die wel nodig[19] is, geldt dat er al jarenlange ervaring is met de selectie van en het toezicht op fabrikanten. Immers, fysiek beveiligde chips worden al vele jaren gebruikt voor allerlei electronische betaalmiddelen.

Ook kan de mobilist de vrijheid gegeven worden zelf te kiezen voor de door hem of haar te gebruiken hulpmiddelen. Bijvoorbeeld kan hij of zij dan kiezen voor een simpele, goedkope gebruikersinterface of voor een hele mooie, maar dure. Kortom, wat betreft de hulpmiddelen kan eventueel vrije concurrentie worden toegestaan. Enerzijds kan vrije concurrentie helpen de kosten te drukken, maar anderzijds kan dat eventueel ook leiden tot versnippering van de markt. Dus als de mobilist te veel vrijheid wordt geboden kan dat eventueel averechts werken op de prijs per eenheid produkt.

Tenslotte herhalen we nog onze eerdere opmerking dat minimalisatie van fysieke beveiliging niet alleen leidt tot lagere apparatuurkosten, maar ook tot lagere operationele kosten (m.n. onderhouds- en inspectiekosten).

Dat de per voertuig benodigde apparatuur voor een aangifte-gebaseerd KMH-systeem inderdaad niet al te veel hoeft te kosten, kan men o.a. afleiden uit een persbericht van begin maart jl. waarin het Oostenrijkse bedrijf Efkon aangaf dat de benodigde On-Board Unit (OBU) en sensor samen ongeveer fl. 100,- à fl. 150,- zouden moeten kosten. Bij het hoogstgenoemde bedrag is een smartcard interface inbegrepen. Omdat het gebruik van smartcards, zoals eerder geschetst, allerminst noodzakelijk is, kan volstaan worden met ongeveer fl. 100,- aan apparatuur in elk voertuig. Vergelijk dit b.v. met de fl. 1300,- voor het kastje[20] van FELA/ASCOM, de leveran-

---

[18] Merk op dat m.n. de beveiliging van een deel van ons nationale betalingssysteem, n.l. van alle betalingen m.b.v. electronische hulpmiddelen zoals pinpassen en chipknips, hier ook op berust.

[19] Althans, bij de hier uitgebreid behandelde variant. Zie ook voetnoten 9 en 16.

[20] Dit bedrag is overgenomen uit het rapport “Effectiviteit en Haalbaarheid van een Geavanceerde Kilometerheffing”, dat in opdracht van de stichting Natuur en Milieu is opgesteld en dat in september 2000 is verschenen onder de vlag van het Economisch Sociaal Instituut (ESI) van de Vrije Universiteit te Amsterdam.

cier van het al eerder aangehaalde Zwitserse positie-gebaseerde systeem voor KMH bij zware vrachtwagens, waarbij de fraudebestendigheid primair berust op fysieke beveiliging en redundantie.

4.8 Overige details en toepassingen

In bovenstaande is alleen een globale schets gegeven van de aangifte-gebaseerde aanpak. Natuurlijk valt er veel meer te vertellen over architectuur, implementatiedetails en allerlei mogelijke toepassingen. Denk bij de eerste twee b.v. aan het kiezen voor een modulaire en open architectuur t.b.v. de flexibiliteit (m.n. aanpasbaarheid en uitbreidbaarheid) of aan het gebruik van 3 aparte processors voor de KMH-instantie, de voertuiggebruiker en het voertuig (resp. zijn eigenaar).

Wat toepassingen betreft is het aantal mogelijkheden bijna onuitputtelijk en sommen we hier alleen een kleine greep op: file-informatie, verkeersstroomanalyse, anonieme trajectsnelheidscontroles, parkeerbeheer, intelligente snelheidsadaptie, betaalstroken, fraudebestendige tachografen en taximeters, preciezer bepalen van uitstoot door verkeer, quotering van verbruiks- of vervuilingsrechten, puntenrijbewijs en verzekeringspremies per kilometer die eventueel afhankelijk zijn van b.v. wegtype en regio. In de volgende twee secties behandelen we alleen de eerste vier voorbeelden.

4.9 Verzamelen van bepaalde verkeersinformatie

Als in voertuigen t.b.v. kilometerheffing apparatuur aanwezig is voor het bijhouden van meterstanden en voor communicatie met de buitenwereld, dan wordt het verzamelen van bepaalde soorten verkeersinformatie een stuk makkelijker. Bijvoorbeeld is het eenvoudig om m.b.v. meterstanden anonieme informatie te verzamelen over de loop van verkeersstromen en over reisvertragingen op bepaalde trajecten, b.v. ten gevolge van een ongeval of verkeersdrukte.

Merk op dat kilometerstanden van auto’s tamelijk uniek zijn: de kans op twee auto’s met precies dezelfde kilometerstand min of meer tegelijkertijd op één en dezelfde plaats is heel klein. Als men dus de kilometerstand van een auto aan het begin van een traject opvraagt en wacht totdat 3 kilometer verderop een auto met die tellerstand plus 3 (of eigenlijk, plus 30 hectometer) passeert, dan weet men dat het vrijwel zeker om precies dezelfde auto gaat en kan men dus ook bepalen hoe lang die auto gedaan heeft over dat traject van 3 kilometer.

Zo kan men eventueel trajectsnelheidscontroles uitvoeren, maar ook doorstroomsnelheden en reisvertragingen van verkeer bepalen. Een voordeel is dat reisvertragingen in minuten veel nuttiger informatie leveren dan filelengtes in kilometers. Want voor de reistijd maakt het nogal wat uit of de voertuigen in de file zich met gemiddeld 20 km/u dan wel 10 km/u voortbewegen, of zelfs helemaal stil staan.

Natuurlijk moet men ook bij dit soort metingen oppassen dat de privacy niet geschonden wordt. Er moet dus voor gezorgd worden dat men niet over lange afstanden of zelfs de hele tijd dezelfde anonieme auto kan volgen. Want b.v. kennis van de plek waar ’s avonds meestal geparkeerd wordt, bedreigt dan alsnog de anonimiteit en de privacy. Omdat de volledige kilometerstand van een auto vaak wel degelijk té uniek is, moet men bij de hierboven geschetste procedure daarom niet de hele meterstand gebruiken, maar b.v. alleen de laatste 4 cijfers.

4.10 Parkeerbeheer

De apparatuur t.b.v. kilometerheffing kan ook benut worden voor betaald parkeren en biedt dan aanmerkelijke voordelen t.o.v. het gebruik van parkeermeters en –automaten op straat. Aan het begin van een parkeerperiode

moet dan aan de chip van de KMH-instantie in het voertuig kenbaar worden gemaakt dat (of wanneer) het betaald parkeren begint en welk tarief moet worden toegepast. Die chip kan daarna zelfstandig de verbruikte parkeerkosten bijhouden en b.v. toevoegen aan het totale bedrag aan verschuldigde verkeersheffingen. Parkeerwachten kunnen langs de geparkeerde voertuigen lopen of rijden en daarbij een draagbaar controlepistool richten op steekproefsgewijs te controleren voertuigen. Als uit de communicatie met de chip van een aangewezen voertuig blijkt dat er niet of te weinig betaald wordt, kan een passende actie ondernomen worden, zoals het geven van een bon of het zetten van een wielklem.

Voor de overheid is de zojuist geschetste toepassing uitermate voordelig, omdat er dan op straat (althans op termijn) geen parkeermeters en –automaten meer nodig zijn. De kosten van aanschaf en onderhoud van deze apparaten komen dan dus geheel te vervallen en ook diefstal uit en vernieling van parkeermeters- en automaten is dan verleden tijd. Voor de parkeerders is het voordeel dat ze geen klein geld voor parkeren bij zich hoeven te hebben en dat ze altijd alleen betalen voor de werkelijk verbruikte parkeertijd. Dus geldt: nooit meer vooraf de benodigde parkeertijd schatten, nooit meer onnodig veel betaald hebben bij een vroegtijdige terugkeer, nooit meer het risico van een bon of wielklem bij een iets te late terugkeer en ook nooit meer grote haast om nog net op tijd terug te zijn.

Daarnaast is het voor beide genoemde partijen voordelig dat het mogelijk wordt om b.v. het eerste uur een (eventueel zelfs tot nul) gereduceerd tarief toe te passen zonder dat hiervan misbruik kan worden gemaakt. Want het is eenvoudig de chip zo te programmeren dat zo'n reductie op het eerste uur parkeren alleen wordt toegepast als aan een aantal voorwaarden is voldaan. B.v. de voorwaarde dat de aangegeven parkeerperiode tenminste, zeg, een half uur na afloop van de vorige parkeerperiode begint en/of dat geparkeerd wordt op een andere parkeerplaats of in een andere parkeerzone. In het laatste geval moet de parkeeraangifte dus ook een of andere aanduiding van de parkeerplaats of –zone omvatten. Dat hoeft geen unieke identificatie[21] te zijn, zodat de privacy dus ook in dit geval goed gewaarborgd kan blijven.

5 Conclusies

Het in de (privacy)wetgeving opgenomen subsidiariteitsbeginsel houdt in dat de overheid een doel op de minst privacy belastende wijze moet verwezenlijken als dat in redelijkheid mogelijk is. Omdat we hebben laten zien dat aangifte-gebaseerde systemen privacyvriendelijker zijn dan positie-gebaseerde systemen voor kilometerheffing, lijkt er derhalve voldoende rechtvaardiging te zijn voor de conclusie dat er géén positie-gebaseerd systeem[22] gebruikt mag of zal gaan worden voor kilometerheffing. Burgers mogen er dus op rekenen dat de eventuele invoering van kilometerheffing niet gepaard zal gaan met een aantasting van de individuele privacy.

Aangifte-gebaseerde KMH-systemen bieden qua apparatuurkosten en fraudebestendigheid belangrijke voordelen t.o.v. alle tot nu toe bekende (ontwerpen voor) KMH-systemen. Dus niet alleen t.o.v. de positie-gebaseerde systemen, maar ook t.o.v. de meer traditionele, aan tachograaf en taximeter verwante systemen met fysiek bevei-

---

[21] De wel benodigde, allerminst unieke 'identificatie' noemen wij een semi-identificatie. Het geven van een precieze definitie van dit begrip zou hier te ver voeren. We volstaan met het geven van een eerste indruk door slechts te verwijzen naar sectie 4.9, waar de 4 cijfers van de kilometerstand een uitstekend voorbeeld van een semi-identificatie geven.

[22] Zie de aan het begin van hoofdstuk 2 gegeven definitie.

ligde tellers. De fraudebestendigheid (met name van de tellers die door KMH-systemen worden bijgehouden) berust bij aangifte-gebaseerde systemen primair op logische en bij alle andere systemen primair op fysieke beveiliging. Doordat het m.b.v. telecommunicatie uitvoeren van steekproefsgewijze controles op willekeurige plaatsen en tijdstippen veel goedkoper is dan steekproefsgewijze fysieke inspecties, kan er bij aangifte-gebaseerde KMH-systemen veel intensiever gecontroleerd worden en kunnen deze systemen dus een hogere mate van fraudebestendigheid bieden dan de tot nu toe bekende systemen. Ook kan bij voldoende intensieve controles volstaan worden met een minimum aan fysieke beveiliging, zodat de kosten van de per voertuig benodigde apparatuur dan veel lager liggen.

Ook bieden aangifte-gebaseerde systemen nog andere voordelen, zoals b.v. lagere operationele kosten en grotere flexibiliteit en dus betere ‘toekomstvastheid’. De operationele kosten kunnen lager gehouden worden, o.a. omdat er minder en/of minder dure fysieke inspecties nodig zijn, omdat er voor onderhoud en reparatie geen of veel minder op betrouwbaarheid geselecteerd en gecertificeerd personeel nodig is èn omdat er veel minder geschillen zullen rijzen over onjuist in rekening gebrachte bedragen t.g.v. onjuist functionerende apparatuur. Met name het sterk teruggedrongen belang van fysieke beveiliging maakt bij aangifte-gebaseerde systemen een modulaire en vooral ook open architectuur mogelijk, hetgeen flink bijdraagt aan een betere aanpasbaarheid en uitbreidbaarheid.

De mogelijkheid tot differentiatie naar o.a. afstand, snelheid, acceleratie, toerental, brandstofsoort en voertuigkenmerken maakt aangifte-gebaseerde KMH-systemen zeer geschikt voor het internaliseren van externe kosten en i.h.b. ook voor het voeren van milieubeleid. De mogelijkheid tot differentiatie naar tijd en plaats maakt ze ook geschikt voor gerichte filebestrijding. Bovendien kunnen desgewenst o.a. betaalstroken, parkeerheffingen en tolheffingen (b.v. bij bruggen en tunnels, maar ook bij andere tolpunten, zoals bij rekeningrijden de bedoeling was) snel, eenvoudig en tamelijk goedkoop worden geïmplementeerd.

In feite biedt de aangifte-gebaseerde aanpak een uitgelezen mogelijkheid tot het opzetten van een nationaal of Europees systeem dat niet alleen een hoge fraudebestendigheid en een uitstekende privacybescherming biedt, maar ook makkelijk uitbreidbaar is met vele toepassingen en dus soepel kan uitgroeien tot een uiterst veelomvattend verkeersinformatie- en beprijzingssysteem. Een kleine greep uit de meteen of later toe te voegen mogelijke toepassingen is: het innen van parkeerkosten, het vergaren van file-informatie, verkeersstroomanalyse, anonieme trajectsnelheidscontroles, intelligente snelheidsadaptie, beter fraudebestendige tachografen en taximeters, preciezer bepalen van uitstoot door verkeer, quotering van verbruiks- of vervuilingsrechten, puntenrijbewijs en verzekeringspremies per kilometer die eventueel afhankelijk zijn van b.v. wegtype en regio.