Van Mobimeter en heffingskaart
Een introductie

Voorwoord

Deze notitie bevat de originele tekst van 13 december 2001 met een ingekort voorwoord.

Aanleiding tot deze notitie was een e.e.a. toe te lichting m.b.t. de heffingseenheid' en 'heffingskaart'. Tevens kwam daar bij de vraag aan de orde naar de zin en de mogelijkheden om technische eisen in de wet formuleren.

In deze notitie wil ik een proeve van een antwoord op deze vragen formuleren.

Om de tekst enerzijds ook voor niet technisch geschoolden leesbaar te houden maar anderzijds weer niet al te populair te maken, is veelvuldig gebruik gemaakt van voetnoten voor technische definities en toelichtingen.

Let wel
De notitie onder grote tijdsdruk in een hoog tempo geschreven. Ik claim bovendien geen juridische expertise, wel technische.

Jan Vis
Adviesdienst Verkeer en vervoer

Inhoud

1. Inleiding

Bij het systeem voor kilometerheffing wordt aangifte gedaan op basis van een in het voertuig zelf berekende heffing.

Voor zover hier relevant spelen daarbij de volgende zaken:

1. De mate de Belastingdienst erop kan vertrouwen dat een ontvangen aangifte ook inderdaad juist is
2. De mate waarin de burger erop kan vertrouwen dat zijn privacy niet in het geding is.

Specialistisch technische zaken als hoe afstanden en locaties voldoende precies gemeten kunnen worden laat ik hier buiten beschouwing. (Daar zijn bovendien betere experts voor).

2. Mobimeter, heffingseenheid en heffingskaart

Uit het voortgangsrapport van de regering 'Betalen per kilometer' valt op te maken dat een Mobimeter tenminste bestaat uit de volgende componenten (zie paragraaf 3.2, fig. 3-1)

1. een sensor
2. een heffingseenheid
3. een heffingskaart
4. een behuizing.

Onduidelijk is of componenten in de figuur 3-1 die buiten de behuizing vallen in het voortgangsrapport al dan niet tot de Mobimeter gerekend worden. Voor deze notitie is dit echter niet relevant.

Ik beperk me hier verder tot de rolverdeling (functiescheiding) tussen een heffingseenheid en een heffingskaart.

De Mobimeter (maar dan exclusief de heffingskaart) is in principe vrij te koop, maar moet voor gebruik wel gecertificeerd worden.

De heffingskaart is een chipkaart die vanwege de Belastingsdienst en/of de zogeheten kilometer service provider wordt verstrekt en waarvan de werking door de verstrekker(s) vertrouwd wordt[1]. De heffingskaart werkt als het ware voor en namens zijn verstrekker(s).

De rolverdeling tussen de heffingeenheid en de heffingskaart is in principe als volgt:

- De heffingeenheid berekent de heffing(en) en registreert en bewaart de nodige gegevens in een interne kilometer administratie.
- De heffingskaart bepaalt de identiteit van de apparatuur in het voertuig, controleert de consistentie van de administratie, garandeert de integriteit van de administratie, stelt de aangifte op en verzorgt de beveiliging van de communicatie met partijen buiten het voertuig (zoals bijv. met een service provider en de Belastingdienst)

De beveiliging van de communicatie met derden omvat bijv. ook de beveiliging van aangiften.
Zo kan de kaart de vertrouwelijkheid van een aangifte garanderen door deze te vercijferen en de authenticiteit[2] ervan door een digitale handtekening[3]. Hierdoor kan een digitale aangifte in principe langs elke willekeurige, veilige of onveilige, electronische weg naar de Belastingdienst verzonden worden.

---

[1] Zoals ook de werking van een Chipkip door de bank vertrouwd wordt en de werking van een SIM-kaart in een mobiele GSM-telefoon door een GSM netwerk operators (bijv. KPN, Ben, enz). Technisch is het bovendien mogelijk om, mocht dit van wenselijk blijken, de kaart zo te construeren dat die zowel door de Belastingdienst als een service provider vertrouwd kan worden zonder dat die twee partijen elkaar ook behoeven te vertrouwen.

[2] **Data origin authentication**
The corroboration that the source of data received is as claimed. [ISO7498-2]

[3] **Digital signature**
Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO7498-2]

In het volgende hoofdstuk wordt nader uitgewerkt welke consistentiecontroles er op een kilometeradministratie uit zijn te voeren en hoe steekproefsgewijs controles kunnen worden uitgevoerd op correct voeren van een kilometeradministratie.

3. Het vertrouwen in een kilometeradministratie

3.1 Inleiding

Uitgangspunt voor een controleerbare kilometeradministratie is een administratie waarin voor zover hier relevant voor elk aangiftetijdvak per afgelegde kilometer het volgende wordt bijgehouden[4]:

1. de locatie van het eindpunt van die kilometer
2. dag en tijd waarop dat eindpunt bereikt is
3. de totaal afgelegde afstand (van het begin of het begin van het tijdvak)[5]
4. de totaal berekende heffing (van het begin of het begin van het tijdvak)[6]

Het vertrouwen in de juistheid van een dergelijke administratie kan worden bevorderd door:

1. vertrouwen het correct functioneren van de apparatuur die gegevens aanlevert (meet) en die de administratie verzorgt (dit kan bijv. d.m.v. certificering, maar is hier verder niet aan de orde)
2. door op deze administratie (direct of achteraf) een aantal consistentiecontroles uit te voeren (zie de volgende paragraaf)
3. door de administratie zodanig te voeren dat de erin opgenomen gegevens later niet meer ongemerkt gewijzigd kunnen worden en
4. door die niet meer te wijzigen gegevens op onverwachte momenten steekproefsgewijs voor de laatst afgelegde kilometer direct langs de kant van de weg op hun juistheid te controleren.

Hoe in de punten 3 en 4 voorzien kan worden komt in paragraaf 3.3.3 "Controles op microaangiften aan een heffingskaart" aan de orde.

Bij het verwezenlijken van de punten 2 en 3 zal, zoals zal blijken, de heffingskaart als enige component in het voertuig die werkelijk door de service provider en de Belastingdienst vertrouwd kan worden, een essentiële rol spelen.

3.2 Consistentiecontroles

Op basis van de kilometergegevens op het eind van twee opeenvolgende kilometers kunnen een aantal controles m.b.t. de laatst afgelegde kilometer worden uitgevoerd. De eindwaarden van de vorige kilometer fungeren daarbij als de beginwaarden voor de laatste kilometer.

Mogelijke consistentiecontroles zijn:

1. Er is over de laatste kilometer een positief tarief berekend
   Dit controleerbaar door de begin- en eindwaarden voor de totaal berekende heffing van elkaar af te trekken. Ook kan eventueel getoetst worden tegen een minimumtarief.
2. De afgelegde afstand is inderdaad niet (veel) meer dan een kilometer
   dit is controleerbaar door de afstand tussen de begin- en eindlocatie van de kilometer te bereken. Die afstand mag wel minder (een blokje rond rijden) maar mag niet meer dan een kilometer zijn. Na een kilometer in Groningen kan het voertuig dus niet ineens in Limburg opdagen.[7]

[4] Nuances als een specificatie per wegvaktype zijn hier gemakshalve buiten beschouwing gelaten.
[5] Dit gegeven is eigenlijk overbodig, want zou gelijk moeten aan het aantal malen dat deze gegevens voor een tijdvak in de administratie zijn opgenomen. Het is hier vooral opgenomen voor de leesbaarheid van de tekst.
[6] In plaats van totalen kunnen ook de heffing voor de afgelegde kilometer worden doorgegeven. De heffingskaart moet dan wel zelf de totalen bijhouden.
[7] Tenzij bijv. verplaatst op een trailer, maar dat zou dan door de houder gemotiveerd moeten kunnen worden.

3. De gemiddelde snelheid over de laatste kilometer
   Op basis het verschil tussen begin- en eindtijd kan de gemiddelde snelheid berekend worden. Deze kan niet negatief of onmogelijk groot zijn. Wat de toegevoegde waarde van deze controle is, dat is echter onduidelijk
4. De totaal afgelegde afstand en de tijd moeten monotoon toenemen.

Merk op dat al deze consistentiecontroles eventueel ook achteraf kunnen worden uitgevoerd.
Het zijn geen controles op de juistheid van de administratie, maar alleen op de interne consistentie ervan.

Als deze controles direct bij het ter beschikking komen van de gegevens worden uitgevoerd, zal dit door de heffingskaart moeten gebeuren. Alleen dan kan de garantie worden gegeven dat eventueel gesignaleerde gebreken ook inderdaad bij het doen van de aangifte gemeld worden[8]. Tevens zal dan gegarandeerd moeten kunnen worden dat de eenmaal gecontroleerde gegevens niet meer onopgemerkt gewijzigd kunnen worden. Hoe dat laatste verwezenlijkt kan worden komt in 3.3.4 "Integriteitcontroles en hash-codes" aan de orde.

3.3 Locatiecontroles

In deze paragraaf wordt een drietal verwante mechanismen geschetst om de juistheid van een kilometeradministratie door steekproeven langs de kant van de weg door middel van steekproeven te kunnen controleren. De eerste twee zijn daarbij vooral bedoeld als didactische inleiding op de derde waarbij gebruik gemaakt wordt van een heffingskaart.

3.3.1 Micro aangiften of betalingen

Bij een microaangifte of -betaling bestaat de aangifte of de betaling uit veel kleine aangiften of betalingen.

Bij kilometerheffing kan men bijvoorbeeld denken aan een aangifte per kilometer. Per aangifte kan dan bijv. worden aangegeven:
1. om welk voertuig het gaat,
2. wat er betaald is of moet worden,
3. wanneer die kilometer gereden is (datum en tijd) en,
4. eventueel, de locatie van die kilometer.

Wanneer een opsporingsambtenaar nu een voertuig op de weg wordt waarneemt, kan achteraf gecontroleerd worden of die waarneming spoort met een reeds gedane aangiften.

Om dit systeem te laten werken moeten de aangiften per kilometer zo snel mogelijk na het rijden ervan gedaan worden. Tenzij de waarneming ongemerkt plaats vindt (en/of aanvullende maatregelen getroffen worden) zijn andere aangiften dan die bij een waarneming in theorie niet te vertrouwen[9].

Nadelen van deze methode in geval van kilometerheffing zijn:
1. het gebrek aan privacy wanneer ook de locatiegegevens worden meegestuurd,
   de kilometeradministratie ligt volledig bij de Belastingdienst,
2. het vereist veel communicatie,
   na elke kilometer moeten er direct de nodige gegevens verzonden worden.

Een voordeel, althans wanneer ook de locatiegegevens worden meegestuurd, is dat de consistentie van de kilometeradministratie nu op elk gewenst moment volledig door de Belastingdienst gecontroleerd kan worden.

In de volgende paragraaf wordt aangegeven hoe het eerste bezwaar deels kan worden ondervangen. In de daarop volgende hoe beide ondervangen kunnen worden.

3.3.2 Micro aangiften of betalingen met bescherming van de privacy

[8] Namelijk door ze op te nemen in de aangifte en vervolgens het geheel door heffingskaart van een digitale handtekening te laten voorzien.
[9] Als de voertuigapparatuur een controle kan zien aankomen zou het – althans in theorie en mits het daarvoor de tijd krijgt – kunnen volstaan met het pas dan registreren van een plausibele route sinds de vorige controle.

De privacy kan met behoud van de mogelijkheden tot handhaving deels worden beschermd door bij een microaangifte of –betaling, niet alle specificerende gegevens mee te sturen maar alleen:

- een identificatie van het voertuig
- het bedrag en
- een hash-code over de overige specificerende gegevens (tijd en locatie).

Aan de hand van dit hash-code kan dan naderhand gecontroleerd worden of overige specificerende gegevens niet gewijzigd zijn[10].

Bij een controle langs de kant van de weg moeten nu alle specificerende gegevens inclusief de hash-code over de laatste kilometer(s) worden opgevraagd. Op basis daarvan kan dan de hash-code gecontroleerd worden en kan worden nagegaan of die hash-code ook is meegezonden bij de laatste microaangifte of -betaling.

Voordeel van deze methode is dat de privacy wat beter beschermd wordt.

Nadelen van deze methode voor kilometerheffing zijn:

1. Meer complexe controles
   er kan ter plaatse niet meer worden volstaan met het waarnemen van het voertuig, maar er moet ook informatie uit het voertuig worden opgehaald,
2. Nog onvoldoende privacy,
   Hoewel de Belastingdienst nu niet meer over de volledige administratie beschikt, kan de dienst aan de hand van het binnenkomen van de microaangiften of –betalingen wel nagaan wanneer er gereden is en, in dit voorbeeld, hoe hard per kilometer.
3. Het vereist veel communicatie,
   na elke kilometer moeten er direct de nodige gegevens verzonden worden.
4. Meer omslachtige procedures voor het controleren van een kilometeradministratie,
   de houder dient de administratie nu zo te bewaren dat de integriteit van de opgaven geborgd blijft (de hash-code moet herberekenbaar blijven).
5. Controle van de consistentie van de administratie is alleen mogelijk bij inzage in de volledige administratie van de houder van het voertuig.

3.3.3 Controles op microaangiften aan een heffingskaart

In dit geval wordt de houder van een voertuig door of namens de Belastingdienst of service provider een chipkaart, de zogeheten heffingskaart, ter beschikking gesteld.

Een dergelijke chipkaart bevat een chip[11] waarop door de Belastingdienst een aantal gegevens zijn geplaatst die door de houder van de kaart niet te lezen of ongemerkt te wijzigen zijn. Ook kan de kaart een op een veilige manier een aantal andere gegevens bewaren en een aantal operaties uitvoeren (bijv. een hash-code of een digitale handtekening berekenen; een bericht vercijferen of een aantal consistentiecontroles op gegevens uitvoeren).

De microaangiften[12] worden nu niet direct aan de Belastingdienst gedaan maar aan een heffingkaart die deze nu namens de Belastingdienst controleert en daarbij tevens de integriteit van die gegevens borgt door over de reeks van individuele microaangiften een hash-code te berekenen.

In geval van kilometerheffing worden bijv. na elke gereden kilometer opgave van die kilometer gedaan in een kilometeradministratie die bewaard wordt door de houder van het voertuig.
In geval van kilometerheffing vindt nu de volgende plaats:

1. De heffingseenheid verzorgt een kilometer administratie zoals in 3.1 "Inleiding" beschreven
2. Direct na het rijden van een kilometer, worden de gegevens over die kilometer ook aangeboden aan de heffingskaart, dit wordt een microaangifte genoemd

[10] Zie 3.3.4 Integriteitcontroles en hash-codes.
[11] Een microprocessor zoals bijv. ook aanwezig op een Chipknip-, een Chipperkaart- of een SIM-kaart voor een mobiele telefoon.
[12] Of hier ook in juridische nog sprake is van een aangifte kan ik niet beoordelen.

3. De heffingskaart berekent een hash-code over de reeks van ontvangen microaangiften waardoor het onmogelijk wordt de tot zover gevoerde kilometeradministratie van de heffingseenheid nog te wijzigen zonder dat dit merkbaar is,
4. De heffingkaart voert op basis van de laatste twee microaangiften de in 3.2 "Consistentiecontroles"beschreven consistentie controles uit en registreert een (samenvatting van) eventueel gesignaleerde gebreken
5. Indien de microaangiften geen totalen maar kilometerbedragen bevat, worden tevens de totalen berekent en bijgehouden.

Bij een controle levert de heffingskaart de gegevens van de laatste twee microaangiften. Door middel van cryptografische technieken kan daarbij tevens gegarandeerd worden dat deze gegevens inderdaad van de door de Belastingdienst en/of Service provider verstrekte kaart afkomstig zijn[13]. De apparatuur kan dan vervolgens controleren of deze gegevens sporen met zijn waarneming. Zo niet dan kan de houder van het voertuig op een foto van het kenteken verder vervolgd worden.[14]

De feitelijke aangifte wordt nu ook door de heffingskaart opgesteld op basis van de ontvangen microaangiften. In deze aangifte worden tevens de berekende hash-code en (een samenvatting van) de bij de controles gesignaleerde gebreken opgenomen. Het geheel wordt nu door de heffingskaart voorzien van zijn digtale handtekening en kan nu langs elke willekeurige, veilige of onveilige, electronische weg aan de Belastingdienst worden aangeboden.

Bij een controle achteraf van de door de heffingseenheid gevoerde kilometeradministratie kan nu op basis van de hash-code gecontroleerd worden dat die dezelfde gegevens bevat als de door de heffingskaart ontvangen microaangiften.

Merk op dat de heffingskaart bij gebruik van deze methode nooit meer dan de laatste twee ontvangen microaangiften weer ter inzage behoeft te geven. Hierdoor is deze kaart niet of nauwelijks privacy gevoelig.

Voordelen van deze methode zijn:

1. Een goede bescherming van de privacy,
   De Belastingdienst beschikt nu niet meer over een volledige kilometeradministratie en de dienst ontvangt nu zelf ook geen microaangiften meer zodat ook niet meer gecontroleerd kan worden wanneer het voertuig gebruikt wordt..
2. Veel minder communicatie,
   alleen de aangiften per tijdvak behoeven te worden doorgegeven, niet meer alle microaangiften.

Resterende nadelen (t.o.v. methode 1) zijn:

1. Meer complexe controles
   er kan ter plaatse niet meer worden volstaan met het waarnemen van het voertuig, maar er moet ook informatie uit het voertuig worden opgehaald,
2. Meer omslachtige procedures voor het controleren van een kilometeradministratie,
   de houder dient de administratie nu zo te bewaren dat de integriteit van de opgaven geborgd blijft (de hash-code moet herberekenbaar blijven).
3. Controle van de consistentie van de administratie is alleen mogelijk bij inzage in de volledige administratie van de houder van het voertuig.

3.3.4 Integriteitcontroles en hash-codes

Deze paragraaf bevat een korte, informele introductie op het gebruik van hash-codes voor het beschermen van de integriteit van (een verzameling van) gegevens.

[13] Dat deze gegevens dan via de heffingseenheid en via een niet te vertrouwen communicatiekanaal verzonden worden doet dan daarbij niet meer ter zake. Verminking van de gegevens onderweg is merkbaar en, wanneer opgemerkt, opgevat worden als ontvangst van onjuiste gegevens waarna verdere vervolging kan volgen.

[14] Let op. De hier beschreven methoden werk alleen als de voertuigapparatuur de controle niet van tevoren kan zien aankomen. Mocht dat wel het geval zin dan zou de administratie met onjuiste gegevens gevoed kunnen worden als het geen controle ziet aankomen en met juiste gegevens als dit wel het geval is. Voor zover de apparatuur een controle pas (zeg) de laatste seconde kan zien aankomen en ook geëist kan worden dat die apparatuur binnen (zeg) een seconde reageert zijn hier echter wel weer beschermingen tegen aan re brengen. Dergelijke beschermingen vallen echter buiten de scope van deze notitie (en het huidige programma van eisen).

Onder integriteit van gegevens versta ik in dit verband de mate waarin er op vertrouwd kan worden dat die gegevens niet gewijzigd zijn.[15]

Let wel, dit wil dus nog niet zeggen dat die gegevens ook juist zijn. Ze kunnen onjuist zijn geregistreerd en/of al eerder voorafgaand aan de bescherming van de integriteit gewijzigd zijn. Merk bovendien op dat in de bovenstaande definitie ook de mogelijke oorzaak (bijv. valsheid of een technische storing) van een wijziging buiten beschouwing wordt gelaten.

Merk tenslotte op dat ook het kunnen wijzigen hier niet ter discussie staat. Hoewel dat ook tot op zekere hoogte voorkomen kan worden (bijv. bij gebruik van een CD, maar vernietigen kan praktisch altijd), gaat het bij integriteit alleen om dat gegevens niet achteraf ongemerkt gewijzigd kunnen worden.

De integriteit van gegevens kan beschermd worden door een zogeheten hash-code, ook wel een fingerprint genoemd.

Een hash-code is een getal dat berekend wordt op basis van een bepaalde representatie (codering) van die gegevens en waarvoor het zeer, zeer onwaarschijnlijk is dat voor aan andere representatie van gegevens hetzelfde getal gevonden wordt.[16]

Een slecht voorbeeld van een hash-code is bijv. de som van de (ASCII) codes voor alle lettertekens uit een tekst. In dat geval zouden bijv. '19 euro' en '91 euro' dezelfde hash-code krijgen en zou een wijziging van de ene tekst in de andere dus niet te detecteren zijn.

In de praktijk worden de gegevens eerst op zeer eenduidige wijze gerepresenteerd[17] en wordt vervolgens voor het berekenen van de hash-code gebruik gemaakt van een cryptografisch algoritme[18]. Op deze wijze wordt het praktisch gezien onmogelijk een tweede representatie van gegevens te vinden (laat staan een tweede geschikte representatie) die dezelfde hash-code oplevert. Het zou zeer vele computerjaren kosten en daardoor èn onbetaalbaar èn pas beschikbaar als niet meer relevant.

Door nu op een gegeven moment de hash-code van een hoeveelheid gegevens aan een derde ter beschikking te stellen, wordt het onmogelijk die gegevens daarna nog te wijzigen zonder dat dat door die derde opgemerkt kan worden.

Bij kilometerheffing is het gebruik van hash-codes bijvoorbeeld van belang waar het uit oogpunt van privacy ongewenst is een totale kilometeradministratie bij een aangifte te voegen, maar de Belastingdienst wel in individuele gevallen controles moet kunnen uitvoeren en daarbij de zekerheid wil dat die administratie dan niet achteraf gewijzigd is.

Dit laatste klemt te meer waar bepaalde opgaven in deze administratie al eerder langs de weg gecontroleerd (kunnen) zijn en toen al in orde bevonden waren. Vooral die opgaven mogen niet achteraf ongemerkt gewijzigd kunnen worden.

---

[15] **Data Integrity**
The property that data has not been altered or destroyed in an unauthorised manner. [ISO7498-2]

[16] **Digital fingerprint**
A characteristic of a data item, such as a cryptographic checkvalue or the result of performing a one-way hash function on the data, that is sufficiently peculiar to the data item that it is computationally infeasible to find another data item that will possess the same characteristics. [ISO10181-1]

[17] Bijv. conform de Distinguished Encoding Rules (DER) [ISO8825]

[18] Een veel gebruikt algoritme is bijv. SHA-1 (Secure Hashing Algorithm 1). Maar er zijn er meer