Radboud Universiteit Nijmegen

RDW

Privacybescherming Anders Betalen voor Mobiliteit

Prof. dr. E. R. Verheul
Prof. dr. B.P.F. Jacobs
Dr. W.G. Teepe
F.D. Garcia

Versie 1.0
2 april 2008
DS-2008-001
Institute of Computing and Information Sciences
Digital Security Group

Inhoudsopgave

Versiebeheer

Versie	Omschrijving	Datum	Auteur
0.1	Discussie document voor de workshop van 22 februari - Aanzet context, dreigingen rond ABvM. - Aanzet gewenste/vereiste functionaliteiten voor de ABvM methode/techniek. - Hoofdlijn beschrijving van een voorstel voor een dergelijke methode/techniek op basis vergadering Maneschijn /Verheul 12 februari	21 februari 2008	E.Verheul
0.2	Document voor de workshop van 27 februari: - Commentaren en suggesties uit workshop van 22 februari verwerkt. - Beschrijving methode/techniek meer gedetailleerd.	25 februari 2008	E.Verheul
0.3	Concept versie rapportage ter commentariëring workshop leden: - Onderverdeling van functionaliteiten in Eisen en Wensen - Relatie Dreigingen met Eisen en Wensen - Relatie Eisen en Wensen met beschreven methode/techniek.	26 februari 2008	E.Verheul
0.99	Concept versie ter afstemming opdrachtgever	18 maart 2008	E.Verheul
1.0	Definitieve versie rapportage (geen wijzigingen op versie 0.99)	2 april 2008	E.Verheul

1. Managementsamenvatting

Achtergrond
In de periode 11 februari – 2 april 2008 heeft de sectie Digital Security van de Radboud Universiteit voor de RDW een onderzoek uitgevoerd naar de privacybescherming binnen het Anders Betalen voor Mobiliteit Eindbeeld concept. De doelstelling van het onderzoek is het komen tot een of meerdere hoofdlijn voorstellen voor een techniek/methode waarmee ABvM-weggebruikinformatie van de ABvM-deelnemer beschikbaar kan komen bij de ABvM-organisatie die:

- de juiste functionaliteit heeft om te kunnen factureren
- de juiste betrouwbaarheid heeft (waaronder fraudebestendigheid)
- de privacy van de deelnemers (feitelijk de eigenaren van motorvoertuigen) voldoende beschermt

Bij de te ontwikkelen techniek/methode wordt rekening gehouden met de taken van de ABvM-organisatie (naar verwachting privaat belegd) en de vier publieke taken die ondersteund moeten worden binnen het ABvM concept. Deze vier publieke taken zijn:

- Handhaving: met een (geautomatiseerde) controle langs de kant van de weg moet kunnen worden vastgesteld of de ABvM-deelnemer al dan niet fraudeert
- Revenu Assurance: deze biedt (boekhoudkundige) zekerheid voor de overheid dat de vereden kilometers ook worden gefactureerd door de ABvM-organisatie en dat revenuen van de gefactureerde kilometers ook worden afgedragen aan de overheid
- Beroep & Bezwaar: de ABvM-deelnemer moet de factuur kunnen toetsen aan gereden kilometers en bij storingen moet de deelnemer over voldoende informatie voor een eventuele klachtafhandeling kunnen beschikken
- Informatieverstrekking: het moet mogelijk zijn informatie te verstrekken aan beleidsmakers van de overheid voor verkeersmanagement, prijsbeleid en statistische doeleinden.

Het onderzoek heeft zich geconcentreerd op personenvervoer en er is niet expliciet gekeken naar vrachtvervoer en naar buitenlandsvervoer. De resultaten van het onderzoek lijken evenwel ook technisch toepasbaar op deze twee typen vervoer, zij dat zich hieromtrent additionele vragenstukken voordoen. Eén van deze vraagstukken is of men buitenlanders kan verplichten om Nederlandse ‘kastjes’ te laten gebruiken. Deze vraagstukken zijn niet onderzocht.

Context onderzoek: Dik versus Dun
Binnen het onderzoek is – in dialoog met de RDW – allereerst de ABvM-context vastgelegd (Sectie 3). Essentieel binnen deze context is dat een motorvoertuig van een deelnemer wordt uitgerust met een ‘Dikke Client’ (OBU) waarbij de ABvM organisatie slechts geaggregeerde informatie ontvangt als basis voor facturering. De OBU wordt niet als ‘trusted’ beschouwd, maar in de OBU bevindt zich een Trusted Element (TE) dat gezien kan worden als vooruit geschoven post van de ABvM-organisatie. Een TE lijkt op een (contact) smartcard met enige additionele functionaliteit die eenvoudig in te passen is op bestaande smartcardtechnologie. De fysieke beveiliging van het TE is van fundamenteel belang voor de ABvM-betrouwbaarheid.

Tijdens het onderzoek is ook kort gekeken naar de ‘Dunne Client’ opzet waarbij plaatsgegevens van ABvM-deelnemers worden verstuurd naar de ABvM-organisatie (of partijen die daarvoor werkzaam zijn). Deze ‘Dunne Client’ opzet is overigens anders dan die onderzocht in het kader van het RDW project Uitwerken Procesarchitectuur ABvM (UPA). Hierbij betrof de ‘Dunne Client’ een zogenaamde DSRC-tag waarmee ABvM-deelnemers slechts op bepaalde plekken (wegkantsystemen) binnen het hoofdwegennet/congestiegebieden hun locatie verstrekten aan de ABvM-organisatie. In de DSRC-tag opzet is vanuit een eerder PwC/RU onderzoek in het kader UPA het voorstel gedaan voor data aggregatie in combinatie met een datakluis.

De ‘Dunne Client’ opzet waar vanuit het huidige onderzoek kort gekeken is, omvat dat plaatsgegevens van ABvM-deelnemers in beginsel vanuit alle locaties op het Nederlandse wegennet worden doorgegeven aan de ABvM-organisatie. De bescherming van plaatsgegevens in deze opzet zal van dermate hoog niveau moeten zijn dat naar mening van de onderzoekers deze opzet in vergelijking met de ‘Dikke Client’ opzet op gespannen voet staat met het proportionaliteits- en subsidiariteitsbeginsel. Naar dit beginsel, beschreven in Artikel 8 (“Recht op Privacy”) van het Europees Verdrag voor de Rechten van de Mens wordt ook verwezen in de Memorie van Toelichting op de Wet Bescherming Persoonsgegevens van 2002. Dit beginsel wordt aldaar als volgt beschreven: “Het doel waarvoor de persoonsgegevens worden verwerkt dient in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze te kunnen worden verwerkelijkt.”

De mening van de onderzoekers is dat in de vergelijking tussen de ‘Dikke Client’ en de ‘Dunne Client’ opzet het proportionaliteits- en subsidiariteitsbeginsel van toepassing is en wel om de volgende redenen:

- de aggregatie binnen de ‘Dikke Client’ opzet is fundamenteel ‘minder nadelig’ voor de bescherming van de persoonsgegevens van ABvM-deelnemers dan in de ‘Dunne Client’ opzet
- de ‘Dikke Client’ opzet lijkt ook niet onredelijk in termen van kosten en implementatiecomplexiteit en –risico’s in vergelijking met de ‘Dunne Client’ opzet

Om die reden hebben wij geen nader onderzoek gedaan naar de beveiliging van de ‘Dunne Client’ opzet. Dit is overigens in lijn met een recente uitspraak [5.] van het College Bescherming Persoonsgegevens, waarin ondermeer wordt gesteld: “Het CBP is van oordeel dat de zogeheten ‘dikke’ voertuigapparatuur vanuit het oogpunt van een adequate bescherming van persoonsgegevens de meest aanvaardbare variant van de heffing van kilometerprijs is.”

Verder verloop onderzoek
In het verder verloop van het onderzoek zijn de eisen en wensen vastgelegd met betrekking tot bovenstaande aspecten (Sectie 5) en als hulpmiddel daarvoor zijn eerst (indicatief) beveiligingsgerelateerde bedreigingen voor ABvM (Sectie 4) geformuleerd. Tijdens een eerste afstemmingsvergadering van RDW en RU is al een basis gelegd voor een methode/techniek voor de realisatie van ABvM met behulp van een ‘Dikke Client’. Deze methode/techniek (Sectie 6) is gaandeweg het onderzoek verder verfijnd.

Deze methode/techniek bestaat uit een kleine computer (On-board Unit of OBU) en een ‘trusted element’, vergelijkbaar met een smartcard. De OBU wordt verondersteld de afgelegde weg op te delen in kleine trajecten en deze te registreren bij het TE. Het TE houdt hieromtrent ‘secure’ tellers bij die vergelijkbaar zijn met tellers in gas- en elektriciteitsmeters. Bij deze registraties levert het TE ook zogenaamde traject-transcripts aan de OBU die vergelijkbaar zijn met kassabonnen. Periodiek levert de OBU, door middel van interactie met het TE, tellerstanden op die naar de ABvM-organisatie moeten worden gestuurd. Ondermeer door digitale ondertekening door de TE van de tellerstanden wordt de betrouwbaarheid daarvan gegarandeerd. Het is essentieel dat de werking van de OBU kan worden gecontroleerd; een belangrijk middel daartoe bestaat eruit dat handhavingteams recente traject-transcripts kunnen opvragen en vergelijken met wat zij visueel waarnemen.

De methode/techniek lijkt op twee uitzonderingen na te voldoen aan de gestelde eisen en wensen (Sectie 7). De eerste uitzondering (eis 9) betreft het gebrek aan een fall-back scenario als de (fysieke) beveiliging van het TE wordt gecompromitteerd. De verwachting is evenwel dat een dergelijk fall-back scenario wel ontwikkeld kan worden in een additioneel onderzoek. De tweede uitzondering (eis 30) betreft het niet kunnen uitvoeren van instantane handhavingscontroles zonder detectie. Voor dit type handhavingscontrole dient de OBU namelijk op de handhavingslocatie uitgelezen te worden hetgeen een actieve en dus in beginsel detecteerbare handeling is. Verbonden hiermee is het risico dat ABvM-deelnemers elkaar op de hoogte brengen van handhavingslocaties. Zoals wij hebben beargumenteerd bij de vergelijking van eis 30 in Sectie 7, biedt het voorstel compenserende ruimte die toegepast kan worden indien dit risico manifest wordt, waaronder de mogelijkheid van controle achteraf.

Nader onderzoek
Het uitgevoerde onderzoek kan gezien worden als een richtingsbepaling voor de methodische en technische basis voor de ABvM infrastructuur op basis van een ‘Dikke Client’. Verder onderzoek is echter noodzakelijk. In de volgende opsomming beperken wij ons tot die aspecten waarin de sectie Digital Security van de RU een belangrijke rol bij zou kunnen spelen:

- Een zowel functioneel als cryptografisch gedetailleerde specificatie van de OBU en het TE die ondermeer een specificatie van de benodigde dataobjecten en functieaanroepen omvat.
- Onderzoek naar smartcardtechnologieën die geschikt zijn om een TE op te baseren.
- Onderzoek naar andere alternatieven en/of hybride methoden/technieken. Een voorbeeld van een dergelijke methode en techniek is die ontwikkeld door W. De Jonge (zie ondermeer [4.]).
- Nader onderzoek naar fall-back scenario’s.
- Ontwikkeling van een *proof of concept* om toetsen of de voorgestelde methoden/technieken voldoende praktisch toepasbaar zijn.

2. Inleiding

2.1 Achtergrond en doelstelling onderzoek

Het project Anders Betalen voor Mobiliteit (ABvM) heeft tot taak een andere manier van betalen te realiseren voor het weggebruik door motorvoertuigen (personenvervoer, vrachtvervoer). Daarbij wordt gedacht aan mechanismen waarbij personen betalen voor het daadwerkelijk gebruik van wegen.

Eind 2007 heeft het kabinet besloten een intelligente On-board Unit (OBU ook wel 'Dikke Client' genoemd) te gebruiken in motorvoertuigen die ondermeer beschikt over GPS voor plaatsbepaling en die in staat is op betrouwbare wijze te communiceren met de ABvM infrastructuur.

2.2 Doelstelling en reikwijdte

De RDW heeft de sectie Digital Security van de Radboud Universiteit (RU) gevraagd hiernaar een onderzoek uit te voeren. De doelstelling van het onderzoek is het komen tot één of meerdere hoofdlijn voorstellen voor een techniek/methode waarmee ABvM-deelnemer weggebruik informatie beschikbaar kan komen bij de ABvM-organisatie die:

- de juiste functionaliteit heeft om te kunnen factureren
- de juiste betrouwbaarheid heeft (waaronder fraudebestendigheid)
- de privacy van de deelnemers (feitelijk de eigenaren van motorvoertuigen) voldoende beschermt.

Bij de te ontwikkelen techniek/methode wordt rekening gehouden met de taken van de ABvM-organisatie (naar verwachting privaat belegd) en de vier publieke taken die ondersteund moeten worden binnen het ABvM concept. Deze vier publieke taken zijn:

- Handhaving: met een (geautomatiseerde) controle langs de kant van de weg moet kunnen worden vastgesteld of de ABvM-deelnemer al niet fraudeert. Daarbij kunnen handhaafteams bijvoorbeeld (verdekt) opgesteld staan naast de (snel)weg of, zoals in de Duitse variant van 'ABvM' voor vrachtvervoer, zelf over de wegen rijdend de controle vanuit de auto doen (in Duitsland door middel van een infrarood verbinding). Ook is het in beginsel mogelijk dat handhavingsteams bij geparkeerde auto's controles uitvoeren.
- Revenu Assurance: deze biedt (boekhoudkundige) zekerheid voor de overheid dat de vereden kilometers ook worden gefactureerd door de ABvM-organisatie en dat revenuen van de gefactureerde kilometers ook worden afgedragen aan de overheid. Er is aangenomen dat geautomatiseerde boekhoudkundige controles de voorkeur verdienen boven handmatige.
- Beroep & Bezwaar: de ABvM-deelnemer moet de factuur kunnen toetsen aan gereden kilometers en bij storingen moet de deelnemer over voldoende informatie voor een eventuele klachtafhandeling kunnen beschikken
- Informatieverstrekking: het moet mogelijk zijn informatie te verstrekken aan beleidsmakers van de overheid voor verkeersmanagement, prijsbeleid en statistische doeleinden.

Het onderzoek heeft zich geconcentreerd op personenvervoer en er is niet expliciet gekeken naar vrachtvervoer en naar buitenlandsvervoer. De resultaten van het onderzoek lijken evenwel ook technisch toepasbaar op deze twee typen vervoer, zij dat zich hieromtrent additionele vragenstukken voordoen. Eén van deze vraagstukken is of men buitenlanders kan verplichten om Nederlandse 'kastjes' te laten gebruiken. Deze vraagstukken zijn niet onderzocht.

2.3 Aanpak en resultaten

- Op 12 februari 2008 heeft een eerste oriënterende vergadering van de RDW en de RU plaatsgevonden in de RDW locatie te Veendam. Hierbij was de heer prof. dr. E.R. Verheul aanwezig vanuit de RU. Aanwezig vanuit de RDW waren de heren ir. G. Maneschijn CISSP, G. Paulusma en A. Uuldriks. Deze vergadering heeft geleid tot een eerste beschrijving van de ABvM-context, de dreigingen daarbinnen alsmede de gerelateerde functionaliteiten voor een ABvM methode/techniek. Op 12 februari hebben Maneschijn en Verheul een idee ontwikkeld voor een dergelijke methode/techniek.
- Op 22 februari 2008 heeft een workshop plaatsgevonden op de RU. Van de RU waren aanwezig de heren prof. dr. B.P.F. Jacobs, dr. W.G. Teepe en prof. dr. E.R. Verheul. De heer ir. G. Maneschijn CISSP was aanwezig vanuit de RDW. Tijdens deze workshop zijn de concepten beschreven in versie 0.1 van het voorliggende document bediscussieerd waarbij het accent lag op de ABvM-context, de dreigingen daarbinnen en de ABvM functionaliteiten.
- Op 27 februari 2008 heeft een tweede workshop plaatsgevonden op de RU. Van de RU waren aanwezig de heren F. Garcia, prof. dr. B.P.F. Jacobs, dr. W.G. Teepe en prof. dr. E.R. Verheul en van de RDW de heren ir. G. Maneschijn CISSP, A. Mulder en G. Paulusma. Tijdens deze workshop zijn de concepten beschreven in versie 0.2 van het voorliggende document bediscussieerd. Eerder ontwikkelde functionaliteiten zijn tijdens deze workshop ingedeeld in gewenste en vereiste functionaliteiten. Verder heeft een indicatieve vergelijking plaatsgevonden tussen deze functionaliteiten en de ontwikkelde ABvM methode/techniek.
- Op 1 maart 2008 is een concept rapportage opgesteld en ter commentariëring naar alle participanten binnen het onderzoek gestuurd. De commentaren zijn verwerkt in een tweede concept versie die op 18 maart 2008 verstuurd is aan de opdrachtgever.
- De definitieve versie van de rapportage is opgeleverd op 2 april 2008. Deze versie is overigens niet inhoudelijk verschillend van de tweede concept versie.

2.4 Leeswijzer

Dit document is als volgt opgebouwd:

- In Sectie 3 staat de beschrijving van de ABvM-context die gehanteerd is in het onderzoek
- In Sectie 4 staan de bedreigingen die zijn voorzien in deze context
- In Sectie 5 staan de (afgeleide) eisen die zijn gehanteerd voor de genoemde techniek/methode
- In Sectie 6 staan een voorstel in hoofdlijn en varianten daarop die in zekere mate voldoen aan de eisen genoemd in Sectie 5
- In Sectie 7 hebben wij een indicatieve vergelijking gemaakt tussen de eisen en wensen

gedocumenteerd in Sectie 5 en het voorstel in Sectie 6
- Sectie 8 bevat een verwijzing naar de geraadpleegde literatuur en documentatie

3. ABvM Context

Bij het onderzoek zijn wij uitgegaan van een context waarin een kleine computer (On-board Unit of OBU) aanwezig is aan boord van motorvoertuigen die vergezeld is van een 'trusted element' (TE). Het TE is onlosmakelijk verbonden met de OBU, bijvoorbeeld door middel van een zegel, en daarmee impliciet met de eigenaar van het motorvoertuig. Het TE maakt een klein onderdeel uit van de OBU. Aan de OBU worden geen eisen rond betrouwbaarheid verondersteld. Dit betekent dat de OBU niet verondersteld is om *trusted* te zijn en dat daarmee input die de OBU levert (door middel van aanroepen) aan het TE gemanipuleerd kunnen worden, bijvoorbeeld doordat de OBU 'gehackt' is. Zoals we hieronder nader zullen uitleggen, sluiten we niet (preventief) uit dat OBUs in opdracht van hun eigenaar frauduleus handelen, maar vereisen wij dat dergelijk handelen door de ABvM-organisatie later kan worden vastgesteld (en bestraft). Het concept sluit aan bij het 'Wallet with observer' concept van David Chaum en Torben Pedersen ([3.]) met dit verschil dat in het concept van Chaum en Pedersen de deelnemer wordt beschermd tegen de kwaadaardige buitenwereld en in het onderhavige concept de buitenwereld (de ABvM-organisatie) wordt beschermd tegen de kwaadaardige deelnemer.

In het onderzoek is de verrekening van het weggebruik bij verkoop van het motorvoertuig aan een volgende gebruiker een aandachtspunt: er moet worden gewaarborgd dat de nieuwe eigenaar niet betaalt voor het weggebruik door de vorige eigenaar en omgekeerd.[1]

Een TE lijkt op een (contact) smartcard met enige additionele functionaliteit die eenvoudig in te passen is op bestaande smartcard technologie. De fysieke beveiliging van het TE (e.g., ter voorkoming van private sleutel extractie) is van fundamenteel belang voor de betrouwbaarheid binnen deze opzet van ABvM. De OBU (en niet het TE) is voorzien van een GPS ontvanger die mogelijk gekoppeld is aan de snelheidsmeter en afstandmeter van de auto (speedo- en odometer) en ook voorzien van (in ieder geval beperkte) kaartinformatie gerelateerd aan die stukken van het wegennet waarvoor meer betaald moet worden dan het standaard tarief.

Fundamenteel binnen ABvM is een concept van 'afgelegde weg' waarvan de specificaties (soort weg, tijdstip gebruik en dergelijke) de uiteindelijke (kilometer) prijs bepalen. In onze context zijn wij ervan uitgegaan dat een rit met een motorvoertuig is opgebouwd uit (kleinere) 'trajecten'. Zie onderstaande figuur. 'Trajecten' bevinden zich tussen de strepen (metingen). Bij een breedmazige trajectopbouw zou de A2 tussen Amsterdam en Maastricht één traject kunnen zijn; en bij een (erg) fijnmazige opbouw zou elke 100 meter tussen twee (groene) hectometers langs de snelweg een traject kunnen zijn. In zijn algemeenheid geldt dat de fijnmazigheid van trajecten in ieder geval zodanig moet zijn dat voldoende nauwkeurige prijsberekening mogelijk is.

[1] *Men kan zich ook voorstellen dat het TE gekoppeld is aan een persoon in plaats van aan een auto zodat men in de auto van iemand anders kan rijden met diens eigen kaart. Dit kan echter ook weer aanleiding geven tot allerlei (geveinsde) storingen en support inspanning van de ABvM helpdesk.*

Wij hebben twee soorten trajectindelingen onderscheiden:

- Statische trajecten
  De ABvM-organisatie deelt het (Nederlandse) wegnet vooraf in stukken (de trajecten) op, waarbij van de begin- en eindpunten de GPS posities zijn gegeven. De OBU houdt bij of deze een dergelijk begin- of eindpunt passeert. Elke passage van een dergelijk punt wordt gelogd, en opeenvolgende punten bepalen welk traject (kennelijk) verreden is. De opzet met DSRC-tags onderzocht binnen het RDW project Uitwerken Procesarchitectuur ABvM (UPA) was gebaseerd op statische trajecten. Mogelijk probleem bij deze opzet zijn nieuwe en buitenlandse wegen.
- Dynamische trajecten
  De OBU bepaalt zelf op regelmatige tijds- of afstandsintervallen, waarvan de minimale en maximale periodiciteit is voorgeschreven, de GPS positie en voert op basis van deze en de vorige GPS meting een *roadmapping* uit: welk stukje weg (het traject) in het afgelopen interval is gereden. Daarbij kan men zich voorstellen dat in bijzondere gevallen een dergelijk traject bestaat uit verschillende (prijs)typen wegen (een stuk stadsweg en een stuk snelweg). De OBU zal dan het gemeten traject verdelen in twee of meer stukken.

In onze context zijn wij uitgegaan van dynamische trajecten, maar de verwachting is dat onze concepten ook van toepassing zijn op statische trajecten. Wij merken nog op dat door middel van trajecten in beginsel ook cordon heffingen, die bijvoorbeeld worden geheven bij het inrijden van een stad, kunnen worden geïmplementeerd. Daartoe kan men kleine delen van toegangswegen beprijzen met een tarief overeenkomend met de cordon heffing. Overigens zal het waarschijnlijk niet eenvoudig zijn een sluitende implementatie van cordon heffingen te implementeren waarbij enerzijds fraude niet mogelijk is en waarbij het anderzijds ook niet mogelijk is dat sommige deelnemers onterecht meerdere malen de cordon heffing moeten betalen.

De OBU/TE zal op enig moment dienen te communiceren met de ABvM-organisatie over de ‘verreden’ kilometers. Hierbij wordt zodanige trajectgerelateerde informatie verstrekt dat op basis daarvan een factuur kan worden geproduceerd. Wij gaan in onze context dus uit van een Post-paid situatie. Voor de communicatie met de ABvM-organisatie komen drie

mogelijkheden in aanmerking:

1. de OBU beschikt over een draadloze verbinding (zoals bijvoorbeeld GPRS UMTS of WiFi) waarbij de verbinding met de ABvM-organisatie permanent aan staat
2. de OBU beschikt over een draadloze verbinding (zoals bijvoorbeeld GPRS UMTS of WiFi) waarbij de verbinding met de ABvM-organisatie automatisch periodiek (bijvoorbeeld één keer per dag) wordt gemaakt wordt gemaakt en op verzoek van de deelnemer
3. de OBU beschikt niet over een draadloze verbinding met de ABvM-organisatie maar de ABvM-deelnemer verstrekt de benodigde informatie zelf via het internet; via een USB-aansluiting van de OBU zou informatie uit de OBU kunnen worden gehaald

Deze mogelijkheden, met name de laatste, voorzien aldus ABvM-deelnemers het initiatief van versturing in eigen hand te nemen. Vanuit privacy perspectief heeft dit voordelen, maar procesmatig heeft het grote nadelen omdat ABvM deelnemers die de versturing niet hebben uitgevoerd, moeten worden benaderd door de ABvM organisatie. ABvM-deelnemers die zelf het initiatief willen houden voor het versturen van gegevens, dienen daarom hiervoor dan ook expliciet verantwoordelijk te worden gemaakt waarbij sancties staan op het niet nakomen daarvan. Inzake het laatste punt merken wij nog op dat het sowieso praktisch kan zijn als de ABvM-deelnemer gedetailleerde reisinformatie uit zijn OBU kan halen (bijvoorbeeld door middel van een USB aansluiting) en deze op zijn PC kan analyseren.

Zoals eerder aangegeven wordt de OBU niet verondersteld *trusted* te zijn zodat de input die de OBU levert (door middel van aanroepen) aan het TE gemanipuleerd kan worden, bijvoorbeeld doordat de OBU ‘gehackt’ is. In OBU’s die geschikt zijn voor ABvM zou verplicht een bepaalde functionaliteit geïmplementeerd moeten zijn hetgeen het doen van bepaalde aanroepen omvat. Het afwijken van deze spelregels kan geconstateerd (en bestraft) worden. De interface met het TE vanuit de OBU zal gespecificeerd worden als (open) standaard waaronder een Application Programming Interface (API). OBUs zullen door verschillende leveranciers kunnen worden geleverd waarbij er waarschijnlijk wel op enig moment een product certificering kan plaatsvinden om zeker te stellen dat de OBU/TE ABvM *compliant* is. Deze certificering zou dan in principe door elk geaccrediteerd laboratorium kunnen plaatsvinden.

Ook de plaatsing van (gecertificeerde) OBU/TEs kan zodanig gereguleerd worden dat alleen geaccrediteerde (auto)bedrijven dit mogen doen. Het idee hierachter is dat de OBU/TE niet eenvoudig van het ene voertuig in het andere voertuig kan worden geplaatst; er bestaan echter ook andere mechanismen voor dan regulering van de fysieke plaatsing. Zo kan de OBU/TE het voertuig authenticeren middels (het toekomstige) EVI (Electronic Vehicle Identification) en vaststellen of hij zich in het ‘juiste’ voertuig bevindt. Uiteraard is de kwaliteit van authenticatie hier een belangrijk aspect.

De mogelijkheid bestaat dat er verschillende private partijen zullen komen die ABvM-facturatie zullen uitvoeren, vergelijkbaar met de situatie op de telefoonmarkt. Verschillende partijen geven dan een eigen TE uit vergelijkbaar met SIMs in de mobiele telefoonmarkt. Handhaving zal echter naar alle waarschijnlijkheid moeten worden uitgevoerd door een publieke partij. Mogelijk dat ook Revenu Assurance plaatsvindt door private (accountancy) partijen. De controles binnen de ABvM-organisatie moeten overigens bij voorkeur gebaseerd

zijn op geautomatiseerde controles.

Zoals ook duidelijk wordt in Sectie 5 gaan wij uit van de ‘Dikke On-Board Unit’ opzet in motorvoertuigen waarbij de ABvM-organisatie slechts geaggregeerde informatie ontvangt als basis voor facturering. Dit betekent dat de gedetailleerde verkeersgegevens (e.g. de trajecten) niet beschikbaar komen voor de ABvM-organisatie om op basis daarvan te factureren en/of te controleren.

Dit is in lijn met het oorspronkelijke Mobimiles concept geïntroduceerd door Roel Pieper in 2001 in [2.]. In het rapport ‘Het Kan!’ (document [1., bijlage 5]) komt men tot een drietal voorwaarden, waarvan de laatste met het aggregatie concept overeenkomt:

V.1. De deelnemer moet tenminste op verzoek ook anoniem kunnen deelnemen, óf
V.2. Er moet voor de voorziening waarvoor betaald moet worden op zichzelf een goed alternatief bestaan, óf
V.3. De verwerkte verbruiksgegevens met betrekking tot het weggebruik moeten zodanig geaggregeerd zijn dat er niet of nauwelijks informatie over verplaatsingen uit herleid kan worden.

Tijdens het onderzoek is ook kort gekeken naar de ‘Dunne Client’ opzet waarbij plaatsgegevens van ABvM-deelnemers worden verstuurd naar de ABvM-organisatie (of partijen die daarvoor werkzaam zijn). Deze ‘Dunne Client’ opzet is overigens anders dan die onderzocht in het kader van het RDW project Uitwerken Procesarchitectuur ABvM (UPA). Hierbij betrof de ‘Dunne Client’ een zogenaamde DSRC-tag waarmee ABvM-deelnemers slechts op bepaalde plekken (wegkantsystemen) binnen het hoofdwegennet/congestiegebieden hun locatie verstrekten aan de ABvM-organisatie. In de DSRC-tag opzet is vanuit een eerder PwC/RU onderzoek in het kader UPA het voorstel gedaan voor data aggregatie in combinatie met een datakluis.

De ‘Dunne Client’ opzet waar vanuit het huidige onderzoek kort gekeken is, omvat dat plaatsgegevens van ABvM-deelnemers in beginsel vanuit alle locaties op het Nederlandse wegennet worden doorgegeven aan de ABvM-organisatie. Naar mening van de onderzoekers zal de bescherming van deze plaatsgegevens van een dermate hoog niveau moeten zijn dat de ‘Dunne Client’ opzet in vergelijking met de ‘Dikke Client’ opzet op gespannen voet staat met het proportionaliteits- en subsidiariteitsbeginsel. Naar dit beginsel, beschreven in Artikel 8 (“Recht op Privacy”) van het Europees Verdrag voor de Rechten van de Mens wordt ook verwezen in de Memorie van Toelichting op de Wet Bescherming Persoonsgegevens van 2002. Dit beginsel wordt aldaar als volgt beschreven: “Het doel waarvoor de persoonsgegevens worden verwerkt dient in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze te kunnen worden verwerkelijkt.”

De mening van de onderzoekers is dat in de vergelijking tussen de ‘Dikke Client’ en de ‘Dunne Client’ opzet het proportionaliteits- en subsidiariteitsbeginsel van toepassing is en wel om de volgende redenen:

- de aggregatie binnen de ‘Dikke Client’ opzet is fundamenteel ‘minder nadelig’ voor de bescherming van de persoonsgegevens van ABvM-deelnemers dan in de ‘Dunne Client’ opzet

- de ‘Dikke Client’ opzet lijkt ook niet onredelijk in termen van kosten en implementatiecomplexiteit en –risico’s in vergelijking met de ‘Dunne Client’ opzet

Om die reden hebben wij geen nader onderzoek gedaan naar de beveiliging van de ‘Dunne Client’ opzet. Dit is overigens in lijn met een recente uitspraak [5.] van het College Bescherming Persoonsgegevens, waarin ondermeer wordt gesteld: “Het CBP is van oordeel dat de zogeheten ‘dikke’ voertuigapparatuur vanuit het oogpunt van een adequate bescherming van persoonsgegevens de meest aanvaardbare variant van de heffing van kilometerprijs is.”

Er is nog een reden waarom de ‘Dunne Client’ opzet naar mening van de onderzoekers niet acceptabel is, namelijk rond de ‘persoonlijke veiligheid’. Uit de centrale registratie van plaatsgegevens binnen de ‘Dunne Client’ opzet kan in beginsel namelijk worden voorspeld waar een bepaald persoon op een bepaalde tijd zal zijn, hetgeen aanslagen / ontvoeringen e.d. van personen kan faciliteren. Een dergelijk risico moet naar mening van de onderzoekers niet gemitigeerd worden met maatregelen maar gewoon worden vermeden.

4. ABvM beveiligingsgerelateerde bedreigingen

Een volledige risicoanalyse rond ABvM ligt niet in de scope van het onderzoek. In het kader van het onderzoek zijn echter wel op informele wijze beveiligingsgerelateerde bedreigingen geïnventariseerd als hulpmiddel bij het opstellen van de functionaliteiten. De onderstaande lijst heeft evenwel niet de pretentie volledig te zijn. De tweede kolom in onderstaande tabel relateert de geformuleerde dreigingen aan de eisen en wensen geformuleerd in de volgende sectie. Daarbij wordt niet gesteld dat de beschreven bedreiging volledig wordt gemitigeerd door de eisen en wensen. Bedreigingen 6 en 17 worden niet gemitigeerd door de geformuleerde eisen en wensen en dienen in ieder geval additioneel te worden gemitigeerd.

#	Beschrijving bedreiging ABvM	# Eisen/ Wensen
1.	De (fysieke) beveiliging van het TE raakt gecompromitteerd.	9
2.	Het systeem is zo complex dat de helpdesk teveel belast wordt met vragen zodat ABvM-deelnemers niet in staat zijn op tijd te betalen (of een excuus hebben dat niet te doen).	1, 2, 3, 4, 5, 7, 32, 33
3.	Het systeem heeft geen controlemechanismen om verbanden te leggen tussen daadwerkelijk (geconstateerd) weggebruik en uitgegane facturen.	19, 20, 21, 22
4.	Onbevoegden halen (gevoelige) informatie uit de OBU van een deelnemer (door middel van inbraak, inbraak op eventuele wireless communicatiekanalen).	8, 10-18
5.	Continu gebruik van GPRS/UMTS vanuit een OBU/TE maakt deelnemers traceerbaar.	8, 17
6.	Onbevoegden storen OBUs zodat facturering (met name die voor henzelf) niet meer mogelijk is.	-
7.	Rijden op andermans kosten (bijvoorbeeld door middel van het clonen van TEs of diefstal).	9, 24-31
8.	Bemachtigen van andermans OBU/TE en vervolgens daarmee frauduleus handelen om hiermee de schuld bij een ander te kunnen leggen (e.g. ‘cat-vangers’).	24-31
9.	ABvM-deelnemers kunnen frauderen door hun OBU/TE soms even uitzetten	24-31
10.	ABvM-deelnemers kunnen frauderen door hun OBU/TE onklaar maken	24-31
11.	ABvM-deelnemers kunnen frauderen door hun OBU/TE met verkeerde GPS / ODO gegevens te voeden	24-31
12.	ABvM-deelnemers kunnen frauderen door een OBU/TE van een ander motorvoertuig te gebruiken	24-31
13.	ABvM-deelnemers hacken de OBU en zorgen ervoor dat deze aanroepen met onjuiste parameters (verkeerde GPS coördinaten bijvoorbeeld) doet aan het TE.	24-31
14.	ABvM-deelnemers zorgen dat er geen of verkeerde reisinformatie wordt opgeleverd waardoor verkeerde facturen ontstaan.	24-31

15.	De ABvM-organisatie incasseert meer geld bij de ABvM-deelnemers dan wordt opgegeven bij de overheid.	19-23
16.	Handhavingsapparatuur verdwijnt en maakt het mogelijk dat onbevoegden OBU/TEs kunnen uitlezen.	12
17.	Vandalisme / obstructie van de OBU/TE op grote schaal om de goede werking van ABvM te frusteren. Voorbeelden hiervan zijn het: - 'flashen' (door middel van een sterk magnetische puls het onbruikbaar maken van apparatuur) - verspreiden van OBU virussen en andere kwaadaardige software	-

5. ABvM eisen / wensen

In onderstaande tabel zijn de eisen / wensen geformuleerd die wij hanteren voor een gewenste ABvM methode/techniek. Hierbij is de volgende indeling gehanteerd:

A. Functionaliteit
B. Privacy
C. Revenu Assurance
D. Handhaving
E. Beroep en Bezwaar
F. Informatie verstrekking

#	A. Functionaliteit	Eis / Wens
1.	Het rekenmodel dat ten grondslag ligt aan ABvM moet eenvoudig uit te leggen zijn aan deelnemers.	**W**
2.	Het rekenmodel moet een overzichtelijke hoeveelheid (prijs)categorieën (‘Goudmerk’, ‘Zilvermerk’, ‘Roodmerk’ etc.) ondersteunen op basis van ondermeer prijsklassen van wegen, tijdstippen, milieutype auto, ‘off-the-chart’, buitenland en ‘geen GPS signaal’.	**E**
3.	Het systeem moet het mogelijk maken een implementatie te maken die voor iedereen bedienbaar is, ook voor computeranalfabeten en/of mensen zonder Personal Computers. *Noot: dit laat onverlet dat het systeem ook technologisch complexe implementaties moet kunnen toestaan waarmee de deelnemer door middel van zijn PC en internet (e.g., Google maps) allerhande analyses kan uitvoeren rond zijn eigen weggebruik.*	**E**
4.	ABvM-deelnemers moeten op elk moment de balans op kunnen (laten) maken van hun weggebruik. *Noot: dit is bijvoorbeeld een belangrijke voorwaarde als een eigenaar zijn motorvoertuig wil verkopen en dus overschrijven naar een andere eigenaar. Men zou zich kunnen voorstellen dat er een knop op de OBU zit getiteld ‘replicate now’ en die de laatste standen opstuurt.*	**E**
5.	ABvM-deelnemers moeten direct na een ‘rit’ kunnen zien wat deze gekost heeft. *Noot: dit is belangrijk omdat deelnemers zo desgewenst hun rijgedrag kunnen aanpassen. Het is niet zo dat daarmee een prijstabel in de OBU/TE ook automatisch actueel gehouden hoeft te worden (hetgeen weer kostbaar is). Het kan ook betekenen dat de OBU zelf de mogelijkheid heeft om de kosten van de rit te berekenen op basis van een prijstabel die de deelnemer zelf intypt; dit heeft daarmee niet de status van een factuur. Veel telefoontoestellen hebben een dergelijk mechanisme overigens ook.*	**W**
6.	Updates van het OBU/TE systeem moeten niet of alleen in uitzonderlijke gevallen noodzakelijk zijn (kaartdata en software).	**E**

7.	ABvM-deelnemers moeten zelf inzicht kunnen hebben in hun weggebruik registratie die is opgeslagen in hun OBU/TE.	**E**
8.	De communicatie door middel van GPRS/UMTS moet zoveel mogelijk beperkt blijven.	**E**
9.	Voorzover de beveiliging van het systeem is gebaseerd op aannamen die niet noodzakelijk toekomstvast zijn (e.g., rond fysieke beveiliging van het TE) dient het systeem een *fall-back* scenario te hebben voor het geval deze aannamen niet meer geldig zijn. Dit is een scenario waarmee – waarschijnlijk met relatief veel personele inspanning van ABvM-medewerkers – het systeem op gecontroleerde wijze naar een nieuwe veilige toestand kan worden gebracht (e.g., uitrol van nieuwe TEs).	**E**
B. Privacy		
10.	De gegevens met betrekking tot het weggebruik aanwezig buiten de OBU/TE moeten zodanig geaggregeerd zijn dat er niet of nauwelijks informatie over verplaatsingen uit herleid kan worden (bron: het rapport 'Het Kan!').	**E**
11.	ABvM-deelnemers moeten in staat zijn hun weggebruik registratie te vernietigen met als uitzondering misschien recente registraties.	**E**
12.	Alle logische toegang tot de OBU/TE door de ABvM-organisatie (handhaving, kaart- en/of software updates) moet geauthenticeerd zijn, waarbij: - deelnemers (op enig moment) worden genotificeerd van een handhaving - deelnemers moeten kunnen vast stellen welke (automatische) ABvM-updates er zich hebben voorgedaan en wanneer Specifiek moet rekening worden gehouden met handhavingsapparatuur die verdwijnt (gestolen, verloren e.d.): dergelijke apparatuur mag geen groot risico vormen voor de (privacy) van deelnemers.	**E**
13.	Van ABvM-deelnemers kan geëist worden meer privacygevoelige gegevens te openbaren aan de ABvM-organisatie indien hun gedrag afwijkt van de spelregels en daarom mogelijk frauduleus is (*revocable privacy*).	**E**
14.	De opzet van het systeem en diens protocollen, dataformaten en (fysieke) interfaces moet 'open' gespecificeerd zijn; er mag geen gebruik worden gemaakt van *proprietary* standaarden.	**E**
15.	De ABvM-deelnemers moeten erop kunnen vertrouwen dat hun OBU/TE geen *covert channels* bevat.	**E**
16.	Alle informatie die verstuurd wordt vanuit de OBU/TE moet inspecteerbaar / leesbaar zijn voor de ABvM-deelnemer door middel van logs.	**E**
17.	ABvM-deelnemers mogen niet verplicht worden constant een (GPRS/UMTS) radioverbinding actief te hebben. *Noot: met een dergelijke verbinding kunnen de bewegingen van ABvM-deelnemers in principe in kaart worden gebracht.*	**E**
18.	Het aantal en typen prijscategorieën van wegen moet zodanig beperkt worden dat de privacy van de ABvM-deelnemer niet in gevaar komt. Hieronder valt ook dat locaties (e.g., bruggen) geen unieke of zeldzame prijscategorieën moeten zijn.	**E**
C. Revenu Assurance		

19.	De registraties die vanuit de OBU/TE worden opgeleverd aan de ABvM-organisatie moeten onweerlegbaar zijn, dat wil zeggen dat de ABvM-deelnemer niet kan claimen dat deze niet uit zijn OBU/TE afkomstig zijn.	**E**
20.	Een partij extern aan de ABvM-organisatie (extern accountant) moet eenduidig kunnen vaststellen dat: - de registraties die vanuit de OBU/TE zijn opgeleverd aan de ABvM-organisatie volledig en compleet zijn - dat de uitgegane facturen corresponderen met deze registraties	**E**
21.	De registraties die vanuit de OBU/TE worden opgeleverd moeten een beperkt aantal fraude gerelateerde excepties kunnen bevatten, zoals bijvoorbeeld een te 'grote' afstand tussen twee opeenvolgende door de OBU gemeten GPS locaties, mogelijk corresponderend met het uitzetten van de OBU/TE (anomalie detectie).	**W**
22.	De handhavingscontroles samen met de registraties vanuit de OBU/TE bieden de ABvM-organisatie voldoende zekerheid dat het daadwerkelijke weggebruik correspondeert met het gefactureerde gebruik.	**E**
23.	De ABvM-organisatie mag de weggebruikgegevens van deelnemers niet ongecontroleerd kunnen aanpassen.	**E**
	D. Handhaving	
24.	De volgende zaken moeten kunnen worden opgevraagd bij handhaving: - status van de OBU/TE (aan/uit) - 'evidence' dat (uiteindelijk) betaald wordt voor het weggebruik waarbij correct is meegenomen: type weg en tijd	**E**
25.	De volgende zaken moeten kunnen worden opgevraagd bij handhaving: - 'excepties', bijvoorbeeld corresponderend met de situatie dat een OBU/TE uit heeft gestaan	**W**
26.	Frauderende ABvM-deelnemers moeten niet in praktische zin in staat zijn – als ze de ABvM handhavingscontrole zien aankomen – hun fraude sporen uit te wissen en ongedetecteerd de controle te passeren.	**E**
27.	Er moet direct kunnen worden geconstateerd of een deelnemer fraudeert. Iemand moet direct staande kunnen worden gehouden zodat geen gezeur achteraf ontstaat. Controle moet ook automatisch kunnen gebeuren (*on-the-spot controle*).	**E**
28.	Het moet eenvoudig mogelijk zijn te controleren of een OBU in een motorvoertuig zich aan de spelregels houdt; ondermeer moet - de handhavingscontrole op afstand mogelijk zijn - de handhavingscontrole relatief goedkoop uit te voeren zijn	**E**
29.	Het moet effectief mogelijk zijn te controleren of een OBU in een motorvoertuig zich aan de spelregels houdt; doordat ondermeer - de plaatsen waar deze controle kan plaatsvinden niet vooraf gebonden zijn aan plaats of tijd - handhavingscontroles opschaalbaar zijn in tijden dat meer fraude lijkt te worden gepleegd - de informatie afkomstig van deelnemer (die kan worden gecontroleerd) binnen zekere grenzen aanpasbaar is	**E**

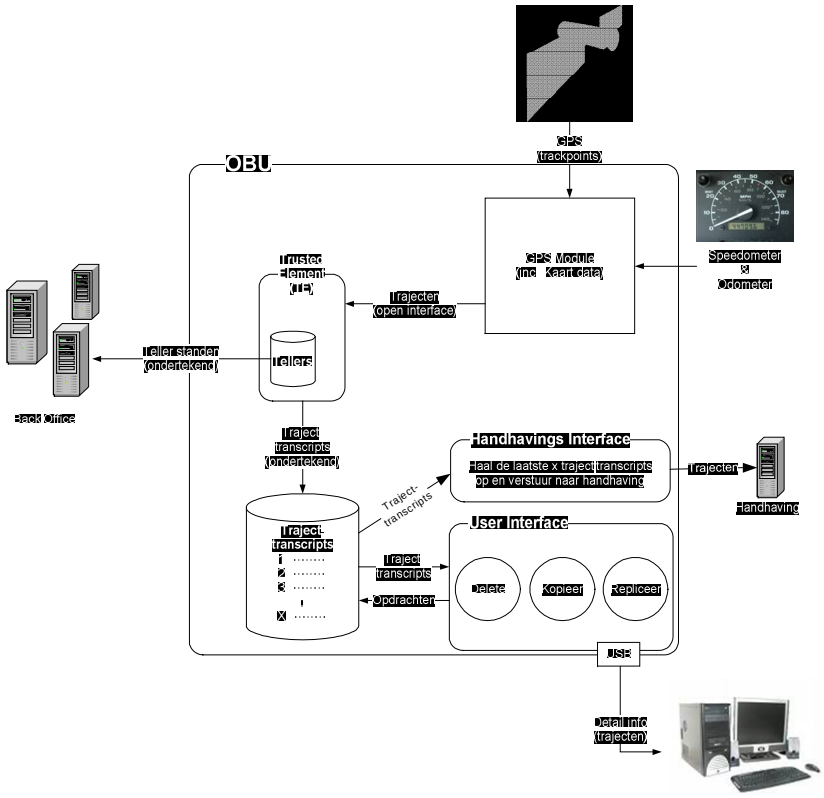
30.	De handhavingscontroles moeten zonder detectie van de deelnemers kunnen plaatsvinden. *Noot:* - *Het idee hier achter is dat als detectie niet onopvallend plaatsvindt, deelnemers mogelijk via een gemeenschappelijk kanaal (internet, radio) elkaar hiervan op de hoogte stellen ('OBU/TE aanzetten op de A2 bij Den Bosch') zoals dat nu ook bij mobiele flitsteams gebeurt. De vraag is of het sociaal acceptabel wordt geacht om hier aan mee te werken, feitelijk werkt men dan namelijk mee aan belastingontduiking.* - *Men kan zich ook het scenario voorstellen dat er verschillende soorten handhavingscontrole apparaten zijn: systemen die echt de controle uitvoeren (met name door middel het maken van foto's) en (goedkopere) systemen die alleen maar kijken of OBU's aanstaan en (nog goedkopere) systemen die niet controleren maar niet te onderscheiden zijn van apparaten die wel een volledige controle uitvoeren.*	**W**
31.	Het moet op een gebruikersvriendelijke manier mogelijk zijn te controleren of een motorvoertuig zich aan de ABvM-regels houdt, zo moeten bijvoorbeeld - de inspanningen van de deelnemer minimaal zijn - de handhavers een motorvoertuig niet te hoeven laten stoppen	**E**
	E. Beroep en Bezwaar	
32.	ABvM-deelnemers moeten inzicht kunnen krijgen in welke factuurgerelateerde informatie naar de ABvM wordt gestuurd en moeten deze factuurgerelateerde informatie kunnen relateren aan enerzijds de daaruit volgende factuur en anderzijds de gedetailleerde reisinformatie in de OBU/TE die zodanig is dat een dispuut oplosbaar is.	**E**
33.	De ABvM-deelnemers moet de factuurgerelateerde informatie en de gedetailleerde reisinformatie uit hun OBU/TE zodanig kunnen exporteren dat de authenticiteit en betrouwbaarheid gewaarborgd is.	**E**
	F. Informatie verstrekking	
34.	Alle ABvM-deelnemers kan worden gevraagd om hun weggebruik in gepseudonimiseerde vorm te verstrekken aan de ABvM organiatie, deelnemers kunnen echter weigeren daaraan mee te werken. De gebruikte pseudoniemen: - veranderen elke dag - zijn niet herleidbaar tot identiteiten door de ABvM-organisatie - zijn niet onderling koppelbaar door de ABvM-organisatie (dat wil zeggen de pseudoniemen van vandaag zijn niet herleidbaar aan die van morgen etcetera). *Noot: de hoeveelheid gegevens kan weleens zo groot zijn dat versturen door middel van GPRS / UMTS te kostbaar is. Als alternatief kan dan gekozen worden voor versturing door middel van internet. Verder kunnen de ABvM-deelnemers die hier aan mee werken financieel worden beloond.*	**W**

6. Voorstel ABvM methode/techniek in hoofdlijn

Het volgende voorstel is in de bijeenkomst op 12 februari tussen ir. G. Maneschijn CISSP en prof. dr. E.R. Verheul onwikkeld en in latere workshops verder verfijnd. Er zijn allerhande variaties mogelijk. Het voorliggende voorstel kan gezien worden als een variant van het systeem beschreven door W. De Jonge in [4]. Behalve een aantal concretere keuzen, bevat het voorliggende voorstel ook een aantal aanvullingen op het systeem beschreven in [4]; deze zijn ondermeer:

- dat de ‘postbus’ uit [4] op cryptografische wijze is geïmplementeerd en
- dat het voorliggende voorstel aanvullend op de dataobjecten ‘Aangiften’ uit [4] die (in onze terminologie) bedoeld zijn voor de ABvM-organisatieook de dataobjecten ‘traject-transcript’ introduceert. Anders dan ‘Aangiften’ zijn traject-transcripts’ privé voor de ABvM-deelnemer; slechts de ‘laatste’ kunnen opgevraagd worden door handhavingsteams langs de kant van de weg. De ‘traject-transcripts’ kunnen ook gebruikt worden door de ABvM-deelnemer om zijn afrekeningen mee te controleren en de deelnemer kan door middel van de traject-transcripts ook onderbouwd bezwaar aantekenen (Beroep en Bezwaar).

Zoals beschreven in Sectie 3 zijn wij uitgegaan van een context waarin een kleine computer (On-board Unit of OBU) aanwezig is aan boord van motorvoertuigen die vergezeld is van een ‘trusted element’ (TE). Het TE maakt een klein onderdeel uit van de OBU. Aan de OBU worden geen eisen rond betrouwbaarheid verondersteld. Het TE is onlosmakelijk verbonden met de OBU, bijvoorbeeld door middel van een zegel, en daarmee impliciet met de eigenaar van het motorvoertuig. Het TE maakt een klein onderdeel uit van de OBU waaraan geen eisen rond betrouwbaarheid worden verondersteld. Dit betekent dat de OBU niet verondersteld is om *trusted* te zijn en dat daarmee input die de OBU levert (door middel van aanroepen) aan het TE gemanipuleerd kunnen worden, bijvoorbeeld doordat de OBU ‘gehackt’ is. Zoals we hieronder nader zullen uitleggen, sluiten we niet (preventief) uit dat OBUs in opdracht van hun eigenaar frauduleus handelen, maar realiseren wij dat dergelijk handelen door de ABvM-organisatie later kan worden vastgesteld (en bestraft).



Een TE lijkt op een (contact) smartcard met enige additionele functionaliteit die eenvoudig inpasbaar is op bestaande smartcard technologie. De fysieke beveiliging van het TE (e.g., ter voorkoming van private sleutel extractie of aanpassing van tellers, zie beneden) is van fundamenteel belang voor de betrouwbaarheid binnen deze opzet van ABvM. De OBU (en niet het TE) is voorzien van een GPS ontvanger die mogelijk gekoppeld is aan de snelheidsmeter en afstandmeter van de auto (speedo- en odometer) en ook voorzien van (in ieder geval beperkte) kaartinformatie gerelateerd aan die stukken van het wegennet waarvoor meer betaald moet worden dan het standaard tarief.

Het voorstel gaat uit van een intelligente TE – bijvoorbeeld in de vorm van een Java card – met daarin een public/private sleutelpaar gebonden in een digitaal (X.509) certificaat. Met dit sleutelpaar is het TE in staat digitale handtekeningen te plaatsen op berichten. Daarbij maakt men verder gebruik van standaard mechanismen rond de geldigheid van certificaten (CRLs, OCSP etc.). Het certificaat is gekoppeld aan een voertuig, mogelijk zelfs door middel van een veld in het certificaat.

Het TE is zodanig beschermd dat de cryptografische sleutels niet uit het TE kunnen worden verkregen (niet exportable sleutels, bescherming tegen side-channel aanvallen). Het TE heeft Common Criteria / ITSEC evaluatie ondergaan tegen een relevant Protection Profile met een hoog *assurance level* (bijvoorbeeld EAL 5+ of vergelijkbaar met het biometrisch paspoort).

In het TE bevindt zich ook een aantal ‘secure’ tellers. Deze tellers corresponderen met de verschillende typen wegen die er zijn (e.g., ‘Goud’, ‘Zilver’, ‘Rood’ etc.) en houden de

totaalstand bij van wat de eigenaar van het TE heeft verreden. De tellers kunnen alleen worden opgehoogd (niet verlaagd) en alleen door middel van bepaalde aanroepen (zie onder). Dit is bijvoorbeeld vergelijkbaar met een elektriciteitsmeter met dag- en een nachtstand. In beginsel behoort elke weg (ook buitenlandse wegen) tot een type en wordt de totaalstand ook bijgehouden. Natuurlijk kunnen eventuele wegen waarvoor niet betaald hoeft te worden in één categorie worden geplaatst.

Het concept is verder dat de OBU periodiek (bijvoorbeeld elke minuut of elke kilometer) verreden trajecten vastlegt in traject-transcripts. Hierbij worden in ieder geval voldoende gegevens vastgelegd die voorzien in de controle van deelnemers achteraf. Een dergelijk traject-transcript kan bijvoorbeeld de volgende gegevens vastleggen:

- de huidige en de vorige positie en eventueel de GPS nauwkeurigheid waarmee gemeten is
- de huidige tijdmeting en de vorige tijdmeting
- specificatie van de weg (A2, A4 etc.); daarbij moeten de trajecten zodanig fijnmazig zijn dat de wegspecificatie eenduidig mogelijk is. Zie Sectie 3.
- hoeveel kilometer het voertuig heeft afgelegd
- prijscategorie: Goud, Zilver, Rood, Buitenland etc.

De OBU voert daartoe een traject-aanroep uit naar het TE met deze parameters waarbij de interne logica van het TE de teller van dat wegtype ophoogt. Omdat de OBU niet *trusted* is, hoeven de gegevens in de aanroep niet correct te zijn. Het paradigma dat wordt gehanteerd is dat OBU's mogen 'liegen' maar dat 'liegen' altijd uit kan komen. Om dit te faciliteren verstrekt het TE na de traject-aanroep een 'transcript' bestaande uit deze parameters getekend met de private sleutel in het TE. Deel van getekende boodschap is ook een opvolgend serienummer dat onder controle staat van het TE (de eerste transcript heeft nummer 1, de tweede 2 etc.). Met dit transcript heeft de OBU eigenaar zich vastgelegd en kan deze tegen de 'lamp' lopen bij een handhavingscontrole (zie beneden).

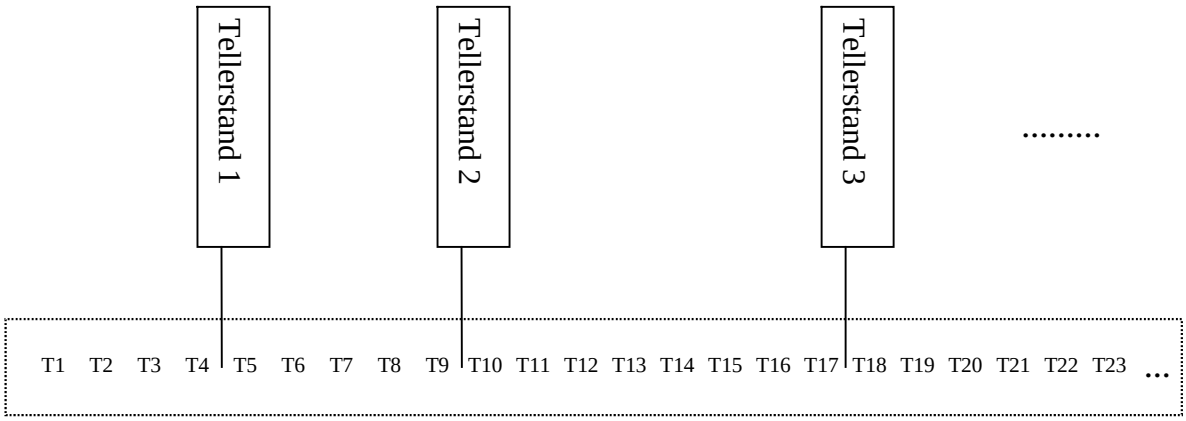
Wij gaan er niet vanuit dat het TE een klok heeft maar het TE houdt wel bij wat de laatst opgegeven tijd is en verstrekt geen transcript als de in de aanroep opgegeven tijd eerder is dan die in de vorige aanroep. Met andere woorden, het TE weigert in zekere mate te anti-dateren. Overigens merken we op dat de GPS in de OBU een uitstekende bron voor nauwkeurige tijd oplevert, dus als de ABvM eigenaar niet probeert de OBU en het GPS signaal te manipuleren dan zal de opgegeven tijd zelden veel afwijken van de 'ware' tijd.

De OBU kan – als de eigenaar dat wil en voorzover de OBU de opslagcapaciteit heeft – al deze traject-transcripts bewaren voor het geval de eigenaar zijn reisgedrag wil analyseren. De OBU logica is echter wel verplicht de meest recente traject-transcripts te bewaren voor handhavingscontroles (zie onder). Door het gebruik van de serienummer kan snel worden vastgesteld of een aantal transcripts aansluitend zijn.

Op gezette tijden dient de OBU (automatisch) te repliceren met de ABvM-organisatie. Hierbij doet de OBU een tellerstand aanroep aan het TE in de zin van 'geef mij een stand van alle tellers'. Het TE tekent deze standen (zoveel Goud, zoveel Zilver, zoveel Rood) in een bericht dat ook voorzien is van een serienummer (om te zorgen dat de OBU niet steeds hetzelfde bericht opstuurt) en bijvoorbeeld – voor redundantie redenen – ook de vorige tellerstanden bevat.

Dit bericht wordt vervolgens door de OBU naar de ABvM-organisatie gestuurd, bijvoorbeeld door middel van GPRS/UMTS op basis waarvan de ABvM-organisatie een factuur kan produceren (factuurbedrag = (verschil standen) x milieufactor x prijs). De OBU heeft ook een knop ‘repliceer nu’ waarmee de OBU niet wacht tot dezelfde repliceer ronde. In de ABvM-organisatie moet wel een automatisch proces zijn dat in de gaten houdt of alle voertuigen wel recent een update hebben gedaan. Voertuigen die dat niet hebben gedaan moeten op zeker moment worden onderzocht.

Schematisch gezien kan men de relatie tussen de trajecten en de periodieke tellerstand opnamen weergegeven als in onderstaand diagram. In het OBU geheugen worden steeds (getekende) traject-transcripts opgeslagen door middel van aanroepen op het TE vanaf de OBU software. Deze zijn aangegeven met T1, T2, T3 etc. Op gezette tijden worden (getekende) tellerstanden (Goud, Zilver, Rood, etc.) opgeleverd door het TE en verstuurd aan de ABvM-organisatie.



OBU geheugen

Instantane handhaving

Instantane handhaving (‘langs de kant van de weg’) in dit concept gaat als volgt. De OBU heeft behalve een ABvM-interface ook nog een handhavingsinterface (bijvoorbeeld gebaseerd op een DRSC of infrarood verbinden). Het TE zal ook zorg kunnen dragen voor de authenticatie van dit handhavingskanaal. De handhavingscontrole moet beginnen met vaststellen of de OBU aanstaat (‘reageert de OBU’). Als dat het geval is kunnen vervolgens de laatste *H* traject-transcripts uitgelezen worden. Hierbij staat de parameter *H* staat voor ‘Historie’, een nader te bepalen getal is, zeg 10.

Vervolgens moet een technische controle plaatsvinden van digitale handtekeningen op de traject-transcripts:

- Kloppen de digitale handtekening in technische zin?
- Zijn de bijbehorende certificaten nog geldig (CA sleutel validatie, CRL/OCSP toetsing)?

Dan moet een controle tussen certificaat en auto plaatsvinden, bijvoorbeeld:
- zijn de certificaten uitgegeven aan het motorvoertuig dat waargenomen wordt? Als het kenteken opgenomen is in het certificaat is dit een eenvoudige test.
- Klopt het milieutype met wat waargenomen wordt?

Tot slot moet gecontroleerd worden of de trajecten in de *H* traject-transcripts stroken met de handhavingsplaats, bijvoorbeeld:
- Zijn de trajecten in lijn met de handhavingplaats?
- Zijn de prijscategorieën correct?

Wij merken nog op dat de gegevens die een motorvoertuig verstrekt in het kader van handhaving in het algemeen niet vertrouwelijk zijn; feitelijk zijn deze gegevens ook gewoon visueel vast te stellen (tenzij de deelnemer fraudeert). Daarbij moet wel de kantekening worden gemaakt dat hoe verder terug de handhavingscontrole kan gaan, hoe privacy gevoeliger kan worden.

De frauduleuze ABvM-deelnemer kan proberen zodra hij het uitlezen signaleert door een handhavingscontrole 'snel' de gevraagde *H* traject-transcripts te maken die de handhaver wil zien (dat wil zeggen met de juiste parameters). Een mitigerende maatregel hiervoor bestaat er uit het TE een minimale tijd te laten vereisen tussen de aanroepen; het TE beschikt weliswaar niet noodzakelijk over een absolute klok maar zijn eigen interne klok levert een mechanisme om de relatieve tijd te meten. Het is essentieel deze relatieve tijd ook op te leggen tussen het 'aanzetten' van het TE en de eerste traject-transcript aanroep omdat anders de vertraging relatief eenvoudig kan worden omzeild.

Handhaving achteraf

In aanvulling op deze weinig 'deelnemer belastende' controles beschreven onder het vorige punt, kunnen ook meer belastende controles plaatsvinden. Hierbij legt men (sommige) deelnemers de verplichting op – bijvoorbeeld die deelnemers waar vaak 'anomalieën' optreden – om een bepaalde historie van traject-transcripts te bewaren voor nacontrole. Vervolgens kan men dan ongemerkt foto's maken van motorvoertuigen en vervolgens de 'anomalie' deelnemers vragen om alle (of alleen de desbetreffende) traject-transcripts ter controle te overleggen. Hier aldus ook sprake van toepassing van het beginsel van revocable privacy zoals besproken in Eis nummer 12 genoemd in Sectie 7. De parameter *T* die correspondeert met de genoemde historie samen met parameter *H* bieden een schaalbare wijze van fraude detectie. Dit type controle is ook passief in de zin dat gezorgd kan worden dat de ABvM-deelnemers de controles niet kunnen detecteren (en anderen hiervan op de hoogte te brengen).

Het verstrekken van traject-transcripts door deelnemers is echter zowel gebruikers- als privacy-onvriendelijk en kan daarom beter niet van alle deelnemers verlangd worden.

Verdere variaties

- Het verplichte repliceer mechanisme richting de ABvM-organisatie biedt ook de gelegenheid om bepaalde excepties mee te sturen. Een ABvM-deelnemer zou bijvoorbeeld geneigd kunnen zijn om zijn OBU/TE alleen op bepaalde wegdelen aan te zetten (bijvoorbeeld op die stukken waarvan hij weet dat er weleens gecontroleerd wordt). Men

kan zich bijvoorbeeld voorstellen dat als de OBU een aanroep doet waaruit blijkt dat het vorige traject (opgeslagen in het TE) niet aansluit op het aangeboden traject, het TE dat constateert en deze exceptie deel laat zijn van de volgende getekende repliceerboodschap: door de handtekening kan de ABvM-deelnemer niet besluiten dit deel van de repliceer boodschap te wissen. Op basis hiervan krijgt de ABvM inzicht in deze excepties en kan hier actie op ondernemen.

- Wat ook mogelijk is om bij ‘ernstige’ excepties een ‘bepaalde’ bit te hebben aanstaan in alle transcripts. Het handhavingsteam ziet dit dan vervolgens en kan besluiten het voertuig staande te houden bijvoorbeeld om deze te laten repliceren (zodat de exceptie details zichtbaar worden).
- In zijn algemeenheid is het een goed idee om uitputtend te kijken wat een ABvM-deelnemer allemaal voor fraude mogelijkheden heeft en te kijken in hoeverre relevante excepties en/of informatie kan worden geplaatst in de repliceerboodschappen.
- Binnen ABvM (of zelfs binnen het TE zelf) kan ook worden vastgelegd hoeveel kilometer er op de teller stond bij de installatie van het TE zodat kan worden vastgesteld of de som van alle tellers in ordegrootte klopt met het verschil in de tellerstanden.

7. Indicatieve vergelijking voorstel met de eisen en wensen

In onderstaande tabel hebben wij indicatief vergeleken of het voorstel beschreven in Sectie 6 de eisen en wensen geformuleerd in Sectie 5 kan ondersteunen. Daarbij hebben wij de volgende kleuren gebruikt:

- Groen, indien ingeschat wordt dat aan de eis kan worden voldaan,
- Oranje, indien de verwachting is dat met enige additionele inspanning aan de eis voldaan kan worden,
- Rood, indien niet aan de eis voldaan kan worden.

In onderstaande tabel zijn geen eisen naar voren gekomen waar niet aan voldaan kan worden, en slechts twee eisen waarvan de verwachting is dat additionele inspanning nodig is om aan de eis te voldoen. Aan de overige eisen lijkt voldaan te kunnen worden. De eerste uitzondering (eis 9) betreft het gebrek aan een fall-back scenario als de (fysieke) beveiliging van het TE wordt gecompromitteerd. De verwachting is evenwel dat een dergelijk fall-back scenario wel ontwikkeld kan worden in een additioneel onderzoek. De tweede uitzondering (eis 30) betreft het niet kunnen uitvoeren van instantane handhavingscontroles zonder detectie. Voor dit type handhavingscontrole dient de OBU namelijk op de handhavingslocatie uitgelezen te worden hetgeen een actieve en dus in beginsel detecteerbare handeling is. Verbonden hiermee is het risico dat ABvM-deelnemers elkaar op de hoogte brengen van handhavingslocaties. Zoals wij hebben beargumenteerd bij de vergelijking van eis 30, biedt het voorstel compenserende ruimte die toegepast kan worden indien dit risico manifest wordt, waaronder de mogelijkheid van controle achteraf.

#	A. Functionaliteit	Eis / Wens	Vergelijking met voorstel in Sectie 6	
1.	Het rekenmodel dat ten grondslag ligt aan ABvM moet eenvoudig uit te leggen zijn aan deelnemers.	**W**	Het voorstel is gebaseerd op trajecten en ‘tellerstanden’ en dat lijkt eenvoudig genoeg om uit te leggen door middel van bijvoorbeeld vergelijkingen met openbaar vervoer en gas-, water en elektriciteit opnamen.	
2.	Het rekenmodel moet een overzichtelijke hoeveelheid (prijs)categorieën (‘Goudmerk’, ‘Zilvermerk’, ‘Roodmerk’ etc.) ondersteunen op basis van ondermeer prijsklassen van wegen, tijdstippen, milieutype auto, ‘off-the-chart’, buitenland en ‘geen GPS signaal’.	**E**	Aan deze eis lijkt voldaan te kunnen worden.	

3.	Het systeem moet het mogelijk maken een implementatie te maken die voor iedereen bedienbaar is, ook voor computeranalfabeten en/of mensen zonder Personal Computers. *Noot: dit laat onverlet dat het systeem ook technologisch complexe implementaties moet kunnen toestaan waarmee de deelnemer door middel van zijn PC en internet allerhande analyses kan uitvoeren rond zijn eigen weggebruik.*	**E**	Aan deze eis lijkt voldaan te kunnen worden.	
4.	ABvM-deelnemers moeten op elk moment de balans op kunnen (laten) maken van hun weggebruik. *Noot: dit is een belangrijke voorwaarde als een eigenaar zijn auto bijvoorbeeld wil verkopen en dus overschrijven naar een andere eigenaar. Men zou zich kunnen voorstellen dat er een knop op de OBU zit getiteld 'replicate now' en die de laatste standen opstuurt.*	**E**	Dit is afhankelijk van de OBU implementaties maar het lijkt dat aan deze eis voldaan kan worden.	

5.	ABvM-deelnemers moeten direct na een ‘rit’ kunnen zien wat deze gekost heeft. *Noot: dit is belangrijk omdat juist zo deelnemers hun rijgedrag zouden kunnen aanpassen. Verder is het niet zo dat daarmee een prijstabel in de OBU/TE ook automatisch actueel gehouden hoeft te worden (hetgeen weer kostbaar is). Het kan ook betekenen dat de OBU zelf de mogelijkheid heeft om dit te berekenen op basis van een prijstabel die de deelnemer zelf intypt; dit heeft daarmee niet de status van een factuur. Veel telefoontoestellen hebben een dergelijk mechanisme overigens ook.*	**W**	Dit is afhankelijk van de OBU implementaties maar het lijkt dat aan deze eis voldaan kan worden.	
6.	Updates van het OBU/TE systeem moeten niet of alleen in uitzonderlijke gevallen noodzakelijk zijn (kaartdata en software).	**E**	Dit is mede afhankelijk van de wijze waarop veranderingen in de beprijzingen tot stand komen, maar het lijkt dat aan deze eis voldaan kan worden.	
7.	ABvM-deelnemers moeten zelf inzicht kunnen hebben in hun weggebruik registratie die is opgeslagen in hun OBU/TE.	**E**	Dit is afhankelijk van de OBU implementaties maar het lijkt dat aan deze eis voldaan kan worden.	
8.	De communicatie door middel van GPRS/UMTS moet zoveel mogelijk beperkt blijven.	**E**	Dit is afhankelijk van de OBU implementaties maar het lijkt dat aan deze eis voldaan kan worden.	

9.	Voorzover de beveiliging van het systeem is gebaseerd op aannamen die niet noodzakelijk toekomstvast zijn (e.g., rond fysieke beveiliging van het TE) dient het systeem een *fall-back* scenario te hebben voor het geval deze aannamen niet meer geldig zijn. Dit is een scenario waarmee – waarschijnlijk met relatief veel personele inspanning van ABvM-medewerkers – het systeem op gecontroleerde wijze naar een nieuwe veilige toestand kan worden gebracht (e.g., uitrol van nieuwe TEs).	**E**	Het huidige voorstel biedt nog geen fall-back scenario tegen met name een compromittatie van het TE. Er lijken echter wel mogelijkheden te zijn om dit realiseren. Hiervoor is additioneel onderzoek noodzakelijk.	
B. Privacy				
10.	De gegevens met betrekking tot het weggebruik aanwezig buiten de OBU/TE moeten zodanig geaggregeerd zijn dat er niet of nauwelijks informatie over verplaatsingen uit herleid kan worden (bron: het rapport 'Het Kan!').	**E**	Aan deze eis wordt voldaan.	
11.	ABvM-deelnemers moeten in staat zijn hun weggebruik registratie te vernietigen met als uitzondering misschien recente registraties.	**E**	Dit is afhankelijk van de OBU implementaties maar het lijkt dat aan deze eis voldaan kan worden.	

12.	Alle logische toegang tot de OBU/TE door de ABvM-organisatie (handhaving, kaart- en/of software updates) moet geauthenticeerd zijn, waarbij: - Deelnemers (op enig moment) worden genotificeerd van een handhaving - deelnemers moeten kunnen vast stellen welke (automatische) ABvM-updates er zich hebben voorgedaan en wanneer Specifiek moet rekening worden gehouden met handhavingsapparatuur die verdwijnt (gestolen, verloren e.d.): dergelijke apparatuur mag geen groot risico vormen voor de (privacy) van deelnemers.		Dit is afhankelijk van de OBU implementaties maar het lijkt dat aan deze eis voldaan kan worden. Het TE kan ook worden ingezet om de logische toegang tot de OBU/TE te beschermen. Verder kan het risico rond het verdwijnen van handhavingsapparatuur worden gemitigeerd door de toegangsbeveiliging tot de TE van deze apparatuur te laten plaatsvinden door middel van digitale certificaten met een erg korte levensduur (een week bijvoorbeeld).	
13.	Van ABvM-deelnemers kan geëist worden meer privacygevoelige gegevens te openbaren aan de ABvM-organisatie indien hun gedrag afwijkt van de spelregels en daarom mogelijk frauduleus is (*revocable privacy*).	**E**	Aan deze eis kan voldaan worden. In principe kan men zelfs incidenteel bij deelnemers waar vaak ‘anomalieën’ optreden verplichten alle traject-transcripts te bewaren voor nacontrole.	
14.	De opzet van het systeem en diens protocollen, dataformaten en (fysieke) interfaces moet ‘open’ gespecificeerd zijn; er mag geen gebruik worden gemaakt van *proprietary* standaarden.	**E**	Aan deze eis lijkt voldaan te kunnen worden.	
15.	De ABvM-deelnemers moeten erop kunnen vertrouwen dat hun OBU/TE geen *covert channels* bevat.	**E**	Dit is afhankelijk van de OBU implementaties maar het lijkt dat aan deze eis voldaan kan worden.	
16.	Alle informatie die verstuurd wordt vanuit de OBU/TE moet inspecteerbaar / leesbaar zijn voor de ABvM-deelnemer door middel van logs.	**E**	Dit is afhankelijk van de OBU implementaties maar het lijkt dat aan deze eis voldaan kan worden.	

17.	ABvM-deelnemers mogen niet verplicht worden constant een (GPRS/UMTS) radioverbinding actief te hebben. *Noot: met een dergelijke verbinding kunnen de bewegingen van ABvM-deelnemers in principe in kaart worden gebracht.*	**E**	Omdat de tellerstanden slechts periodiek behoeven worden doorgegeven, lijkt aan deze eis kan voldaan te kunnen worden.	
18.	Het aantal en typen prijscategorieën van wegen moet zodanig beperkt worden dat de privacy van de ABvM-deelnemer niet in gevaar komt. Hieronder valt ook dat locaties (e.g., bruggen) geen unieke of zeldzame prijscategorieën moeten zijn.	**E**	Dit is mede afhankelijk van de wijze waarop beprijzingen tot stand komen, maar het lijkt dat aan deze eis voldaan kan worden.	
	C. Revenu Assurance			
19.	De registraties die vanuit de OBU/TE worden opgeleverd aan de ABvM-organisatie moeten onweerlegbaar zijn, dat wil zeggen dat de ABvM-deelnemer niet kan claimen dat deze niet uit zijn OBU/TE afkomstig zijn.	**E**	Omdat tellerstanden digitaal ondertekend worden door de deelnemers zelf, lijkt aan deze eis voldaan te kunnen worden. Wij merken wel op dat de juiste geautomatiseerde tools moeten ontworpen en geïmplementeerd om deze controles te kunnen faciliteren. Het risico bestaat dat deze instrumenten ‘vergeten’ worden tijdens het ABvM implemenatie project.	
20.	Een partij extern aan de ABvM-organisatie (extern accountant) moet eenduidig kunnen vaststellen dat: - de registraties die vanuit de OBU/TE zijn opgeleverd aan de ABvM-organisatie volledig en compleet zijn - dat de uitgegane facturen corresponderen met deze registraties	**E**	Het geheel van digitaal ondertekende tellerstanden en de steekproefsgewijze handhavingscontroles waarvan de parametrisering nog nader te specificeren is door middel van de Historie parameter *H*, lijkt te kunnen voldoen aan deze eis.	

21.	De registraties die vanuit de OBU/TE worden opgeleverd moeten een beperkt aantal fraude gerelateerde excepties kunnen bevatten, zoals bijvoorbeeld een te ‘grote’ afstand tussen twee opeenvolgende door de OBU gemeten GPS locaties, mogelijk corresponderend met het uitzetten van de OBU/TE (anomalie detectie).	**W**	Dergelijke excepties kunnen in de tellerstanden worden opgenomen zodat aan de eis voldaan lijkt te kunnen worden.	
22.	De handhavingscontroles samen met de registraties vanuit de OBU/TE bieden de ABvM-organisatie voldoende zekerheid dat het daadwerkelijke weggebruik correspondeert met het gefactureerde gebruik.	**E**	Omdat tellerstanden digitaal ondertekend worden door de deelnemers zelf, lijkt aan deze eis voldaan te kunnen worden. Wij merken wel op dat de juiste geautomatiseerde tools moeten ontworpen en geïmplementeerd om deze controles te kunnen faciliteren. Het risico bestaat wel dat deze tools ‘vergeten’ worden.	
23.	De ABvM-organisatie mag de weggebruikgegevens van deelnemers niet ongecontroleerd kunnen aanpassen.	**E**	Omdat tellerstanden digitaal ondertekend worden door de deelnemers zelf, lijkt aan deze eis voldaan te kunnen worden.	
	D. Handhaving			
24.	De volgende zaken moeten kunnen worden opgevraagd bij handhaving: - status van de OBU/TE (aan/uit) - ‘evidence’ dat (uiteindelijk) betaald wordt voor het weggebruik waarbij correct is meegenomen: type weg en tijd	**E**	Aan de eis lijkt voldaan te kunnen worden.	
25.	De volgende zaken moeten kunnen worden opgevraagd bij handhaving: - ‘excepties’, bijvoorbeeld corresponderend met de situatie dat een OBU/TE uit heeft gestaan	**W**	Aan de eis lijkt voldaan te kunnen worden.	

26.	Frauderende ABvM-deelnemers moeten niet in praktische zin in staat zijn – als ze de ABvM handhavingscontrole zien aankomen – hun fraude sporen uit te wissen en ongedetecteerd de controle te passeren.	**E**	Doordat het TE in opzet niet toestaat in korte tijd (delay parameter *D*) meerdere traject-transcripts op te leveren lijkt aan deze eis kunnen voldaan. Daarbij is het van belang om tot een evenwichtige keuze voor parameter *T* te komen: een grote *T* biedt veel controle mogelijkheden maar minder privacy. Verder is het van belang dat het TE bij het aanzetten ook een bepaalde tijd wacht voor een traject transcriptie op te leveren omdat men anders de werking van de delay parameter kan omzeilen.	
27.	Er moet direct kunnen worden geconstateerd of een deelnemer fraudeert. Iemand moet direct staande kunnen worden gehouden zodat geen gezeur achteraf ontstaat. Controle moet ook automatisch kunnen gebeuren (*on-the-spot controle*).	**E**	Aan de eis lijkt voldaan te kunnen worden.	
28.	Het moet eenvoudig mogelijk zijn te controleren of een OBU in een motorvoertuig zich aan de spelregels houdt; ondermeer moet - de handhavingscontrole op afstand mogelijk zijn - de handhavingscontrole relatief goedkoop uit te voeren zijn	**E**	Middels het uitlezen van de ‘laatste’ traject-transcripts lijkt aan deze eis voldaan te kunnen worden.	
29.	Het moet effectief mogelijk zijn te controleren of een OBU in een motorvoertuig zich aan de spelregels houdt; doordat ondermeer - de plaatsen waar deze controle kan plaatsvinden niet vooraf gebonden zijn aan plaats of tijd - handhavingscontroles opschaalbaar zijn in tijden dat meer fraude lijkt te worden gepleegd - de informatie afkomstig van deelnemer (die kan worden gecontroleerd) binnen zekere grenzen aanpasbaar is	**E**	Middels het uitlezen van de ‘laatste’ traject-transcripts lijkt aan deze eis voldaan te kunnen worden. De parameter *H* maakt de effectiviteit van de handhaving configureerbaar.	

30.	De handhavingscontroles moeten zonder detectie van de deelnemers kunnen plaatsvinden. *Noot:* - *Het idee hier achter is dat als detectie niet onopvallend plaatsvindt, deelnemers mogelijk via een gemeenschappelijk kanaal (internet, radio) elkaar hiervan op de hoogte stellen ('OBU/TE aanzetten op de A2 bij Den Bosch') zoals dat nu ook bij mobiele flitsteams gebeurt. De vraag is of het sociaal acceptabel wordt geacht om hier aan mee te werken, feitelijk werkt men dan namelijk mee aan belastingontduiking.* - *Men kan zich ook het scenario voorstellen dat er verschillende soorten handhavingscontrole apparaten zijn: systemen die echt de controle uitvoeren (met name door middel het maken van foto's) en (goedkopere) systemen die alleen maar kijken of OBU's aanstaan en (nog goedkopere) systemen die niet controleren maar niet te onderscheiden zijn van apparaten die wel een volledige controle uitvoeren.*	**W**	Omdat het uitlezen van de traject-transcripts door de handhavingsteams een 'actieve' operatie is deze in principe te detecteren is door de deelnemers. Daarmee lijkt aan deze eis niet voldaan te kunnen worden voor de reguliere handhavingscontroles. In aanvulling op deze weinig 'deelnemer belastende' controles kunnen echter ook meer belastende controles maar passieve controles plaatsvinden. Hierbij legt men deelnemers de verplichting op – bijvoorbeeld die deelnemers waar vaak 'anomalieën' optreden – om een bepaalde historie van traject-transcripts te bewaren voor nacontrole. Vervolgens kan men dan ongemerkt (foto's) maken van motorvoertuigen en vervolgens de 'anomalie' deelnemers vragen om alle (of alleen de desbetreffende) traject-transcripts ter controle. Het laten verstrekken van traject-transcripts is zowel gebruikers- als privacy onvriendelijk en kan daarom beter niet van alle deelnemers verlangd worden.	
31.	Het moet op een gebruikersvriendelijke manier mogelijk zijn te controleren of een motorvoertuig zich aan de ABvM-regels houdt, zo moeten bijvoorbeeld - de inspanningen van de deelnemer minimaal zijn - de handhavers een motorvoertuig niet te hoeven laten stoppen	**E**	Voor het uitlezen van de traject-transcripts is in principe geen inspanning benodigd van de deelnemer zelf.	
E. Beroep en Bezwaar				

32.	ABvM-deelnemers moeten inzicht kunnen krijgen in welke factuurgerelateerde informatie naar de ABvM wordt gestuurd en moeten deze factuurgerelateerde informatie kunnen relateren aan enerzijds de daaruit volgende factuur en anderzijds de gedetailleerde reisinformatie in de OBU/TE die zodanig is dat een dispuut oplosbaar is.	**E**	De opzet van de traject-transcripts en tellerstanden maken dat aan deze eis voldaan lijkt te zijn waarbij dan wel gezorgd moet worden dat de OBU's de traject-transcripts en tellerstanden exporteerbaar maken en dat de juiste software beschikbaar is om deze informatie inzichtelijk te maken.	
33.	De ABvM-deelnemers moet de factuurgerelateerde informatie en de gedetailleerde reisinformatie uit hun OBU/TE zodanig kunnen exporteren dat de authenticiteit en betrouwbaarheid gewaarborgd is.	**E**	Dit is afhankelijk van de OBU implementaties maar het lijkt dat aan deze eis voldaan kan worden.	

	F. Informatie verstrekking			
34.	Alle ABvM-deelnemers kan worden gevraagd om hun weggebruik in gepseudonimiseerde vorm te verstrekken aan de ABvM organiatie, deelnemers kunnen echter weigeren daaraan mee te werken. De gebruikte pseudoniemen: - veranderen elke dag - zijn niet herleidbaar tot identiteiten door de ABvM-organisatie - zijn niet onderling koppelbaar door de ABvM-organisatie (dat wil zeggen de pseudoniemen van vandaag zijn niet herleidbaar aan die van morgen etcetera). *Noot: de hoeveelheid gegevens kan weleens zo groot zijn dat versturen door middel van GPRS / UMTS te kostbaar is. Als alternatief kan dan gekozen worden voor versturing door middel van internet. Verder kunnen de ABvM-deelnemers die hier aan mee werken financieel worden beloond.*	**W**	In het TE kan ook een pseudonimiseersleutel worden opgenomen zodat het lijkt dat aan deze eis voldaan kan worden.	

8. Referenties

[1.] “Het KAN!, Techniek, organisatie, handhaving en kosten van varianten van Anders Betalen voor Mobiliteit”, LogicaCMG, Capgemini, GetID, 14 juni 2005.

[2.] “MobiMiles, Bewust op weg’, Roel Pieper, 10 april 2001.

[3.] “Wallet Databases with Observers,” D. Chaum & T.P. Pedersen, Advances in Cryptology CRYPTO'92, Ernest F. Brickell (Ed), Springer-Verlag, pp. 1-14.

[4.] “Systemen voor fraudebestendige en privacyvriendelijke kilometerheffing”, W. de Jonge, beschikbaar op http://www.cs.vu.nl/~wiebren/TIP/files/IR487body.pdf

[5.] “Schriftelijke inbreng ten behoeve van de hoorzitting 'Anders Betalen voor Mobiliteit'”, College Bescherming Persoonsgegevens, 23 januari 2008.