In sneltreinvaart je privacy kwijt

te verschijnen in Privacy & Informatie, themanummer volgsystemen, oktober 2008

Dr. W.G. Teepe[1]

Trefwoorden: OV-chipkaart, WBP, anoniem reizen, privacy, attribute-based authorisatie, identity-based authorisatie

Inleiding

De OV-chipkaart is een nieuw elektronisch betaalmiddel voor het openbaar vervoer in Nederland, dat de vervoersbewijzen op papier zal moeten vervangen. Bij gebruik van de OV-chipkaart wordt het reisgedrag tot in detail bijgehouden, wat gevolgen heeft voor de privacy van de reiziger. Tot zover zal het bij de meesten bekend zijn.
Maar wat wordt er nou precies bijgehouden, en hoe? Wie kan er allemaal bij deze hoeveelheid aan gegevens? Hoe verhoudt zich dit tot de WBP? In dit artikel wordt een overzicht gegeven waarmee deze en andere vragen beantwoord kunnen worden. Daartoe wordt ingegaan op de opzet van de kaart, en de pijn- en discussiepunten met betrekking tot privacy, waaronder het al dan niet anoniem kunnen reizen met korting.

Velen zullen zich de nieuwsberichten nog herinneren over de gebleken beperkte beveiliging van de OV-chipkaart. Eigenlijk staat dat onderwerp bijna helemaal los van de privacy van de OV-chipkaart. De beveiliging die gebrekkig gebleken is, is de beveiliging tegen het vervalsen van kaarten, zodat het mogelijk is te reizen zonder voldoende te betalen. Beveiliging van persoonsgegevens tegen mogelijk ongewenst gebruik was nauwelijks aan de orde. Dat laatste onderwerp staat hier centraal.

[1] Wouter Teepe is verbonden aan de Digital Security groep van de Radboud Universiteit Nijmegen, en betrokken bij het Centre for Cybercrime Studies (Cycris).

Opzet en architectuur

De OV-chipkaart is het afgelopen halfjaar veelvuldig in het nieuws geweest. Dat is iets anders dan zorgvuldig of gedetailleerd: journalisten hebben net zoals ieder ander mens de neiging zaken die ze niet snappen weg te laten of te vereenvoudigen. Toch is enig rudimentair begrip van de opzet en architectuur wel van belang in de analyse van de privacy van de OV-chipkaart. Daarom volgt hier een exposé met een beknopte uitleg van de ontstaansgeschiedenis, de kaartsoorten, de chips die in de pas gebruikt worden, de gegevens die op deze chips worden opgeslagen, en de gegevens die centraal worden opgeslagen.

Voorgeschiedenis

Sinds 1980 kent Nederland de strippenkaart, een nationaal vervoerbewijs voor het streekvervoer. Men kan in Groningen een strippenkaart kopen, en er in Nijmegen mee de bus in. Voor een eerlijke verdeling van de opbrengsten van de kaartverkoop, alsook van de subsidies van de rijksoverheid, is het van belang te weten waar de strippenkaarten (alsook de diverse abonnementen) "verstookt" worden. Tot op heden worden deze vervoersbewegingen geschat op basis van steekproeven. Deze schattingen geven een globaal beeld, maar hebben een beperkt detail. Toen enige jaren geleden de politieke discussie begon over "onrendabele lijnen" in het streekvervoer, werd het pijnlijk duidelijk dat hoewel de onrendabele lijnen ongetwijfeld zullen bestaan, men geen gedetailleerd inzicht had in welke lijnen dat eigenlijk waren.
Zo ontstond de behoefte aan gedetailleerde en nauwkeurige informatie over de reizigersvolumes in het openbaar vervoer: een tabel die voor (ieder stukje van) elk traject aangeeft hoeveel reizigers er per jaar gebruik van maken.
Om in deze behoefte te voldoen is de OV-chipkaart bedacht: simpel gezegd een elektronische variant van de strippenkaart in bankpasformaat, waarbij de afstempelautomaat bijhoudt hoeveel er verreden wordt, en waar. Door alle gegevens van alle afstempelautomaten op één hoop te gooien, ontstaat er dan vanzelf het gewenste gedetailleerde overzicht.
Veel belanghebbende partijen zijn met dit idee aan de haal gegaan en hebben er hun eigen doelen en wensen aan toegevoegd. Ik noem enkele voorbeelden. Als vervoerders ook inzicht krijgen in hoe op hun lijnen het reizigersvolume zich van uur tot uur verhoudt, dan kan het kostbare materieel mogelijk efficiënter worden ingezet. Verschillende vervoerders zien in de OV-chipkaart een (wonder)middel tegen hoge zwartrijdpercentages. De RET wil de sociale veiligheid op de stations verhogen, door alleen mensen met geldig plaatsbewijs op de perrons toe te laten. De NS zou graag per persoon uitgesplitst willen zien waar men rijdt, om mensen van op maat gesneden advies te kunnen voorzien (d.w.z. direct marketing).
Reizigersorganisaties zagen ook mogelijke gemaksvoordelen voor de reizigers, maar hebben op 22 september 2008 hun vertrouwen in de OV-chipkaart opgezegd. Een belangrijke (zij het niet de enige) reden voor het opzeggen van het vertrouwen is het gebrek aan privacy voor gebruikers van de OV-chipkaart.

Drie soorten kaarten

Één en ander heeft geleid tot het ontwerp van de OV-chipkaart met drie kaartsoorten: de *persoonsgebonden* kaart, de *anonieme* kaart en de *wegwerpkaart*.

1. De persoonsgebonden kaart staat op naam, en wordt op termijn het enige kaartje waarmee persoonsgebonden reisproducten zoals trajectkaarten en voordeelurenkaart gebruikt kunnen worden. Verder is de persoonsgebonden kaart drager van een reistegoed. Gemaakte reiskosten worden aan de hand van het reisgedrag berekend en afgeboekt van het tegoed. De houder kan het tegoed handmatig bij een automaat opwaarderen, maar ook een incassomachtiging afgeven waarmee zijn tegoed automatisch wordt bijgevuld.
2. De anonieme kaart is een uitgeklede versie van de persoonsgebonden kaart: hij is drager van een reistegoed, maar kan niet gebruikt worden in combinatie met kortingen zoals de voordeelurenkaart van de NS. De kaart kan worden opgewaardeerd met munten of met een pinbetaling.
3. De wegwerpkaart is een kaart die geen reistegoed draagt, maar slechts één enkele specifieke reis of retourtje. Bij aankoop wordt vastgelegd welke reis dit is, en na de reis heeft het kaartje geen functie meer. Dit is dus het enige kaartje waarbij de reiziger zich op voorhand vastlegt op het te reizen traject. De wegwerpkaart is niet beschikbaar voor reizen met de NS.

Strikt gesproken is de anonieme kaart niet anoniem, maar pseudoniem: van de kaart zijn alle reisbewegingen te volgen, het is alleen onbekend wie de gebruiker is. Wanneer de anonieme kaart of de wegwerpkaart met een pinbetaling wordt gekocht of opgewaardeerd, verschaft de bank gegevens van de bankpashouder (waaronder de naam) aan de verkoper van het OV-chipkaart-reistegoed. Daarmee kan een anonieme kaart aan een persoon gekoppeld worden. Of dat structureel gebeurt is natuurlijk maar zeer de vraag. Bij strafrechtelijk onderzoek kan het en zal het ongetwijfeld ook gebeuren. Feit is allicht dat er sporen worden achtergelaten waarmee de identiteit van de koper van een specifieke kaart achterhaald kan worden.

Wil men pseudoniem blijven zonder dergelijke identificerende sporen achter te laten (dit is een pleonasme), dan zal men met een anonieme kaart moeten reizen en dus geen gebruik kunnen maken van kortingen. Ook zal volledig met muntgeld betaald moeten worden, voor een tweedeklas treinkaartje Groningen Maastricht is dan 36,70 euro aan munten nodig. Wil men anoniem reizen zonder dat verschillende reizen met elkaar in verband gebracht kunnen worden (ook dit is een pleonasme), dan zal men voor elke (trein)reis een nieuwe anonieme kaart moeten kopen van 7,50 euro. Voor reizen met het streekvervoer zal men dan voor elke reis een nieuwe wegwerpkaart moeten kopen.

Het is van belang hierbij het volgende conceptuele verschil tussen anonimiteit en privacy te onderkennen. Anonimiteit is een absoluut begrip: je laat herleidbare sporen na of niet. “Een beetje anoniem zijn” is net zo onmogelijk als “een beetje zwanger zijn”. Privacy daarentegen is een relatief begrip: er kan een bepaalde mate van bescherming van gegevens zijn. Bijvoorbeeld dat de NS alle details van je treinreizen zou kennen, maar belooft deze gegevens niet met andere partijen te delen, en belooft de gegevens slechts op een bepaalde manier te gebruiken.

De anonimiteit van de anonieme kaart is dus zeer betrekkelijk: men zal enige toeren moeten uithalen om er echt anoniem mee te reizen. Een niet-anonieme kaart biedt dezelfde reis tegen een vaak lagere prijs en met beduidend meer gemak.

RFID en Mifare

De OV-chipkaart maakt gebruik van RFID-technologie, waarbij in het pasje een kleine chip en een antenne zijn weggewerkt. De chip kan communiceren met een *reader* (de elektronische variant van de afstempelautomaat) door hem binnen 10 centimeter afstand van de reader te brengen. Een reader controleert de geldigheid en reistegoed van het kaartje, schrijft er enkele gegevens op en opent dan het bijbehorende poortje.
Elke RFID-chip geeft als hij "aangesproken" wordt door een kaartlezer een identificatienummer af, dat nodig is om protocoltechnische redenen (*anti-collision*). Veel typen chips, doorgaans de oudere en de eenvoudigere, geven elke keer *hetzelfde* identificatienummer af: het serienummer ("vaste UID") van de chip. Dit nummer kan gebruikt worden als pseudoniem voor de kaart, en als persoonsgegeven van de kaarthouder zodra de koppeling tussen het nummer en de kaarthouder gemaakt is. Het in het voorbijgaan treffen van een bekende burger volstaat in principe om de vaste nummers van diens RFID-chips te achterhalen. Zo'n vast nummer kan door kwaadwillenden gebruikt worden om speciale apparatuur te maken die alléén reageert als een bepaalde kaart(houder) in de buurt komt. Verschillende moderne en complexere typen chips geven echter iedere keer een *ander* identificatienummer af ("random UID"). Dit zorgt ervoor dat de kaart(houder) niet te volgen is op basis van het UID. De chips die in de OV-chipkaart gebruikt worden hebben een vast UID, die in het Nederlandse biometrische paspoort hebben een random UID.
De RFID-chip in de OV-chipkaart is functioneel gezien niet veel meer dan een stukje geheugen dat gelezen en gedeeltelijk ook beschreven kan worden. In de persoonsgebonden en de anonieme kaart is dit geheugen afgeschermd met een cryptografische module die in de chip, de Mifare Classic van NXP, zit ingebouwd. De wegwerpkaart heeft de eenvoudiger Mifare Ultralight chip van NXP aan boord, die geen enkele cryptografische beveiliging kent.
De keuze voor deze chips is bijzonder ongelukkig geweest. In januari 2008 demonstreerde Radboud-student Roel Verdult dat de Ultralight chip in de wegwerpkaart ook door onbevoegden uit te lezen en na te bootsen is. Als gevolg hiervan is reizen met nagemaakte en gemanipuleerde wegwerpkaarten mogelijk. In maart 2008 werd door de Minister van Binnenlandse Zaken bekend gemaakt dat een breder team van de Radboud Universiteit Nijmegen ook zwakheden in de cryptografie van de Mifare Classic had gevonden[2]. Kort daarop werd duidelijk dat hiermee ook de persoonsgebonden en anonieme varianten van de OV-chipkaart gevoelig zijn voor manipulatie.
Er zijn zeer kort samengevat twee soorten manipulatie. Een kaart kan worden teruggezet in een eerdere toestand, waarmee je reistegoed terug kunt zetten. Een kaart kan ook worden gekloond, waarmee het reistegoed op nieuwe lege blanco kaarten gekopieerd kan worden.
Kortom, het bleek dat de OV-chipkaart niet afdoende beveiligd is tegen reizen zonder daarvoor te betalen. De vervoerssector heeft aangegeven dat mochten individuele reizigers gedupeerd raken doordat hun kaart "bestolen" is, de sector deze schade zal vergoeden.

---

[2] Minister van Binnenlandse Zaken en Koninkrijksrelaties G. ter Horst, brief *Chiptechnologie (toegangs-)passen*, 12 maart 2008, kamerstuk 31200-VII-50, kenmerk 2008-0000119577. Zie ook http://www.ru.nl/ds/research/rfid/ en F.D. Garcia e.a. *Dismantling MIFARE Classic*, proceedings of ESORICS 2008.

Privacy op de pas zelf

Wie beschikking heeft over de pas kan bij een verkoopautomaat een bonnetje afdrukken met de laatste 10 transacties, (zijnde de 4 tot 5 meest recente reizen). Op de buitenkant van de kaart staan de naam en pasfoto van de houder gedrukt. Persoonsgebonden kaarten die worden uitgegeven door de NS hebben ook een magneetstrip, maar die magneetstrip wordt nauwelijks gebruikt, en is ook niet op afstand uit te lezen. Deze laat ik dan ook buiten beschouwing.
Er is door enkele betrokkenen benadrukt dat deze recente beveiligingsproblemen van de chip nauwelijks gevolgen hebben voor de privacy van de reiziger[3]. Op de "oude varianten" van persoonsgebonden reisproducten, zoals de voordeelurenkaart, staat de geboortedatum gewoon afgedrukt. Het enige persoonsgegeven dat op de chip van de persoonsgebonden kaart staat, en dus als gevolg van de recente beveiligingsproblemen achterhaald kan worden, is de geboortedatum. Vergeleken met het oude abonnementsbewijs is dat nu ook weer niet zo'n groot probleem of verschil. Zo gaat althans de redenering ongeveer. Het is van belang dit toch wat meer in perspectief te plaatsen.
Ten eerste is het zo dat als de beveiligingsproblemen weinig gevolgen hebben, dit niet betekent dat de privacy daarom prima gewaarborgd is: het is slechts *even* goed of slecht als *zonder* die problemen. Over de mate van privacybescherming zonder die problemen kunt u zelf oordelen in de hierop volgende paragrafen.
Ten tweede is er een onderscheid tussen het met inkt afgedrukt zijn van een gegeven, en het op de chip opgeslagen zijn. Om de inkt te lezen moet er een zichtlijn zijn van de lezer naar de pas, voor het uitlezen van de chip is nabijheid nodig. Het uitlezen van de chip is te automatiseren en daardoor ook eenvoudig op te schalen. Dit gaat niet op voor op afstand het lezen van gedrukte tekst. Allicht kan gesteld worden dat deze twee manieren van opslaan van de geboortedatum verschillende wijzen van beveiliging kennen. Het is dus niet op voorhand zo dat de nieuwe manier van opslaan voldoende veilig is omdat de oude manier dat kennelijk was.
Ten derde is het van belang precies te zijn over welke gevoelige gegevens de (persoonsgebonden) kaart mogelijk lekt. Zonder uitputtend te zijn benoem ik drie zaken die de kaart kan prijsgeven aan kwaadaardige apparatuur: het *vaste UID van de chip*, de *geboortedatum* en het *reisgedrag* (d.w.z. de meest recente reizen).
Op zich is het vaste UID van een chip niet zo'n bijzonder gegeven, ware het niet dat de kaart dit nummer prijsgeeft aan iedere kaartlezer die er beleefd om vraagt. In 1985 publiceerde het blad *Bluf!* een lijst met adresgegevens van bepaalde werknemers van het ministerie van Economische Zaken. Op vergelijkbare wijze kan iemand nu lijsten van RFID-chipnummers van bepaalde burgers op het internet publiceren (anoniem, nog wel!). Precies om dit type scenario te voorkomen is er bij het Nederlandse biometrische paspoort ervoor gekozen chips te gebruiken met een random UID. Bij toegangspassen wordt tegenwoordig steeds vaker gekozen voor chips met een random UID. Hier geldt het principe van de zwakste schakel: zodra er maar één van alle RFID chips die iemand bij zich draagt (paspoort, OV-chipkaart, toegangspassen, etc.) een vast UID prijsgeeft, is alle moeite voor niets geweest.

---

[3] Staatssecretaris van Verkeer en Waterstaat J.C. Huizinga-Heringa, brief *OV-chipkaart Counter expertise*, 14 april 2008, kamerstuk 23645-196, kenmerk VENW/DGP-2008/3843.

De OV-chipkaart is geen nicheproduct, maar zal door "bijna alle" Nederlanders gebruikt worden, er zijn er nu al 2,5 miljoen van in omloop. Als de OV-chipkaart een vast UID heeft, worden er dus miljoenen zwakste schakels uitgedeeld.
De geboortedatum en het reisgedrag staan op het afgeschermde geheugen van de kaart. Trans Link Systems (TLS) geeft echter zelf aan dat door de genoemde beveiligingsproblemen, de geboortedatum achterhaald kan worden[4], wat allicht suggereert dat extra beveiligingslagen (zoals bijvoorbeeld AES encryptie) ontbreken.
Of het lekken van de geboortedatum en het reisgedrag een probleem is, is zeker geen eenvoudige vraag, en kan niet zonder meer met "nee" beantwoord worden. Rop Gonggrijp heeft in dit kader een illustratief experiment gesuggereerd. Ik noem het het Rop-poortje. Een Rop-poortje ziet eruit als een anti-diefstalpoortje zoals je die in veel winkels aantreft. Het bevat een krachtige kaartlezer die van alle langslopende mensen de geboortedatum en reisgegevens van de OV-chipkaart uitleest. Op het poortje is een luidspreker bevestigd die reageert op de gegevens op de kaart: als de persoon jarig is wordt een verjaarsliedje gezongen. Soms wordt de leeftijd van de persoon omgeroepen. Soms reageert het poortje op de laatst afgelegde reizen, in de trant van "wat deed jij vorige week donderdag in Rhoon?" Als een poortje deze informatie kan uitlezen, is het duidelijk dat ook andere partijen dit in principe kunnen. Wanneer het Rop-poortje daadwerkelijk gebouwd wordt, zal waarschijnlijk snel duidelijk worden of burgers het lekken van dergelijke gegevens bezwaarlijk vinden.
Het op deze manier lekken van informatie kan worden voorkomen door als pashouder de OV-chipkaart altijd op te bergen in een aluminium foliehoesje. Dit doet afbreuk aan het gebruiksgemak van de OV-chipkaart, omdat de pas bij elke transactie even uit het hoesje moet worden gehaald. Zulke hoesjes zijn verkrijgbaar, maar niet makkelijk te vinden. Aluminiumfolie voor keukengebruik volstaat ook en is overal te koop.

Centrale backoffice

De OV-chipkaart is de nieuwe variant van de strippenkaart en het treinkaartje. De nieuwe OV-chipkaart-backoffices kennen echter geen historische voorganger.
In de oude situatie tastten de streekvervoerders in het duister over het reisgedrag van individuele personen: het was en is onmogelijk om strippenkaarten te "volgen". De NS heeft op basis van haar papieren kaartjes al een redelijk zicht op het globale reisgedrag, omdat ze veel kaartjes verkoopt waarop vertrekpunt en een bestemming zijn vastgelegd. Wie zijn treinkaartjes daarnaast met pin betaalt, kan in theorie door de NS gevolgd worden: De NS dan kan zien wie welke kaartjes koopt, maar *niet* wanneer die kaartjes precies gebruikt worden en door wie. Het is naar de mening van de auteur zeer onwaarschijnlijk dat de NS zulke analyses ook daadwerkelijk uitvoert. De WBP staat het gebruik van betaalgegevens voor iets anders dan het verwerken van de betaling zelf ook niet toe, zo blijkt uit een CBP-rapport over het Amsterdamse GVB[5]. Informatietechnisch gezien *kan* het wel.
In dit perspectief is de OV-chipkaart-backoffice van TLS een revolutie. De backoffice is een dagelijks bijgewerkte database van alle met OV-chipkaart gemaakte reisbewegingen, compleet met plaats, tijd en kaartnummer. Bij de persoonsgebonden kaarten compleet

[4] Trans Link Systems, Persbericht *OV-chipkaart voldoende veilig*, 29 februari 2008, alsook *Aanvalsplan OV-chipkaart*, 29 februari 2008.
[5] College bescherming persoonsgegevens, *OV-chipkaart: Verwerking van persoonsgegevens ten behoeve van de OV-chipkaart bij het GVB te Amsterdam*, 15 januari 2008.

met identiteit van de reiziger. Er zijn nog enkele andere, kleinere centrale databases voor bijvoorbeeld beheer en uitgifte van kaarten, maar deze laat ik hier buiten beschouwing.
De centrale database van reisbewegingen wordt voor de volgende doelen gebruikt:

1. Het oorspronkelijke doel: om de opbrengsten van de kaartverkoop eerlijk onder de vervoerders te verdelen. Dit gebeurt grofweg naar ratio van de geproduceerde passagierskilometers.
2. Naar aanleiding van de beveiligingsproblemen van de gekozen chips: om te detecteren óf, en zo ja met wélke kaarten er gemanipuleerd wordt. Deze kaarten worden geblokkeerd.
3. Als dienst: om reizigers online inzage te geven in hun eigen reisgedrag. Dit is enigszins vergelijkbaar met de website van Albert Heijn waar mensen hun boodschappengeschiedenis kunnen inzien.

In deze lijst ontbreekt marketing, dat onderwerp komt later aan de orde bij de *decentrale* backoffices die er ook nog zijn.
Er zijn nog enkele mogelijke Grote Geïnteresseerden in de centrale database: diensten uit het veiligheidsdomein, zoals de politie en de AIVD. Gedetailleerde reisgegevens van individuen kunnen interessant zijn voor inlichtingenwerk (op welke plekken komt iemand regelmatig?) en opsporing (alibi's). Op basis van de huidige wetgeving zijn dergelijke organisaties gerechtigd inzage te vorderen in de database[6]. In bepaalde gevallen wordt er ook daadwerkelijk gebruik gemaakt van dat recht, en is er feitelijk directe inzage in databases van private marktpartijen[7]. De Britse MI5 heeft in een vergelijkbaar geval (de Londense Oyster card) toegang tot de reisgegevens van bepaalde personen, en heeft aangegeven de *hele* centrale database van de Oyster card in te willen kunnen zien[8].
Het is de auteur uitdrukkelijk niet bekend of Nederlandse veiligheidsdiensten op het moment interesse voor reisgegevens hebben geuit, en of zij ook feitelijk gebruik maken van OV-chipkaart-databases. Allicht zal eventuele interesse nu nog getemperd worden door het beperkte gebruik van de OV-chipkaart op dit moment.
De database van reisbewegingen heeft een beperkt nut bij het volgen van kundige gemotiveerde personen die anoniem wensen te blijven. Zij gebruiken voor iedere reis een nieuwe anonieme kaart of een wegwerpkaart. Lieden die zichzelf een alibi willen verschaffen kunnen een kennis met hun persoonsgebonden OV-chipkaart op pad sturen om de gewenste sporen te maken.

---

[6] A. Vedder e.a., *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw (Study 49)*, Den Haag: Rathenau Instituut, 2007.
[7] H. Bosma e.a. *Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse.* Den Haag: Adviescommissie Informatiestromen Veiligheid 2007.
[8] G. Hinsliff, *MI5 seeks powers to trawl records in new terror hunt*, website The Guardian, 16 maart 2008.

Pijn- en discussiepunten

Uit het bovenstaande relaas wordt duidelijk dat privacy of anonimiteit geen harde ontwerpeis was, maar veeleer een "extra eigenschap" die later aan het ontwerp is toegevoegd. Dat het niet echt gelukt is om volledige anonimiteit toe te voegen blijkt uit de ingewikkelde toeren die men uit moet halen om anoniem te reizen, en uit het mogelijke scenario dat diensten uit het veiligheidsdomein naar de reisbewegingen kijken. Het zou zeer wel kunnen dat deze diensten voldoende zelfbeheersing hebben om slechts spaarzaam met bevoegdheden om te gaan, of wellicht onvoldoende uitgerust zijn om diepgravende analyses uit te voeren[9]. Staan blijft dat de borging van de privacy afhankelijk is van de vermogens en onvermogens van de verwerkende partijen, en niet in de technische architectuur is verankerd.
De belangrijkste pijnpunten met betrekking tot privacy bij de OV-chipkaart zijn (1) dat gedetailleerde reisinformatie van reizigers überhaupt opgeslagen wordt, (2) dat deze informatie mogelijk voor (onder andere) direct marketing gebruikt zou kunnen worden, en (3) dat er prijsdruk is om niet-anoniem te reizen.
Belangrijke gerelateerde discussiepunten bij de OV-chipkaart zijn (1) of de verwerking van de persoonsgegevens in overeenstemming is met de WBP, en (2) of verwerking van gedetailleerde reisinformatie überhaupt technisch noodzakelijk is.
In de komende paragrafen zal dieper worden ingegaan op deze pijn- en discussiepunten, waarbij speciale aandacht wordt gegeven aan de (on-?)mogelijkheid tot anoniem reizen met korting.

Reisgegevens bij de vervoerders

De centrale backoffice wordt niet gebruikt voor marketing. Dit lijkt anders te liggen voor de vervoerders, die ieder ook een eigen backoffice hebben (in OV-chipjargon heet dit Level 3). De centrale TLS backoffice (Level 4) wordt gevoed vanuit deze decentrale backoffices van de vervoerders.
Elke vervoerder verzamelt alle transactiegegevens van alle readers onder haar beheer in haar eigen decentrale (Level 3) database. Elke nacht worden de nieuwe aanvullingen op deze databases gekopieerd naar de al besproken centrale (Level 4) database van TLS. Technisch gesproken kan TLS dus alle transacties inzien, en de vervoerders alleen de transacties die betrekking hebben op de vervoersbewegingen op hun eigen infrastructuur.
Volgens eigen zeggen voldoet TLS met haar centrale database ruimschoots aan de vereisten van de WBP. Het CBP is echter kritisch over de (Level 3) databases van enkele vervoerders.
Op 15 januari 2008 publiceerde het CBP een rapport over het Amsterdamse GVB[10]. Het CBP oordeelt dat het GVB betaalgegevens in strijd met de WBP verwerkt, dat het GVB reisgegevens niet zonder expliciete toestemming mag gebruiken voor (direct) marketing doeleinden, en dat de database onvoldoende organisatorische en technische beveiligingsmaatregelen kent.
Op 16 januari 2008 hield de Tweede Kamer een rondetafelgesprek over de OV-chipkaart. Er ontspon zich daar een discussie tussen vertegenwoordigers van het CBP en

[9] B.P.F. Jacobs en W.G. Teepe, *Over vermogen en onvermogen*, P&I 2007, p. 142—146.
[10] College bescherming persoonsgegevens, *OV-chipkaart: Verwerking van persoonsgegevens ten behoeve van de OV-chipkaart bij het GVB te Amsterdam*, 15 januari 2008.

de NS, die als die ook maar als enige indicatie mag gelden, duidde op een langslepend en zeer fundamenteel verschil van mening over het gebruik van de vergaarde reisgegevens. De discussie tussen NS en CBP draait in hoofdzaak om het bekende onderscheid tussen opt-in en opt-out. De NS wil haar persoonlijke dienstverlening (d.w.z. direct marketing) stoelen op opt-out, het CBP vindt dat volgens de WBP marketing alleen op basis van opt-in is toegestaan. Het CBP heeft toen aangegeven het praten met de NS "bijna moe te zijn" en "zonodig te gaan handhaven".
Op 29 februari 2008 presenteerden de staatssecretaris, TLS en de bij TLS aangesloten vervoerders het "Aanvalsplan OV-chipkaart", dat hierover een paar veelzeggende passages bevat:

> De OV-bedrijven hebben aangegeven tot 2010 geen OV-chipkaart-reisgegevens te gebruiken voor direct-marketingdoeleinden.

en:

> Daarnaast zijn de OV-bedrijven en het Cbp in overleg over het gebruik van globale reisgegevens voor serviceverlening en marketingdoeleinden. Zowel de OV- bedrijven als het Cbp hebben de staatssecretaris ruimte gevraagd zodat zij hun constructieve overleg af kunnen ronden. Op 17 april 2008 is het overleg afgerond. Het Cbp neemt dan een definitief standpunt in, waarna de OV-bedrijven conclusies trekken. OV-bedrijven zullen, indien dan interpretatieverschillen met het Cbp resteren niet overgaan tot handelen in strijd met interpretaties van het Cbp. De OV-bedrijven hebben dan overleg met de staatssecretaris over de dan ontstane situatie. Partijen houden de mogelijkheid het oordeel van een rechter te vragen over (onderdelen van) een interpretatie.

Sindsdien is het stil op dit front. Wel kan geconstateerd worden dat er ruimte zit tussen recente uitspraken van de NS en de (oorspronkelijke) visie van het CBP. Het CBP schrijft in een uit 2005 daterend visiestuk[11]:

> De niet op naam gestelde kaarten die vervoerders gaan introduceren moeten gebruikt kunnen worden onder faire voorwaarden: er mag geen situatie ontstaan waarin reizigers zich, bijvoorbeeld door prijsdruk, gedwongen zien om met gepersonaliseerde kaarten te reizen waar zij dit niet willen.

In een rondetafelgesprek in de Tweede Kamer op 16 juni 2008, kreeg de commercieel directeur van de NS de volgende vraag van de SP[12]:

> Waarom wil de NS het niet mogelijk maken een reisproduct met korting op een anonieme kaart te laden, waarbij de conducteur controleert op het recht op korting zoals dat nu ook het geval is? […]

Ze antwoordde letterlijk als volgt:

> Het antwoord is eigenlijk heel eenvoudig: het voordeelurenabonnement is een persoonlijk abonnement en niet een kaartgebonden abonnement, zo is dat vandaag niet en zo is dat in de toekomst ook niet. Een kaartgebonden abonnement zou de mogelijkheid bieden om de kaart aan eenieder door te geven om daarop te reizen. En zo is dit abonnement en ook andere abonnementen die we hebben niet bedoeld.

---

[11] College bescherming persoonsgegevens, *Privacy en de OV-chipkaart*, 16 november 2005.

[12] Deze twee citaten zijn een transcriptie van de videouitzending op het web van het desbetreffende rondetafelgesprek door de huidige auteur.

> Wat de achterliggende reden van uw vraag is zoals u aangaf zijn de privacy wellicht zorgen daarachter. Nou daarvoor wil ik nogmaals benadrukken dat de privacy voor alle persoonsgebonden kaarten ten alle tijden gewaarborgd is.
> Het ook heugelijk om hier te vermelden dat we met CBP over de onderwerpen die er liepen in principe overeenstemming bereikt hebben, dat we even in afwachting tot de laatste zaken rond de kraak en de privacy van de kaart daar het CBP daar ook over zal rapporteren.
> Dus er is geen reden om te veronderstellen dat er de privacy in het algemeen in het gedrang komt, en een anonieme kaart en een persoonsgebonden abonnement laten zich nou eenmaal niet verenigen.

Bij navraag bij het CBP (door de auteur, begin september 2008) bleek echter dat er nog geen overeenstemming is en dat de partijen nog steeds in overleg zijn.

Informatieminimalisatie

Om de hele discussie over anoniem reizen met korting te kunnen plaatsen is het goed uiteen te zetten wat daar eigenlijk mee bedoeld kan worden, en hoe dat gerealiseerd kan worden.
Alle OV-abonnementen in Nederland zijn persoonsgebonden en niet overdraagbaar. Dat was zo, en het is niet te verwachten dat dat zal veranderen. Als je dus met korting reist, kan allicht worden afgeleid dat je één van de vele abonnementshouders in Nederland bent. De vervoerders kunnen een lijst maken van alle mensen die korting hebben. Maar die lijst is zo groot dat je praktisch kunt stellen dat het verschil met "volledige anonimiteit" slechts een academisch onderscheid is.
De manier waarop er in de levenscyclus van een (trein)kaartje wordt omgegaan met de korting en de privacy verschilt nogal tussen de oude situatie (voordeelurenkaart) en de nieuwe situatie (OV-chipkaart).
In de oude situatie koopt de reiziger een reductiekaartje zonder daarbij zijn identiteit prijs te geven. Het recht op korting wordt gecontroleerd door een conducteur die kijkt of iemand met een reductiekaartje ook een abonnement heeft dat die korting rechtvaardigt. De conducteur kijkt naar een pasje, vergelijkt wellicht of de pasfoto gelijkenis vertoont met de reiziger, maar houdt geen logboek bij, noch in het hoofd, noch met externe hulpmiddelen.
In de nieuwe situatie geeft de reiziger zijn identiteit prijs bij aanschaf van het reductiekaartje. Er is geen mogelijkheid om hieraan te ontkomen, anders dan af te zien van de reductie dan wel af te zien van de gehele reis. Het prijsgeven van de identiteit is niet kortdurend: er wordt in de centrale backoffice gelogd dat de kaart, waarvan de houder bekend is, een bepaalde reis afgelegd heeft of zal gaan afleggen. Bij kaartcontrole verifieert de conducteur of de OV-chipkaart geldig is, en of de reiziger dezelfde persoon is als de kaarthouder. Het is technisch onmogelijk om op een OV-chipkaart een reductiekaartje te laden als er geen kortingsabonnement is, dit zal de conducteur dan ook niet hoeven controleren[13].
Kortom, het moment van controleren op het recht op korting is verschoven van tijdens kaartcontrole naar de aanschaf van het vervoersbewijs. Maar tegelijkertijd wordt ook de

[13] Het lijkt ook niet eenvoudig een reductiekaartje te laden als er wél recht op korting is, getuige Vincent Dekker, "Ov-chip en trein gaan niet samen", Trouw/De Gids 27 mei 2008, p. 10—11.

identiteit van de kaarthouder gelogd, terwijl in de oude situatie je er gerust op kon zijn dat de controlerend conducteur je identiteit snel weer zou vergeten.
In mooi technisch Engels kan je stellen dat er effectief van attribute-based authorisatie (heb jij recht op korting?) wordt overgestapt op identity-based authorisatie (wat is je naam?). Waar je je bij attribute-based authorisatie nog kon verbergen in de anonimiteit van een zeer grote groep kortingskaarthouders, is er bij identity-based authorisatie geen enkele anonimiteit jegens de vervoersbedrijven.
De vraag dient zich aan of dit nodig is. Is er een technische oplossing die in een OV-chipkaart-achtige setting aan attribute-based authorisatie doet?
Het antwoord luidt "ja!". De oplossing heet "zero-knowledge", dit is een tak binnen de cryptografie waarbij informatie op *spaarzame* maar *overtuigende* wijze wordt uitgewisseld. *Spaarzaam* in de zin dat er wordt afgesproken welke informatie uitgewisseld moet worden, en dat het wiskundig hard gemaakt kan worden dat er geen enkele andere informatie ("zero bits of knowledge") wordt uitgewisseld of gelekt. *Overtuigend* in de zin dat wiskundig hard gemaakt kan worden dat de partij die probeert te overtuigen de boel niet kan bedonderen. De overtuiging waar hier sprake van is, is dat de kaarthouder of diens kaart de kaartautomaat er van overtuigt dat er sprake is van recht op korting. Geen enkele andere informatie slaat uiteraard op de identiteit van die kaarthouder, waarover geen enkele bit gelekt hoeft te worden.
Het idee van zero-knowledge stamt uit de jaren tachtig van de vorige eeuw en is sindsdien volop in ontwikkeling. Begin deze eeuw zijn er belangrijke resultaten geboekt die toepasbaar zijn in het OV-chip-domein (i.h.b. het Idemix-project van IBM[14] en het werk van Stefan Brands[15]). Hoewel het idee niet nieuw is, is het nog niet "field proven": zero-knowledge wordt nog niet of nauwelijks gebruikt in mobiele betalingen. De eerlijkheid gebiedt ook te zeggen dat de hiervoor benodigde rekenkracht een bottleneck is, die uiteraard met het sneller worden van chips langzamerhand zal verdwijnen. Het "OV-chip 2.0" project van de Radboud Universiteit Nijmegen[16] is mede opgezet om de praktische toepasbaarheid hiervan te onderzoeken en een eerste prototype te bouwen.

Noodzaak tot verwerking?

Het bestaan van zero-knowledge oplossingen heeft een direct verband met het toepassen van de WBP in het OV-chip-domein.
De WBP schrijft (kort samengevat) voor dat persoonsgegevens slechts verwerkt mogen worden als dit noodzakelijk is[17]. Noodzakelijk voor het uitvoeren van een duidelijk omschreven en overeengekomen doel. Voor het kunnen bepalen van het recht op korting kan het volgende gesteld worden. Als er oplossingen bestaan waarbij het tonen van de identiteit van de kaarthouder niet nodig is, is het dus niet noodzakelijk de identiteit te tonen. Het is dan nog maar een kleine stap tot de conclusie dat de WBP voorschrijft dat in dat geval de identiteit van de kaarthouder helemaal niet verwerkt mag worden. Als de identiteit slechts verwerkt mag worden als het noodzakelijk is, is het dus impliciet verplicht om technieken te gebruiken die géén identiteitsgegevens verwerken.

---

[14] http://www.zurich.ibm.com/security/idemix/
[15] S.A. Brands *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy*, MIT Press, augustus 2000. Zie ook
http://www.credentica.com/the_mit_pressbook.html
[16] https://ovchip.cs.ru.nl/OV-chip_2.0 gefinancierd door NLnet.
[17] Art 8. WBP.

Een omvangrijk en complex project als de OV-chipkaart heeft een lange aanloop. Toen deze aanloop rond de millenniumwisseling werd ingezet bestond zero-knowledge al lang, maar de eerder genoemde technieken van IBM en Brands lagen nog op de tekentafel. Hier dringt zich een tweetal vragen op. Als eerste:

1. Waar ligt de bewijslast voor de noodzakelijkheid van verwerking van persoonsgegevens?

In het geval van de OV-chipkaart is er, ergens in het hele proces, kennelijk geoordeeld dat het verwerken van identificerende gegevens noodzakelijk is. Het is de auteur niet bekend of dit oordeel impliciet en stilzwijgend tot stand is gekomen, of dat hier een onderzoek aan te pas is gekomen.
De auteur heeft veel betrokkenen gesproken, en heeft daarbij geen aanwijzingen gevonden dat een dergelijk onderzoek is uitgevoerd. Een dergelijk onderzoek zou, als het bestaat, tot de conclusie moeten zijn gekomen dat de zero-knowledge technieken die op het moment van onderzoek bestonden, ontoereikend waren voor attribute-based authorisatie. Anders had men immers niet de vervolgconclusie kunnen trekken dat verwerking van persoonsgegevens noodzakelijk zou zijn. Zowel vanuit maatschappelijk als vanuit wetenschappelijk perspectief zijn de overwegingen van een dergelijk onderzoek zeer interessant en relevant.
De WBP geeft geen expliciet uitsluitsel over welke partij de verantwoordelijkheid draagt voor de noodzakelijkheidstoets. Hoewel het niet onlogisch zou zijn te veronderstellen dat de verwerker deze verantwoordelijkheid draagt, zou het goed zijn als het CBP hier uitsluitsel over geeft.
Overigens geeft de memorie van toelichting van de WBP dit uitsluitsel wel voor journalistieke verwerking. Daarover wordt gesteld[18]:

> Bij de toepassing van de noodzakelijkheidsnorm zal degene die de gegevens verwerkt steeds moeten afwegen of de betreffende verwerking voldoen aan beginselen van proportionaliteit en subsidiariteit.

In dit licht is het ook opmerkelijk dat het eerder genoemde OV-chip 2.0 onderzoek, over de toepasbaarheid van zero-knowledge, niet plaatsvindt op instigatie van de overheid of partijen uit de OV-sector. Het onderzoek is een initiatief van de Radboud Universiteit Nijmegen en wordt gefinancierd door de onafhankelijke non-profit NLnet Foundation.
De tweede vraag die zich opdringt is:

2. Moet een bestaande infrastructuur worden aangepast als er nieuwe en betere technieken voor privacybescherming beschikbaar komen?

In het geval van de OV-chipkaart is de aanbesteding van de centrale infrastructuur in juli 2003 afgerond. Door deze timing kwamen de technieken van IBM en Brands waarschijnlijk te laat. Het is allicht niet proportioneel om van TLS te verwachten dat zij op stel en sprong migreert naar een systeem dat deze technieken toepast. Maar het zou ook opmerkelijk zijn als een systeem tot in lengte van dagen slechts een matige privacybescherming hoeft te kennen, puur op basis van de vrij toevallige datum waarop het systeem oorspronkelijk is vastgesteld.
Een zeer strikte interpretatie van de WBP zou een verplichte migratie op stel en sprong suggereren. Echter, het lijkt er meer op dat er bij het opstellen van de WBP geen rekening is gehouden met het inpassen van later beschikbaar komende technieken voor de bescherming van privacy. Een richtsnoer, visie of uitspraak van het CBP op dit punt is dan ook van harte welkom.

[18] MvT WBP Art 3 lid 2, kamerstuk 25892-3, bladzijde 74.

Rekeningrijden

De discussie over anonimiteit en privacy met betrekking tot vervoersgegevens is niet uniek voor het openbaar vervoer. Ook bij het autovervoer staat een grootschalige elektronische rittenregistratie voor de deur, in de vorm van rekeningrijden. Ook daarbij is er de keuze tussen meer en minder privacyvriendelijke oplossingen. De Minister van Verkeer en Waterstaat zei daarover in het RTL nieuws van 30 januari 2008 het volgende[19]:

> Als we het zo gaan vormgeven, kan de overheid alleen maar zien hoeveel kilometers je hebt gereden, en misschien ook nog van hoeveel heb je in de spits gereden, want daar kan een iets andere prijs aan vasthangen. Maar niet meer dan dat. En je kunt alleen als automobilist zélf uit je auto de detailgegevens halen: Waar was ik op welk moment? Maar niemand anders kan daar aan.

Dit suggereert allicht dat er bij rekeningrijden gekozen zal worden voor een meer privacyvriendelijke oplossing. In vergelijking daarmee is de OV-chipkaart in zijn huidige vorm stukken minder privacyvriendelijk.

Het is dan niet ver meer tot de conclusie dat je privacy afhankelijk is van of je met de auto of met het openbaar vervoer reist. Die conclusie is dichtbij, maar is nu nog niet gerechtvaardigd. Rekeningrijden figureert al lang op de politieke agenda, maar veel details staan nog niet vast. Bij de OV-chipkaart staan de details wel vast, maar is er sprake van zoveel (politiek) rumoer dat de details wellicht alsnog zouden kunnen veranderen. Desalniettemin is het zaak ervoor te waken dat geen dergelijk onderscheid naar vervoermiddel niet ontstaat. Niet iedere reiziger heeft een reële keuze tussen openbaar vervoer en auto.

[19] Dit citaat is een transcriptie van de uitzending op het web door de huidige auteur.

Conclusie

Met dit relaas is nog lang niet alles gezegd over de privacy van de OV-chipkaart, maar zijn eigenlijk vooral de belangrijkste punten aangestipt. Toch lijkt het mogelijk alvast een paar zaken te constateren.
De doorsnee reiziger in het openbaar vervoer heeft met de OV-chipkaart stukken minder privacy dan met strippenkaart en papieren treinkaartje. Volledig anoniem reizen is nog wel mogelijk, maar dat vereist achtergrondkennis, motivatie, geld en een ijzeren discipline van de reiziger. Daarmee staat de OV-chipkaart op gespannen voet met de WBP, zo lijkt het.
Het opslaan van gedetailleerde reisgegevens en de prijsdruk zijn het gevolg van ontwerpkeuzes in de architectuur en opzet van de OV-chipkaart. Het lijkt erop dat er alternatieve oplossingen bestaan, waarbij anoniem reizen mogelijk is, en huidige tarief- en controlestructuur kan worden gehandhaafd.
Dit staat in contrast met de situatie omtrent rekeningrijden, waar oplossingen worden overwogen die voor anoniem rijden geen extra inspanning van de automobilist vragen.
Het is van maatschappelijk belang alternatieve oplossingen nader te onderzoeken. Het is de vraag of zulke alternatieven bij het ontwerp van de huidige OV-chipkaart overwogen zijn. Als deze overweging is gemaakt, dan is zij waarschijnlijk bijzonder informatief en waardevol. Als deze overweging niet is gemaakt, dan werpt de vraag zich op wie dat had moeten doen.
Als de alternatieve oplossingen daadwerkelijk toepasbaar zijn, betekent dit dat de huidige OV-chipkaart ook in dit opzicht op gespannen voet staat met de WBP.

Tot slot

Dit artikel had nooit tot stand kunnen komen zonder de kennis die is opgedaan in een groot aantal gesprekken met direct betrokkenen. Hun aantal is te groot om ieder bij naam te noemen, maar uitdrukkelijke dank voor hun tijd en openheid is op zijn plaats. De auteur was en is nauw betrokken bij de ontwikkelingen rondom de OV-chipkaart en de Mifare Classic aan de Radboud Universiteit Nijmegen.