Automatisering Gids

Experts breken lans voor privacy in architectuur kilometerheffing

Laatste update: 19-12-2008 door: Geert Kelfkens

Wetenschappers van de Vrije Universiteit Amsterdam en de Radboud Universiteit Nijmegen hebben voor de kilometerheffing een fraudebestendig systeem ontwikkeld dat de privacy van de automobilist optimaal beschermt. Volgens hen is de voorgestelde architectuur te combineren met een eenvoudig ('dun') kastje in de auto.

De voorbereiding voor de landelijke invoering van de kilometerheffing is in volle gang. Het ministerie van Verkeer en Waterstaat heeft echter nog niet onthuld hoe de architectuur van het systeem eruit gaat zien. Dat zal waarschijnlijk pas gebeuren op het moment dat de openbare aanbesteding van het project begint.

De beveiligingsspecialisten Wiebren de Jonge van de Vrije Universiteit en Bart Jacobs van de Radboud Universiteit schetsen in een artikel voor de nog te publiceren uitgave Lecture Notes in Computer Science (LNCS) een privacyvriendelijke en toch fraudebestendige architectuur voor de kilometerheffing. Zij willen zo de aanzet geven voor een openbare discussie over het te kiezen systeem. Tot dusver is zo'n debat niet of nauwelijks gevoerd. Uiteindelijk gaat het volgens de onderzoekers om een politieke keuze.

De bezorgdheid van beide wetenschappers is onder meer ingegeven door de gang van zaken rond de OV-chipkaart, vertelt Jacobs. "Bij de OV-chipkaart zagen we dat als in achterkamertjes wordt bedacht hoe een systeem moet worden ingericht, dat niet altijd de beste oplossing geeft. Ik ben voorstander van een openbare discussie. Ons artikel legt een kader op tafel voor een mogelijke oplossing, vanuit de invalshoek van privacybescherming en fraudebestrijding."
Uitgangspunt van De Jonge en Jacobs is dat de kilometerheffing er niet toe mag leiden dat de gangen van elke automobilist stelselmatig zijn te volgen. Dat gevaar is reëel als wordt gekozen voor een simpel, 'dun' kastje in de auto (On-Board Equipment, OBE) dat alle locatiegegevens naar een centrale backoffice stuurt. Een 'dik' kastje dat zelf de ritprijzen berekent en alleen bedragen doorstuurt biedt meer privacy, maar is complexer en duurder.

De Jonge en Jacobs kiezen voor een decentrale architectuur waarin de privacybescherming diep is ingebouwd. Uitgangspunt is dat de gebruiker de controle moet hebben over zijn eigen gegevens. De kostenberekening kan desgewenst plaatsvinden in de OBE, bij een serviceprovider of met een open-sourceapplicatie op de pc van de automobilist zelf.

Centraal in het voorstel staat het begrip 'hashing'. Dat is een vorm van encryptie in één richting waarbij gegevens worden 'verhaspeld' tot een digitale vingerafdruk, een gecodeerde waarde waaruit de oorspronkelijke data niet meer zijn te reconstrueren. De OBE slaat tijdens de rit gegevens over de afgelegde wegtracés op. Eenmaal daags stuurt het kastje een 'hash' van de ritgegevens naar een backoffice en eens per kwartaal het verschuldigde totaalbedrag. De backoffice kan interactief draadloos verifiëren of de juiste gegevens zijn ingediend. Steekproefcontroles, waarbij foto's van passerende auto's worden genomen, moeten garanderen dat de gebruiker niet met het kastje heeft geknoeid.

In de opzet van De Jonge en Jacobs is ook een 'dik' kastje in de auto mogelijk, bijvoorbeeld geïntegreerd in een navigatiesysteem. De gebruiker kiest er dan zelf voor dat een bedrijf als TomTom de verrekening van de kilometerheffing verzorgt en daarnaast aanvullende diensten levert.

Het volledige artikel van De Jonge en Jacobs
Verschenen in: Automatisering Gids nr. 51, 2008