Verslag Landelijke Smart Mobility Ronde Tafel Security

Dinsdag 10 mei 2016

Tijdstip: 10:00 – 12:00
Locatie: Sweco, De Holle Bilt 22, De Bilt;

PdL
DITCM INNOVATIONS | WWW.DITCM.EU
10-5-2016 VS 0

Verslag Landelijke Smart Mobility Ronde Tafel Security

Deelnemers

Gilles Ampt	(voorzitter)
Joelle vd Broek	DITCM
Peter de Lannoy	ANL / DITCM
Jeroen Doumen	Irdeto
Marcel Otto	Ministerie I&M
Hellen Havinga	RWS
Josee Sombekke	SIMS4U
Oene Kerstjens	Sistron
Titus Visser	St. aanpak Voertuigcriminaliteit
Willem de Boer	Technolution
André Smulders	TNO
Arjan Geluk	UL Software & Security
Peter Goossens	Vialis
Sjoerd-Jan Wiarda	TNO
Koen Fransen	Thales
Gregory Neven	IBM
Eric Verheul	KeyControls

Agendapunten

1. Welkom en opening
2. Verslag en acties bijeenkomst 29 januari
3. Bespreking en vaststelling verslag PKI dry run workshop 19 februari
4. Toelichting GSMA embedded SIM specification voor Connected Vehicle toepassingen – *Arjan Geluk, UL Software & Security*
5. Presentatie onderzoeksresultaten toepasbaarheid ABC4Trust voor C-ITS – *Eric Verheul, KeyControls*
6. Design principes voor WG5 certificate policy – *Gilles Ampt*
7. Stappenplan voor Security en privacy framework voor Hybride connectiviteit – *Marcel Otto, I&M Connecting Mobility*
8. Rondvraag
9. Sluiting

Kort verslag van het besprokene

Ad agendapunt 1,2, 3:
Welkom, opening en verslagen 29/1 en 19/2 *(zie vergaderstukken)*

Het verslag Security tafel van 290116 en ook de weergave van de resultaten “Workshop Vertrouwensdiensten” van 190216 worden goedgekeurd en door de Tafel vastgesteld.
Opgemerkt wordt dat veel issues uit de workshop ofwel in de “hybride”agenda terugkomen ofwel gerelateerd zijn aan EU-WG5 acties.

Ad agendapunt 4:
Toelichting GSMA embedded SIM specification voor Connected Vehicle toepassingen
– Arjan Geluk, UL Software & Security (zie presentatie)

Arjan Geluk laat in zijn presentatie zien dat de “embedded SIM” (eUICC) naast de vele overige toepassingen met name in de automotive een sterke bijdrage levert om Connected Car ontwikkelingen te versnellen. Kenmerkend is dat deze Sim vast verbonden is met het voertuig, op afstand kan worden geprogrammeerd. Enkele voordelen zijn dat van operator kan worden gewisseld en meerdere SIM profielen kan bevatten. Een en ander leidt tot lage operationele kosten en is “Vendor lock-in” geen thema.
Opgemerkt wordt dat de levensduur van de crypto – security tot nu toe weinig negatieve ervaringen heeft opgeroepen.

Ad agendapunt 5:
Presentatie onderzoeksresultaten toepasbaarheid ABC4Trust voor C-ITS
– Eric Verheul, KeyControls (zie presentatie)

Eric Verheul heeft in opdracht van Connecting Mobilit/ de ronde tafel Security een Quick Scan gedaan op mogelijke toepassing van ABC4trust technieken als verbetering van de ITS aspecten betrouwbaarheid, voertuig privacy en efficiency. Hij laat in zijn presentatie zien dat binnen de gekozen scope de ABC technieken veelbelovend zijn, maar momenteel nog niet aan alle technische randvoorwaarden voldoen. Daarentegen is met de huidige crypto grafische technieken (met wellicht enkele standaard aanpassingen) al een heel betere balans tussen de genoemde aspecten te bereiken. Hiertoe presenteert Eric het zgn. IFAL concept, Issue First Activate Later. Dit is een optimalisatie van de huidige ETSI standaard waarbij de short tem pseudoniem certificaten bijv. voor 10 jaar vooraf worden uitgegeven maar slechts 10 minuten geldig zijn (niet hergebruikt worden) en in batches van bijv. 3 maanden op hele efficiënte wijze kunnen worden geactiveerd. Dit is niet alleen privacy vriendelijker, maar biedt ook effectieve bescherming tegen Sybil attacks. De tussentijdse activitatie is een effectieve alternatieve revocatie maatregel, waarvan het tijdsinterval instelbaar is.
Een uitgebreide lijst met referenties is in de presentatie als bijlage ingesloten. Wellicht kunnen de resultaten meegenomen worden in WG5 van het C-ITS platform

Ad agendapunt 6: Design principes voor WG5 certificate policy
- Gilles Ampt

Dit agendapunt wordt opgeschoven naar de volgende vergadering.

Ad agendapunt 7:
Stappenplan voor Security en privacy framework voor Hybride connectiviteit – Marcel Otto, I&M Connecting Mobility

Marcel Otto legt uit dat dit stappenplan dat binnen de Tafel A&I een en ander wordt uitgewerkt, en nog redelijk abstract is. Dit rapport is binnenkort op de site te vinden. In augustus – september zullen in expertsessie(s) alle tafels in gelegenheid gesteld worden de om de implicaties te bekijken. In juni komt er wellicht groen licht om met EU subsidie de “hybride communicatie” uit te werken. Oene Kerstjens vraagt namens de Brabant corridor wat de Security tafel kan bijdragen en of er hiertoe een speciale inhoudelijke sessie kan worden belegd.
Er wordt voorgesteld om op Tafel niveau naar één convergerende optie toe te werken (via de PKI architectuur of bv via de service providers) . Afgesproken wordt dat Joelle dit overleg via de Tafelvoorzitters nog voor de zomer probeert te plannen.

Ad agendapunt 8,9: Rondvraag en afsluiting
Geen bijzonderheden

Acties / Wrap up:

Nr	Actie	wie	Wanneer
100516			
7	**Tafelbreed overleg inplannen over convergerende benadering hybride communicatie**	**JvdB**	**Voor de zomer**