



Security projecten overleg 9 maart 12.30-15.00
Utrecht

9 maart 2018

Joelle van den Broek, Marcel Otto, Gilles Ampt
SECURITY | [HTTP://SMARTMOBILITYCOMMUNITY.EU/](http://SMARTMOBILITYCOMMUNITY.EU/)
9 MAART 2018

Security projecten overleg 9 maart 12.30-15.00 Utrecht

Doel: Afstemmen en vaststellen security activiteiten komende periode, incl. actiehouders, ten aanzien van de communicatie bij de ontwikkeling en uitvoering van C-ITS diensten.

Genodigden: betrokken experts en verantwoordelijken van C-ITS projecten in NL

Aanwezigen vanuit projecten resp Standards & Practices- thema Security:

- Oene Kerstjens, MobilityMoves
- Ronald Adams, InterCor
- Abraham Bot, ITS Corridor
- Onno Tool (vervangt Paul Spaanderman), C-Roads
- Sebe Vogel, Concorda
- Vincent Habers, Talking Traffic
- Henk Schuurman, RWS div projecten
- Marcel Otto, Connecting Mobility/ SMCS&P
- Wim Broeders, SMCS&P/ DITCM/ A&I
- Gilles Ampt, SMCS&P/ DITCM
- Joelle van den Broek, SMCS&P/ DITCM

Samenvatting en afgesproken acties:

Conclusie is dat we een gemeenschappelijke ambitie hebben om m.b.t. security een zo concreet mogelijk actieplan te maken, actiehouders benoemen en zorgen voor de uitvoering. Door samenwerking kunnen we elkaar versterken en zorgen dat diensten interoperabel zijn.

Afgesproken zijn de volgende acties:

- 1) Q&A: inzichtelijk maken welke belangrijke vragen m.b.t. security leven er en welke antwoorden / informatie of voorzieningen al beschikbaar en bruikbaar zijn, wanneer welke hoofdkeuzes te maken zijn en de gevolgen daarvan, Q&A op drie niveaus: technisch, procesinrichting of organisatie en financieel-economische aspecten
- 2) Concreet actieplan: document dat inzicht geeft in wat er nodig is voor security (Q&A), wie daarvoor wat gaat doen (en verantwoordelijk is) met een time lijn gekoppeld aan projectmijlpalen, beleidsprioriteiten en internationale mijlpalen.
- 3) Deze (1+2) bespreken in volgend overleg te plannen in April.
- 4) Onno checkt in WG2 of Talking Traffic op 27 maart in de C-Roads TF1 meeting in Eindhoven een presentatie kunnen geven. Gilles coördineert dit met TF1 en Talking Traffic.
- 5) Abraham overlegt of Talking Traffic een testauto wil meesturen naar het PKI testfest eind april in Reims.

Gilles maakt een opzet voor 1 en 2 en stuurt die na afstemming met Marcel en Joelle aan de anderen ter aanvulling. Zodat er bij de volgende meeting een plan ligt waar iedereen al input op heeft aangeleverd en we tijdens de meeting snel concreet kunnen worden.

Agenda:

12.30: Welkom door Joelle van den Broek en Marcel Otto, Smart Mobility Community For Standards & Practices + kort rondje voorstellen en verwachtingen

12.45: Inleiding door Talking Traffic:

- wat gaan zij in 2018 doen op gebied van Security/ PKI?
- welke behoeften heeft TT daarbij projectoverschrijdend?
- welke keuzes moeten gemaakt worden en waarom?
- wat zijn de uitkomsten van TT enquête hierover?

13.00: Inleiding door ITS Corridor / InterCor:

- wat gaan zij in 2018 doen op gebied van Security/ PKI?
- welke behoefte heeft RWS daarbij projectoverschrijdend?
- welke keuzes moeten gemaakt worden en waarom?

13.15: Korte inleiding vanuit Concorda

13.30: Inleiding door Gilles Ampt en Marcel Otto:

- Wat is de status mbt security policy van Brussel?
- welke ontwikkelingen zijn er vanuit C-Roads op gebied van security?
- wat betekent dat voor de komende periode?

13.45- 14.00: korte pauze/ uitloop

14.00-14.45: Discussie (gespreksleiding Joëlle)

- Wat moet er op korte termijn en wat op lange termijn gebeuren tav Security?
 - Inhoudelijk resp. procesmatig
 - 'Need to have' versus 'Nice to have'
 - Timeline: 'Volgend' op internationale ontwikkelingen resp 'vooruitlopend op'
- Wie staat waarvoor aan de lat (wat in projecten, wat vanuit Beleid I&W, wat vanuit DITCM team/ experts)?

14.45-15.00: Wrap up en concrete afspraken/ actieplan

15.00: Afsluiting

Intro achtergrond en aanleiding door Joelle en Marcel:

- In nieuwe beleidsagenda is (Cyber)Security een belangrijk thema, de Minister geeft aan security belangrijk te vinden.
- Ook op de Europese agenda is Security een aandachtspunt en wordt regelmatig input vanuit 'Nederland' gevraagd, dan wel komen richting gevende resultaten, zoals uit C-Roads en C-ITS Werkgroepen.
- Vanuit eerdere gesprekken met zowel projecten als beleidsmensen, is een werkagenda voor Standards & Practices opgesteld, met daarbinnen Security als thema./
- In deze sessie willen we de activiteiten verder oplijnen, concreet maken door te weten wat vanuit de projecten op dit gebied plaats (gaat) vind(t)(en), welke projectoverkoepelende vragen er zijn, en welke keuzes we moeten maken gekoppeld aan de tijdslijnen van projecten en Europese (beleids)agenda's mbt security.
- Uitgangspunt is 'brengen en halen': dus projecten voeren onderdelen van de werkagenda uit en leveren bouwstenen op voor een nationaal framework, vanuit landelijke en internationale ontwikkelingen worden resultaten verspreid, toegevoegd, aangevuld. Zodat niet ieder project zelf alles uit hoeft te zoeken en we concrete stappen maken.

Voorstelronde/verwachtingen:

- Iedereen benadrukt dat we geen papieren studies willen, maar concrete acties. Met als doel vanuit toch al geplande acties elkaar versterken? '1+1=3'
- Neem 3-4 onderwerpen die in meerdere projecten spelen als case, met focus kunnen we elkaar concreet helpen
- Focus op "wat nu" nodig is/ beschikbaar is.
- Communicatie van resultaten en acties is belangrijk
- Internationale afhandeling: wat doen we hier, wat internationaal. Waarin zijn we volgend en waarin willen we pro actief zelf wat doen
- Maak security onderdeel van interoperabiliteit/ dutch profiles
- Ik wil weten welk bouwsteen mijn project levert binnen het grote geheel en dat dat van elkaar bekend is
- Ik wil zicht krijgen op de security behoefte over projecten heen: wat zijn de kwetsbaarheden, wat is de rode draad/ gemene delen, wat zijn gezamenlijk te beantwoorden vragen. Marktpartijen participeren in meerdere projecten – hoe zitten zij erin?.
- Mijn project ontwikkelt zelf niets aan security, maar ik wil graag gebruik maken wat van andere projecten beschikbaar is
- Prioritering: wat moeten we op KT doen, welke keuzes en acties, wat kan wel even blijven liggen nog.
- Ik wil weten wat de minimale set met acties is die ik als wegbeheerder moet doen mbt security.
 - Hoe reageren op policy documenten vanuit het C-ITS platform
 - Wie/wat moet CIV doen tav security?
- De Community for Standards & Practices moet de internationale tafels en de projecten tafel verbinden
- We willen concreet aan de slag: ik wil scherp krijgen wat precies en wie doet het inhoudelijk werk? Wie vanuit projecten? Liefst vooraf helder hebben wie en met welke capaciteit wat vanuit projecten gaat opleveren zoals dat nu ook met Dutch Profiles plaats vindt.

Talking Traffic (Vincent Habers)

Vincent geeft een toelichting hoe security binnen het partnership Talking Traffic geregeld is. Een aantal punten die specifiek besproken zijn:

- De verantwoordelijkheid voor Security ligt bij Cluster 2 partijen. Dit is een projectkeuze. Voorbeeld: Priority dienst: voor het voertuig moet worden vastgesteld dat hij idd bevoegd is prioriteit aan te vragen bij de VRI, verantwoordelijkheid via cluster 2 partij, Hierbij zijn tijdelijke keuzes gemaakt tav taken en verantwoordelijkheden tav PKI certificaten-uitgifte, passend/anticiperend op EU afspraken die er komen.
- Talking Traffic gaat inzichten opleveren die niet alleen op projectniveau, maar NL breed van belang zijn:
 - Het PKI certificaten-fabriekje': Hoe werkt het in de praktijk?

- Wat zijn de kosten van zo'n 'PKI fabriekje' en wat is het effect in waardeketen?
- De iVRI standaard is ingericht op 'hybride' en als zodanig opgenomen in de Dutch Profiles en ingebracht bij C-Roads. TT gebruikt hierbinnen vooral het cellulaire gedeelte, Maar NH gaat bijv wel Wifi-p gebruiken in haar projecten.
 - Authenticatie aan voertuig- danwel 2 kanten op (ook authenticatie aan VRI kant)
 - Uitwisselbare keuzes, Hybride, Cellulaire en Wifi-p oplossingen.
- Wie is security officer? En hoe gaan we om met de daarmee gepaard gaande kosten? Geaccrediteerde certificaten zijn duur. Hebben we het over verversen van 4x per jaar of meerdere keren per dag (onnodig voor een RSU omdat deze niet anoniem hoeft/mag zijn) . En dit bij 3000 van de 6000 dit jaar te vervangen VRI's. Komen deze kosten bij de wegbeheerder of bij de gebruiker?
- Wie beheert de lijst "blacklist"? Cluster 1 partijen monitoren misbehaviour van cluster 2 partijen.
- Projectgebonden is gekozen voor Siemens die de PKI keys bewaart in de digitale kluis. Er is gekeken naar mogelijke alternatieven, w.o. RDW, maar daar is nu niet voor gekozen. Ofwel in TT is het proces ingericht, maar de spelers zijn straks anders.
- Dit moet halverwege 2018 gereed zijn.
- Internationale interoperabiliteit voor iVRI en security gaat waarschijnlijk een rol spelen in de grensstreek.
- Sebe geeft aan dat vanuit NH in Concorda, Fiat uitgaat dat de wegkant betrouwbaar is en dat PKI certificaten op berichten van i-Vri naar auto zouden moeten gaan.

Abraham Bot (InterCor)

- InterCor voert een Security aanpak uit volgens een drietrapsraket:
 - A. PKI Testfest april in Frankrijk. Testopzet in NL volgens ETSI TS 103 097 v1.2.1. Daarna met testauto naar Frankrijk en daar laten zien dat het daar ook werkt. RDW heeft partij gecontracteerd die PKI-certificaten levert namens RDW en RWS. Dit is een "offline" oplossing.
 - B. InterCor maakt in het najaar de transitie naar de nieuwe standaard (v1.3.1).
 - C. Eind dit jaar moet ook de online oplossing ingericht zijn.
- Met techniek is InterCor een heel eind op dreef; proces en organisatie moet nog ingericht worden. Aspecten die spelen die over de projecten afgestemd zouden moeten worden:
 - Een project kan niet altijd halverwege op een nieuwe standaard overgaan en kiest een moment opname. Wie bepaalt welke standaarden je gebruikt?
 - Welke rollen zijn er? En waar moeten die landen? RDW staat nu opgesteld voor voertuigen in NL. Maar nu gaat het ook om wegkantstations. Is dat een verantwoordelijkheid dadelijk voor de VRI wegbeheerder of de VRI leverancier?
 - En wat kost dat nou?
- Concreet genoemde actie: kunnen we een TT auto meesturen naar de testfest in Frankrijk?

Sebe Vogel (Concorda)

- In Noord Holland worden testen uitgevoerd (2019) met Fiat en Chrysler in Amsterdam en Rotterdam. Betrokken zijn KPN, TASS en Brabant. Naast Nederland participeren nog 4 landen.

- Er ligt een voorstel van Escript om alle projectpartners te voorzien van PKI-certificaten op basis van de nieuwste ETSI standaard (v1.3.1). NXP vindt het nog te vroeg voor v1.3.1.
- Voor Concorda is er behoefte aan landelijke keuzes, die men niet op projectniveau Concorda wil gaan beslissen. Met name aangaande 5G, LTVE kant, MEC Computing (Model Edge Computing) waar men in Brabant mee gaat experimenteren (itt Amsterdam die focust op cellulair).
- Tijdslijn: Juni 2018 ligt er een implementatie plan, 2018-2019 Implementatie, keuzes moeten dan gemaakt zijn.

Gilles Ampt (Europese ontwikkelingen):

- Overzicht gegeven van de ITS security werkgroepen binnen ETSI, EC en C-Roads waar Nederland actief in participeert. Tevens kort overzicht van de onderwerpen die binnenkort gaan spelen en belangrijk voor Nederland zijn. Zie ook de slides die bijlage bij dit verslag zijn.
- Een van de prangende onderwerpen is security certificering van ITS stations. Dit voorjaar wordt een concreet voorstel verwacht van de Duitsers (BASt en BSI), die dan beoordeeld moet worden op de gevolgen bij invoering in NL. Dit voorstel wordt besproken in TF1 van C-Roads.
- Frankrijk heeft de regie t.a.v. Security in InterCOR.
- Vanuit Nederland willen en kunnen we op dit thema geen koploper zijn maar volgend (uitgezonderd enkele issues als IFAL en betere wijzigingsstrategie van AT's). Er zijn nog veel zaken die die nog uitgetest moeten worden, liever dat Duitsland en Frankrijk de kinderziekten eruit halen en dat wij dan de 'best practices' en resultaten kunnen overnemen. We moeten dan wel goed volgen en weten wat speelt bij de Nederlandse projecten en stakeholders zodat we tijdig kunnen anticiperen en beïnvloeden.
- Concrete actie: 27 maart is er een C-Roads TF1 (security) meeting in Eindhoven. Het zou goed zijn om de bevindingen vanuit Talking Traffic hier in te brengen. Onno neemt dit mee als verzoek in WG2 en koppelt terug. Goed voorbereiden.

Acties:

Gilles werkt een Q&A en concreet actieplan uit en stuurt die na afstemming met Marcel rond (zie samenvatting acties op pagina 1): genoemd zijn de volgende vragen (Q) tijdens de sessie:

Operationeel → concreet voorstel met vragen en antwoorden op

- Wanneer moeten welke keuzes gemaakt worden?
- Wanneer is wat beschikbaar vanuit welk project of internationale werkgroep?
- Welke vragen meenemen in welke projecten?
- Welke versies van standaarden worden in welk project gebruikt? Wanneer nieuwe versies te verwachten?
- Wanneer zijn welke testfests gepland en wat komt daaruit?
- Wanneer moeten we een gedragen reactie geven op de delegated act?
- Wanneer is nieuwe regelgeving te verwachten en van kracht, inclusief Europese uitvoeringsorganisaties?
- Wanneer moeten we als NL welke besluiten nemen?

- Wat wordt in de testfests getest, welke elementen waar/ welk project/test/internationaal
- Hoe liggen de acties in de tijd?
- Welke implementaties kunnen we delen?

Strategisch:

- Welke strategische afwegingen?
- bv volgen of anticiperen.
- Bv alleen reviews op EU, DU, FR en daarna gebruiken.

Over 1 maand nieuwe afspraak. Er ligt dan een concreet voorstel dat we kunnen bespreken.