



# Verslag Thema-sessie “PKI voor Connected voertuigen”

---

Donderdag 5 oktober 2017

Tijdstip: 13.30 – 15.30 uur  
Locatie: Talking Traffic, Van der Valk Utrecht

GJA  
WWW.DITCM.EU  
5 OKTOBER 2017

Beter Benutten



Connecting  
Mobility

## Verslag Thema-sessie “PKI voor Connected voertuigen”

### Deelnemers

ongeveer 30 deelnemers

### Agenda

#### 1. Inleidingen - Security behoeftes van Connected-ITS projecten

- a. Talking Traffic en iVRI – Vincent Habers (Talking Traffic)
- b. InterCOR en C-Roads – Gilles Ampt (InterCOR)
- c. PPA en Socrates – Hans Kramer (RWS)
- d. Noord-Brabant en Mobility MoveZ – Oene Kerstjens (Provincie Noord-Brabant)

#### 2. Inleidingen – PKI- dienstenontwikkeling voor Connected ITS-toepassingen

- a. Security agenda van de EC en PKI voor V2X-ITS-toepassingen – Gilles Ampt (lid C-ITS platform)
- b. Planningsproces voor PKI-dienstenontwikkeling – Ido Vlaminckx (RWS)

#### 3. Gedachtenwisseling tussen aanwezigen over behoefte en positionering van PKI

- o.l.v. Gilles Ampt (thematrekker Security van de Smart mobility community)

#### 4. Conclusies en afronding

Bijlage: draft paper “Management samenvatting van het belang van een PKI voor C-ITS”

### Kort verslag van het besprokene

#### Talking Traffic

Vincent Habers licht toe dat er een security-behoefte is in zowel Cluster 3 als Cluster 2. In cluster 3 staan centraal de voorrangsvoertuigen zoals zwaailichten die prioriteit moeten kunnen krijgen van een iVRI. Daar is een specifieke behoefte aan voertuig-certificaten die de autorisatie representeren van de rechtmatigheid van een prioriteitsaanvraag. In cluster 2 gaat het om de authenticatie van de (cloud dienst) service providers.

## InterCOR

Gilles Ampt licht toe dat in InterCOR voor enkele use cases de interoperabiliteit wordt gespecificeerd en getest gaat worden tussen partners in Frankrijk, Engeland, België (Vlaanderen) en Nederland (RWS, Noord-Brabant, Helmond, provincie Utrecht). Voor de G5 (wifi-P) diensten staat in het voorjaar van 2018 een PKI-testfest gepland dat in Frankrijk zal plaatsvinden. Hiertoe heeft het project in Nederland via RWS een inkooptraject gestart waarbij QuoVadis de PKI-certificaten zal leveren voor Wegkant-stations en RDW voor de voertuigen.

## PPA, Socrates en Concorda

Hans Kramer licht vanuit de Praktijk Proef Amsterdam allereerst de doelstellingen van de 3 projecten toe. Waar Socrates gericht is op deelnemende service providers als TomTom en Here, doen in Concorda voor testdoeleinden ook autonoom rijdende voertuigen mee (level 3 en 4) van o.a. Fiat. In de projectplanning zijn begin 2018 voertuigcertificaten nodig.

## Noord-Brabant

Oene Kerstjens licht toe dat Mobility MoveZ heel binnenkort de dialoog-workshops start waarin security wordt meegenomen. Er is voornamelijk geen specifieke behoefte aan PKI-certificaten. Binnen InterCOR zal gemeente Helmond voor GLOSA waarschijnlijk werken zonder PKI. Op de vraag wat er gaat gebeuren met de PKI van Spookfiles op de A58 antwoorden betrokken partijen dat deze PKI een leerdoelstelling had en niet is opgezet om doorontwikkeld te worden voor deployment. De service providers van Spookfiles A58 zijn voor een mogelijk vervolg geïnteresseerd om aan te haken als er een nieuwe PKI komt voor meerdere projecten.

## Security PKI agenda van de EC

Gilles Ampt licht toe dat de EC in de periode 2018 – 2021 investeert in de totstandkoming en operatie van de centrale diensten die nodig zijn voor de interoperabiliteit van de verscheidene PKI's van de landen en fabrikanten. Dit zal gebeuren conform de in juni 2017 gepubliceerde certificate policy ([https://ec.europa.eu/transport/sites/transport/files/c-its\\_certificate\\_policy\\_release\\_1.pdf](https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf)). Onderdeel van het plan van de EC is ook de operatie van een Root-CA. Voor sommige projecten als InterCOR komt dit te laat.

Marcel Otto zegt dat ook nog een bredere security policy afgerond en geïmplementeerd moet worden, voor de governance van de vele rollen, posities en procedures. Hij verwacht dat de security policy pas in 2019 operationeel zal zijn.

## RWS dienstontwikkeling voor PKI

Namens Ido Vlaminckx die op het laatste moment verhinderd is, geeft Gilles Ampt een doorkijk vanuit het perspectief van RWS. RWS kan van een reeds gecontracteerde en geaccrediteerde partij gebruik maken om een productiestraat in te laten richten voor ITS-certificaten. De beoogde partij hiervoor is QuoVadis. Ook andere wegbeheerders alsook leveranciers, die certificaten namens de wegbeheerders dienen te installeren, kunnen hier naar verwachting ook gebruik van maken.

## Plenaire discussie

Gilles Ampt geeft een korte samenvatting van de gepresenteerde behoeftes van security certificaten van de projecten.

Eric Koenders vult aan dat Talking Traffic een ander uitgangspunt hanteert voor de authenticatie van voertuigen en dat dit gaat gebeuren via de eigen service provider. Er is dan een authenticatie nodig van de service provider die vertrouwd moet worden door andere partijen. Dit concept heet een proxy. De vraag is hoe dan de authenticatie end-to-end geborgd kan worden. Dat moet wel duidelijk zijn. Ook is de vraag hoe een proxy zich verhoudt tot de EU certificate policy, waar het uitgangspunt is dat de communicatie en ondertekening door de lokale C-ITS unit geschiedt en niet door een service provider.

De politie-organisatie werkt voor hun voertuigen met een bestaande service provider omdat de locatiegegevens van voertuigen op de meeste momenten confidentieel zijn en niet gedeeld mogen worden met derden.

Namens de stad Utrecht wordt genoemd dat er al in januari certificaten nodig zijn.

## Ad agendapunt 9: Conclusie en afsluiting

1. De eerste conclusie wordt gemaakt dat in de samenwerking de focus dient te liggen op organisatie en governance. De techniek van de certificaten is volgend en niet leidend.
2. Voor de korte termijn kunnen alle aanwezigen zich vinden in de aanpak van RWS om PKI-certificaten voor wegkantstations te laten realiseren en dat waar gewenst ook andere partijen van deze faciliteit gebruik kunnen maken.  
Daarbij wordt opgemerkt dat dit niet betekent dat andere partijen daarvoor worden uitgesloten, zeker niet op de langere termijn. RWS gaat in ieder geval vooralsnog geen regie voeren op uitgifte van ITS-certificaten.
3. Evenzo kunnen alle aanwezigen zich vinden in de voorlopige rol van RDW voor de uitgifte van PKI-certificaten aan voertuigen.
4. Op korte termijn is er behoefte om vast te stellen of de 3 projecten InterCOR, Talking Traffic en PPA/ Concorda concreet kunnen samenwerken in het opzetten van de governance van PKI-certificaten alsook de inkoop en levering van certificaten. Hiertoe zullen de projectvertegenwoordigers in klein comité i.s.m. Gilles Ampt namens de Security Community stappen zetten. Daarbij is aandacht nodig voor het verschil in status van de projecten. Bij Talking Traffic gaat het als enige om echte deployment en dat stelt dus ook hogere eisen. Bijv. als het gaat om de scheiding van de rollen van een Registratie-autoriteit (EA) en Autorisatie-autoriteit (AA) omwille van de data-protectie/ privacy.

De bijeenkomst wordt gesloten om 15.30 uur. Alle aanwezigen worden hartelijk bedankt voor hun aanwezigheid en bijdrage.