Leading partners in Smart Mobility

DITCM Innovations

Workshop resultaten CONCEPT

DRY RUN C-ITS VERTROUWENSDIENSTEN

Gilles Ampt
DITCM INNOVATIONS | WWW.DITCM.EU
19-2-2016

Workshop resultaten CONCEPT

Deelnemers

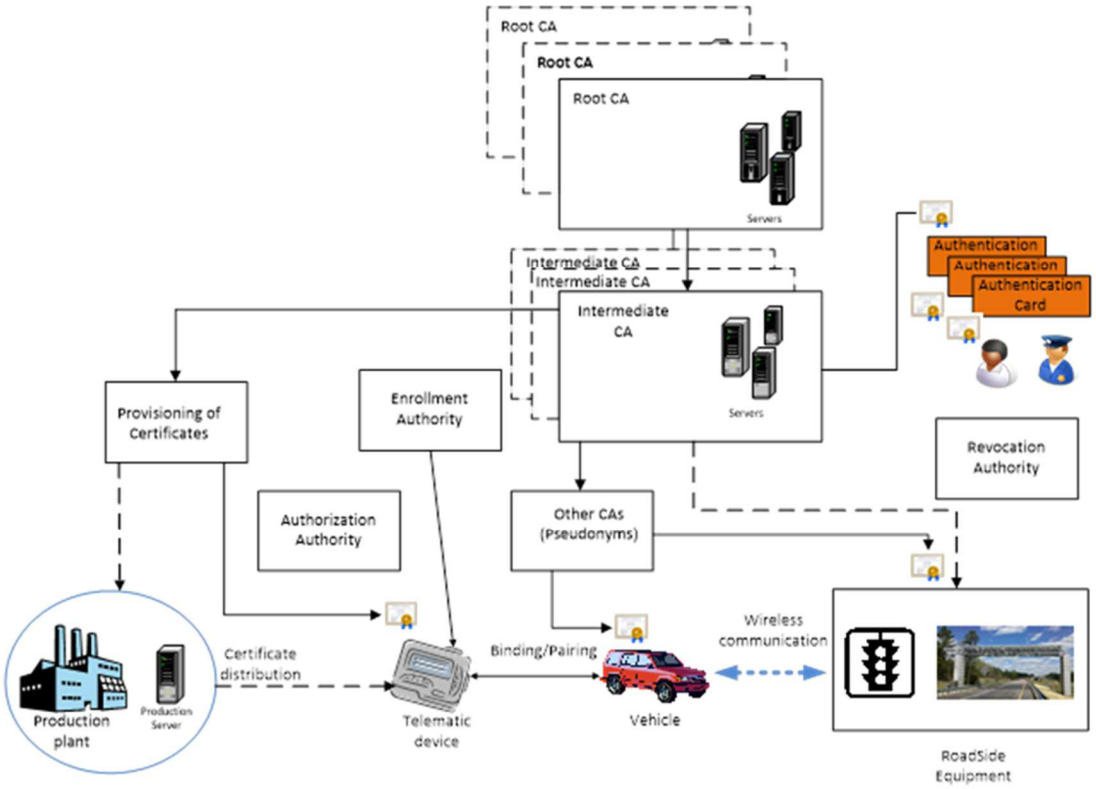
Gilles Ampt	facilitator
Tom Alkim	RWS
Zeger Baelde	RDW
Michiel Beck	I&M/ DGB
Leo Bingen	SIMS
Joëlle van den Broek	DITCM
Willem de Boer	Technolution
Jeroen Doumen	Irdeto
Peter Goossens	Vialis
Hellen Havinga	RWS
Ronald de Jong	ANWB
Peter de Lannoy	DITCM
Gerben van der Lei	Fox-IT
Kees Moerman	NXP
Marcel Otto	Connecting Mobility
Geert Pater	RDW
André Smulders	TNO
Josée Sombekke	SIMS
Ton Zwiers	Agentschap Telecom

Inleiding en aanleiding

Afgelopen jaar heeft WG5 Security van het C-ITS platform van de EC een eerste opzet uitgewerkt van het PKI trust model gebaseerd op de randvoorwaarden en specificatie van ETSI voor V2X berichtenverkeer via Wifi-P.

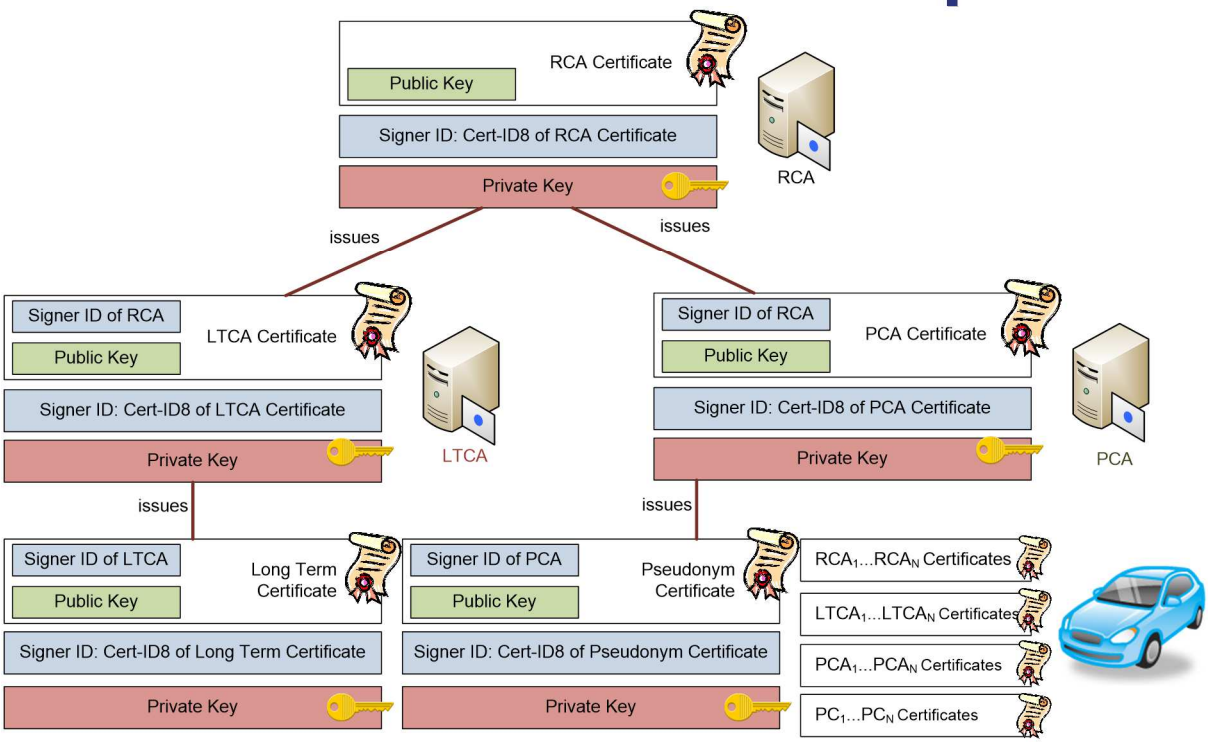
Alle ITS-stations die deelnemen aan dit V2X berichtenverkeer dienen te beschikken over een geldig digitaal (PKI) certificaat. Vanwege de privacy van automobilisten wordt er gewerkt met sets van wisselende pseudonym-certicaten waardoor individuele voertuigen niet structureel door hun omgeving kunnen worden gevolgd.

Onderstaand schema van WG5 is een illustratie van de opzet van de PKI voor V2X toepassingen.



De planning van WG5 is om in het voorjaar van 2016 het implementatieplan voor de PKI op te stellen voor onderwerpen als de Root CA alsook de certificering van ITS-stations t.b.v. grootschalige Day One implementaties van C-ITS. De planning van implementatie is 2019.

Het Car2Car consortium levert belangrijke input aan WG5 en heeft de PKI infrastructuur iets verder uitgewerkt als hieronder. Deze plaat is niet gebruikt bij de inleiding tijdens de workshop en is hier bedoeld voor de verslaglegging.

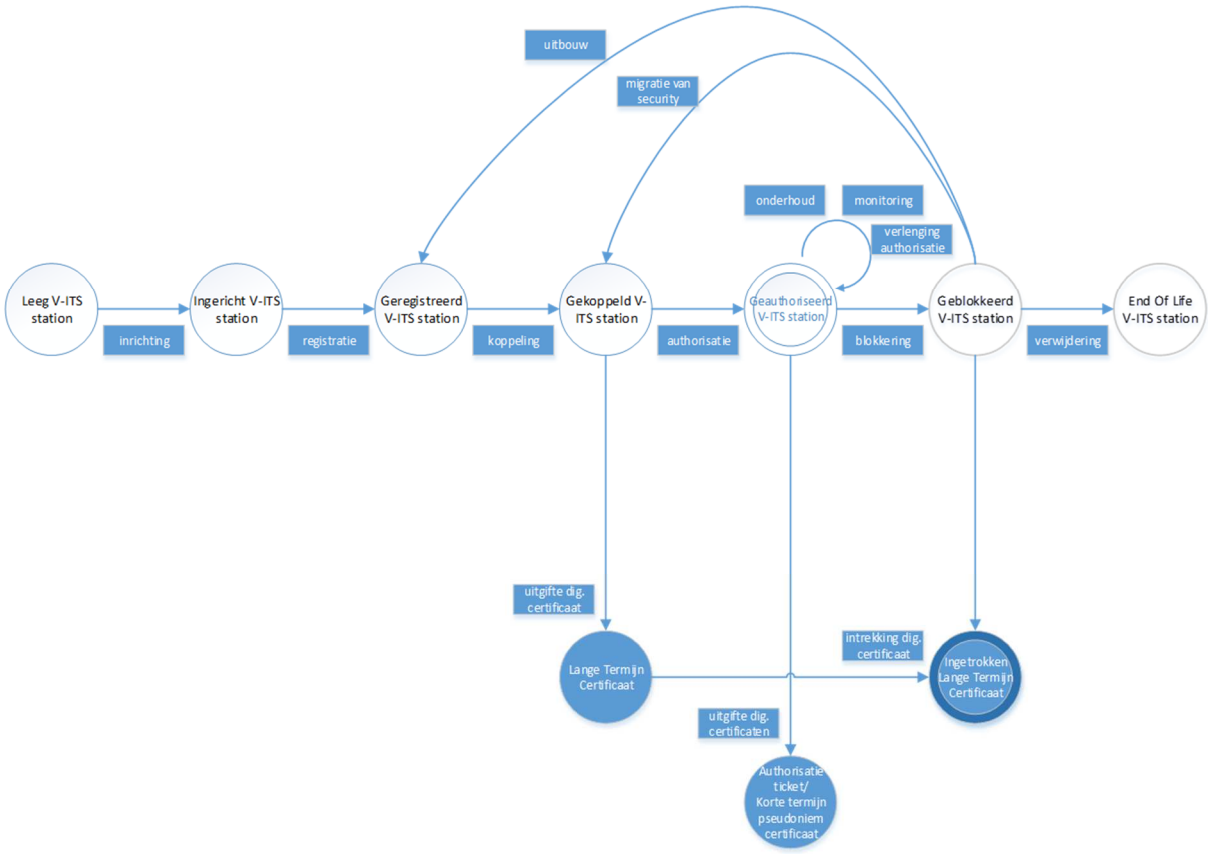


Het doel van de workshop is om met betrokken partijen en experts de totale levenscyclus van V-ITS stations te doorlopen evenals de tot dusverre in WG5 geïdentificeerde rollen die moeten worden ingericht en uitgevoerd om V-ITS stations operationeel en beveiligd te maken. Dit geeft alle betrokkenen in dit stadium inzicht in de resultaten van WG5 tot nog toe waardoor betrokkenen effectiever kunnen inspelen op de lopende totstandkoming van het implementatieplan. Tegelijkertijd kunnen door de workshop de resultaten van WG5 op hoofdlijn tussentijds worden gevalideerd.

De workshop is beperkt tot de ITS-stations in voertuigen (V-ITS stations). ITS-stations die onderdeel gaan uitmaken van de weginfrastructuur (R-ITS stations) zijn buiten beschouwing gebleven, evenals andere categorieën van ITS-stations (niet voertuig- of weginfra-gebonden). In de workshop is niet ingegaan op specifieke use cases van C-ITS en V2X. Vanwege de tijd is ook niet meer ingegaan op de mogelijke invulling van de rollen in het trust model voor C-ITS en V2X.

De resultaten van de workshop zijn openbaar. De individuele bijdrages van deelnemers zijn dat niet.

Rollen m.b.t. V-ITS life cycle



Rol:	**WAT ALS deze rol er NIET zou zijn of zou falen?**
<u>Provisioning entity (Inrichtingsbedrijf)</u> (Entiteit die een fabrieksklaar C-ITS station- volgens een secure proces- inricht en gereed maakt voor aanbieding aan het C-ITS domein)	• Onduidelijk welk certificaat in welk device/ voertuig zit
<u>Enrolment / Registration Authority</u> (Entiteit die een certificaat uitgeeft dat het V-ITS station is toegelaten en geregistreerd)	• Geen link met kenteken
	• Misbruik van rollen; geen vertrouwen
	• Andere methodes, bijv. reputation based of majority voting on events
<u>Linking/ Pairing entity (Koppelingsentiteit)</u> (Entiteit die het V-ITS station fysiek, logisch en secure koppelt aan een voertuig)	• Ook andere modaliteiten kunnen meedoen als voertuig
	• Koppeling naar persoon i.p.v. voertuig
	• Geen oplossing voor hogere authorisaties (bv. Politievoertuig)
	• Geen binding met fysieke

	eigenschappen van het voertuig
	• Zelf klussen, minder vertrouwen in de betrouwbaarheid
	• Goedkeuring vragen na zelf-inbouw/ aanmeldproces
Authorization Authority (Entiteit die digitale certificaten uitgeeft waarmee het V-ITS station operationeel wordt)	• Geen privacy
	• Geen geauthoriseerde en authentieke berichten
	• Geen verantwoordelijkheid voor uitgifte aan bv. politie-voertuigen
Misbehavior Authority (Entiteit die de geldigheid van digitale certificaten voortijd intrekt, daarvan een centrale lijst bijhoudt en distribueert).	• Misbruik van gestolen of verloren certificaten; verlies van vertrouwen
	• Identiteitsfraude
	• Authorisatiefraude
Verwijderingsbedrijf (Entiteit die het V-ITS station – volgens secure processen- ontmanteld om het buiten gebruik te stellen	• Geen vrijwaringsbewijs
	• Fraude, hergebruik van certificaten
Componenten leverancier (nieuwe rol)	• Welke security requirements (bv Common Criteria) implementeren?
	• Welke cost trade offs moeten gemaakt worden?
	• Welke anti-tampering maatregelen te nemen?
	• Hoe veel certificaten moet een C-ITS station aankunnen?

Rollen m.b.t. Public Key Infrastructure (PKI)

Rol:	**WAT ALS deze rol er NIET zou zijn of zou falen?**
Policy Authority (Entiteit die de regels bepaalt over de geldigheid van digitale certficaten en de randvoorwaarden voor de uitvoerende authoriteitenn in het certificatenstelsel)	• Zonder regels gaat het niet werken, komt C-ITS niet tot stand
	• Gebrek aan interoperabiliteit (bijv. over authorisaties)
	• Geen borging van privacy bij aanvragen van authenticatie-tickets
	• Variatie in hardening van enrolment en registratie authorities
	• Niemand zou elkaar vertrouwen
Trust model manager (Entiteit die het operationele en taktische beheer uitvoert van de vertrouwens-infrastructuur (PKI) volgens de security policy)	• Geen uniformiteit door storingen en vanwege veiligheid
	• Verouderde of verschillende versies, wild-west
	• Rol is overbodig, mits er voldoende toezicht is (functiescheiding)
	• Vraag: CA en RCA doen toch toezicht?
RCA (Root CA) (Entiteit die garant staat voor de echtheid en de betrouwbaarheid van alle in haar naam uitgegeven digitale certificaten)	• Systeem wordt niet meer vertrouwd
CA (Entiteit die bevoegd is om, namens de Root CA, operationele digitale certificaten uit te geven alsook die certificaten verifieert)	• Systeem is niet meer vertrouwd
	• CA kan publieke of private partij zijn
Misbehavior Authority (Entiteit die de geldigheid van digitale certificaten voortijd intrekt, daarvan een centrale lijst bijhoudt en distribueert).	• Misbruik van gestolen of verloren certificaten; verlies van vertrouwen
	• Identiteitsfraude
	• Authorisatiefraude

Rollen m.b.t. certificering

Rol:	**WAT ALS deze rol er NIET zou zijn of zou falen?**
Compliance assessment governing body (Entiteit die de security eisen van C-ITS stations bepaalt en de processen hoe conformiteit aan die eisen wordt vastgesteld)	• Onbetrouwbare kastjes, geen vertrouwen, geen C-ITS
	• Elke partij kan deelnemen
	• Alleen vooraf (typegoedkeuring) of ook tijdens life cycle (APK)?
	• Alleen voor C-ITS functies en niet voor iets anders?
Compliance assessment lab	• Zelfcertificering (niet gewenst)
(Entiteit die de conformiteit van C-ITS stations aan security eisen onderzoekt en vaststelt)	• Geen systeemintegriteit
	• Onbetrouwbaar C-ITS station kan niet worden verwijderd
Operations/ Monitoring (Entiteit die zicht houdt op het operationele functioneren van het C-ITS netwerk en alle actieve C-ITS stations)	• Geen controle van de frequentie-bezetting
	• Geen zicht op zwakke plekken in het systeem
	• Geen controle op systeemniveau
	• Geen signalering van hacking
Onderhoudsbedrijf (Entiteit die het V-ITS station periodiek of af hoc onderhoudt, test en inspecteert, bijv. op beschadiging van het beveiligingszegel)	• Geen integriteitscontrole tijdens gebruik; vertrouwensbreuk
	• Geen herstel van defecten, geen preventie
	• V-ITS station moet "voor het leven" worden ontworpen
	• Vragen: frequentie, hoe (fysiek, software over the air), wie ?
Migratiebedrijf (Entiteit die security veranderingen uitvoert of doorvoert in het V-ITS station)	• Inoperationeel station kan niet teruggezet worden naar operationeel
	• Geen crypto update
	• Geen firmware update (na veroudering)
	• Identiteit kan niet wisselen
	• Beperkte levensduur, levensduur

	telecom-protocol is korter dan van voertuig
Hacker (nieuwe rol: white hat hacker)	
Meldpunt vulnerabilities (nieuwe rol)	

Issues m.b.t. Privacy en Authorisaties

	Vragen:
<u>Privacy</u>	
Automobilist (eigenaar, berijder)	• Mag ik kastje uitschakelen?
	• Mag ik kastje omzeilen (door GPS onklaar te maken)?
	• Heb ik inspraak in WIE de informatie mag gebruiken? (verzekeringen, commercieel)?
Uitgifte korte termijn certificaten	• Business model. Wie betaalt?
	• Is privacy een recht of plicht?
	• Hoe veel? Hoe vaak? Hergebruik?
	• Is er keuze voor de automobilist, berijder?
Korte/ Lange termijn certificaten-koppeling	• Wie bepaalt wie de ID-koppeling van een pseudo-certificaat mag maken? Is een rood licht-overtreding al genoeg, of is het beperkt tot een misdrijf?

Overige geparkeerde issues

	Toelichting:
<u>Over de Scope van de workshop</u>	
• Wegkantsystemen (R-ITS stations)	Workshop focus is op V-ITS stations (voertuigen)
• After market	Belangrijk voor de snelheid van de introductie van C-ITS
• Motorfietsen	
• Business case manager	Wie kijkt er naar een goede business case, ook voor security?
• Marketing naar consumenten	
• Wetgever	
• Aansprakelijkheid	Hoe om te gaan met aansprakelijkheid?
• Verzekeraar	Wat wordt de rol van de verzekeraars?
<u>Inhoudelijk</u>	
• Prioritering van berichten	Prioriteit van verwerking berichten is van direct belang voor de verkeersveiligheid
• Intrekken van authorisaties	Kan een enkele authorisatie worden ingetrokken zonder intrekking van het LTC (long term certificate)?
• Nationale uitzondering op UN/EU regelgeving?	
• Gesloten of open systeem?	Wordt C-ITS een gesloten systeem of open voor andere toepassingen, zowel wat betreft het gebruik van het radiofrequentie-spectrum als voor additionele (ITS) toepassingen?

Conclusies

Voorop zal moeten staan de borging van het vertrouwen in het systeem enerzijds en de betaalbaarheid anderzijds. In de workshop was er gerede twijfel over de business case van de voorgestelde vertrouwensinfrastructuur. Zowel vertrouwen als betaalbaarheid zijn noodzakelijk om C-ITS op substantiële schaal te introduceren.

Enkele invalshoeken om stappen te zetten die voor een doorbraak kunnen zorgen voor het aspect betaalbaarheid (business case):

1. Waar gaat de automobilist voor betalen? Voor welke use case? Wordt dit een doorbraak vanuit de autonome klantvraag (de markt)? Of is er wetgeving nodig, bijv. van de EC?
2. Kun je met minder security toe, bijv. minder certificaten? Hoe kun je meer risico-gebaseerde benadering toepassen, met focus op de risico's van een leidende use case?
3. Welke alternatieven zijn er voor trusted information op basis van C-ITS en PKI? Kijk naar de totale use case (functionaliteit) en betrek de alternatieve beschikbare informatie bronnen (connected, sensoren). Vele use cases zullen meerdere databronnen gebruiken (hybride).
4. Welke integratie is er mogelijk met andere in-car toepassingen met hoge eisen aan security en/of connectivity? Denk aan EDR, e-Call, OEM-toepassingen.
5. Wordt C-ITS een open of gesloten systeem? Kunnen marktpartijen (verzekeraars, startups, etc) toepassingen ontwikkelen die gebruik maken van de C-ITS infrastructuur (radiofrequentie, C-ITS stations)?

Dit zijn enkele principiële punten waar een sterke visie op nodig is en die kansen bieden voor een gezonde business case. Vanuit security perspectief dienen in deze fase ook de volgende vragen te worden beantwoord.

6. Van wie is de C-ITS infrastructuur? Wie wordt eigenaar en heeft het voor het zeggen? OEM's, de automobilist/voertuigeigenaar, wegbeheerder, telecom provider, service of technology provider?
7. Wie draagt het risico van verlies van vertrouwen in het C-ITS systeem of een specifieke ITS-toepassing (use case)?

Een gedegen visie op bovenstaande punten is noodzakelijk voordat bepaalde rollen in de vertrouwensinfrastructuur worden ingevuld.