Verslag Workshop Authenticatie en Autorisatie in de ketens van Talking Traffic

Donderdag 16 november 2017

Tijdstip: 15.30 – 17.15 uur
Locatie: Talking Traffic, Postiljon Bunnik

GJA
WWW.DITCM.EU
16 NOVEMBER 2017

Beter Benutten

Verslag Workshop Authenticatie en Autorisatie in de ketens van Talking Traffic

Deelnemers

• Vincent Habers	I&M/ Talking Traffic
• Eric Koenders	Dynniq
• Eddy Verhoeven	Siemens
• Twan Hamelynck	KPN
• Inge de Meulenaere	Ericsson
• Gilles Ampt	Security Community Smart Mobility S&P

Bevindingen functionele behoeftes van prioriteit aanvragen bij IVRI

Vloot

- OV-lijnbussen/ trams
- Hulp- en nooddiensten (zwaailichten)
- Vrachtwagens (met zware of gevaarlijke lading)

Security aspecten van de berichtketen voor iVRI - prioriteitsaanvragen

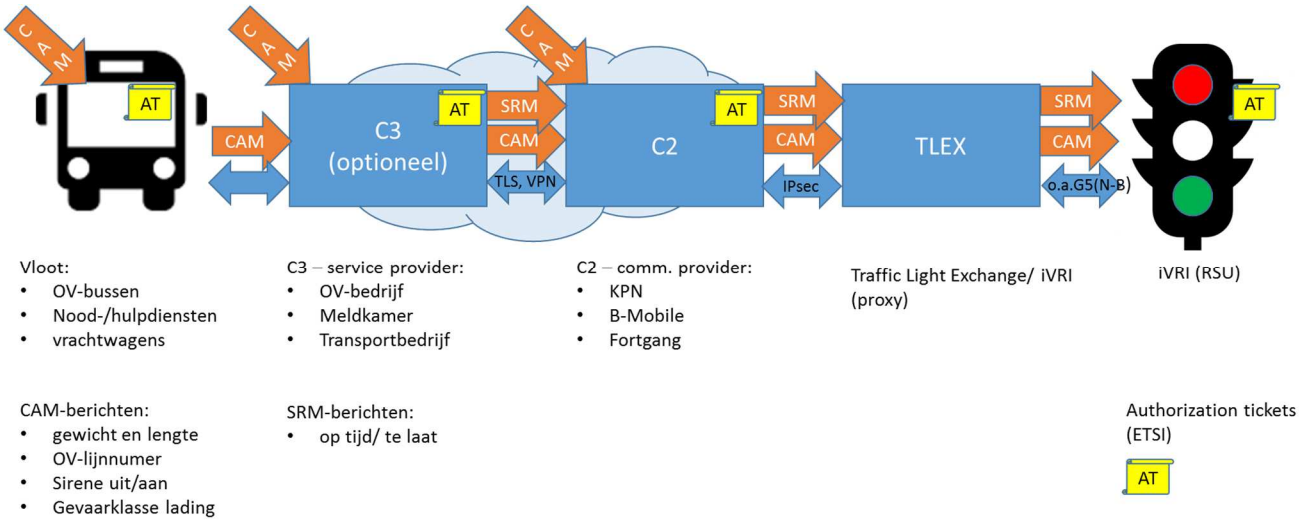
- authenticatie en autorisatie t.b.v. prioriteitsaanvragen vanwege het inherente risico van misbruik van onechte identiteiten, onechte autorisaties dan wel onechte omstandigheden (bussen of vrachtwagens die blijken leeg te rijden of zwaailichten die inactief zijn).
- voorrangsregels en acceptatieregels voor prioriteitsaanvragen zijn de bevoegdheid van elke individuele wegbeheerder (is onderdeel van lokaal verkeersbeleid).
- confidentialiteit, integriteit en beschikbaarheid – geen specifieke eisen besproken.

Berichtenstructuur

- via CAM- en SRM-berichtenstructuur (conform ETSI-ITS) t.b.v. prioriteitsaanvraag bij iVRI
- identiteit van de entiteit die CAM en SRM ondertekent is afhankelijk van welke entiteit deze berichttypes in de keten initieert.

Koppelvlakken in de keten

Tijdens de sessie is het volgende overzicht gemaakt van de koppelvlakken tussen de clusters en de endpoints van de iVRI-keten.



Figuur- koppelvlakken in de iVRI-keten.

De rollen van cluster 2 en cluster 3-consortia zullen soms worden uitgevoerd door één enkel consortium; dit is afhankelijk van het betreffende consortium.

Technisch gesproken wordt het merendeel van de koppelvlakken (interfaces) gerealiseerd met algemene datacommunicatiestandaarden met security eigenschappen, zoals TLS, VPN en IPSec, danwel proprietary koppelvlakken van service providers.

Alle voertuigen maken gebruik van cellulaire netwerken dan wel andere mobiele communicatienetwerken. De iVRI-installaties zullen allemaal voorzien worden van connectiviteit met het cellulaire netwerk. ETSI G5 (wifi-P) wordt binnen Talking Traffic niet gebruikt.

Het initiëren van CAM-berichten in de keten kan op drie plaatsen geschieden en is een implementatiekeuze van de service provider(s). CAM kan geïnitieerd worden in het voertuig, cluster 3 service provider of cluster 2 communicatie service provider. De eerste optie is zoals de gebruikte ETSI standaard is bedoeld; in de andere twee opties is er een loskoppeling van de identiteit van de ondertekenaar van het bericht (t.w. een service provider) en het voertuig. Deze afwijking van de ETSI-standaard kan mogelijke gevolgen hebben (in de toekomst) voor schakels verderop in de keten, i.h.b. de iVRI. Actiepunt is dat Gilles Ampt en Eric Koenders nader naar de mogelijke impact gaan kijken en beoordelen of het nodig, wenselijk en haalbaar is om de ETSI-standaard hierop aan te passen.

Gebruik van PKI en certificaten

Voor de ondertekening van de CAM-berichten en SRM gaan PKI-certificaten conform ETSI-ITS worden gebruikt. Het gebruik van de ETSI-standaard is losgekoppeld van de gebruikte communicatie-technologie.

Het is nog onduidelijk wat de root of trust moet gaan zijn voor iVRI in Nederland en hoe internationale aansluiting gaat worden verkregen. Gilles licht kort toe dat de EC voor het realiseren van deze interoperabiliteit nu de noodzakelijke initiatieven neemt. Resultaten hiervan zullen niet voor 2019 beschikbaar zijn. Het is hier onbekend hoe Volkswagen vanaf 2019 wil gaan voorzien in ITS-certificaten als zij C-ITS-diensten gaan lanceren.

De ITS-PKI die in Nederland gaat worden ingericht voor de InterCOR testFest in Frankrijk en beschikbaar komt voor april 2018 zal gebruikt gaan worden door andere Nederlandse testprojecten en pilots. Waar Talking Traffic/ iVRI behoefte aan heeft is een produktie-PKI met continuïteit van dienstverlening.

Desgevraagd wordt er gesproken over mogelijke alternatieven voor PKI en certificaten, zoals blockchain. Gilles licht toe dat voor ITS hiervoor internationaal nog helemaal geen ontwikkelingen lopen en om die reden op afzienbare termijn niet opportuun is. Er kan desgewenst onderzoek worden uitgezet naar de mogelijke geschiktheid en toepassing van blockchain in ITS, maar dat vraagt een andere horizon.

Tijdspad

De eerste certificaten voor iVRI zullen nodig zijn begin 2018. Hier kunnen de ”InterCOR” PKI in Nederland en evenmin de EC PKI niet in voorzien.

Siemens voorziet om zelf een CA te gaan inrichten om op kleine schaal certificaten te gaan uitgeven t.b.v. iVRI. Gilles vindt het raadzaam de geldigheid van de eerste certificaten te beperken zodat er later kan worden overgestapt op nieuwe certificaten die internationale aansluiting vinden.

Acties

- Impact onderzoek van Service providers die CAM-berichten namens een voertuig ondertekenen binnen de ETSI standaard – korte termijn – Gilles Ampt en Eric Koenders.
- Aansluiting bij EU-PKI voor ITS te heroverwegen als er meer zekerheid is over de tijdslijn van de EU, en de aansluiting van Nederland hierop voor voertuigen en wegbeheerders meer vorm krijgt – medio 2018 – n.t.b.