

Smart Mobility community

Projectenoverleg Security

Gilles Ampt en Marcel Otto

Utrecht - 9 maart 2018



Agenda

- C-ITS platform en WG Security – resultaten en toekomst
- C-Roads en TF1 (Security) – stand van zaken
- ETSI WG ITS en WG5 Security – prioriteiten standaardisatie
- Security uitdagingen in ITS voor Nederland – wat te doen?

C-ITS platform (tot september 2017)



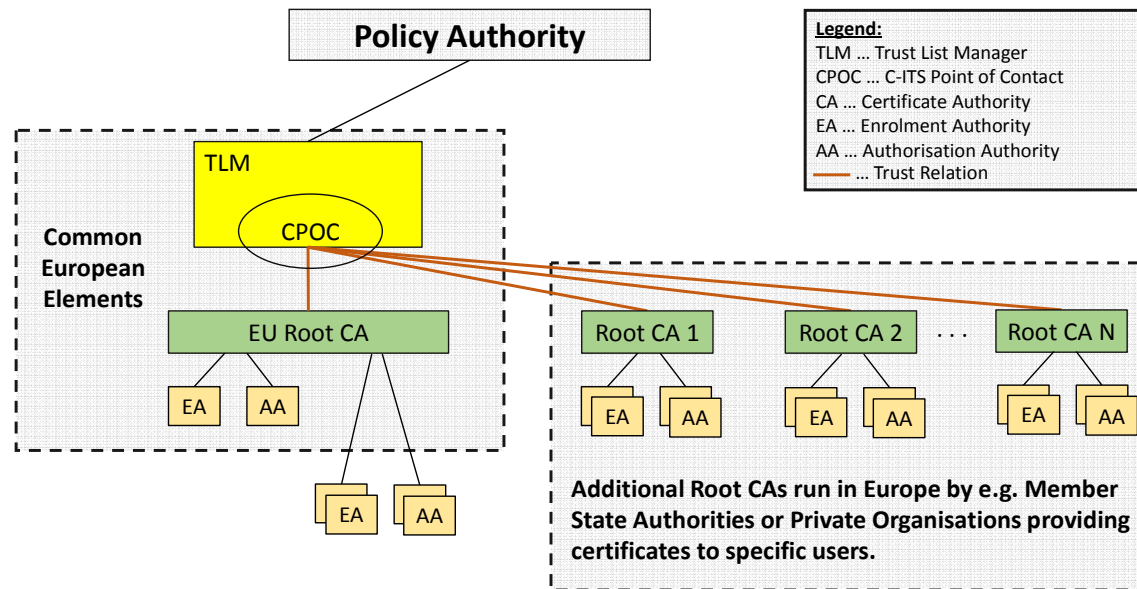
- Initiatief EC DG MOVE om invoering C-ITS te versnellen (publiek/ privaat)
- Diverse deliverables w.o. die van WG Security (2 policies in 2017)
- WG Security zal waarschijnlijk doorgaan als expert stakeholder-groep:
 - Updates van policies (minimaal 1x per 3 jaar)
 - Klankbord voor ontwikkeling van centrale EC Trust services v.a. 2018
- Actieve vertegenwoordigingen in WG Security van:
 - Wegbeheerders/ lidstaten: D (BAST, BSI), F (Scoop), A, NL, B, UK, S
 - OEM's: Renault, VW, Opel, Volvo, C2C-CC
 - Industrie: Kapsch, NXP, Gemalto, ENX, IBM, Bosch
 - EC: DG MOVE (voorzitter), JRC

EU Certificate Policy/ Security Policy Highlights

- Releases 1.0 gepubliceerd juni 2017 resp. december 2017
- PKI-interoperabiliteit binnen EU (publiek/ privaat)
 - Centrale trust services
 - Selectie van ETSI standaards
- Security certificering voor C-ITS stations
 - Internationale erkenning van certificeringen (SOG-IS/ Common criteria)
 - Crypto agility (selectie van ECC algoritmes)
- Governance bodies (volledige governance reikwijdte)
- Privacy/ Data protectie
 - Aanbevelingen (gebruik van pseudoniemen, bewaartermijnen data)
- Tijdslijn voor invoering
 - Onderscheid tussen pre-deployment en deployment



Centrale Trust Services voor C-ITS (PKI)



EC investeert in unieke TLM/ CPOC plus een EU Root CA van 2018 - 2021

https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf



C-Roads / Governance



- EU co-funded project van 16 lidstaten tot eind 2020
 - MoU met C2C-CC
- Hét EU platform voor pre- & early deployment van C-ITS en Hybride ITS
- Taskforce Security (WG2/ TF1)
 - Implementatie-feedback op C-ITS security standaards en policies
 - Interoperabiliteit van security-maatregelen t.b.v. hybride ITS
 - Groeipad van pre-deployment naar deployment
 - Migratieplanning naar nieuwste ETSI-standaard (TS 103 079 v1.3.1)

ETSI work items standaardisatie ITS Security (2018)



- Uniformering EU met USA (IEEE C-ITS standaard) – afronding
 - Incompatibiliteit in ETSI-security standaard vanaf oktober 2017
- EU PKI Trust List/ Revocatie List – afronding
 - Opdracht van EC C-ITS platform
- Privacy effectiviteit (pseudonym change strategie) – studiefase
- Threats, Vulnerabilities & Risk assessment – update
- Misbehavior detection – startfase
- Distributieproces van certificaten – optimalisatie
- Crypto agility – afronding
 - Migratie-eis van EU certificate policy
- Testprotocol – update

Welke *overige* security randvoorwaarden voor ITS deployment staan open?

- Misbehavior detectie, misbehavior reporting en Handhaving
- Risico-gebaseerde revocatie-policy voor ITS stations
- Geldigheid van pseudoniemen (risico Sybil attack = identiteitsfraude)
- Uitkomst van Privacy impact analyse C-ITS
- Hybride security (i.h.b. autorisatie/ authenticatie op applicatie-niveau)
- Security updates van ITS stations (voor levensduur van > 3 jaar)
- Interoperabele autorisatie-structuur t.b.v. specifieke ITS services

- Opstellen Nederlandse baseline ITS Security i.s.m. stakeholders
- Vergelijken met minimum security-eisen van EU policies
- *Change request proces voor EU-certificate policy (en security policy) gaat binnenkort beginnen.*

Uitdagingen voor Nederland



- Fasering van ontwikkeling en uitrol van ITS infrastructuur
 - Toekomstvastheid en volledigheid van C-ITS specificaties
 - Migratie van Pre-deployment naar Deployment
 - Integratie van Hybride ITS en C-ITS
- Security certificering van ITS stations
 - Beschikbaarheid van Protection Profiles voor RSU's
 - BAST en BSI (D) gaan medio 2018 specificaties delen en publiceren
- Beschikbaarheid en governance van PKI services t.b.v. ITS
 - RSU-certificaten vs. Voertuig-certificaten
 - Opzet en beheer van ITS service permissions (SSP's)
- Aansluiting van alle publieke en private stakeholders en projecten bij de nationale en internationale beleids- en reviewprocessen
 - Organisatie van wisselwerking en synergie
 - Invulling van rollen, taken en bijdragen per ontwikkelfase

Procesvoorstel internationaal



- Hoe organiseren we ons structureel t.b.v. C-ITS platform, C-Roads, ETSI ?
 - Invloed op beleid en regelgeving
 - Reviews m.b.t. security standaarden en policies
 - Change requests m.b.t. security standaarden en policies
 - Rollen van DGMo, RWS (CIV), RDW.
 - Rol Agentschap Telecom (toezichthouder PKI).
 - Rol industrie: leveranciers projecten/services, security experts
- C-Roads TF1 meeting in Eindhoven (HQ HERE) op 27 maart 2018:
 - Presentatie hybride casus TT – bv. priority request public transport (TF2)



Smart Mobility community

Projectenoverleg Security

Gilles Ampt en Marcel Otto

Utrecht - 9 maart 2018

