Start landelijke tafel Security voor C-ITS diensten

Waar staan we nu en hoe verder?

Combining strenghts for future mobility

Need for security

- Showstopper for the trust of the public and politics in ITS
- Uncertain risks, counter-measures and responsibilities
- Need for sharing and developing expertise in this field
- Learning by doing with design, tests and procedures

Wat ligt nu op tafel?

1. Whitepaper Cyber Security & Privacy
2. Activiteitenplanning CM Security en Privacy
3. EU C-ITS Platform WG5 Security en Certification

Wat zijn ambities van Connecting Mobility?

1. Meer kennis en bewustzijn bij NL belanghebbenden over problemen en oplossingen op terrein van security bij C-ITS
2. Gecoördineerde en gedragen activiteiten vanuit NL partijen passend bij de ambities om koploper te zijn in ITS

Issues white paper

- Standaardisatie
  vooral V2X communicatie
- Security ‘by design’
  o.b.v. risico analyses
- Certificering en testen
  toepassingen
- Public Key Infrastructure
- Privacy eisen: o.a. zeggenschap over data en veiligheidsniveaus
- Analyseer gedrag van eindgebruikers

Identified barriers and solutions

	Barriers	Solutions
1	Lack of policies and organizations: no architecture for PKI with RCA for long term and short term certificates	Define them on level of nations, EU, UN accept more RCA's by cross-certification differentiated for infra and vehicles
2	Different requirements on use of algorithms, curves and key lengths	Start with ETSI standards , NIST curves and short keys. Prepare for transitition with crypto agility for life time vehicles
3	Unclear validation or revocation, duration and storage of keys	Use protection profiles from common criteria portal with an automatic deactivation after misuse in short time

Issues WG5 C-ITS Platform

- Trust models based on PKI/RCA
  (9 modellen met 20 criteria)
- Testing conformance, certificication and type approval
- Revocation of trust:
  - passive: wait for expiration offender
  - active: warning potential victims
  - deactivate the offender
- Cryptography: agility and curves
- Interoperability and interfaces
  (with USA and others)

Planned activities in NL

- Matching projects and measures in time based on use cases
- Supporting risk-assessment: methodology, suppliers and practice with use cases
- Guidelines with practical examples for developers and buyers
- Portal and helpdesk for sharing knowledge and communication
- Creating and up-dating research agenda for the long-term