Rijkswaterstaat
Ministerie van Infrastructuur en Milieu

De Ontwikkeling van een EU PKI systeem voor V2X communicatie

- Vertrouwd en Veilig -

25 september 2015

G. Lamaitre
RWS Security Centre

RWS Ongeclassificeerd

European Commission

C-ITS Platform

Workgroup 5: Security & Certification

Cooperative ITS Corridor
Joint deployment

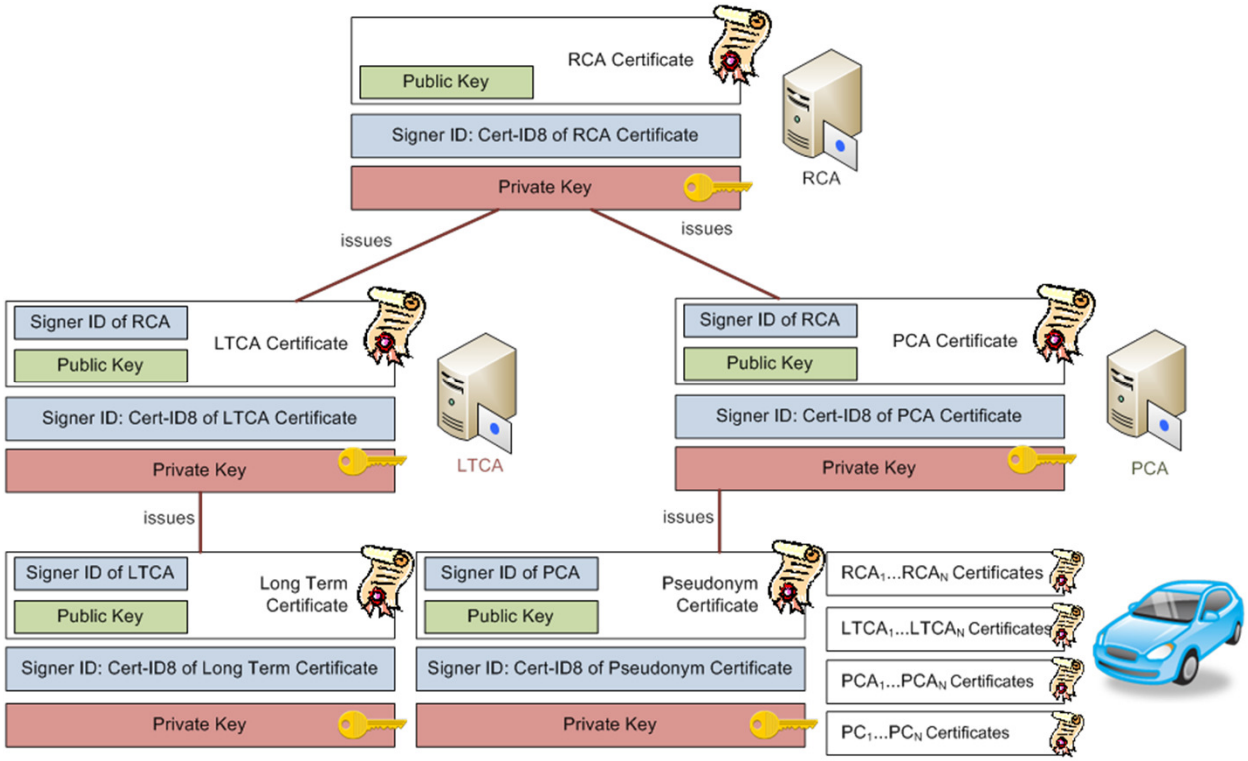
Doelen van C-ITS en de rol van Security

- Waarvoor dient C-ITS Infrastructuur?
  - communicatie tussen voertuigen, andere voertuigen en wegverkeersinfrastructuur (het technische antwoord)
- Met welk doel?
  - Het ondersteunen van nieuwe toepassingen voor:
    - Het verbeteren van de verkeersveiligheid
    - Het verbeteren van het efficiënt gebruik van de weg
    - Het vergroten van het comfort van de weggebruikers
- Waarom security belangrijk?
  - Het verkeersveiligheidsaspect resulteert in hoge security eisen
  - Veel samenwerkende organisaties: veilige uitwisseling van data in een vertrouwde omgeving

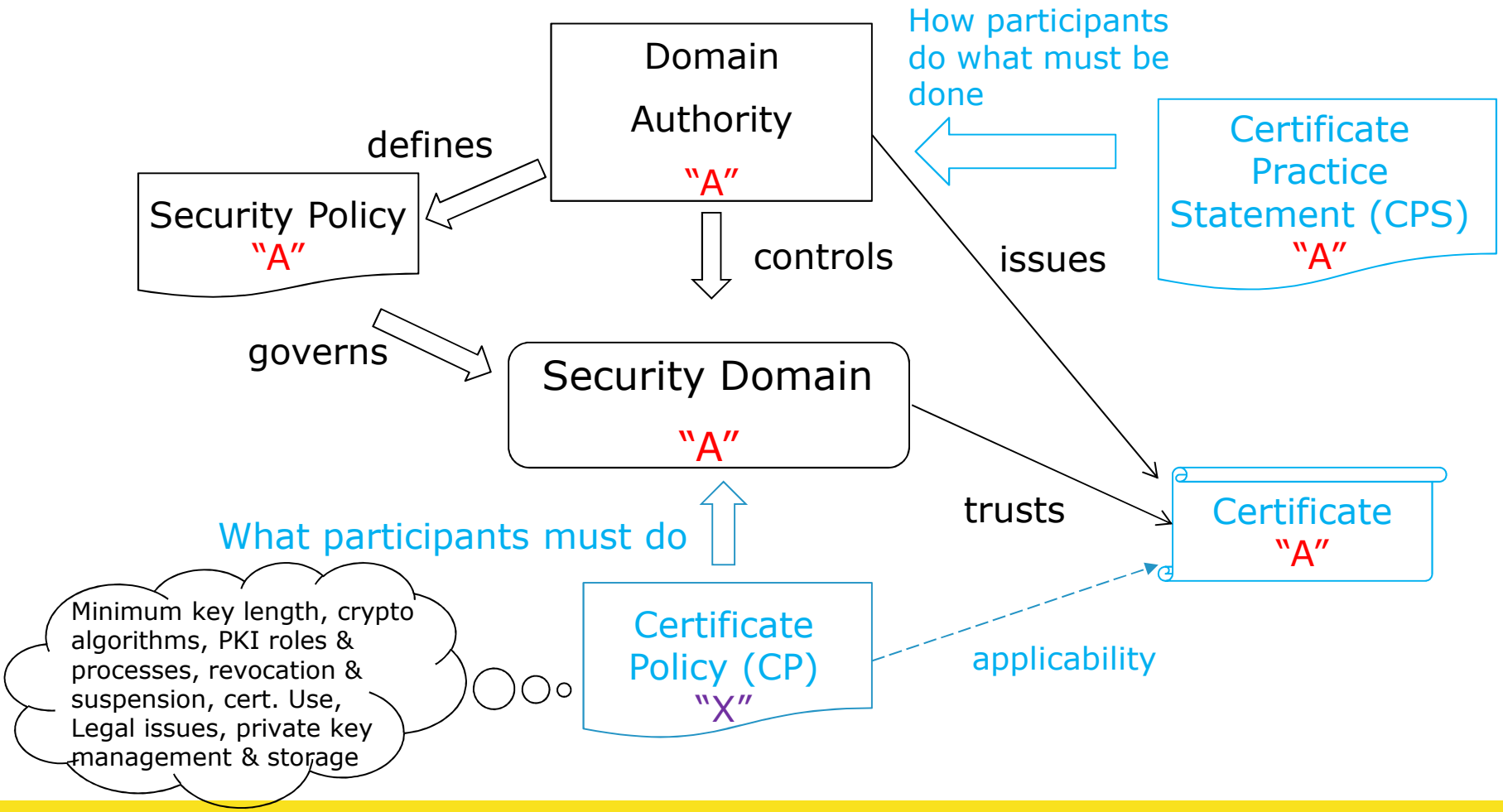
Vertrouwde omgeving – het C-ITS Trust model

- EU-wide Trust model voor alle Europese lidstaten
- Implementeren door middel van:
  C-ITS Credential Management System (EU CCMS)
- Onderdelen van een EU CCMS:
  - Public Key Cryptografisch systeem met bijbehorende Public Key Infrastructure (PKI) als key management omgeving
  - PKI policy
  - PKI organisatie structuren
  - PKI processen

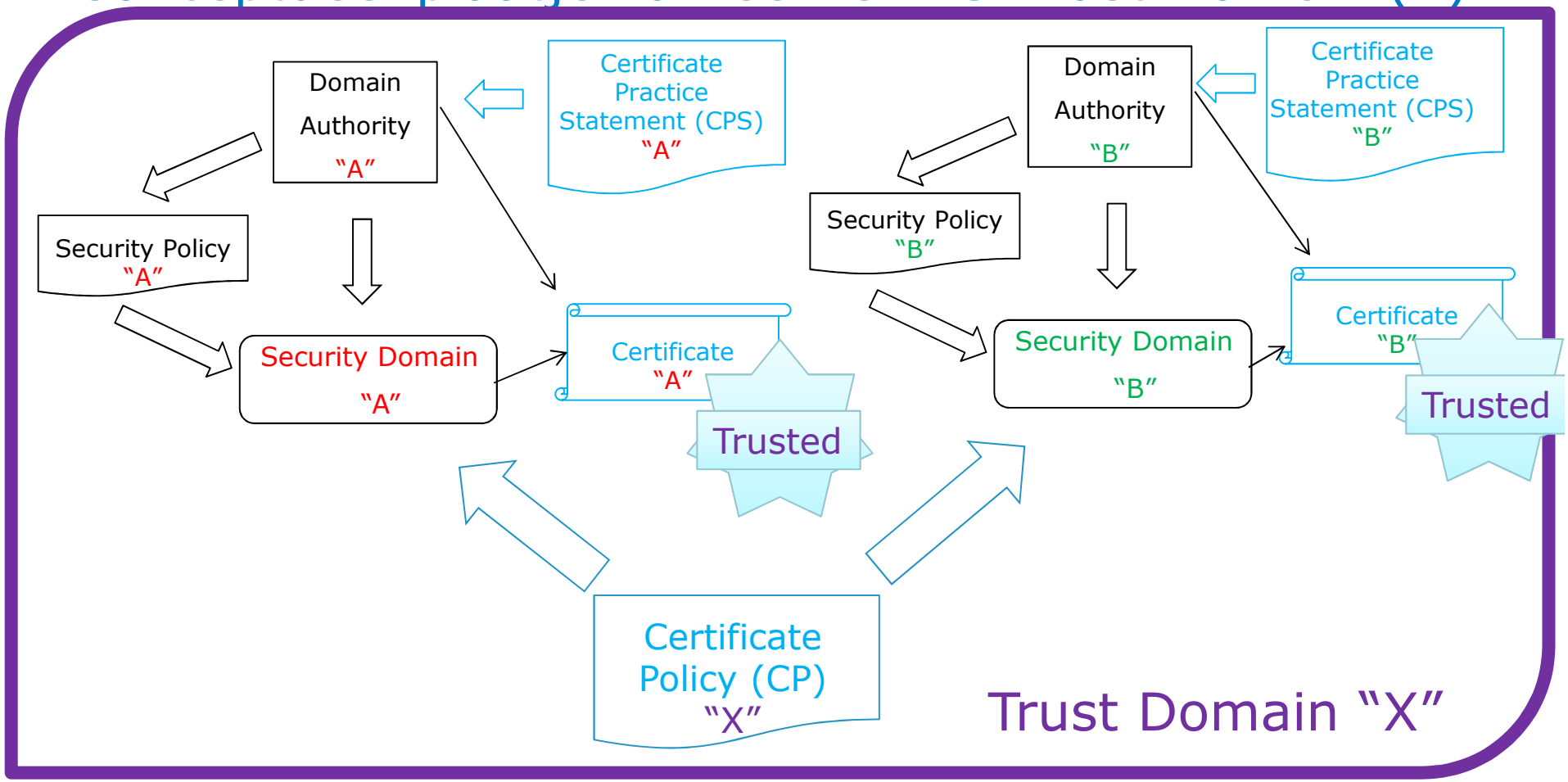
Voorbeeld: Car2X PKI architectuur



Conceptueel plaatje van een C-ITS Trust Domein (1)



Conceptueel plaatje van een C-ITS Trust Domein (2)



“Extending Trust” tussen “Authorities”

- Eindgebruikers van een PKI in staat stellen om certificaten van en andere PKI te vertrouwen.
- Methode: Cross-certification (een CA certificeert een andere CA en eventueel vice versa)
- Binnen een Trust Domain: Intra-domain cross-certification
- Tussen gescheiden Trust Domains: Inter-domain cross-certification

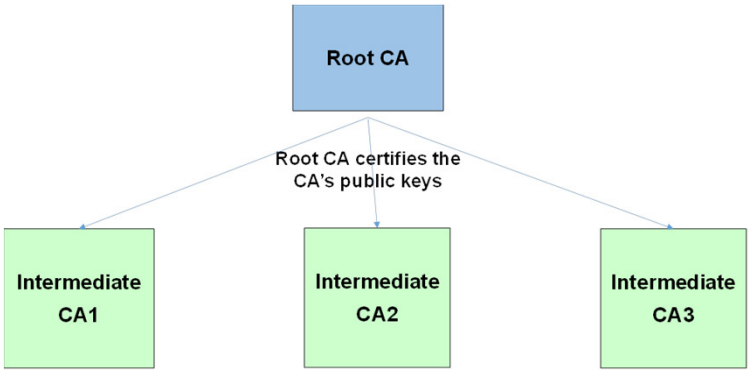
Welke modellen om uit te kiezen?

	Eén Root CA	Meer dan een Root CA
Één Domein	* Hierarchisch trust model **(optie 1)** *-> 1 security policy en 1 CP*	* Federation of Root CA's **(optie 2a)** * Bridge CA **(optie 2b)** * Certificate Trust List (CTL) **(optie 2c)** *-> 1 CP, geharmoniseerde security policies*
Meer dan een domein	-	* Federation of Root CA's **(optie 3a)** * Bridge CA **(optie 3b)** * Certificate Trust List (CTL) **(optie 3c)** *-> geharmoniseerde CP's (ook algorithmen en certificate formats van de anderen ondersteunen), verschillende security policies*

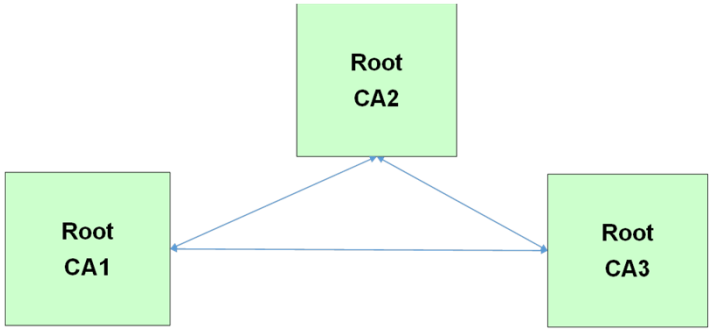
Niet geschikt voor C-ITS:

- Delegate CA **(optie 4)**
- Web of Trust (PGP) model **(optie 5)**

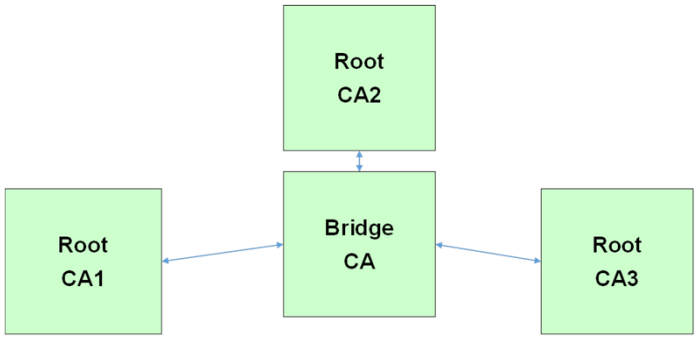
PKI topologiën



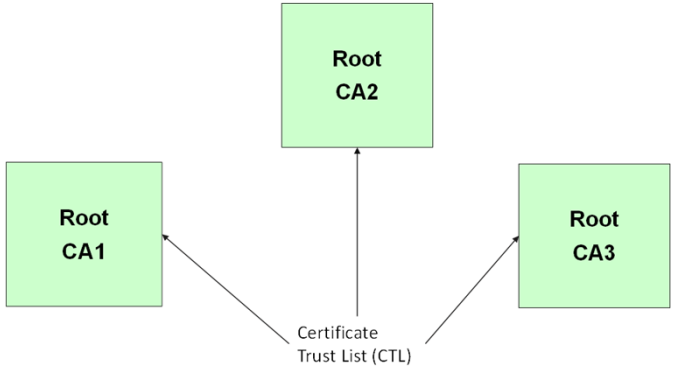
1. Hierarchisch



2/3 a. Federation



2/3 b. Bridge CA



2/3 c. CTL

Aanbevelingen van Werkgroup 5

- Deploy one common trust model for whole EU
  - Day One:
    - single trust domain (let op ≠ one single Root CA)
    - Certificate Trust List (optie 2c)
  - Toekomst:
    - multiple interoperable trust domains
    - CTL in multi-domains (optie 3c) *of* Bridge CA in multi-domains (optie 3b)
- Aanpassen legislative and regulatory framework
- Opzetten onafhankelijke governance structuur
- Financiering
- C-ITS Compliance assessment (C-ITS station certification and testing)
- Uitwerken Privacy requirements op basis van output van Werkgroup4

Einde

- Vragen?

Geplande oplevering advies Werkgroep 5 is januari 2016