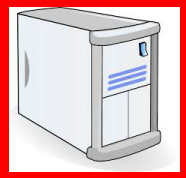
A58 Security implementatie

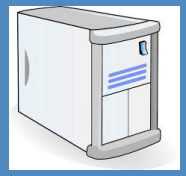
Door P. Goossens, 23 november 2015

een VolkerWessels onderneming

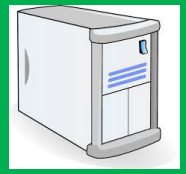
Data

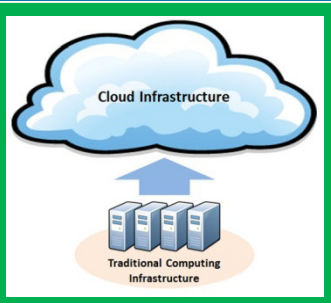


Dienst



Coöperatieve applicatie hosting





Voorbeeld: PCP A58 “Spookfile” project

- Security geagendeerd

- Werkgroep security samengesteld
  - > Security specialisten
  - > Opdrachtgevers
  - > Jurist
  - > Vertegenwoordigers vanuit de 3 percelen

Proces in de PCP A58

Digitaal certificaat

Encryptie -> inhoud niet leesbaar

Digitaal onderteken -> bron authenticatie

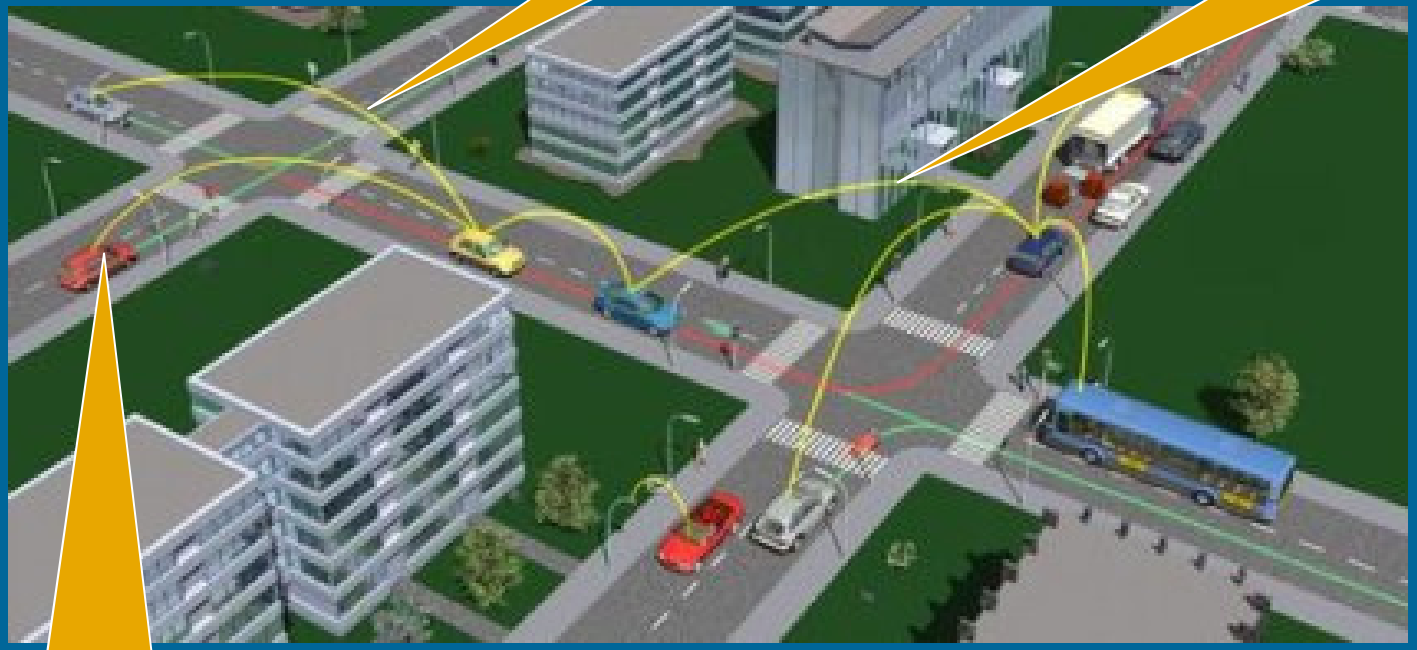
Digitaal onderteken is niet hetzelfde als encryptie

Begripsvorming

Veiligheidstoepassingen
- CAM en DENM berichten

Encryptie?

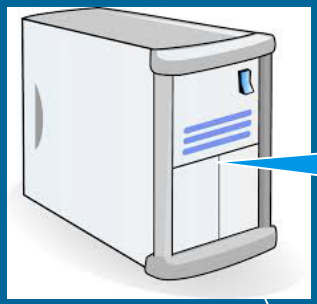
Integriteit?



Bron Authenticatie?

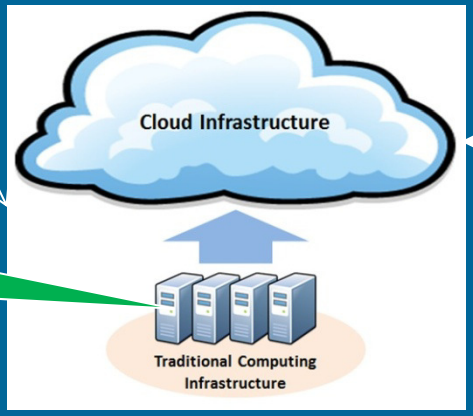
Privacy concerns?

Security is een container begrip



P2 server verstuurt snelheidsadvies

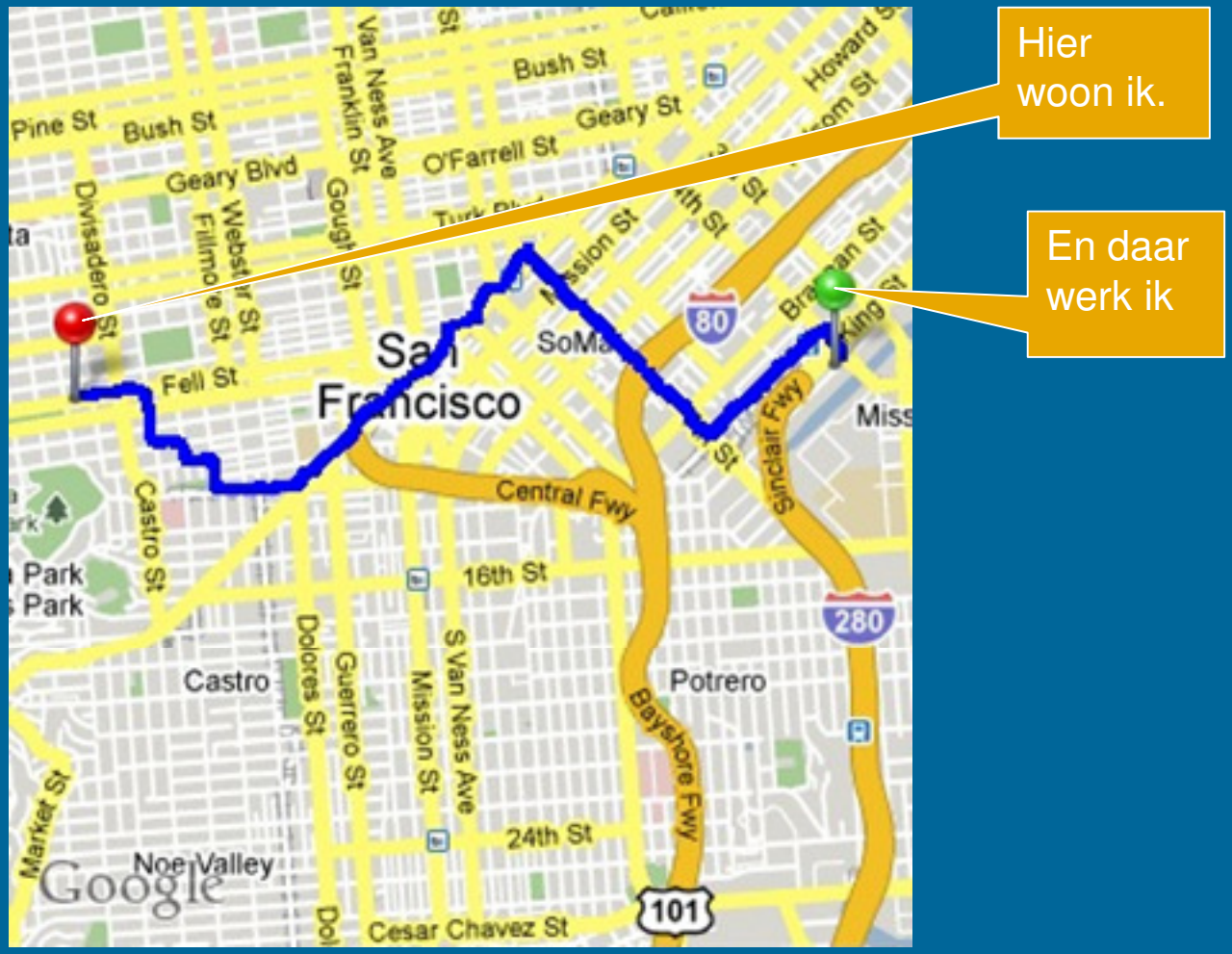
Cooperatief bericht met snelheisadvies



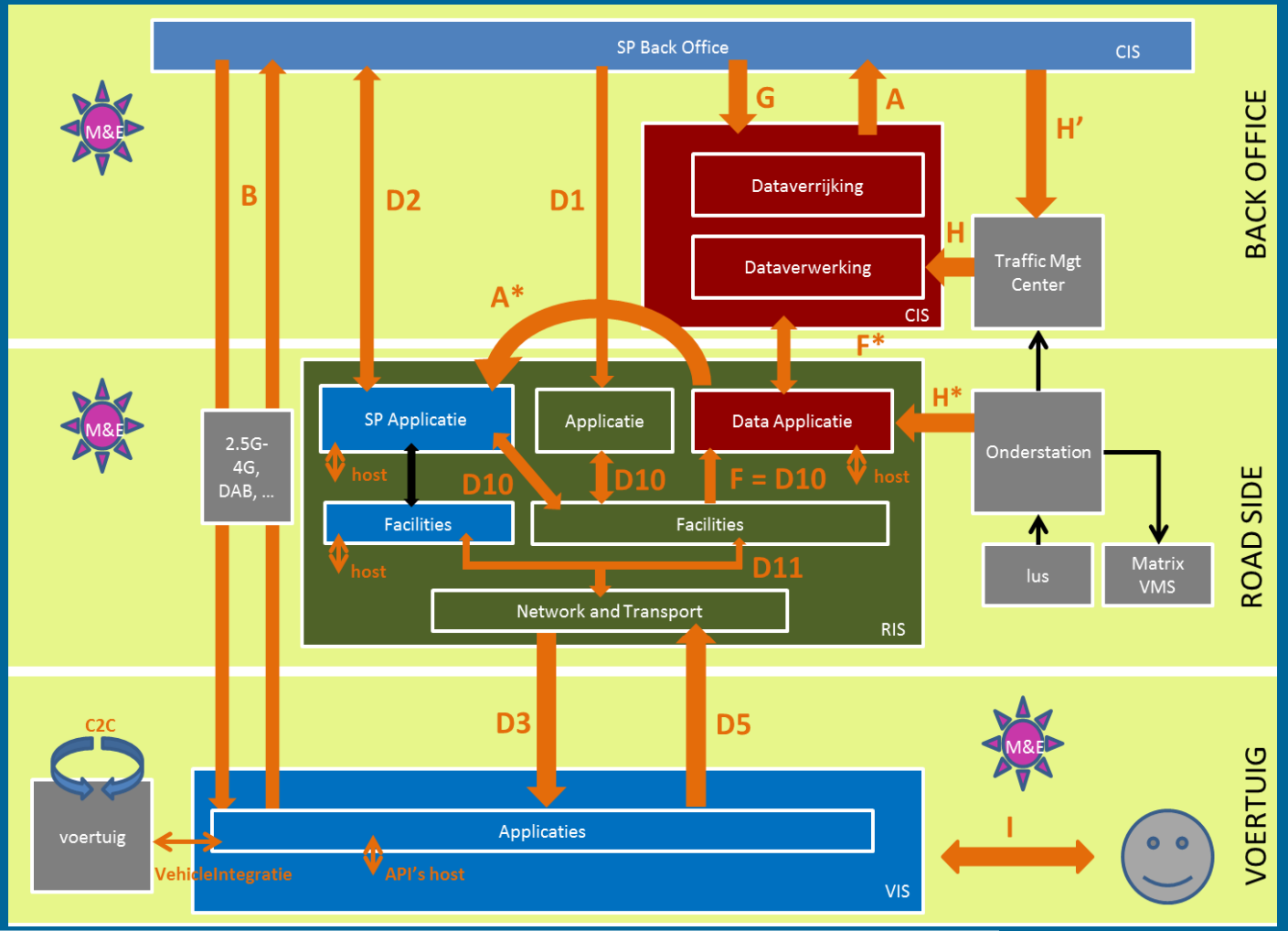
P3 RIS applicatie server verstuurt snelheidsadvies

Security beschouwen in de gehele keten

- Trace + kaart = privacy issue
- Kaarten zijn vrij beschikbaar
- Trace = privacy issue
- Maatregelen
  - > Kop en staart afknippen
  - > ID's wisselen

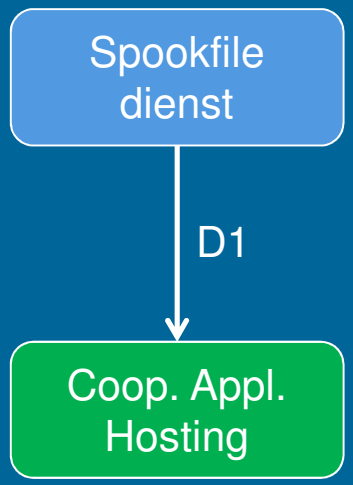


Begripsvorming omtrent Privacy en traces



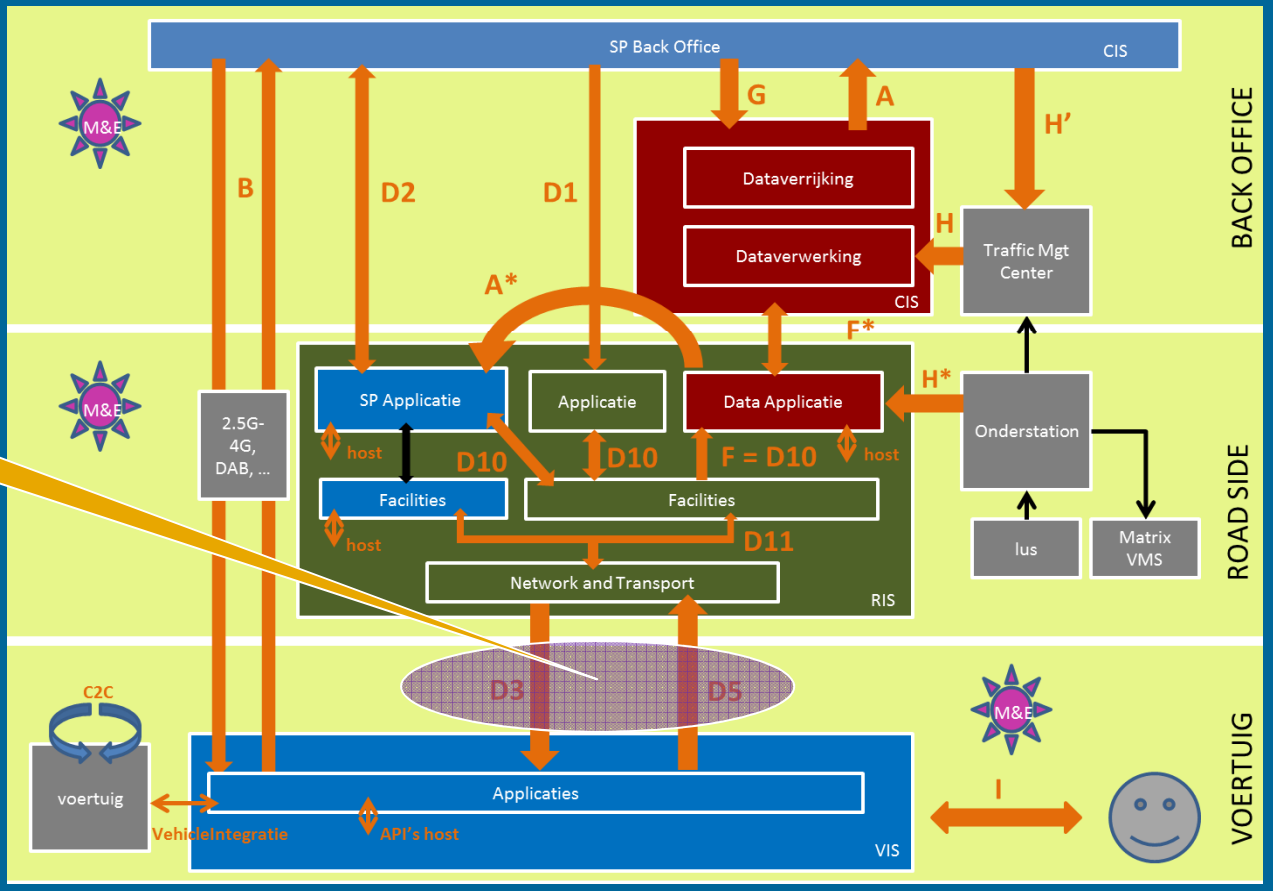
High Level Architecture

- Interface D1 **Advies**
  - > Bedreigingen
    - Manipulatie adviezen
    - Injecteren niet valide adviezen
    - Misbruik interface om roadside te hacken.
  - > Data eigenschappen op de interface
    - **Geen vertrouwelijkheid**
    - **Authenticiteit**
    - **Integriteit**
    - In de mindere mate: authorisatie
  - > Maatregelen
    - Server en client side authenticatie op basis van HTTPS



	Data eigenschappen					Data context		Risico analyse en beheersing		
Id	Type Data	Vertrouwe-lijkheid	Verificatie (authenticatie)	Integriteit	Toegang (autorisatie)	Percelen	Netwerk type	Bedreigingen/Kwetsbaarheden	Voorstel technische maatregelen	Organisatorische beheersmaatregelen
A	Verkeersdata, inclusief microdata	**	**	**	*	P1-P2	webservice o.b.v. http over publiek internet	Ongeoorloofd meeluisteren naar privay gevoelige gegevens Manipulatie verkeersdata Ongeoorloofd gebruik dienst	1. Server side HTTPS + API key voor client authenticatie.2. Gebruik maken van wisselende ID's. 3. Knippen kop en staart van ID traces.	Gecontroleerde uitgifte van API-KEYs.
A*	Verkeersdata, inclusief microdata.	**	**	**	*	P1-P2	Lokaal netwerk	Ongeoorloofd meeluisteren naar privacy gevoelige gegevens Manipulatie verkeersdata Ongeoorloofd gebruik dienst SP Applicatie kan potentieel verkeersdata lekken via D2 naar backoffice.	1. Lokaal netwerk afschermen 2. Interface uitrusten met vorm van authorisatie, middels een API-KEY	Beheerste ICT omgeving SP Applicatie kan potentieel verkeersdata lekken via D2 naar backoffice. Hier moeten afspraken over gemaakt worden.
G	FCD	**	**	**	*	P1-P2	webservice o.b.v. http over publiek internet	Ongeoorloofd meeluisteren naar privacy gevoelige gegevens. Manipulatie FCD Ongeoorloofd gebruik dienst	1 Server side HTTPS + API key voor client authenticatie 2. Gebruik maken van wisselende ID's. 3. Knippen kop en staart van ID traces.	
H	- Verkeersdata; macrodata zonder identifiers - beeldstanden		*	**		P1-RWS	Publiek internet	Ongeoorloofde besturing matrix VMS Manipulatie verkeersdata/ beeldstanden	Koppelvlak H zijn koppelvlakken die reeds geïmplementeerd zijn door bijv NDW, RWS hier kunnen wij dus geen eisen over opstellen	De oplossing voor de uitstaande SOW's zijn nog niet afgerond. Afhankelijk hiervan moeten hiervan nog een analyse maken.
H'	Adviezen, 'ter informatie' aan de wegverkeersleiders		*	*		P2-RWS	Publiek internet	Injecteren niet valide adviezen om daarmee RWS op het verkeerde been te zetten	2: Server side HTTPS + API key voor client authenticatie	
H*	Lusdata en beeldstanden		*	**		P3	Glasvezelnetwerk langs tracé tot in RSU appl. Server	Manipulatie lusdata en beeldstanden	Gesloten netwerk creëren door P3 partij i.s.m. RWS (fysieke maatregelen en ICT maatregelen zoals plaatsen firewalls).	Uitgangspunt: er is geen fysieke koppeling met het VIC-net.
F*	Verkeersdata, inclusief microdata	**	**	**	*	P1-P3	Publiek internet	Ongeoorloofd meeluisteren naar privacy gevoelige informatie Manipulatie verkeersdata Misbruik interface om roadside te hacken	VPN tunnel vanwege: - Volledige afscherming van het Internet - Bieden van mogelijkheid aan P1 partij om zelf andere (beheer) protocollen toe te kunnen passen.	Opmerking: het doorgeven van mircrodata over deze interface is een zwak punt vanuit privacy oogpunt. Beter is (privacy by design) alleen macrodata door te geven.
D1	Advies		**	**	*	P2-P3	Publiek internet	Manipulatie adviezen Injecteren niet valide adviezen Kans op vermenging adviezen van verschillende service providers Misbruik interface om roadside te hacken	Server en client side authenticatie op basis van HTTPS	
D2	Onbekend, is afhankelijk van oplossing service provider	*	**	**	*	P2-P3	Publiek internet	Misbruik interface om roadside te hacken	VPN tunnel vanwege: - End-to-end beveiligd kanaal (data layer) - Bieden van mogelijkheid aan P1 partij om zelf andere (beheer) protocollen toe te kunnen passen.	Afhankelijk van de uitvoering van het interface is er sprake van een risico op lekken van privacy gevoelige micro-data. Dit moet getoetst worden.
B	Persoonlijke FCD / adviezen	***	**	**	*	P2	Telecomprovider netwerk; G3,G4	Ongeoorloofd meeluisteren naar privacy gevoelige informatie Manipulatie adviezen Ongeoorloofd gebruik dienst	HTTPS aan server side. Username/password authenticatie aan client side Gebruik maken van wisselende ID's. Knippen kop en staart van ID traces.	
D10	FCD / adviezen	**	**	*	*	P1-P2-P3	Lokaal netwerk	Ongeoorloofd meeluisteren Manipulatie verkeersdata Ongeoorloofd gebruik dienst	Lokaal netwerk afschermen Authorisatie, bijv. middels API-KEY	
D11	FCD / adviezen	**	**	*	*	P1-P2-P3	Lokaal netwerk	Ongeoorloofd meeluisteren Manipulatie verkeersdata Ongeoorloofd gebruik dienst	Lokaal netwerk afschermen Authorisatie, bijv. middels API-KEY	
D3	Advies; 'JAM';CAM;DENM; TSM. TSM kan privacy gevoelige data bevatten?		*	**		P3-P2	Wifi-p; ad hoc	Ongeoorloofd meeluisteren Injecteren valse ITS berichten	Coöperatieve PKI infrastructuur gebaseerd op ETSI standaarden	
D5	Verkeersinformatie, microdata in een geografisch gebied met een straal van 1000m CAM;DENM	**	*	**		P3-P2	Wifi-p; ad-hoc	Ongeoorloofd meeluisteren naar privacy gevoelige gegevens Injecteren valse ITS berichten	Coöperatieve PKI infrastructuur gebaseerd op ETSI standaarden	Aansluiting blijven zoeken bij de maatregelen zoals gedefinieerd in de ETSI standaarden.
X	Hosting server		*	**	**	P1-P2-P3	Onderdeel van gesloten domein	Overnemen van een virtuele server op de roadside	Afschermen van publiek internet	Regelen authorisatie op virtuele machines
M	Logging Uitgangspunt ook pricacygevoelige gegevens worden gelogd	**		*	*	P1-M&E P2-M&E P3-M&E	????	Ongeoorloofd meeluisteren Manipulatie logging?	Anonimiseren van persoonsgegevens	Deze interface moet nog nader worden bestudeerd

Cooperatieve interface

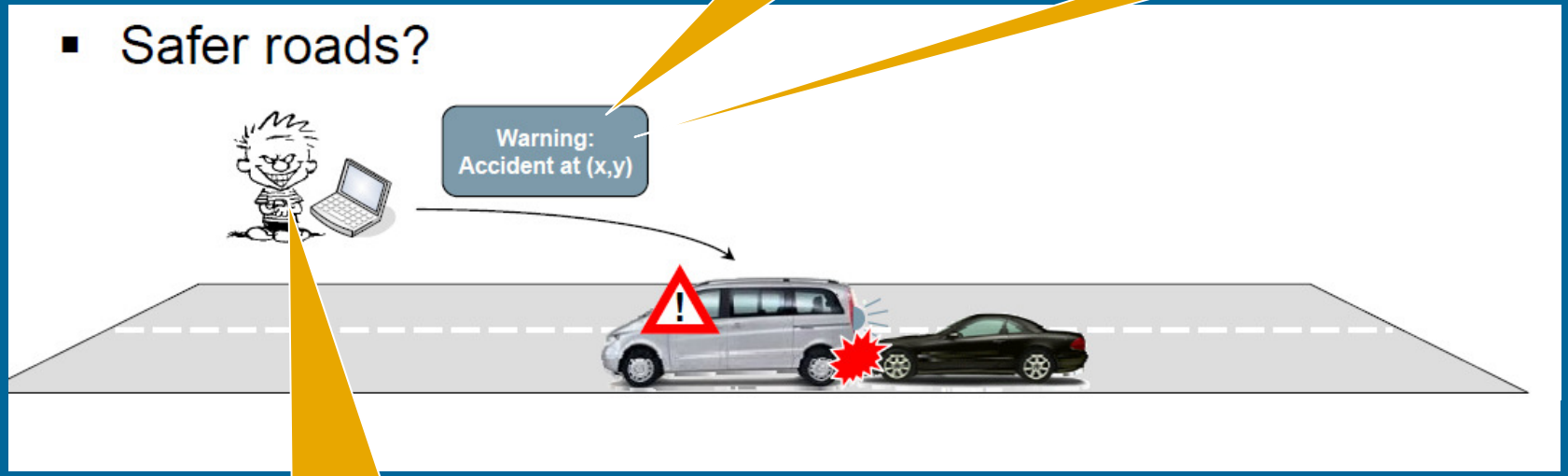


Coöperatieve berichten en security

Veiligheidstoepassingen
- CAM en DENM berichten

Encryptie?

Integriteit

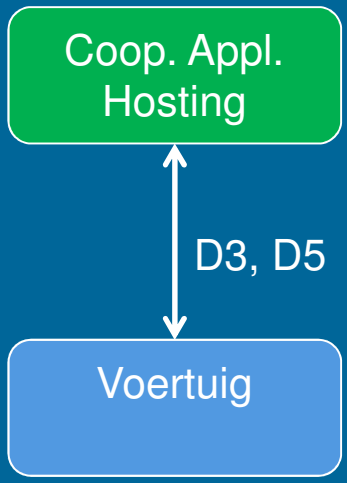


Bron Authenticatie

Privacy
concerns

Coöperatieve berichten en security

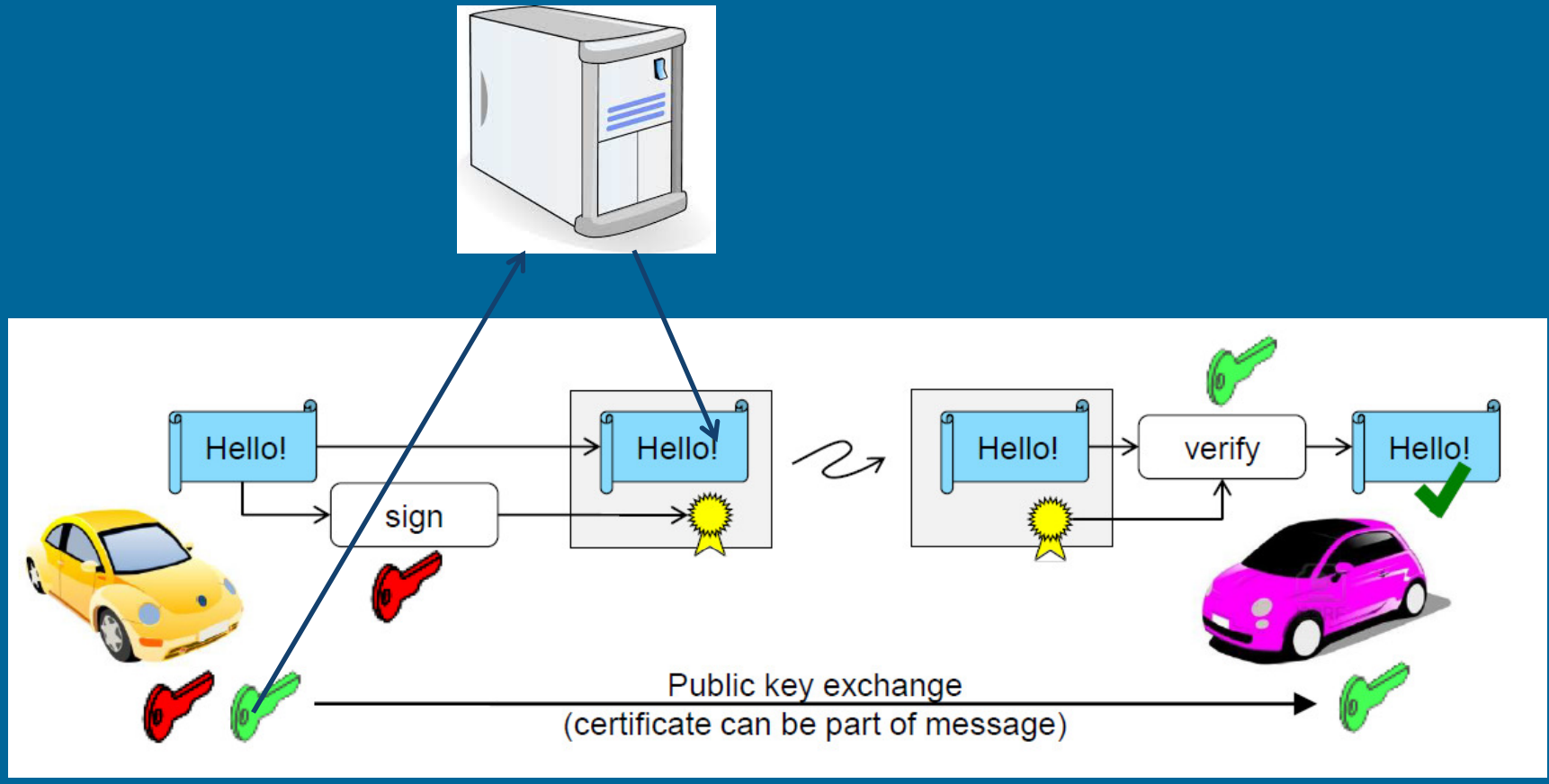
> D3:**Adviezen** (‘DENM’)
  - Niet geheim
  - Integriteit
  - Bron verificatie
> D5: **xFCD** (CAM)
  - Niet geheim (per definitie; zie ETSI en use cases)
  - Integriteit
  - Bron verificatie
  - Conflicterend met privacy



Uitdagingen

1. Bron verificatie & integriteit waarborgen
2. Privacy beschermen

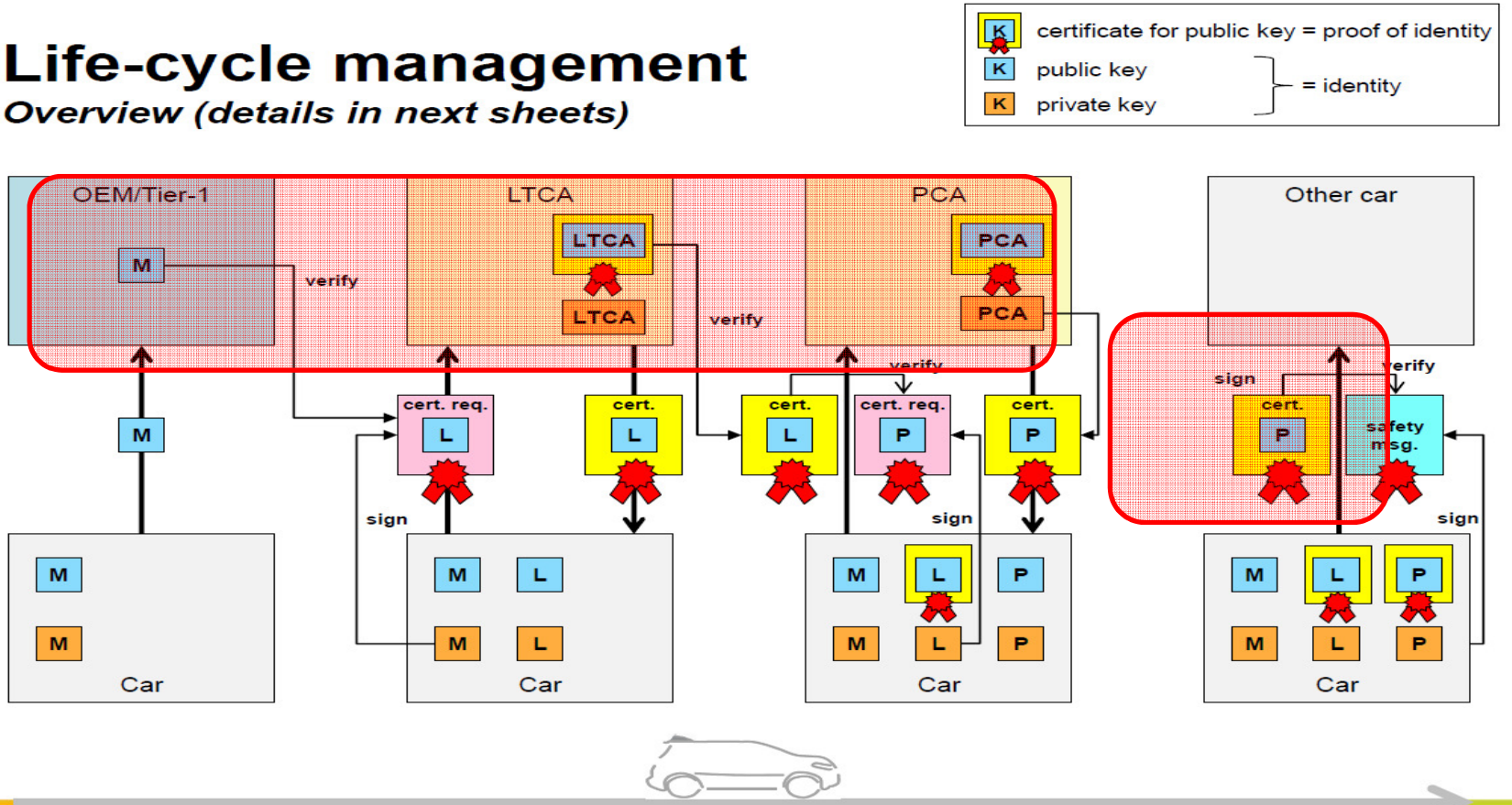
Cooperatieve berichten en security



PKI voor dummies

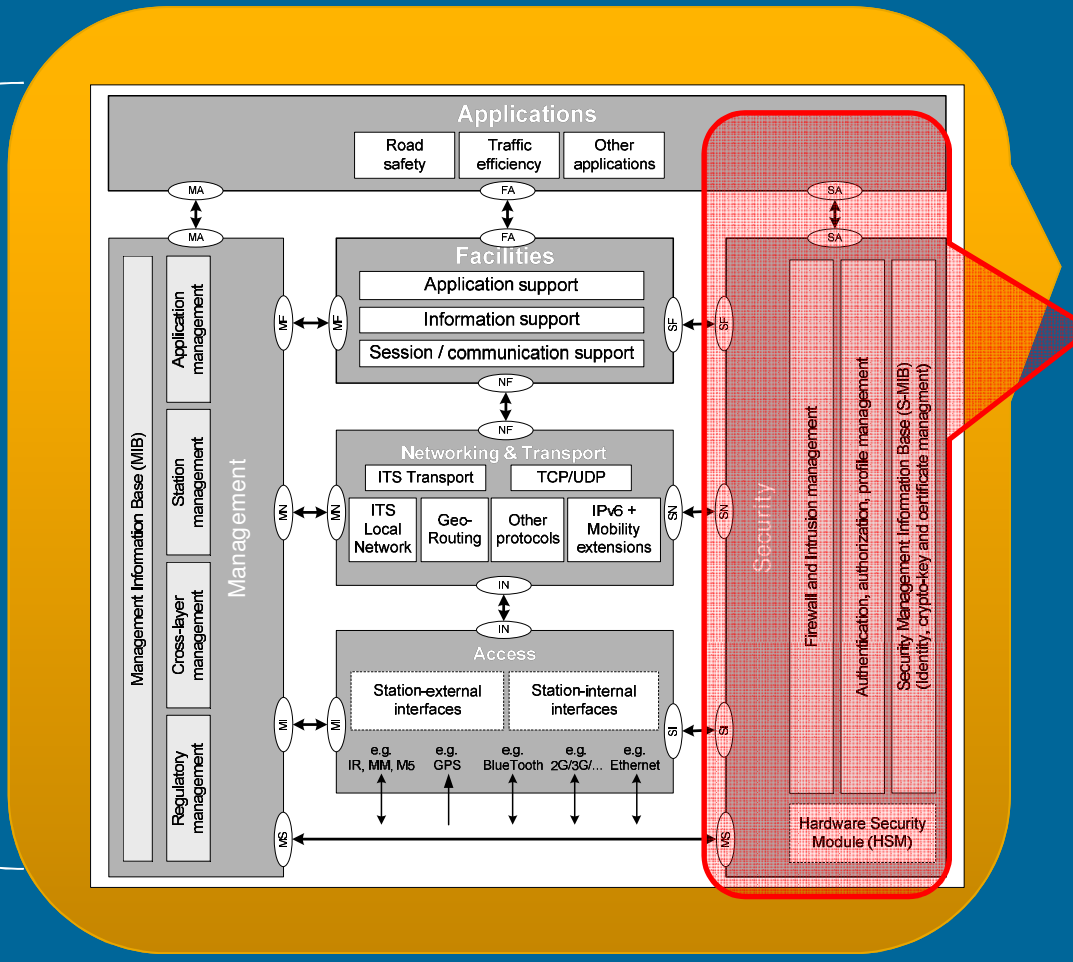
Life-cycle management

Overview (details in next sheets)



1

Technologie implementeren

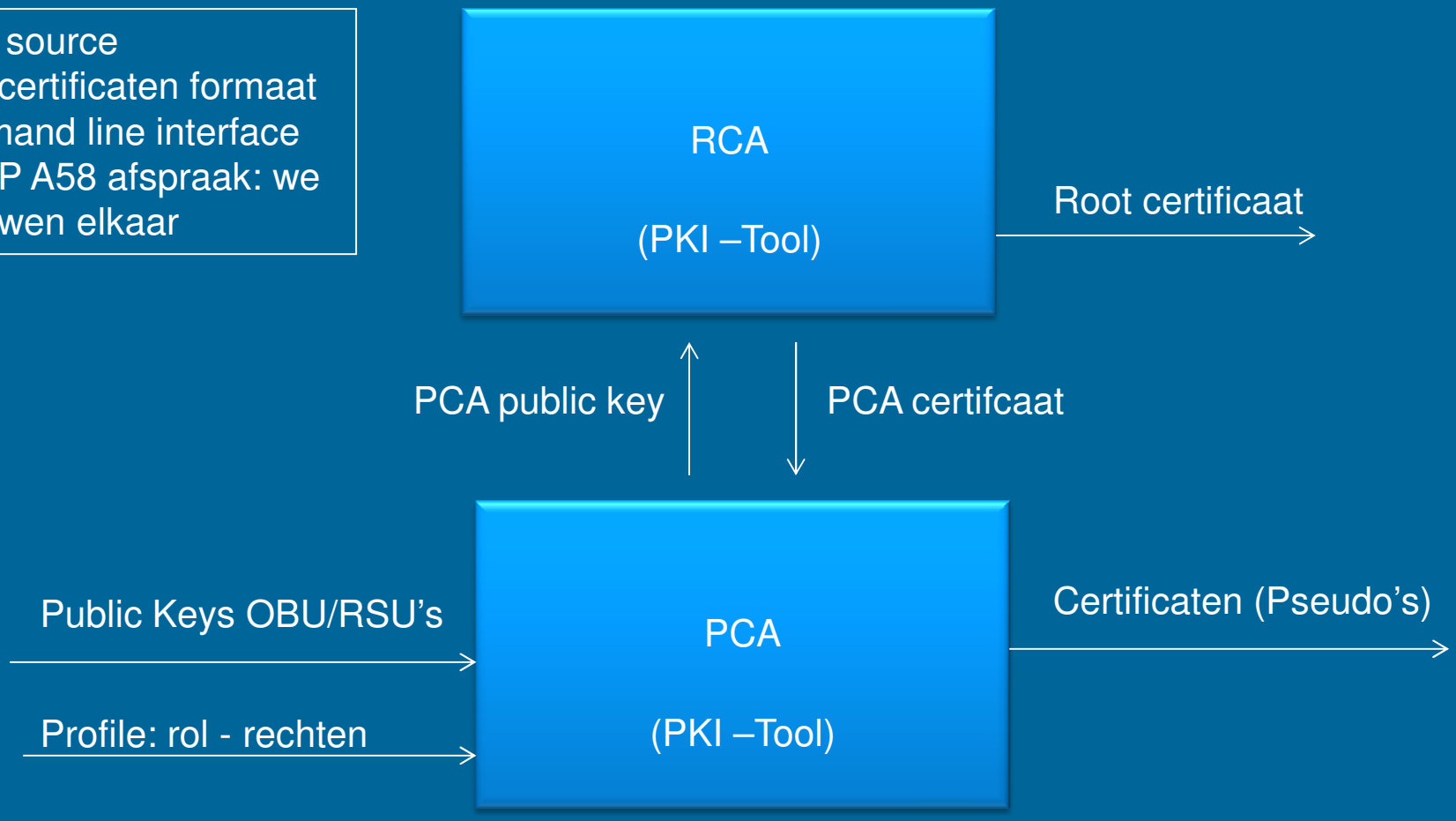


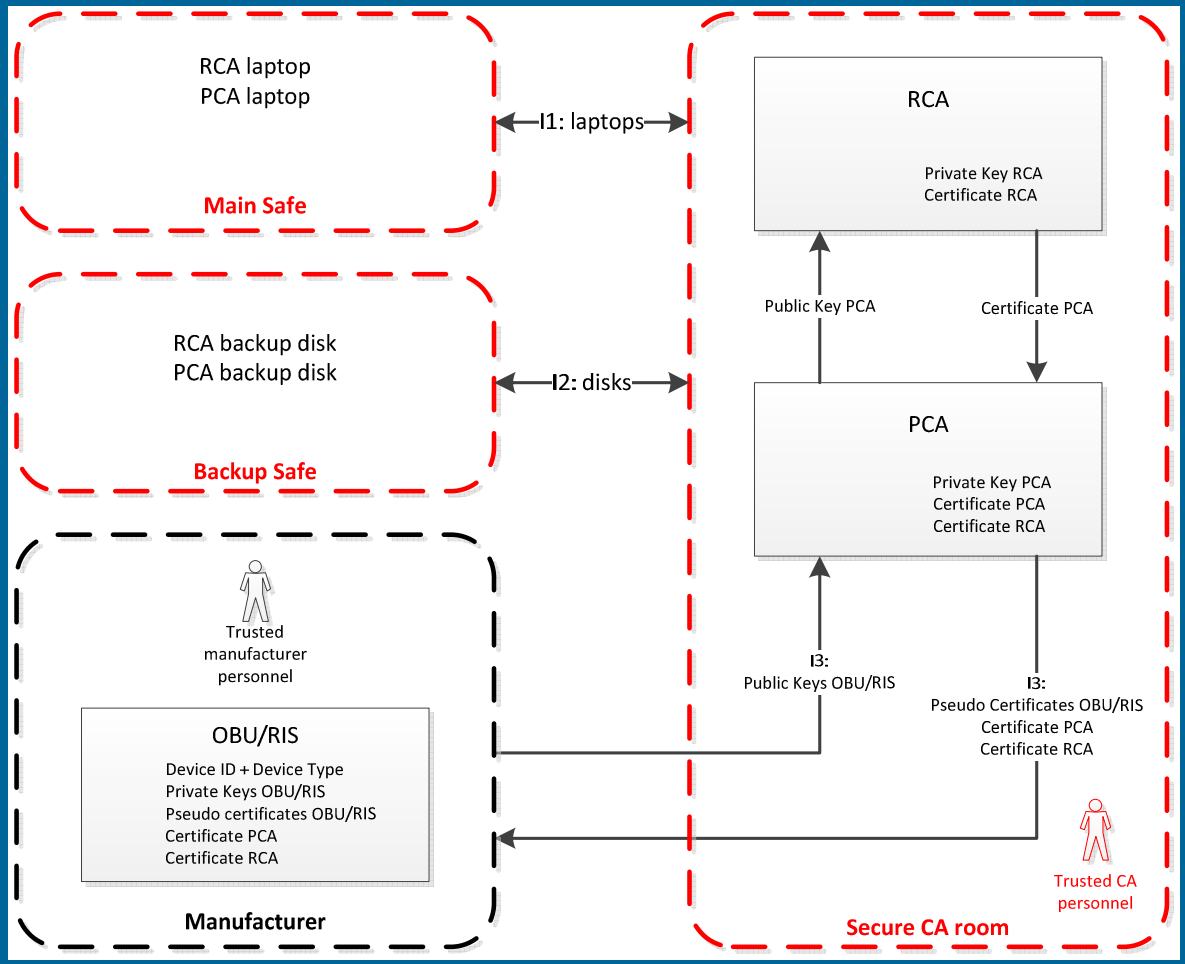
- Ondertekenen
- Verifieren
- Chain of trust
- Key management
- Opslaan certificaten
- Praktijk testen

Technologie implementeren in de C-ITS Stations

PKI Tool: RCA en PCA

- Open source
- ETSI certificaten formaat
- Command line interface
- In PCP A58 afspraak: we vertrouwen elkaar





Organiseren: secure room, interfaces en procedures

Role	Responsibility
Trusted CA person	Responsible for handling and operating the RCA and PCA laptops
Trusted manufacturer person	Responsible for distributing public device keys to the PCA, receiving the pseudo certificates for a device and keeping the link table secret
Auditor	An independent person responsible for verifying the compliancy of the procedure execution by the trusted personnel
Incident manager	Responsible for handling an incident
Incident response team	An “ad hoc” team, formed by the incident manager, to handle an incident.

Rollen

- PKI tool is opgeleverd

- Momenteel worden labtesten uitgevoerd
  > Generen certificaten
  > Testen Over The Air communicatie met ondertekende berichten
  > Betrokken partijen: Siemens, Technolutiuon, V-Tron en Vialis

- Uitvoeren ‘sneaker’ sessies (genereren van certificaten)

- Uitrol PKI infrastructuur gepland voor eind 2015 op A58 tussen Eindhoven en Tilburg

Status

- Technologie van signen en verifiëren van berichten is goed gespecificeerd (ETSI)
- Digitaal ondertekend berichten verkeer tussen verschillende partijen functioneert goed
- Complexiteit zit hem in organiseren van PKI, niet de techniek.
  - > Instanties en bevoegdheden
  - > Profile, rollen, rechten
  - > Inspecties, keuringen
  - > Life cycle management
  - > Incident management

Conclusies

Vragen?