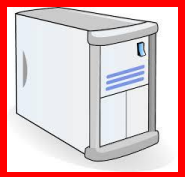
Aanpak A58 security issues

Door P. Goossens, 31 oktober 2014

- Het PCP A58 “Spookfile project”
- Security, wat is dat en delen we hetzelfde beeld?
- Security aanpak
  > Analyse High Level Architecture
  > Over The Air interface en security
- Conclusies

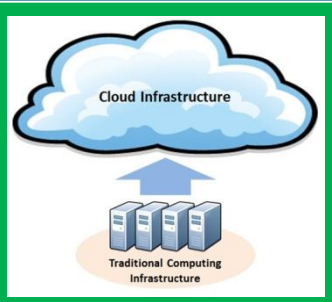
Overzicht

Data



Dienst

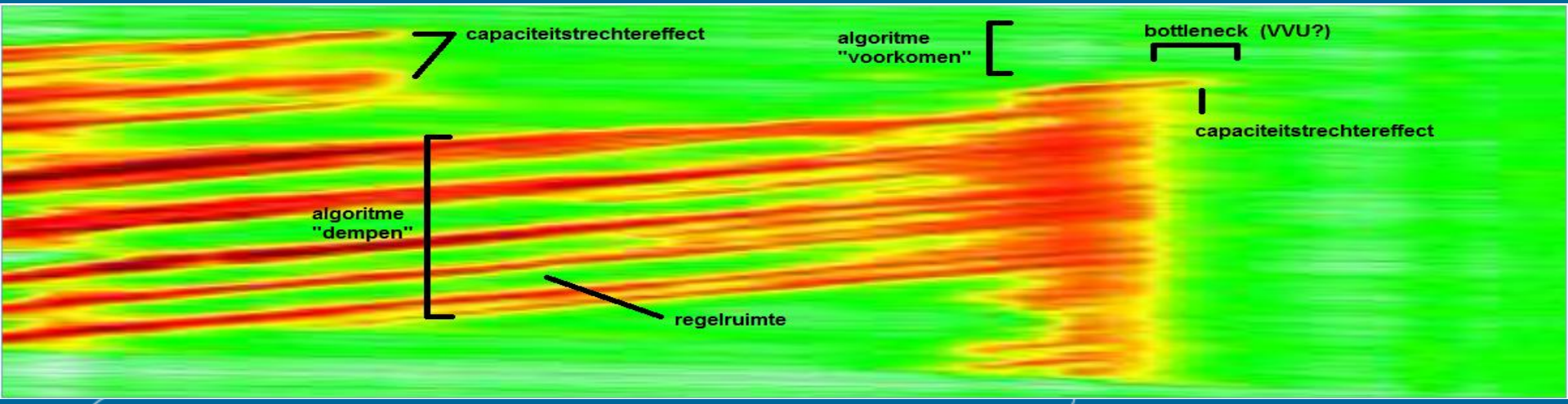
Coöperatieve applicatie hosting



PCP A58 “Spookfile” project

Tilburg

Eindhoven



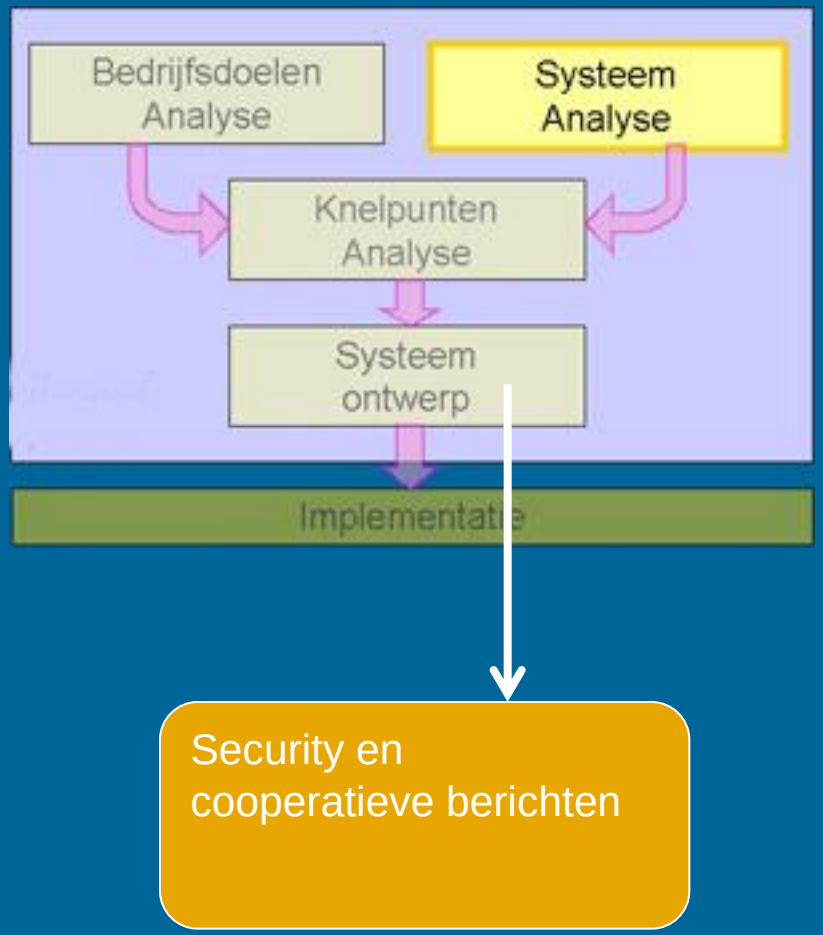
PCP A58 “Spookfile project”

- Security geagendeerd

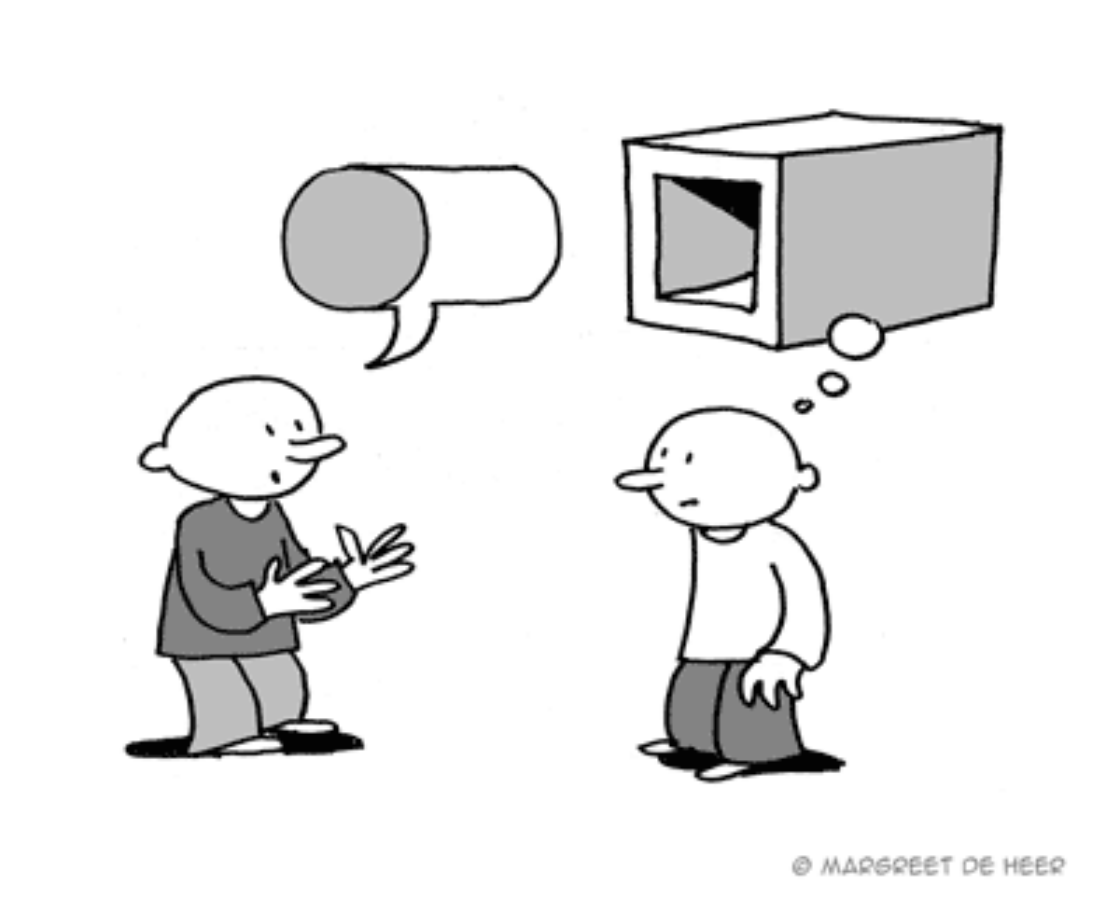
- Werkgroep security samengesteld
  > Security specialisten
  > Opdrachtgevers
  > Jurist
  > Vertegenwoordigers vanuit de 3 percelen

Proces in de PCP A58

- Security aanpak geformuleerd
  > Systeem analyse
  > Security en coöperatieve berichten



Proces in de PCP A58

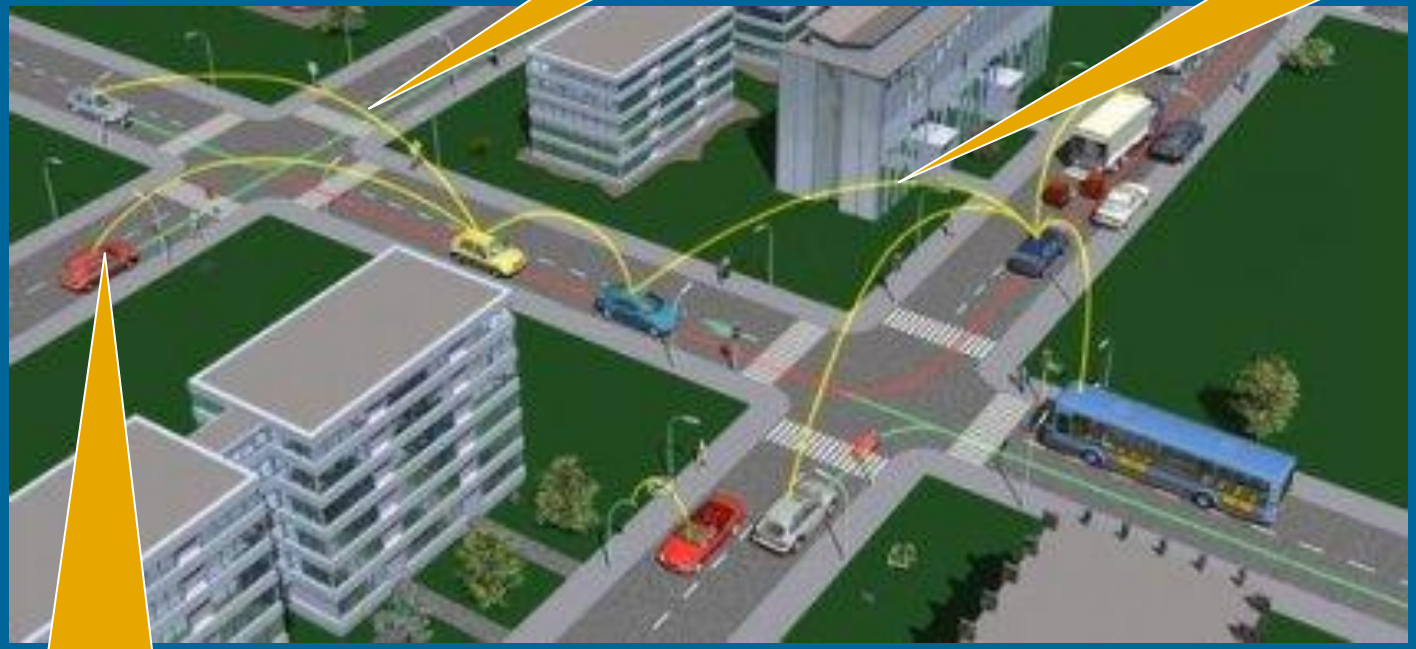


Elkaar gaan begrijpen

Veiligheidstoepassingen
- CAM en DENM berichten

Encryptie?

Integriteit?



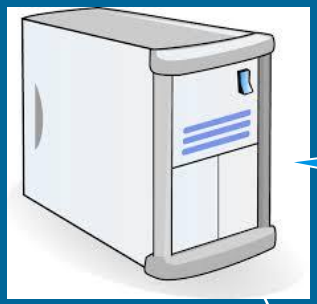
Bron Authenticatie?

Privacy concerns?

Security is een container begrip

Digitaal onderteken is niet hetzelfde als encryptie

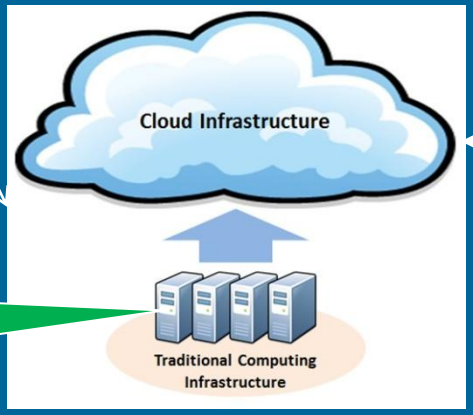
Begripsvorming



P2 server verstuurt advies X

Cooperatief bericht met advies X

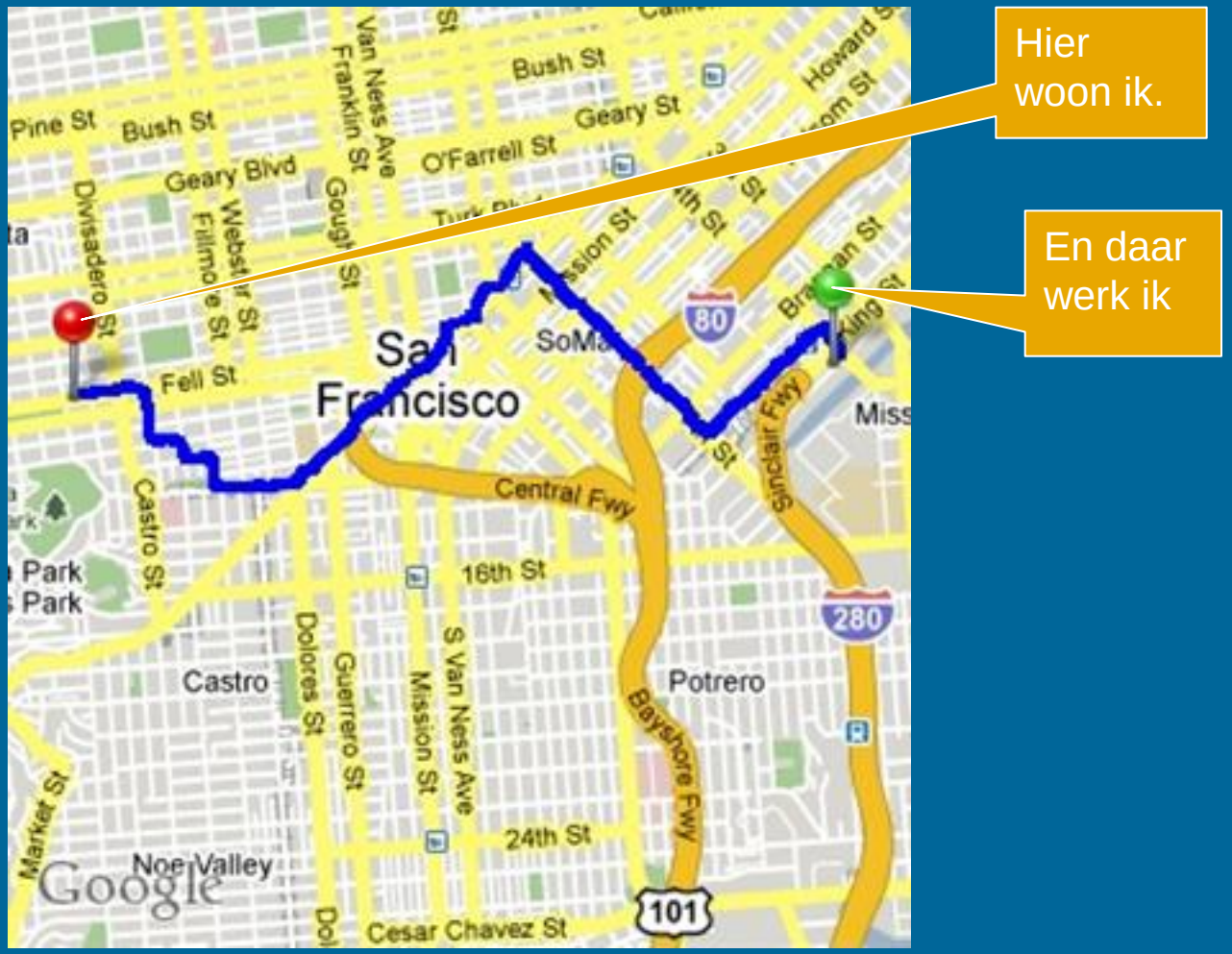
Schaal-baarheid



P3 RIS applicatie server verstuurt advies X

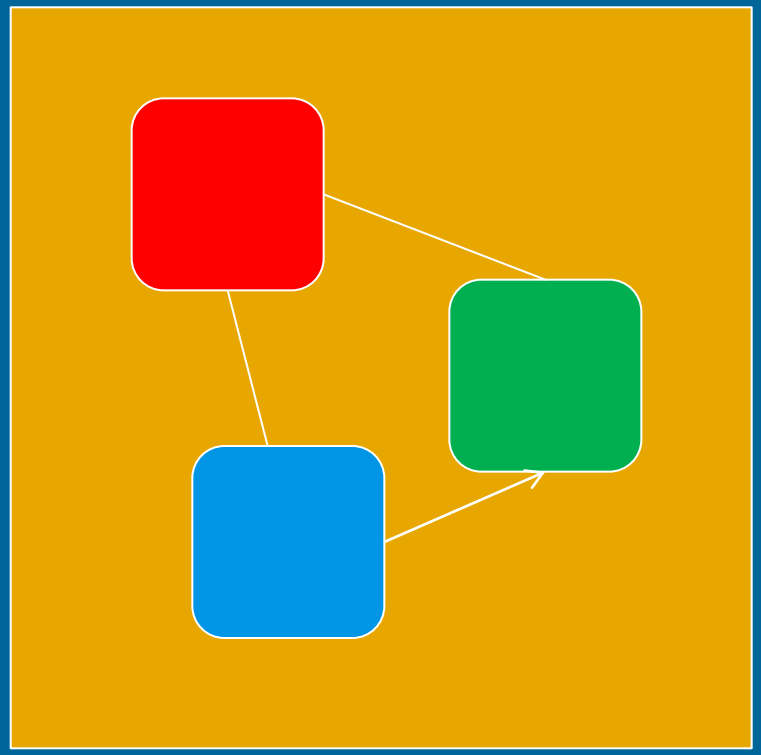
Voorbeeld begripsvorming (bron verificatie / schaalbaarheid)

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

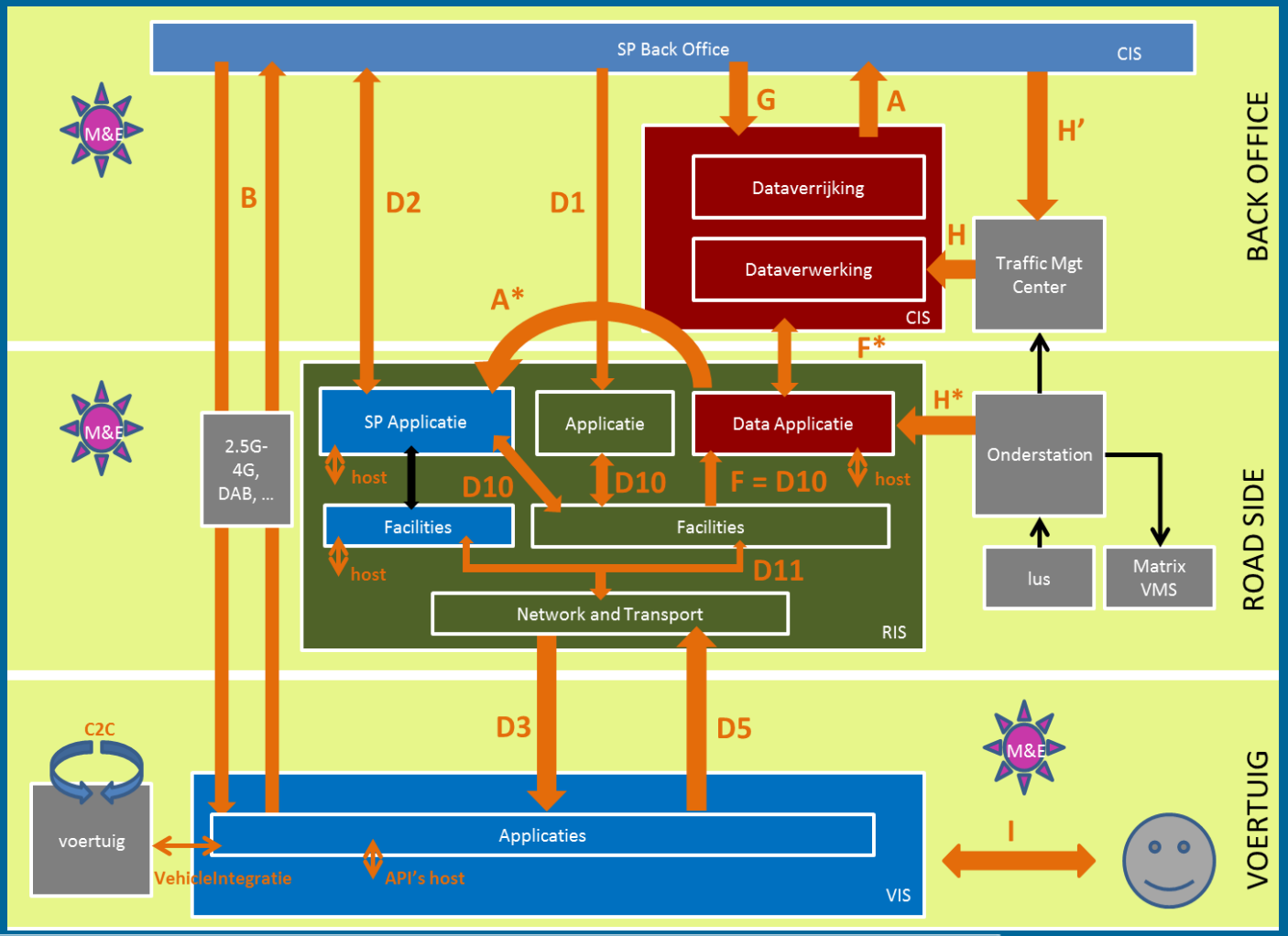


Begripsvorming omtrent Privacy en traces

- Bedreigingen
  - > Manipulatie adviezen
  - > Injecteren niet valide adviezen
  - > Roadside te hacken.
- Type data op interfaces
  - > Vertrouwelijk
  - > Integriteit
  - > Toegang
  - > Authenticiteit
- Maatregelen
  - > ICT
  - > Proces
  - > Fysiek

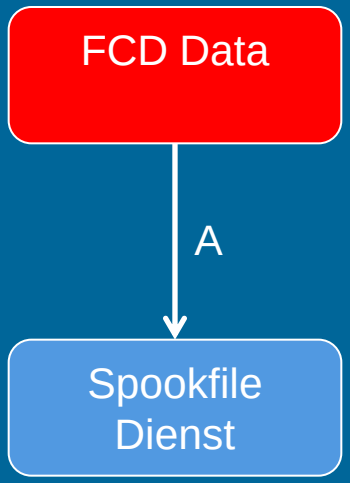


Systeem aanpak security



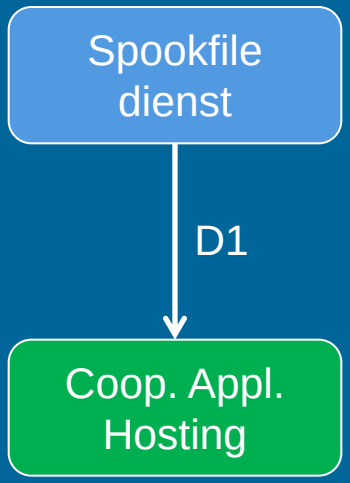
High Level Architecture

- Interface A **Verkeersdata**
  - > Bedreigingen
    - Ongeoorloofd meeluisteren (privacy),
    - Manipulatie verkeersgegevens,
    - Ongeoorloofd gebruik dienst.
  - > Data eigenschappen op de interface
    - Vertrouwelijkheid
    - Verificatie
    - Integriteit
    - In de mindere mate: authorisatie
  - > Maatregelen:
    - Server side HTTPS + API key voor client authenticatie.
    - Gebruik maken van wisselende ID’s
    - Knippen kop en straat ID traces



Data eigenschappen, bedreiging en maatregelen

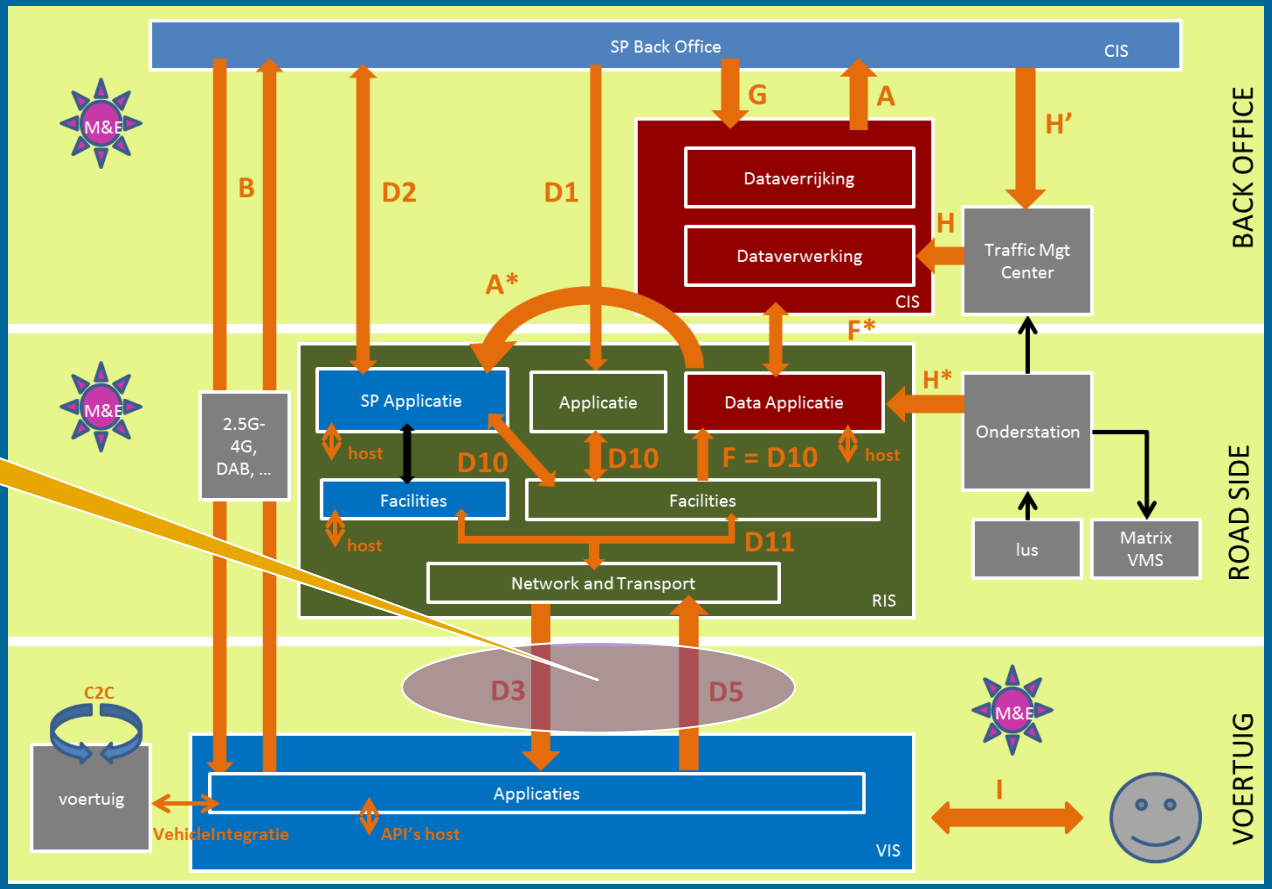
- Interface D1 **Advies**
  - > Bedreigingen
    - Manipulatie adviezen
    - Injecteren niet valide adviezen
    - Misbruik interface om roadside te hacken.
  - > Data eigenschappen op de interface
    - Geen vertrouwelijkheid
    - Verificatie
    - Integriteit
    - In de mindere mate: authorisatie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



Eisen stellen aan data eigenschappen op de interfaces

	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 privacy 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

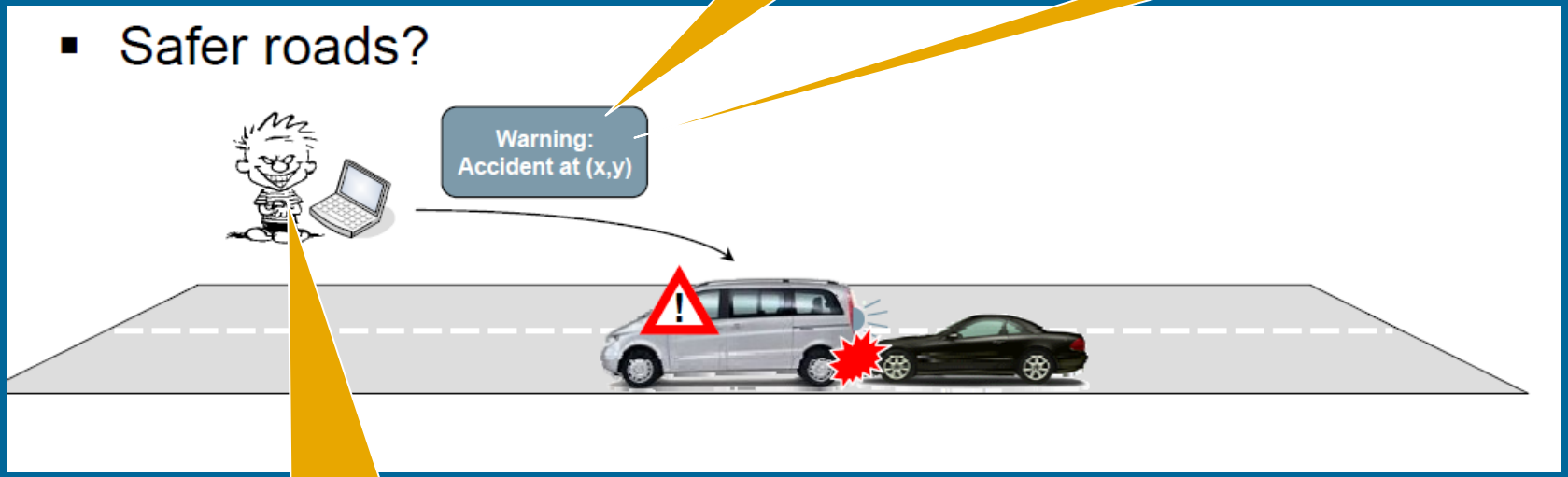


Coöperatieve berichten en security

Veiligheidstoepassingen
- CAM en DENM berichten

Encryptie?

Integriteit



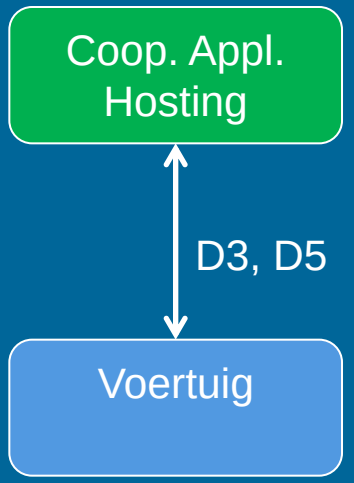
Bron Authenticatie

Privacy
concerns

Coöperatieve berichten en security

> D3:**Adviezen** (‘IVI’)
  - 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

- Friendly chain
  - Doel : technische implementatie kennis opdoen
  - Zelf organiseren en zo klein mogelijk houden

- Pre-commerciele trusted chain

  > Organisatie die gedurende een aantal jaren projecten ondersteund.

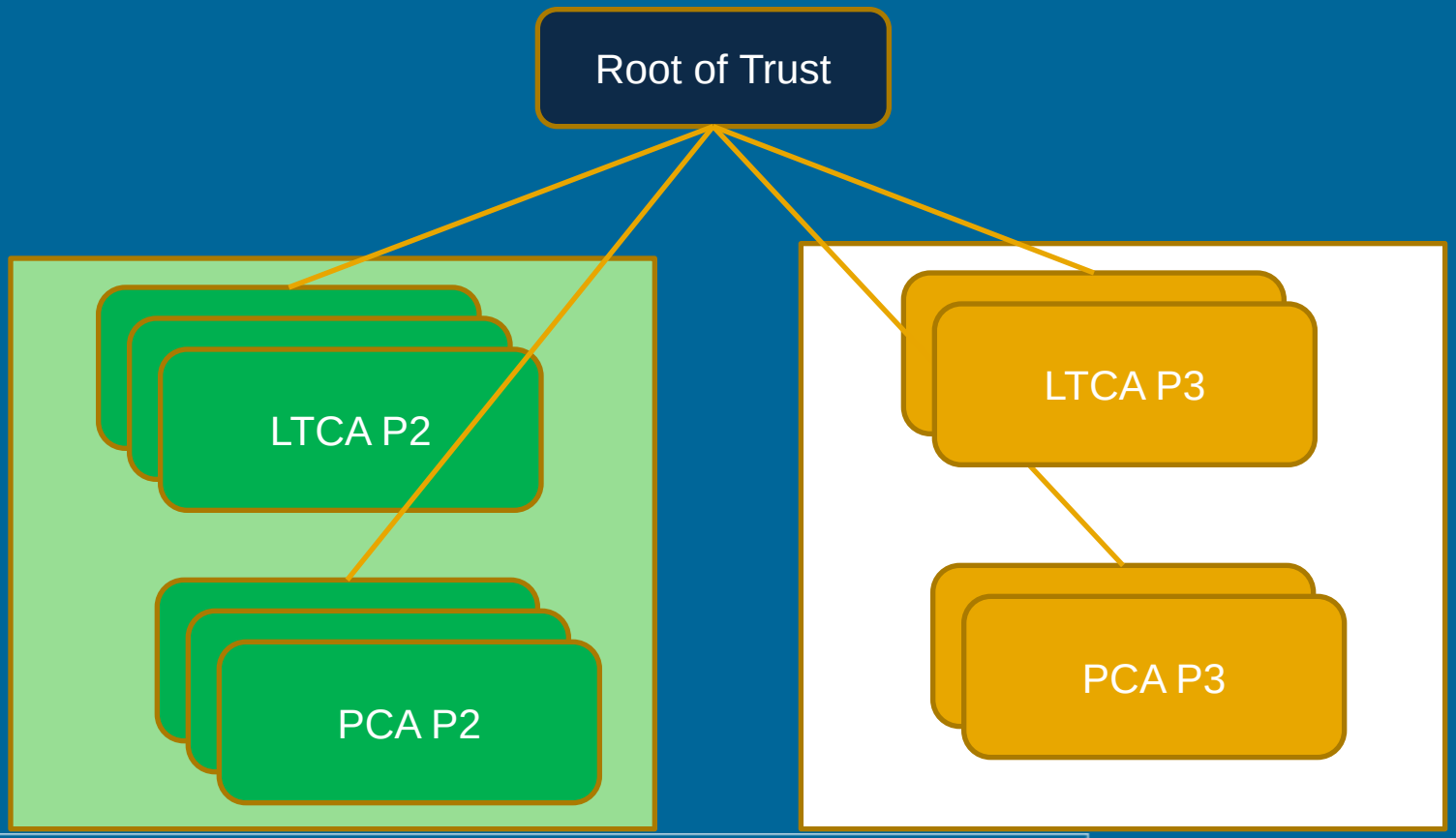
- Trusted chain

  > Aanhaken op EU brede initiatieven

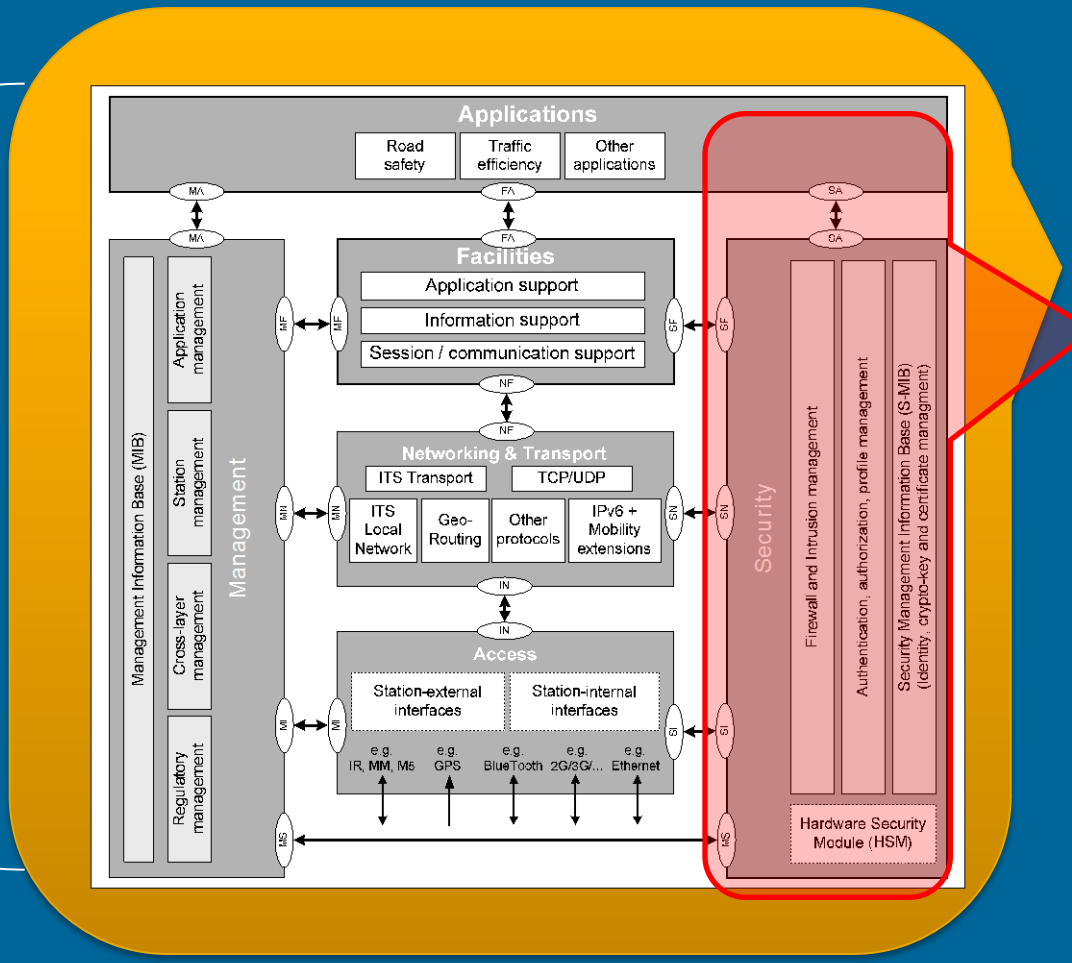
Scope: “Friendly Chain”

Gezamenlijk ontwikkelen
Elke perceel richt eigen LTCA en PCA in

Doelstelling: eenvoudig zelf technologie kunnen implementeren



Ontwerp “Friendly Chain of Trust”



Ondertekenen

Verifieren

Chain of trust

Key management

Opslaan certificaten

Praktijk testen

Technologie implementeren in de C-ITS Stations

- Niet alle specificaties zijn gereed
  > Niet op standaarden gaan vooruitlopen
  > Met name interfaces rondom LTCA en PCA onduidelijk
  > Interface tussen de C-ITS stations wel helder

- Veel details nog beperkt tot C2C Consortium

- Weinig handson ervaring: mooi!

Uitdagingen implementatie coöperatieve KPI

- Security gaat verder dan alleen de coöperatieve Over The Air interfaces, beschouw het gehele systeem.

- Veel aandacht nodig voor proces
  > Er zijn veel stakeholders bij security betrokken
  > Het kost tijd om met elkaar het juiste jargon te ontwikkelen en elkaar te begrijpen
  > Is voorwaarde om te komen tot een goede security architectuur

- Coöperatieve KPI infrastructuur bevind zich nog in de ontwikkelingsfase

- Het niet beschikbaarheid hebben van een coop. PKI infrastructuur staat de uitrol van coöperatieve technologie in de weg.

Conclusies

Vragen?