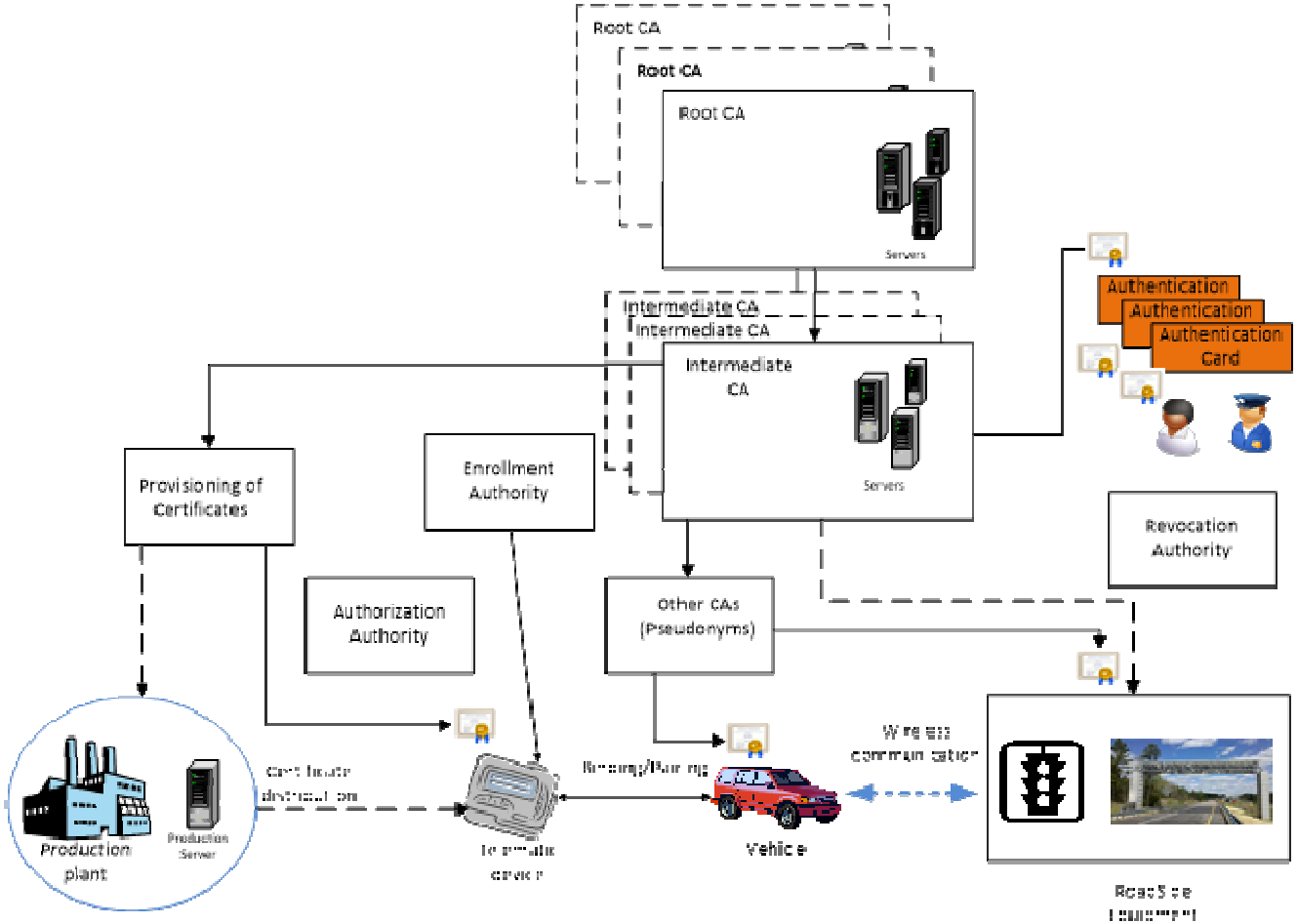
IFAL Proof-of-Concept
Doelstelling en testaanpak

Gilles Ampt en

Willem de Boer

6 December 2016

C-ITS security trust model (PKI)



Source: C-ITS platform

Short term certificate requirements (Pseudonym identity certificates)

1. Reliability of messages
   - Sender Authorization & Revocation (authorization tickets)
   - Sender Identification (authentication)
   - Message integrity (digital signature)
2. Privacy protection
   - Hide vehicle's identification and driving history
3. Functionality – Vehicle identifiability within the traffic flow
   - Linkable sequence of messages to an individual vehicle
4. Operational efficiency
   - Communications overhead, processing, storage
   - Costs, simplicity and scalability

Short term pseudonym certificate parameters (current understanding)

Operational lifetime (validity):	1 week
Operational use (each time):	max. 5 – 30 minutes
Concurrently valid certificates:	20 certificates (for one week)
Issuance and activation:	3 years (pre-loaded in one batch)
Revocation:	no

- Privacy protection effectiveness questions
- Security risks introduced
  - Sybil attacks
  - No effective revocation control
- Acceptance risks (will this be good enough)

Short term pseudonym certificate parameters

… IFAL proposal (Issue First Activate Later)

Operational lifetime (validity):	*5 - 10 minutes*	*More effective privacy protection*
Operational use (single use):	5 – 10 minutes *(no reuse)*	
Concurrently valid certificates:	*1 certificate*	*Sybil attack countermeasure*
Issuance :	10 years (pre-loaded)	
Revocation:	no	
Activation:	*every 3 months - every week*	*Revocation control measure*

- *Italics is further detailing of IFAL to current standards and policy developments*

Technolution

A58 PKI