Alternative Applications of the SCMS V2X Infrastructure

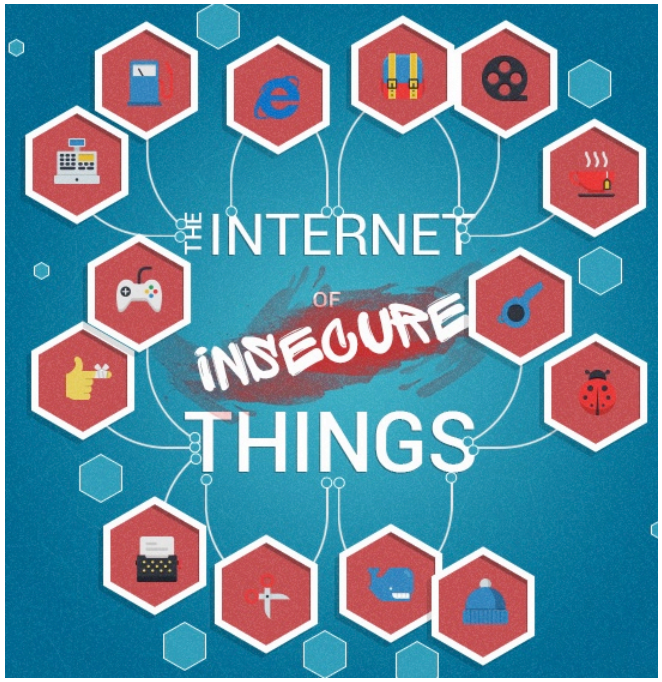
Brian Romansky

TRUSTPOINT

Impactful Innovation

"In the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials"

IoT Security Focus



Most IoT security solutions focus is on perimeter and channel protection

- Provide secrecy of the message, but does not protect the privacy of the participants
- An observer with a radio can track movement of individuals and repeat visitors
- Authenticating agent knows full details of all parties in the transaction

Privacy-Preserving Authentication

- Ability to prove attributes of your identity without disclosing full details

- Ability to engage in multiple transactions without linking them to a single user

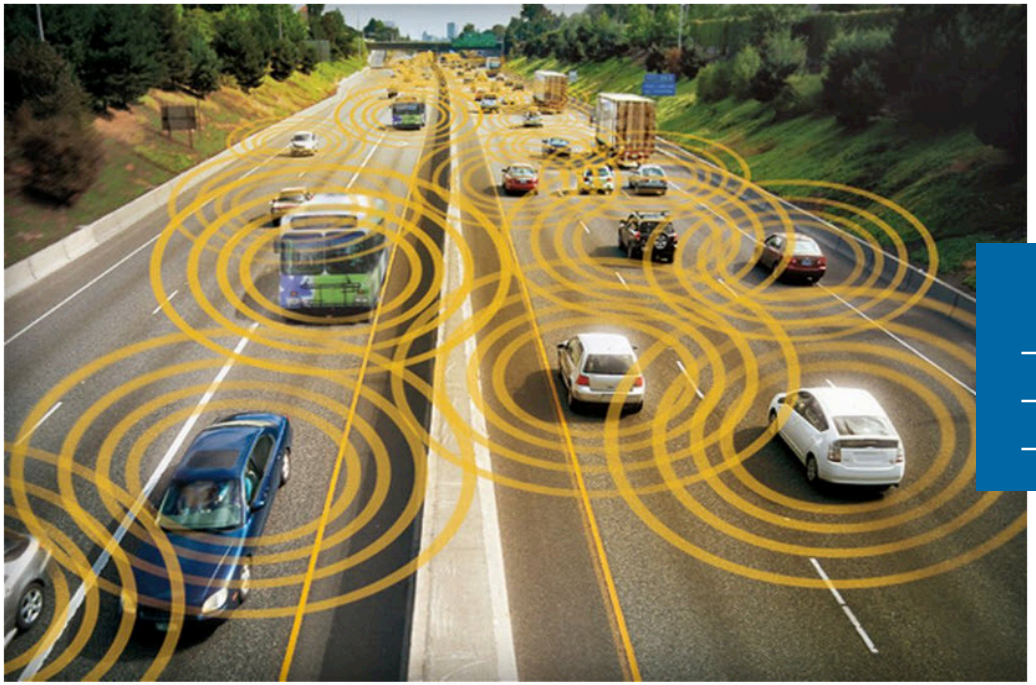
Is this one person showing up 3 times, or 3 different individuals?

Existing Algorithms

- Significant research into privacy-preserving authentication and anonymous rights management
  - Idemix (IBM) – Zero-Knowledge Proofs
  - U-Prove (Microsoft) – Blind Signatures

- Most schemes are based on novel cryptographic techniques
- Hardware and infrastructure development is in early stages
- Few solutions support realistic solutions for braches and "misbehavior" detection or CRL distribution

V2X Technology for Collision Avoidance



(USDOT)

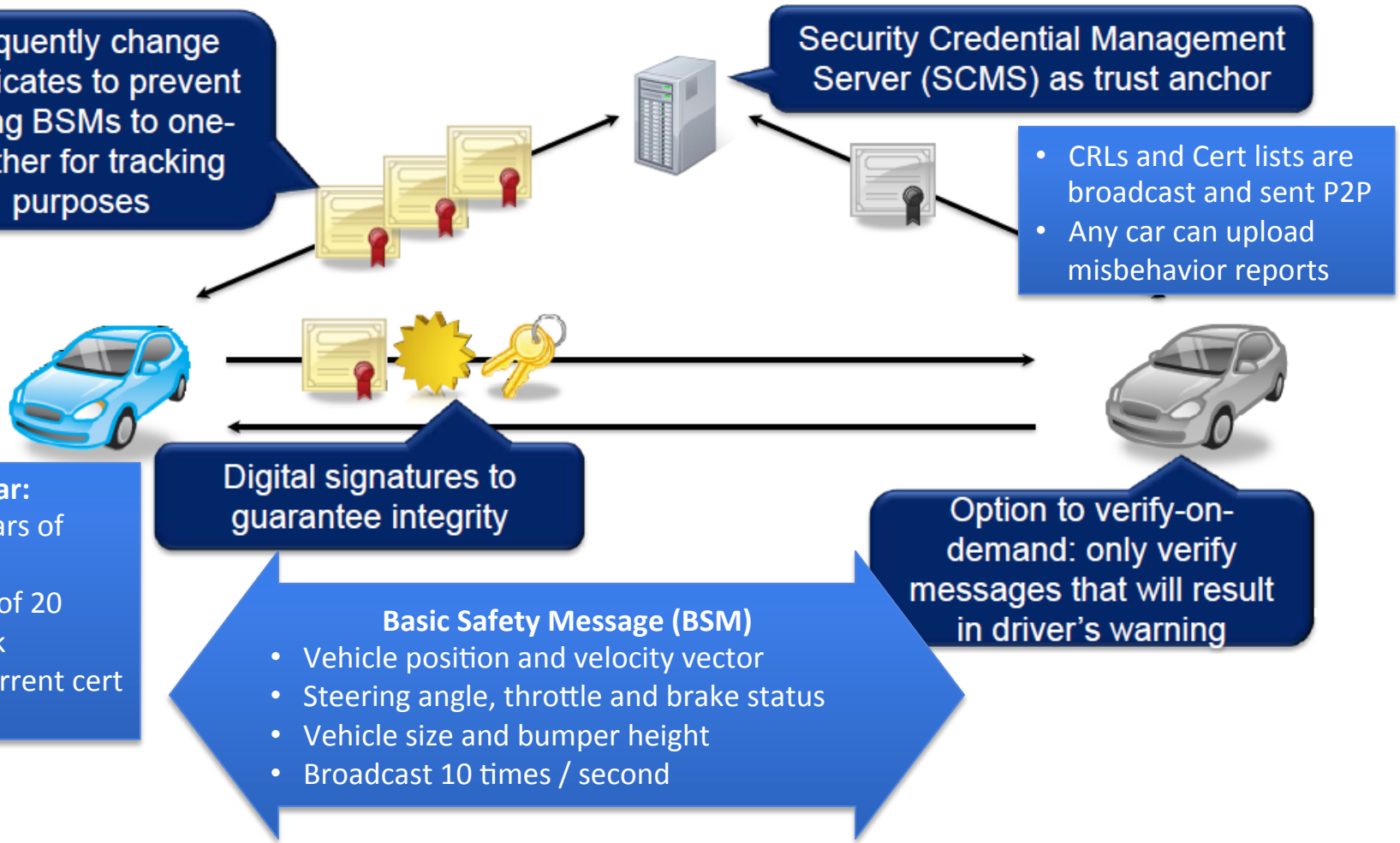
2014 Crash Data

- 6 million reported vehicle crashes
- 2.3 million injuries
- 32,675 fatalities

From "2014 Motor Vehicle Crashes: Overview"
http://www-nrd.nhtsa.dot.gov/Pubs/812246.pdf

- Potential for an 80% reduction in non-alcohol related collisions
  http://www.safercar.gov/staticfiles/safercar/v2v/V2V_Fact_Sheet_101414_v2a.pdf
- Augment existing Advanced Driver Assistance Systems (ADAS) technology
- Improve interoperability between human drivers and autonomous vehicles
- Enable advanced infrastructure and emergency management solutions
- Privacy is a critical design requirement

V2V Safety Application



V2V System Properties

Unique Properties:

- Scales up to 17M new vehicles per year, total population of ~260M vehicles
- Pseudonym Certificates – batches of 20 per week, change every 5 minutes
- Peer-to-peer authentication of messages
- Efficient certificate distribution
- Support for misbehavior investigation and CRL distribution

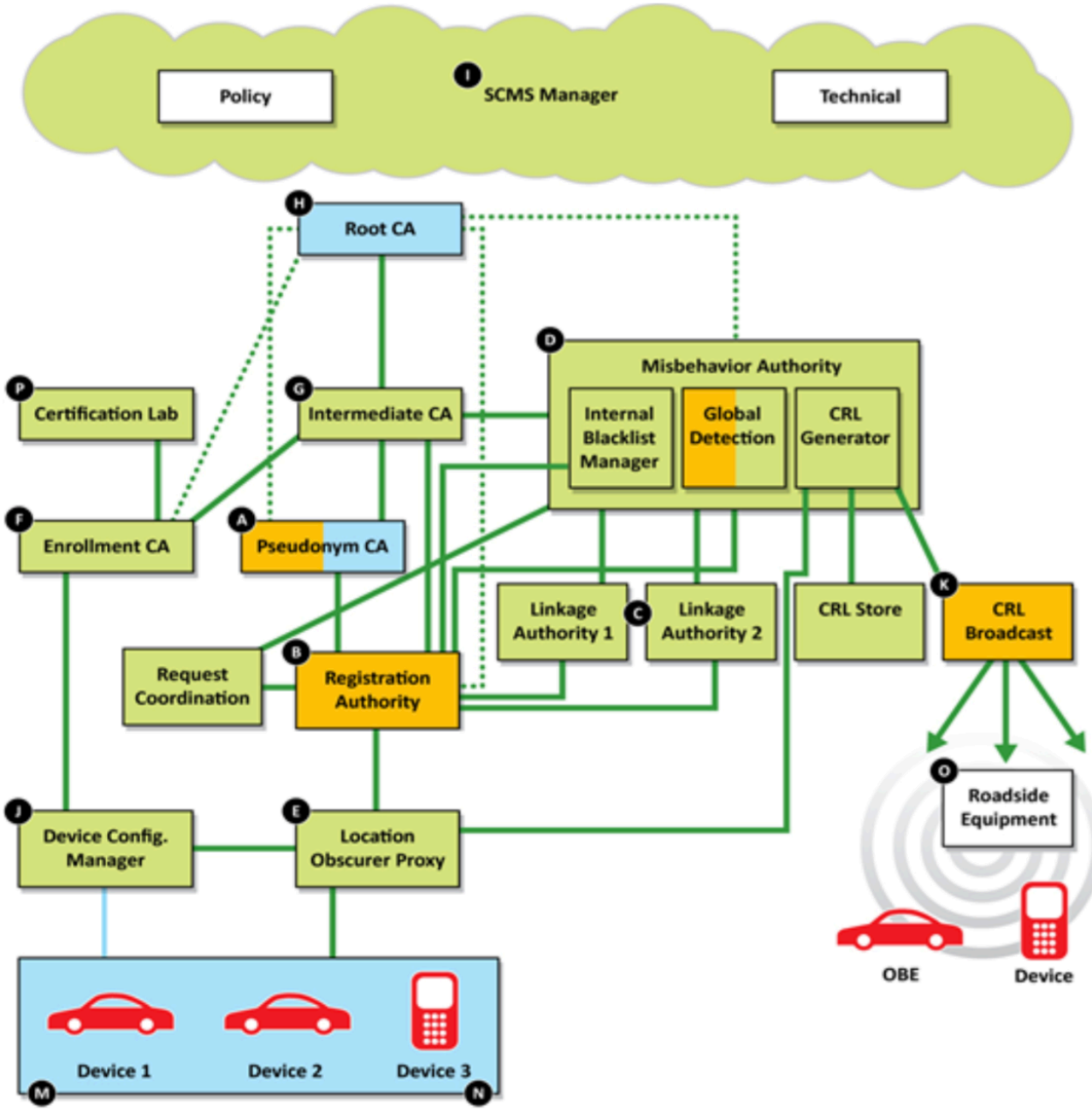
SCMS Design Elements:

- Relies on mature algorithms (ECC, AES, SHA-256)
- Distributed Multi-Vendor Support
- No single back-end component can break privacy
- High-performance, low-cost chipsets
- CRL and Blacklist management
- Designed to work with intermittent network access

Security Credential Management System

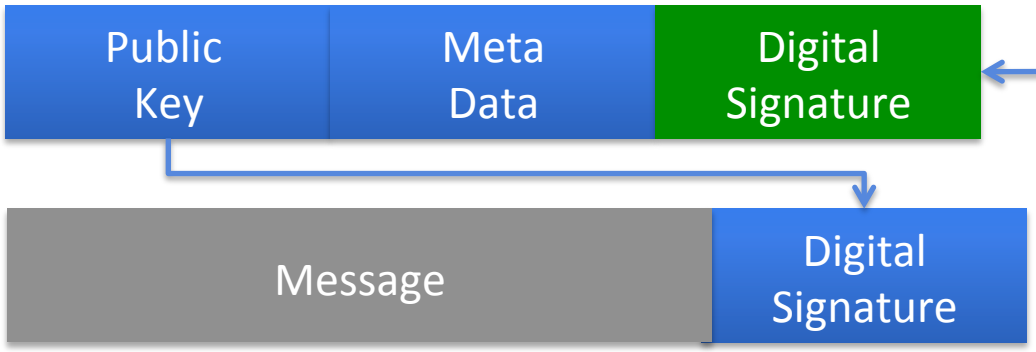
Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application

http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf



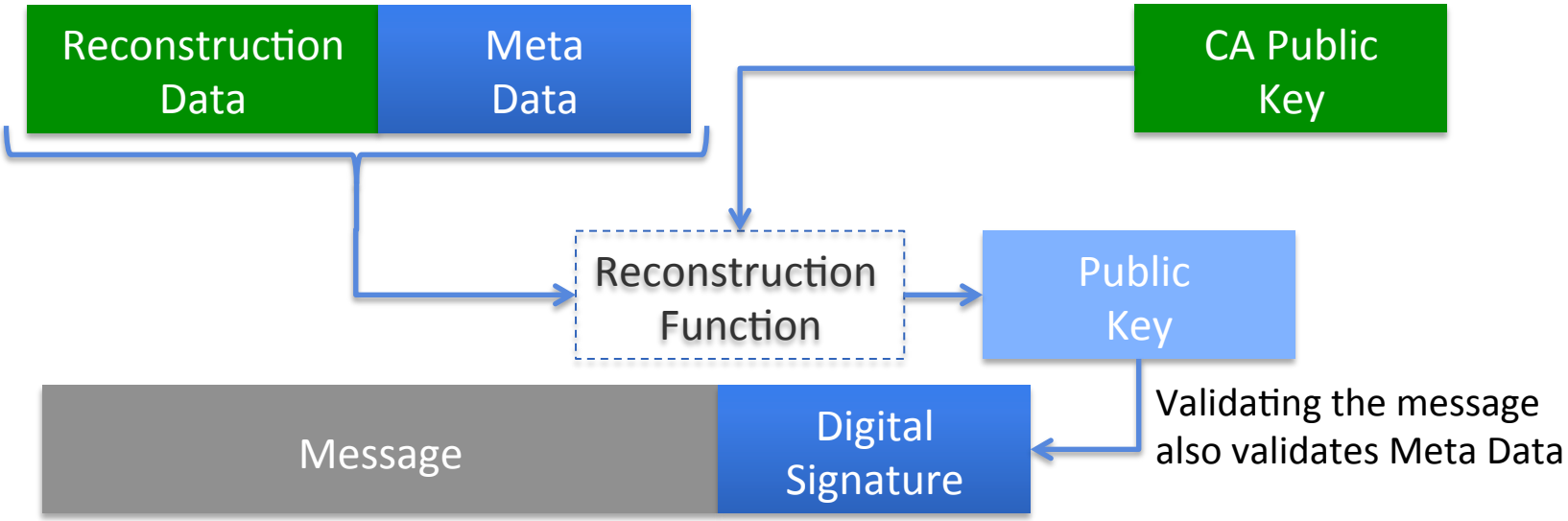
ECQV Implicit Certificates

Typical digital certificate has 3 parts: ~150 Bytes



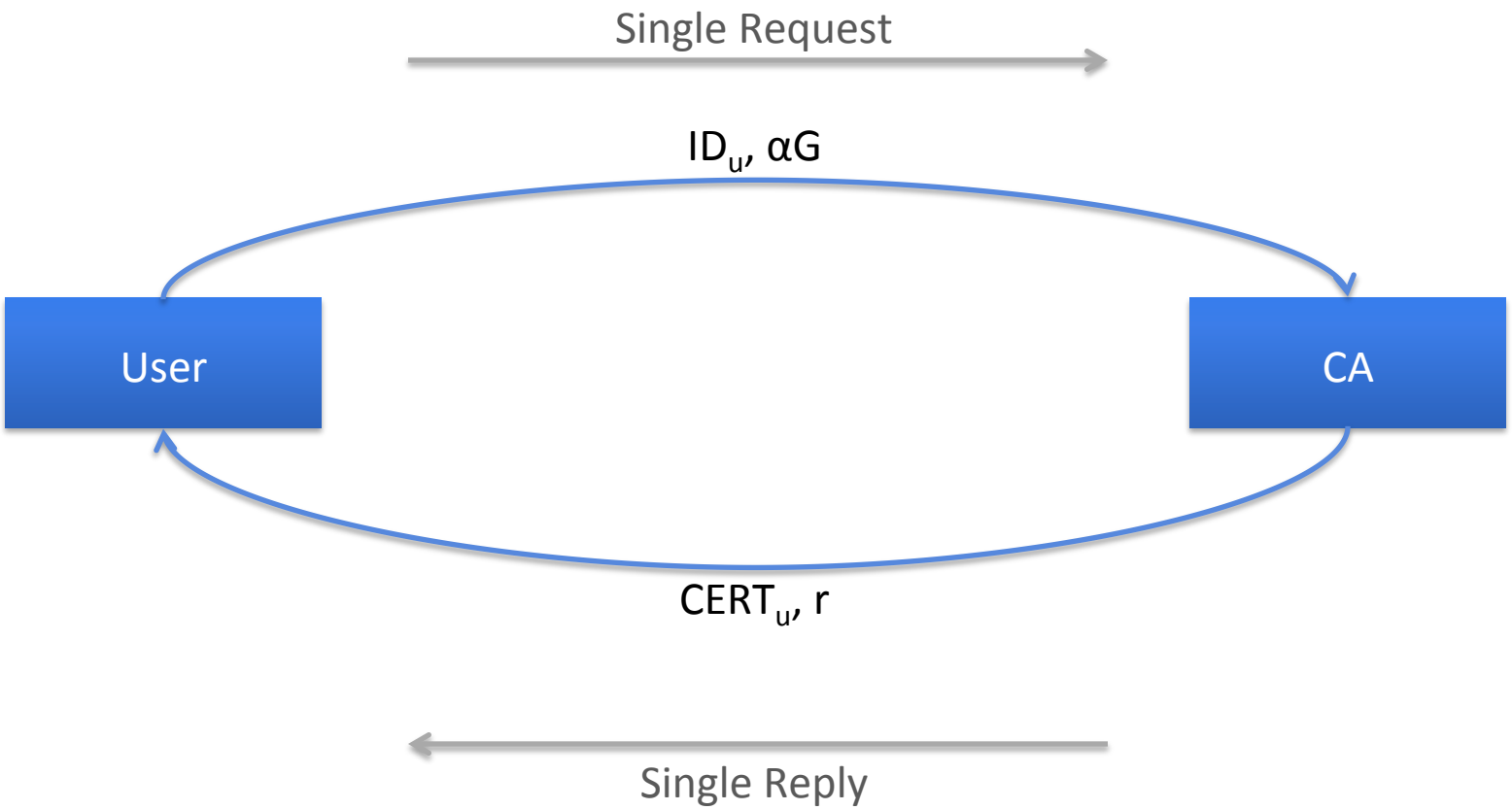
User must know:

Implicit certificate is much smaller: ~90 Bytes

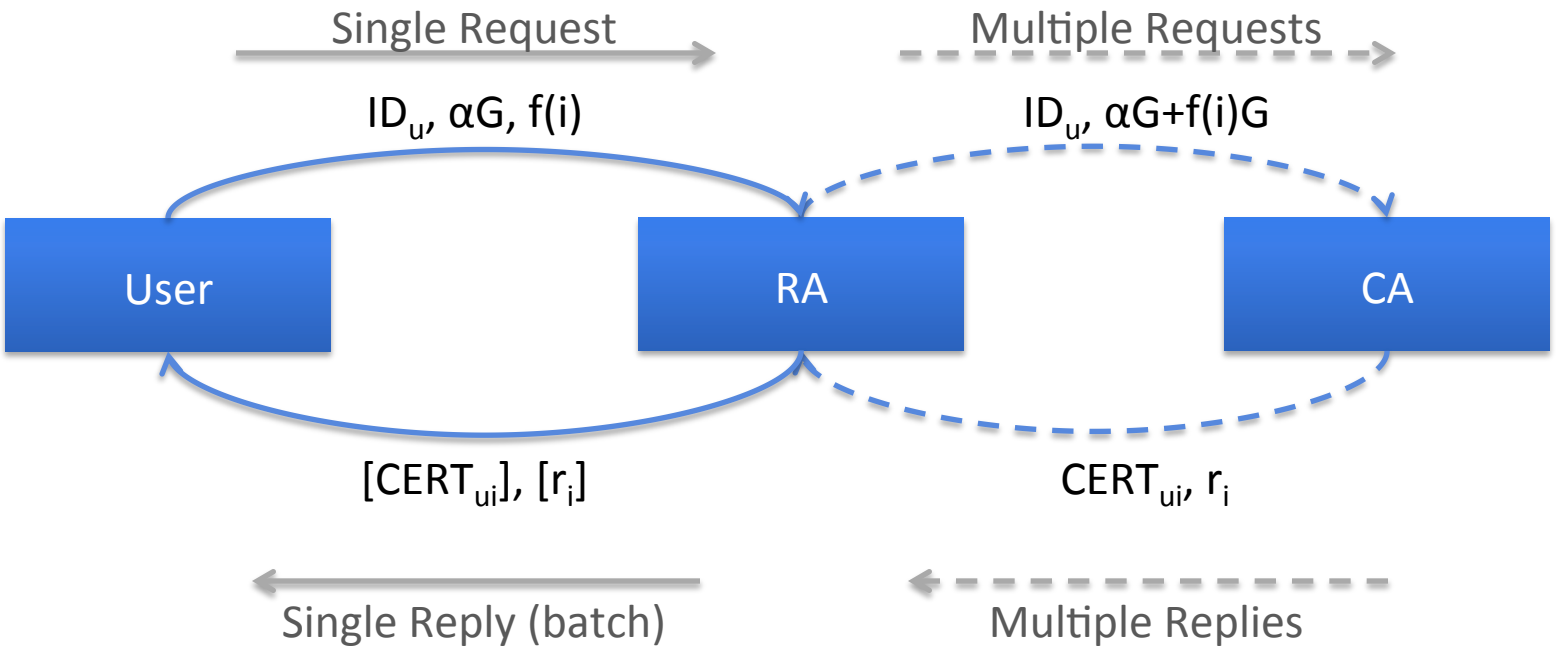


Full details at: https://en.wikipedia.org/wiki/Implicit_certificate

Typical Certificate Request/Response



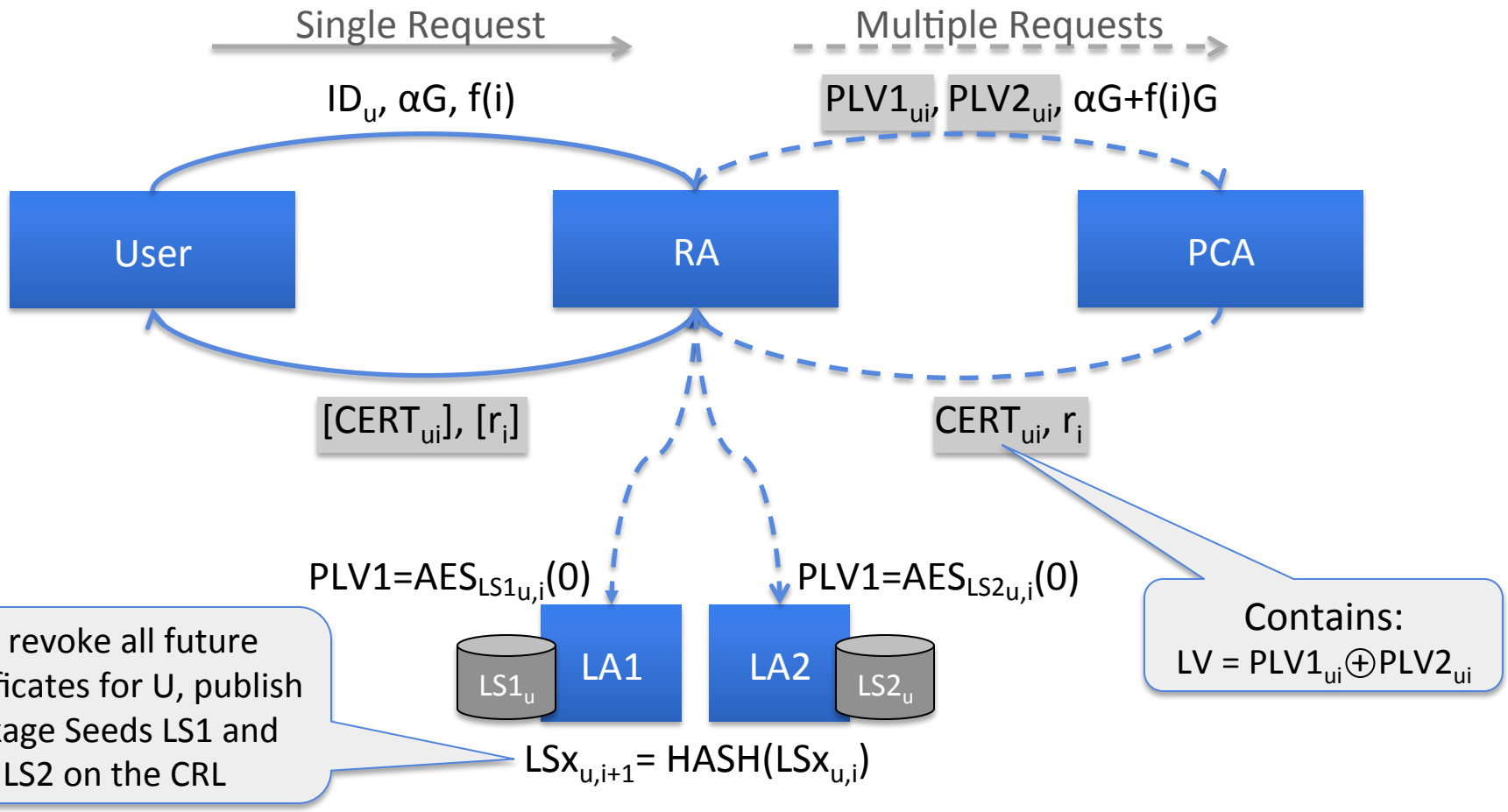
Butterfly Key Expansion



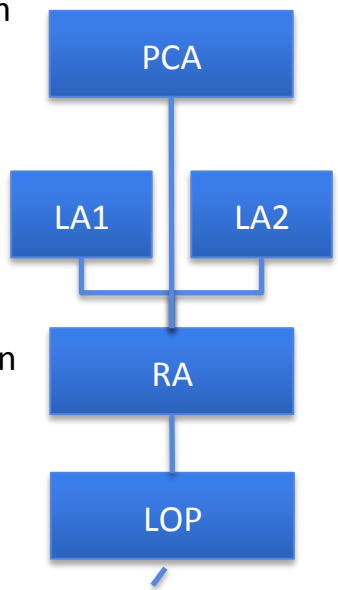
f(i) is an Expansion Function

"A Security Credential Management System for V2V Communications", IEEE Xplore
Whyte, Weimerskirch, Kumar, Hehn
http://www.chesworkshop.org/ches2014/presentations/CHES_2014_Invited.pdf

Pseudonym Certificates



Certificate Issuance



Pseudonym **C**ertificate **A**uthority

Linkage **A**uthority

Registration **A**uthority

Location **O**bscurer **P**roxy

- PCA signs and encrypts individual pseudonym certs
- Certificate includes encrypted LV

- Linkage Authorities provide an encrypted Pre-Linkage Value (PLV) that can link back to the identity of the vehicle (for revocation)

- RA Validates that each vehicle has a valid enrollment cert
- RA breaks apart the batch request, mixes CSRs from multiple cars

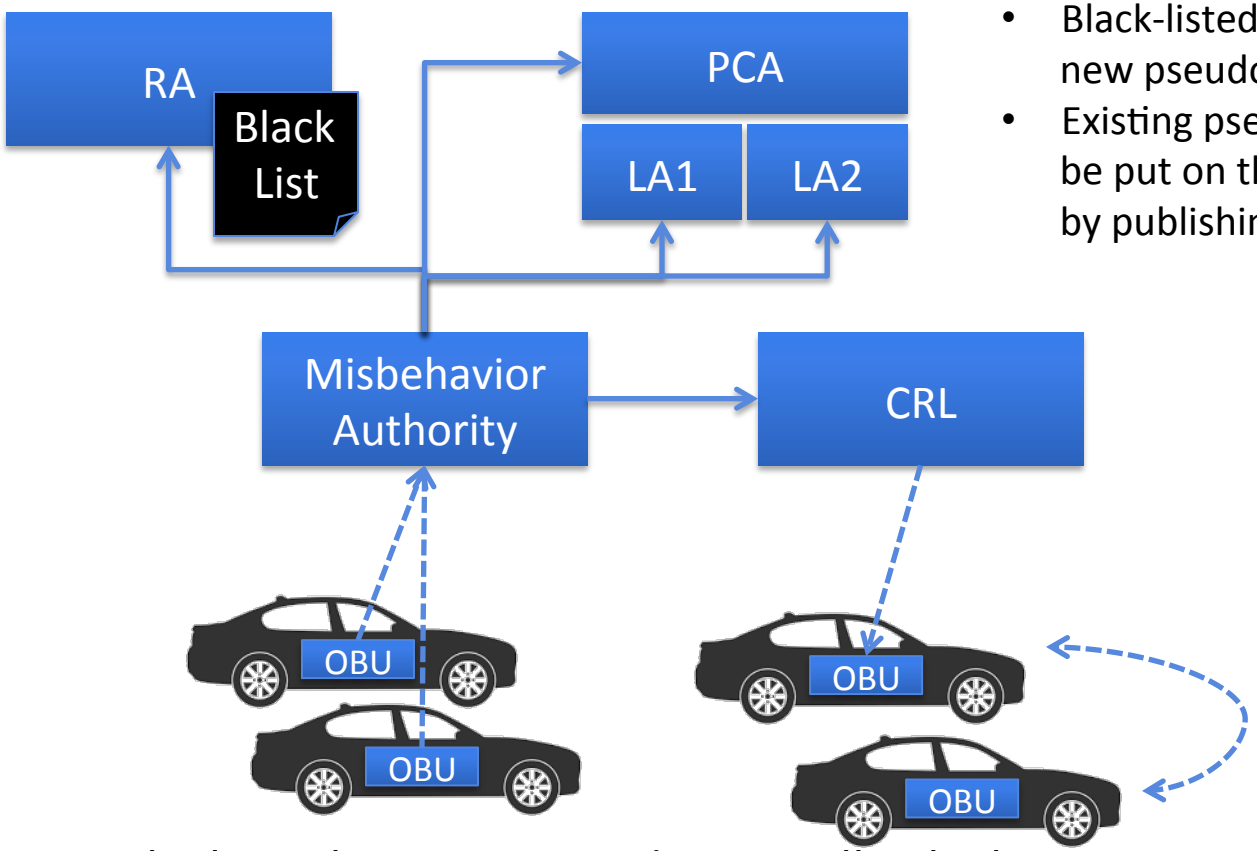
- LOP removes any information about the vehicle network connection that might give away location

Component Knows
Certificate Content Only
Linkage Seed Only
Identity Only
Network Address Only

On **B**oard **U**nit

- Vehicles request a batch of pseudonym certificates (3120 for initial batch)

Misbehavior Detection and Revocation



- Black-listed OBUs can not get new pseudonym certificates
- Existing pseudonym certs can be put on the CRL as a group by publishing the LV

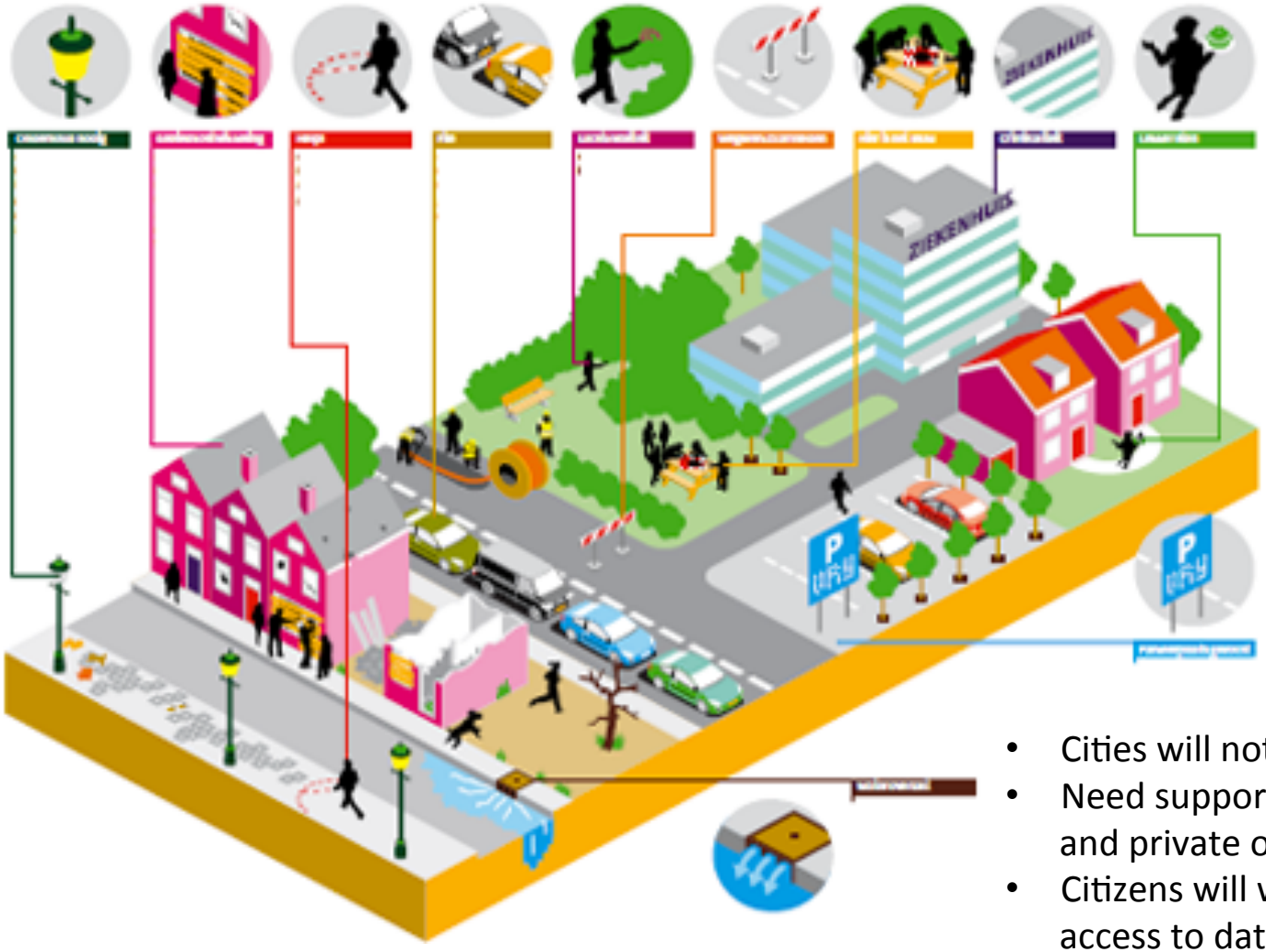
Vehicles submit encrypted misbehavior reports

All vehicles must acquire the latest CRL – download or P2P

Use Case: Opt-In Sensor Networks

- Opt-in sensor networks with trusted but anonymous participants
  - Use any personal device to report “local” metrics
  - Collect “trusted”, anonymous data
  - Commercial fleet operators may choose to participate if the network does not disclose their logistics
  - No need to post-process to “anonymize” data, no threat of server divulging identity
- Enable anonymous access to local data
  - Authorized users can request access to restricted content without divulging their identity

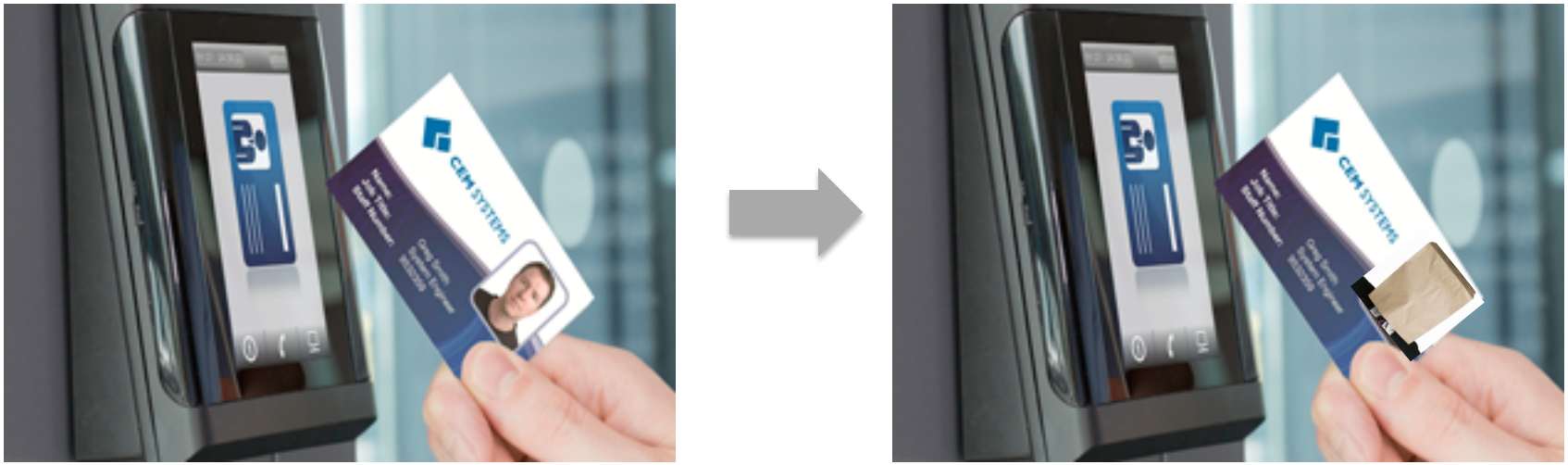
Example: Smart City Integration



- Cities will not own all sensors
- Need support from commercial and private opt-in participants
- Citizens will want anonymous access to data and services

Use Case: Membership Validation

- Pseudonym certificates can have properties that validate membership in a group
  - Requires a large group such that membership does not remove anonymity
  - Repeat visits by the same individual can not be tracked by the access control authority



SCMS Application Parameters

Metric	V2V Value	Notes
i-Period	1 week	Life span for one batch of certificates
Batch Size	20 certificates	Number of simultaneously valid pseudonym certificates
In-Use Period	5 minutes	Each pseudonym certificates is only used for 5 minute intervals
Validity Model	Concurrent	Batch certificates can be sequential or or concurrent
Connectivity Model	Intermittent	The SCMS assumes intermittent network access for all cars, alternative systems may assume reliable connectivity

Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application
http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf

Challenges to Adopting SCMS for IoT

- DSRC (802.11p) is licensed specifically for V2X applications
  - Alternative implementations must choose a communications channel suitable to the application
  - Potential Options:
    - Bluetooth LE in "Advertising" mode
    - UDP broadcast packets over an "open" IP network
- SCMS back-end system is complex and regulated
  - Non-vehicle applications will require an independent instance
  - Groups of applications will require an independent SCMS Manager
  - One SCMS Manager can authorize independent ICAs
- IP Protection
  - Some techniques may require licensing for non-safety applications

Conclusion

- SCMS is an instance of an anonymous authentication solution, specifically designed for V2X
- The system has properties that may be valuable for non-vehicle applications
  - Efficient pseudonym certificates
  - Scalable back-end infrastructure
  - Misbehavior detection and revocation
  - Investments in specialized chipsets and APIs
- One independent SCMS manager could support a variety of anonymous authentication solutions