Security and Privacy
Understanding the Prototype
V2V Safety Security Design

Public Workshop: Enabling a Secure Environment for Vehicle-to-Vehicle and Vehicle-to-Infrastructure Transactions

April 19 – 20, 2012

Tom Schaffnit

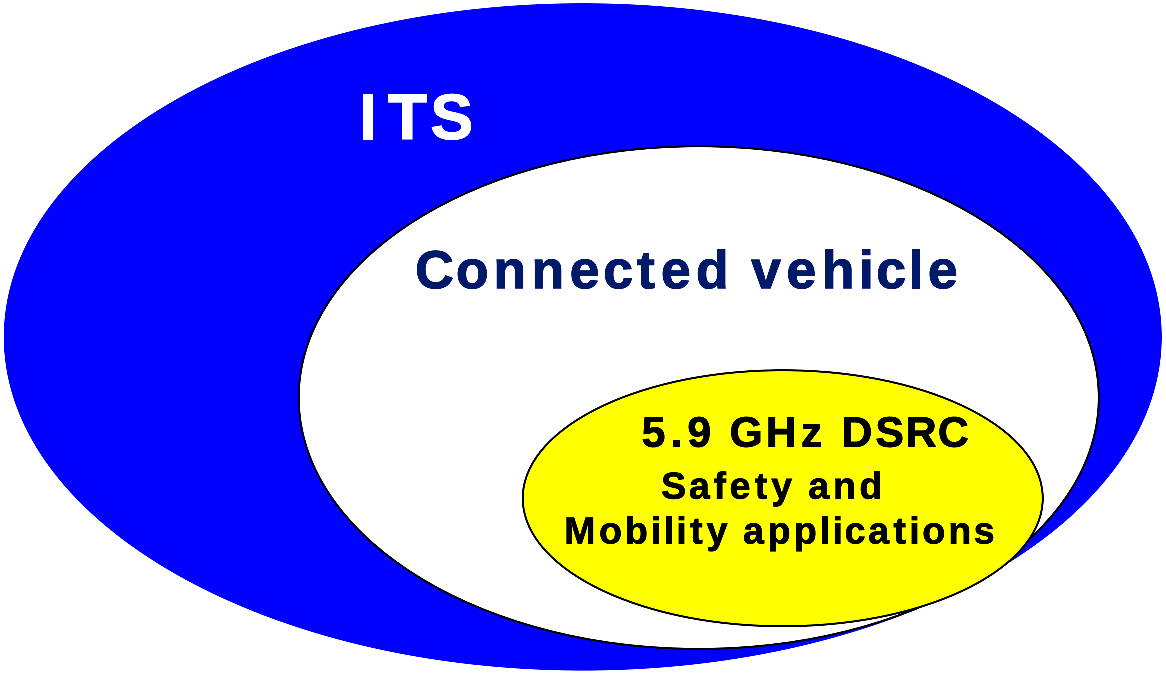
VII Consortium (VIIC) – Who we are

- Industry consortium (Michigan 501 (c6) non-profit) consists of nine light-duty vehicle manufactures.

CHRYSLER
TOYOTA
BMW
Mercedes-Benz
GM
NISSAN
Ford
HONDA

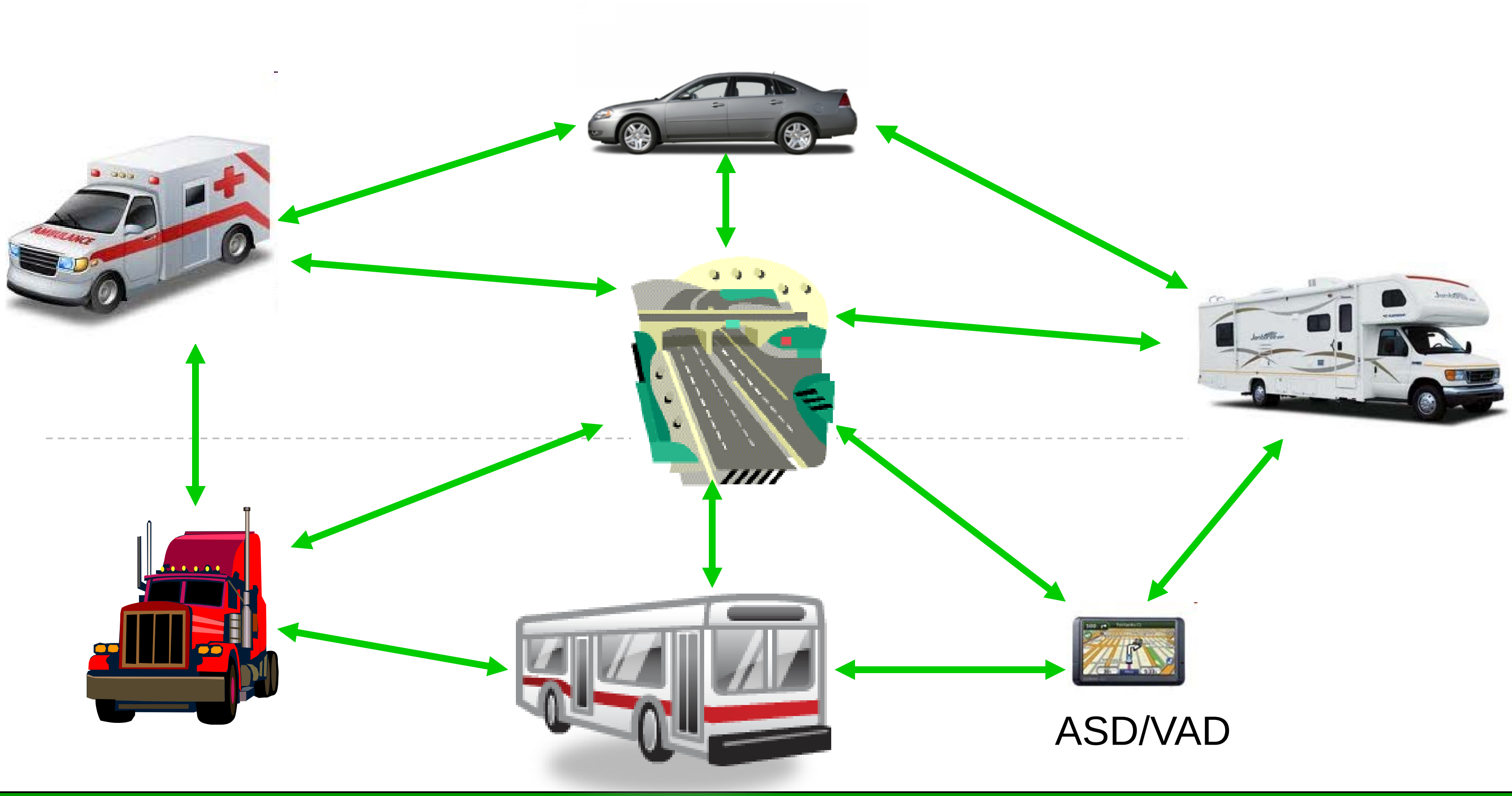
VIIC focus within the Connected Vehicle Initiative

The Connected Vehicle initiative encompasses a wide range of evolving technologies developed by many government, industry, and academic partners. The VIIC is primarily focused on <u>deployment</u> of cooperative safety and mobility applications based on 5.9 GHz DSRC

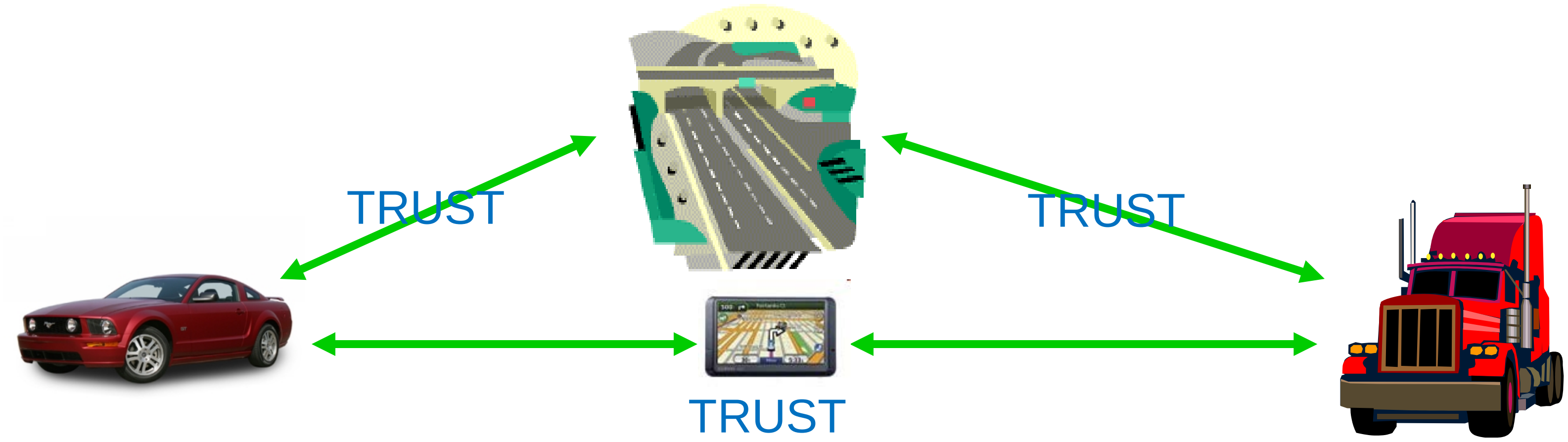


Vehicle Connectivity

DSRC communications among vehicles, devices and roadways



Key Enabler – Security



Messages to/from other vehicles, devices and the Infrastructure must be trustworthy

- Autonomous vehicle safety applications depend upon sensor data from within the same vehicle
- Cooperative safety and mobility applications depend upon data from other vehicles, other off-board devices and from the infrastructure
- This data must be trustworthy in order for a cooperative system to work

Why We Need Security

The receiver of a message is not able to determine, without additional mechanisms, whether

- ➢ a message originates from a trustworthy and legitimate device, and whether
- ➢ the message was modified between sender and receiver

Devices found to be transmitting “bad” messages need to be removed from the system until repaired or replaced:

- ➢ defective devices
- ➢ hacked devices

VIIC Policy Goals for V2V Security

- Anonymity for mandatory services
- Non-Trackability for mandatory services
- Protection from Attacks on System Integrity
- Prevention of Unauthorized Access to Personally Identifiable Information (PII)
- No User Fees for mandatory services
- Stable, Long-term Policy and Technology with backward compatibility (decades rather than years)

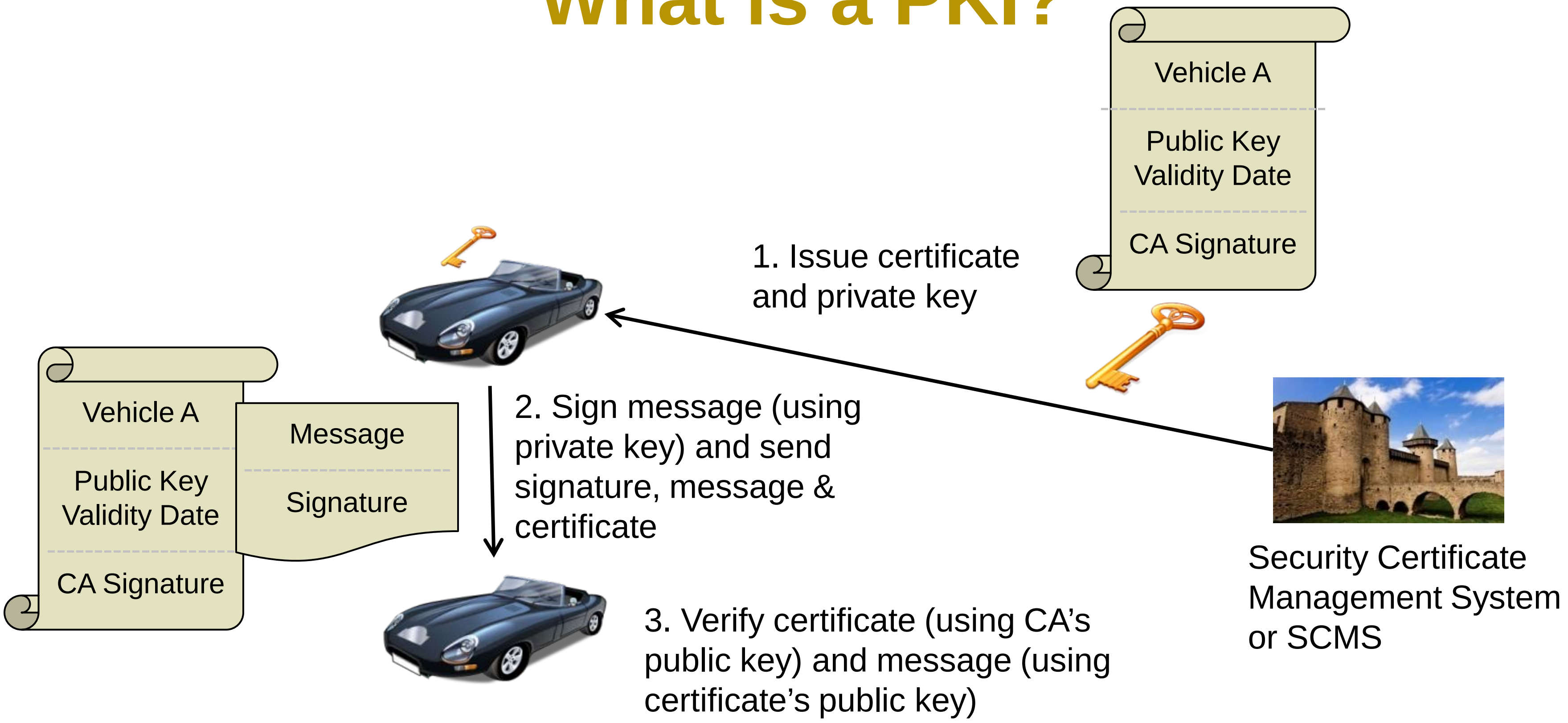
Security System Scope & Limitations

The following slides describe a prototype security system designed by the Crash Avoidance Metrics Partnership (CAMP) Vehicle Safety Communications 3 Consortium as part of cooperative projects with the USDOT for V2V safety applications:

- ➢It has not been designed for nor has it been analyzed for applicability to V2I safety applications or non-safety applications that are part of the wider connected vehicle and infrastructure deployment scenario

- ➢Additional security requirements for full deployment need to be analyzed and developed

What is a PKI?



Vehicle A

Public Key
Validity Date

CA Signature

1. Issue certificate and private key

Vehicle A

Public Key
Validity Date

CA Signature

Message

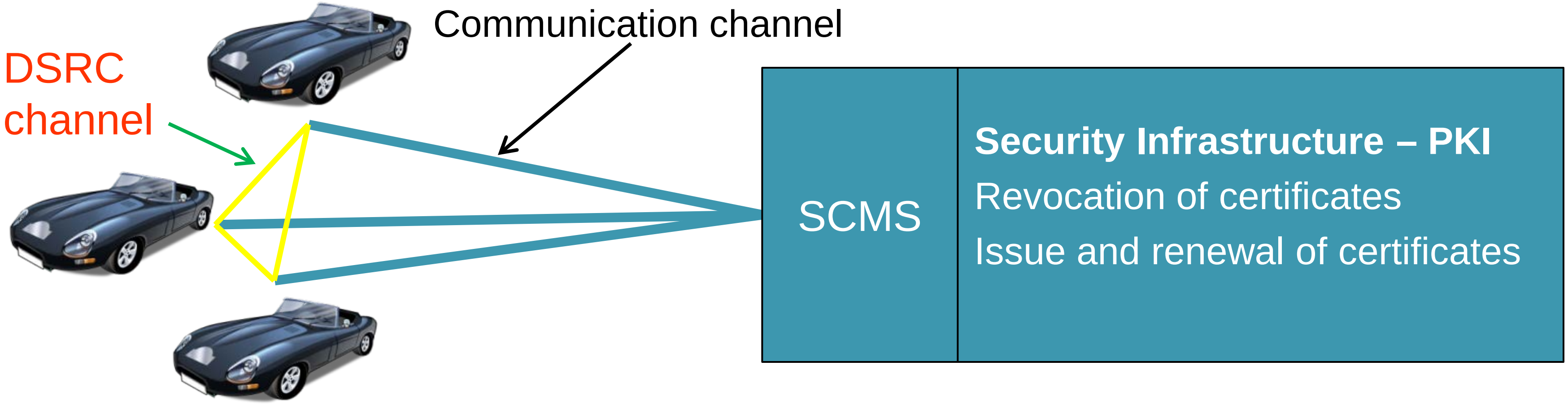
Signature

2. Sign message (using private key) and send signature, message & certificate

3. Verify certificate (using CA's public key) and message (using certificate's public key)

Security Certificate Management System or SCMS

Analysis of PKI



Security Infrastructure – PKI

Revocation of certificates

Issue and renewal of certificates

- Communication Channel from Vehicles *to* SCMS
  - Goal: Report Certificates That Are Being Used to Send ‘Bad’ Messages (Bad Sensor Data or Malicious Data)
- Communication Channel *from* SCMS to Vehicles
  - Goal: Update Vehicles with New Certificate Revocation List
  - Goal: Issue New Certificates

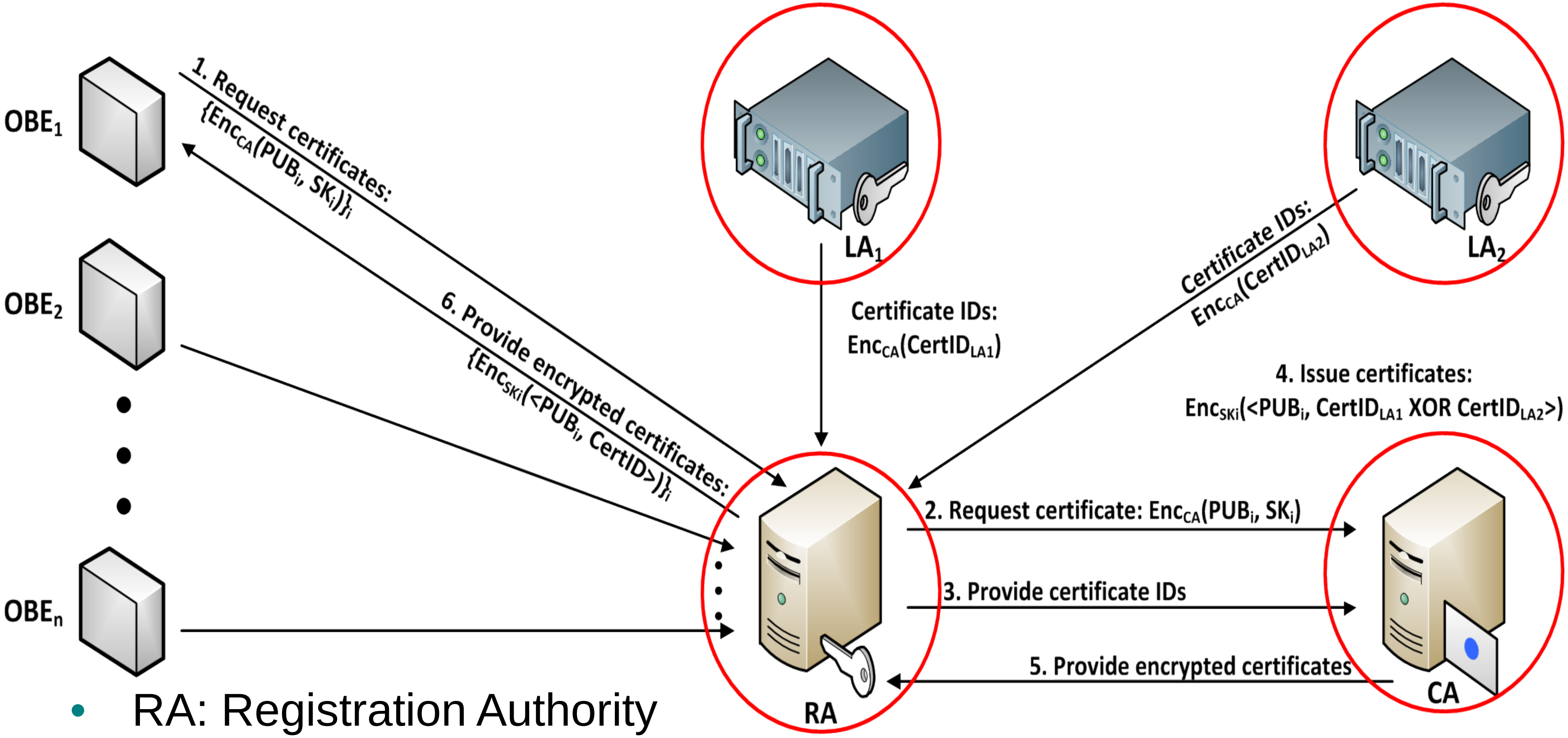
Security Design Balance

Safety

Privacy

Security

Split SCMS Overview



OBE$_1$
OBE$_2$
OBE$_n$
1. Request certificates: $\{Enc_{CA}(PUB_i, SK_i)\}_i$
6. Provide encrypted certificates: $\{Enc_{SKi}(<PUB_i, CertID>)\}_i$
LA$_1$
LA$_2$
Certificate IDs: $Enc_{CA}(CertID_{LA1})$
Certificate IDs: $Enc_{CA}(CertID_{LA2})$
4. Issue certificates: $Enc_{SKi}(<PUB_i, CertID_{LA1}$ XOR $CertID_{LA2}>)$
2. Request certificate: $Enc_{CA}(PUB_i, SK_i)$
3. Provide certificate IDs
5. Provide encrypted certificates
RA
CA

- RA: Registration Authority
- CA: Certificate Authority
- LA: Linkage Authority

Issuing Certificates: RA & CA

- RA is the point of contact for an OBE
- RA shuffles OBE’s requests (over all OBEs and all requests)
- CA issues certificates

Efficient Revocation: LAs

- Each OBE will receive thousands of certificates per year
  - Traditional revocation (include each certificate identifier in CRL) impossible: huge CRLs
- Include a “Linkage ID” in each certificate
  - Basically an decrypted identifier
  - To revoke: include decryption key on CRL
  - Smart design: publishing decryption key on CRL allows OBEs to derive any future Linkage ID but no past Linkage ID

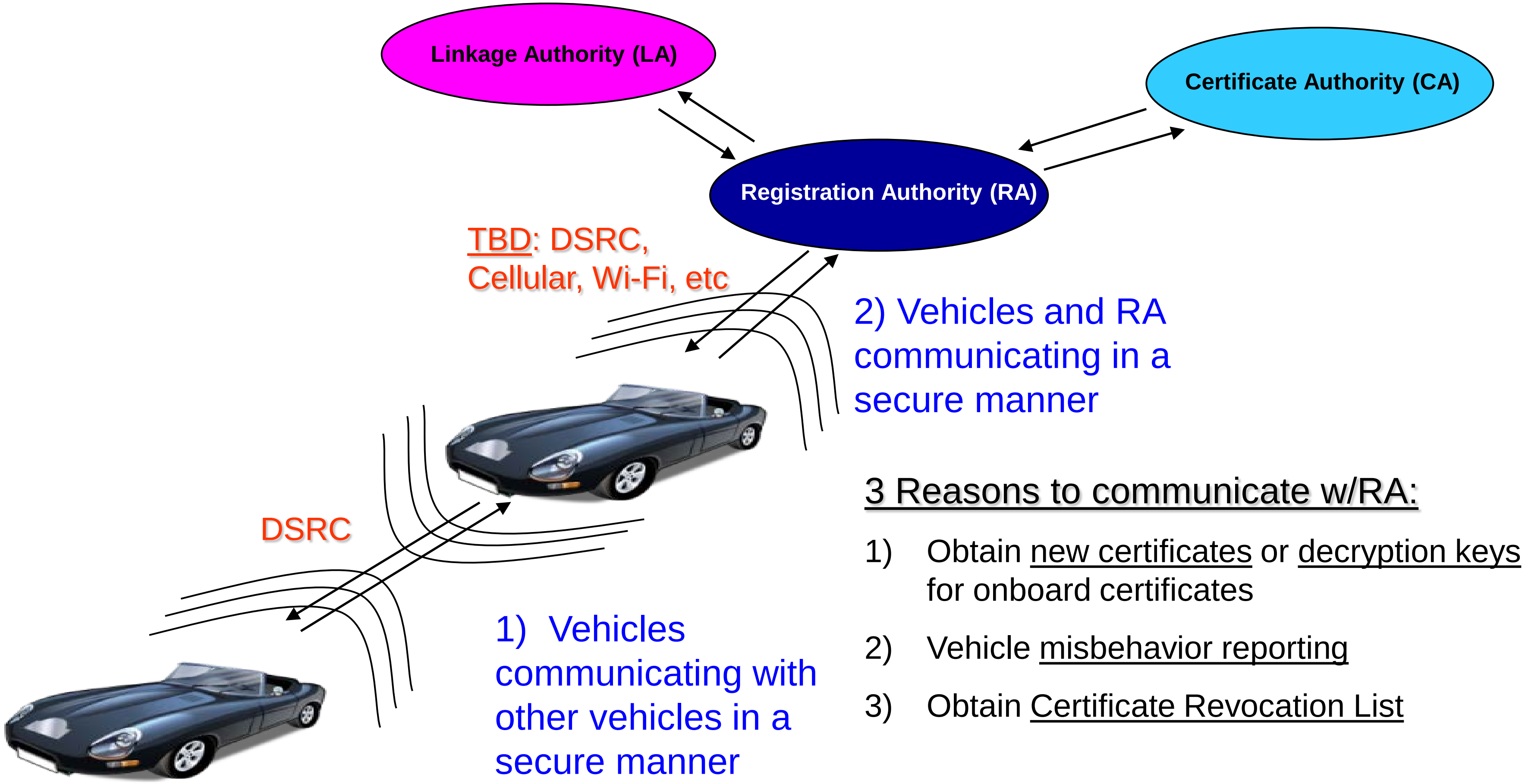
Split Certificate Management Authority

- RA(s) *knows who requested certificates*, but does not know *what* is in the certificates

- CA *knows certificate content*, but does not know *who* requested certificates

- LA(s) *knows the linkage IDs*, but does not know *who* requested the certificates

Communication Mechanisms for the Connected Vehicle System



Linkage Authority (LA)

Certificate Authority (CA)

Registration Authority (RA)

TBD: DSRC, Cellular, Wi-Fi, etc

DSRC

2) Vehicles and RA communicating in a secure manner

1) Vehicles communicating with other vehicles in a secure manner

3 Reasons to communicate w/RA:

1) Obtain new certificates or decryption keys for onboard certificates
2) Vehicle misbehavior reporting
3) Obtain Certificate Revocation List

Key Questions for Further Study

Can a V2V security solution for a mandated system with no reliance on public funding be identified that:

- Meets the technical requirements,
- Meets the policy goals to an acceptable degree, and
- Has a viable business case

➢ For communication networks, further study will consider:

Cellular

DSRC

Other potential networks that are identified

Potential combinations of two or more networks

➢ And other policy issues, such as governance, privacy, liability, etc.

Thank You