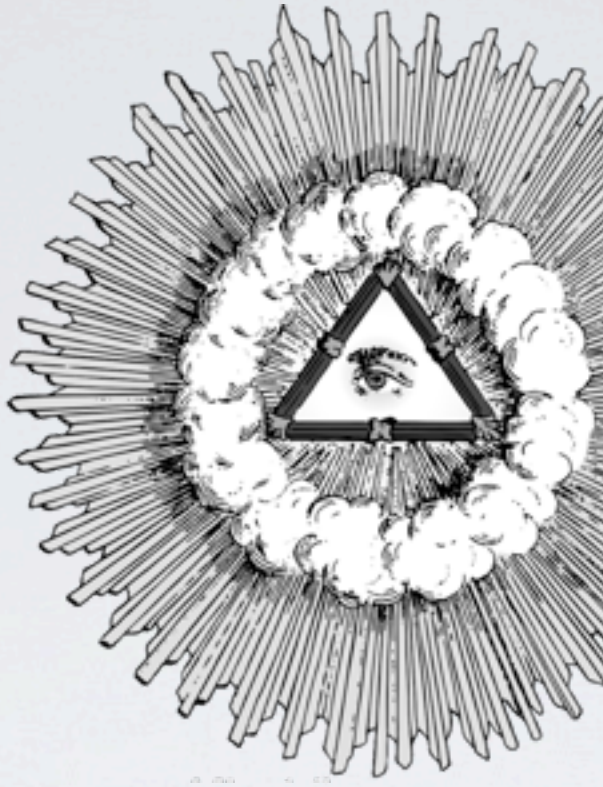


PRIVACY AND THE CAR OF THE FUTURE

Consideration for the coming connected vehicle

whoami

- BSEE, digital communications
- Many years as a network engineer
- Santa Clara University Law student
- Research assistant providing technical expertise on privacy audits and reviews
- Contracted by auto consortium to review privacy of proposed vehicle to vehicle safety network

STANDARD DISCLAIMER

IANAL (Yet)

But if you know anyone looking for summer interns....

NON-STANDARD DISCLAIMER

A current NDA covers some of my work here (but not very much)
The focus will be on published information and standards.

WHAT IS THIS PROJECT?

- DSRC: Digital Short Range Communications
  - (Where “short” == 380m)
- Vehicle to Vehicle
- Vehicle to infrastructure in Europe
  - Not having to wait for a light on an empty street again.

WHY IS IT BEING DEVELOPED?

Photo Credit: Jason Edward Scott Bain

Safety

NON-TRIVIAL IMPACT ON AUTO DEATHS

- World Health Organization estimates 25% of vehicle deaths each year can be prevented.
- Fatigue and distracted driving accidents reduced.
- Blind Corners, fog and limited visibility accidents reduced.

Photo: Public Domain

WILL THIS REALLY HAPPEN?

IT ALREADY IS

HOW SOON?

- Hardware is already being shipped.
- Some software issues still in the air
- The US Dept. of Transportation is considering mandating this for all new cars. (Decision to come later this year.)
- German government is considering infrastructure.

WHAT IS DSRC

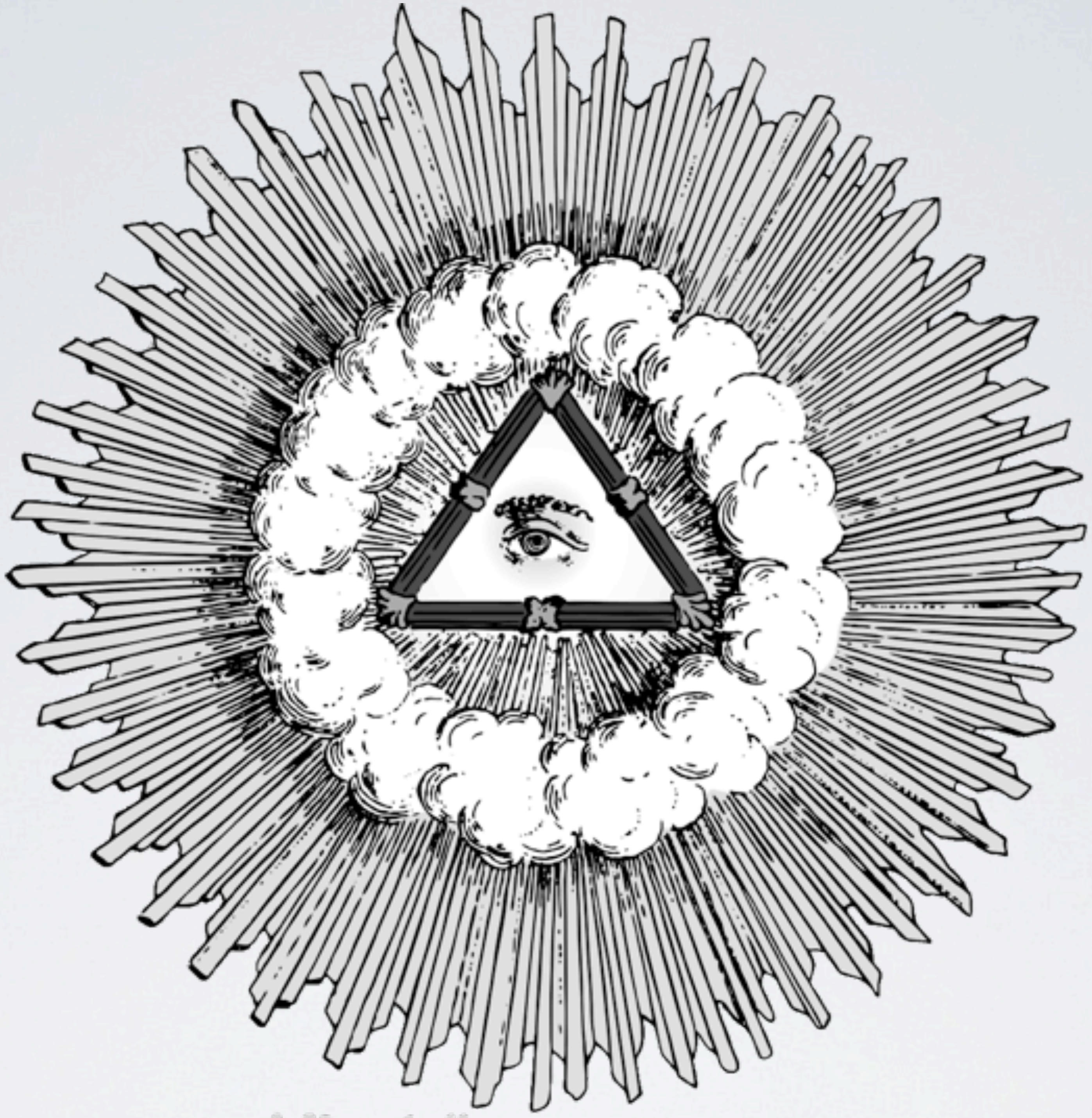
- Basic safety messages sent out every 10 seconds.
- All message carry a standard glob: values for pre-defined vehicle trajectory and operational data.
- Cars process data and warn driver.

Photo Credit: US Dept. of Transportation

WHAT DSRC IS NOT

Photo Credit: US Dept. of Transportation

- CANbus
- OnStar (or any other remote service)
- (Direct) support for autonomous driving *mechanisms*.



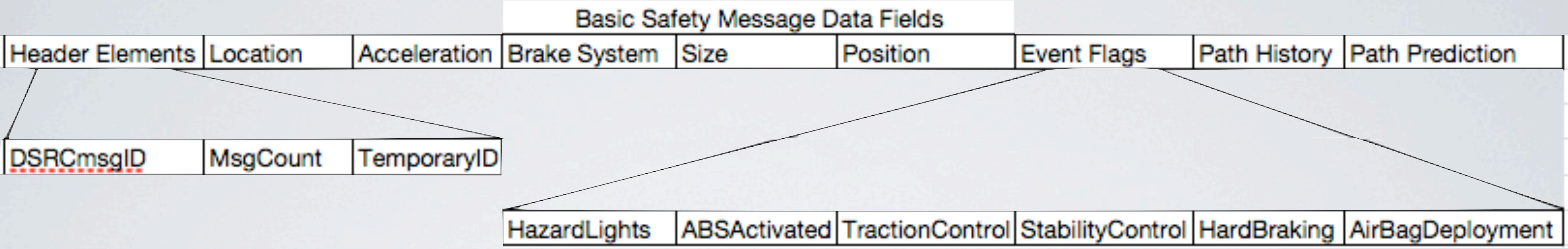
TECHNICAL DETAILS

RADIO PROTOCOL

- 5.9GHz reserved in US and Europe
- Signaling standard: IEEE 802.11p
- Similar to "slotted aloha"
- All zero <u>source</u> address for vehicles

Photo Credit: NASA

BASIC SAFETY MESSAGE



Basic Safety Message Data Fields

Header Elements	Location	Acceleration	Brake System	Size	Position	Event Flags	Path History	Path Prediction

DSRCmsgID	MsgCount	TemporaryID

HazardLights	ABSActivated	TractionControl	StabilityControl	HardBraking	AirBagDeployment

- Standard: SAE J2735
- ~50 fixed data elements
- “only” interface to radio

PARAMETERS FOR EFFECTIVENESS

- Density
  - Benefit derived from other vehicles' use
  - Greater usage means greater effectiveness
- Confidence
  - Most messages must be trustworthy
  - People must trust information broadcast

VALIDITY?

- All messages are cryptographically signed
- Signing certificates issued by central authority
- Issued based on system fingerprint
- Revocation for "malfunctioning" equipment
- System should invalidate itself if internal checks fail

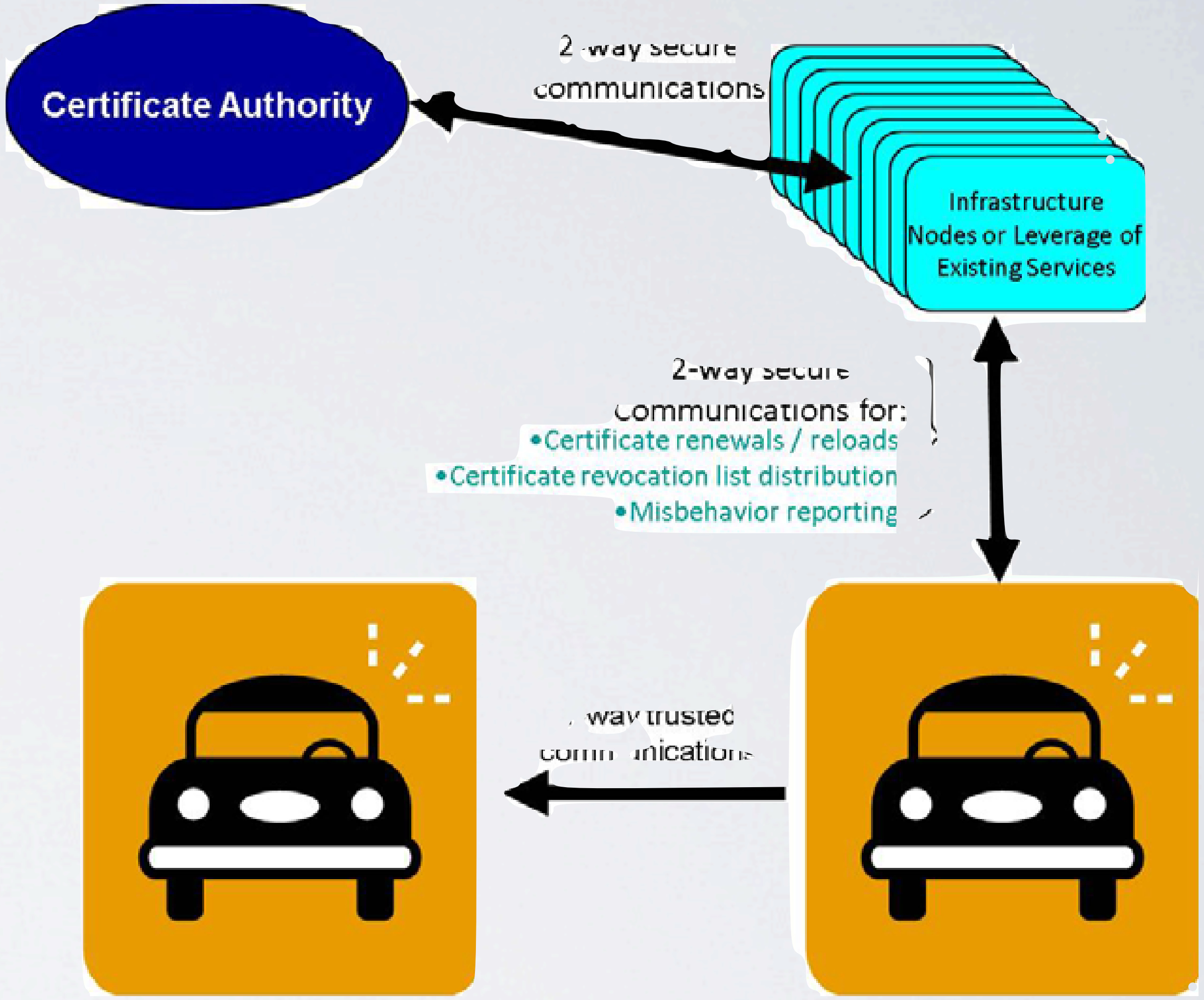
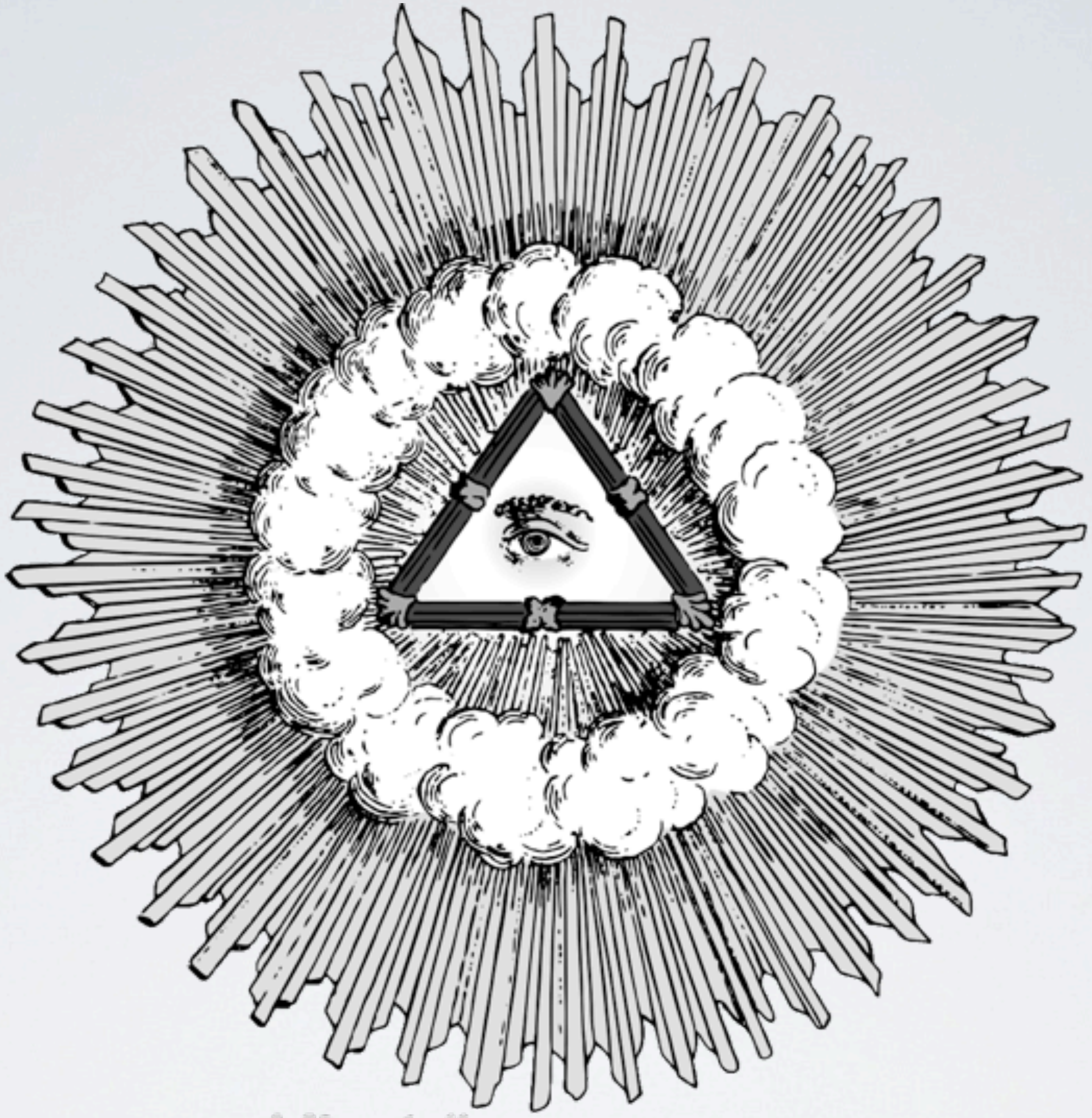

Certificate Authority
2-way secure communications
Infrastructure Nodes or Leverage of Existing Services
2-way secure communications for:
•Certificate renewals / reloads
•Certificate revocation list distribution
•Misbehavior reporting
way trusted comm inications

Image source: US Dept. of Transportation

CERTIFICATES

- Limited time use to prevent tracking
  - Reused?
- Periodically refreshed (and malefactors reported)
  - How often?
- Permanent blacklist



PRIVACY?

EXAMPLE: LAW ENFORCEMENT

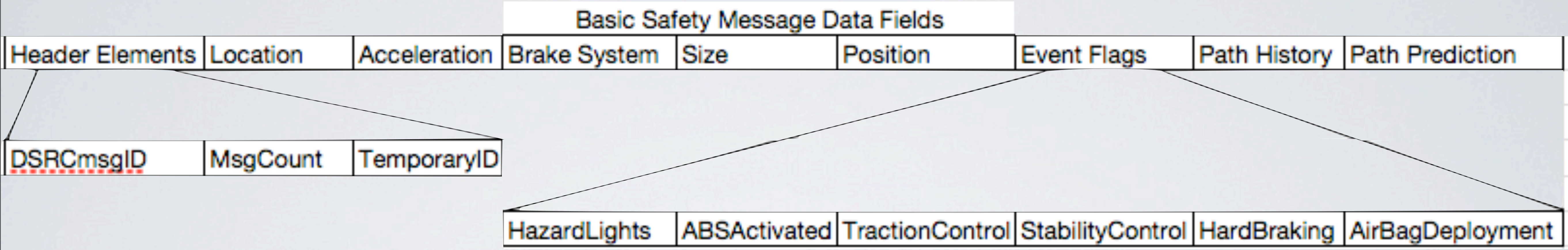
- What can they do with this?
- Correlate location, speed to independent identification? (cameras?)

Photo Credit: Alex E. Proimos

MAC LAYER

- All zero source (for vehicles) / no destination
- Unrouteable!
- No significant privacy concern *as is*.
- Any algorithm to make network routeable will make vehicles trackable.

BSM



Basic Safety Message Data Fields

Header Elements	Location	Acceleration	Brake System	Size	Position	Event Flags	Path History	Path Prediction

DSRCmsgID	MsgCount	TemporaryID

HazardLights	ABSActivated	TractionControl	StabilityControl	HardBraking	AirBagDeployment

- “Temporary” ID could become persistent with bad app
- Open source apps suggested for processing and acting on message data
- Is this the only thing the unit will transmit?

CERTIFICATES

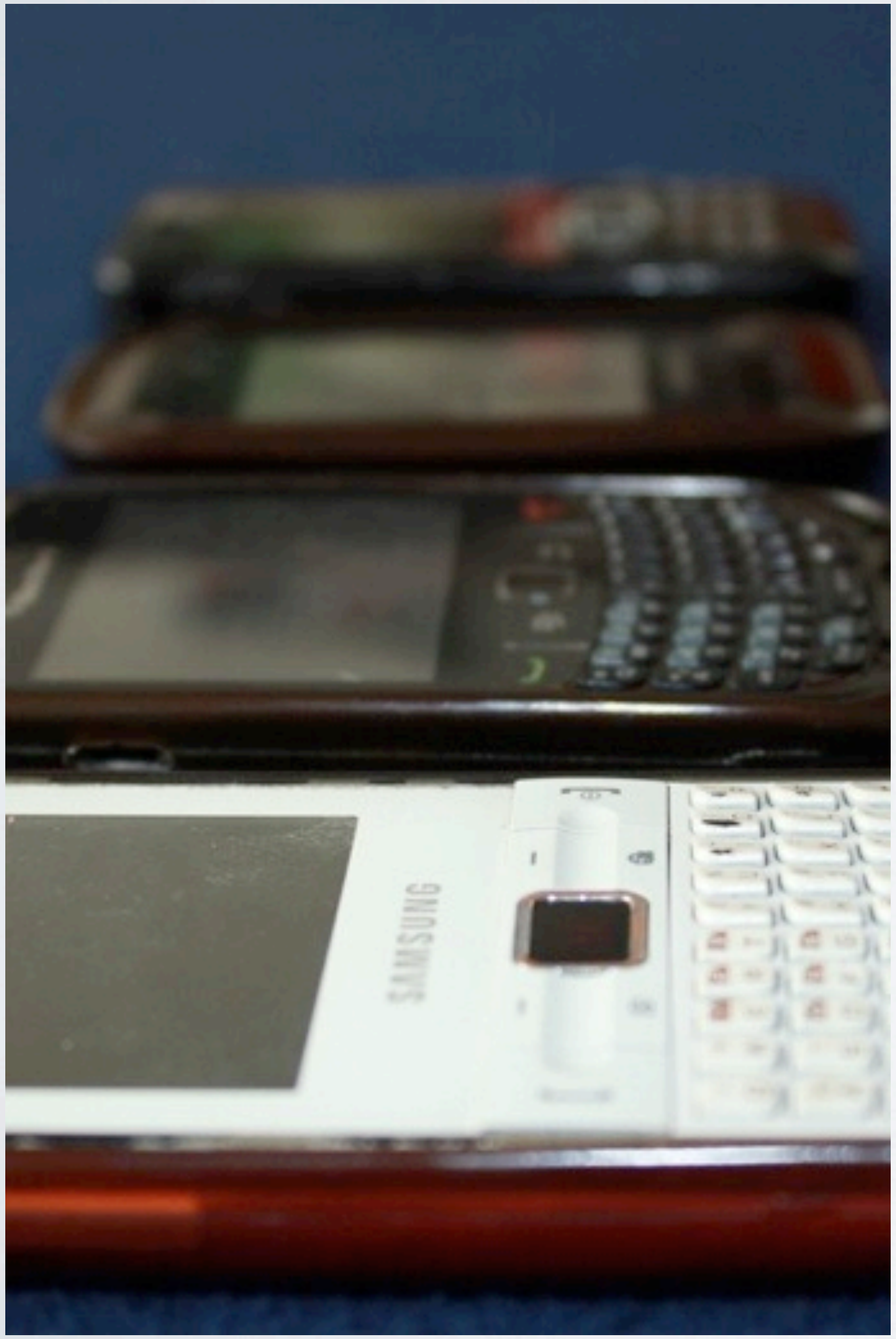
- Identity/Validity conflict
  - Solution: constantly changing certificates
  - Revocation by fingerprint
- Issuing authority?

FINGERPRINTS

- "No" correspondence between fingerprint and car
- "hard coded" into device
- If revoked, entire unit must be replaced to function

Photo Credit: NIST

CERTIFICATE DELIVERY



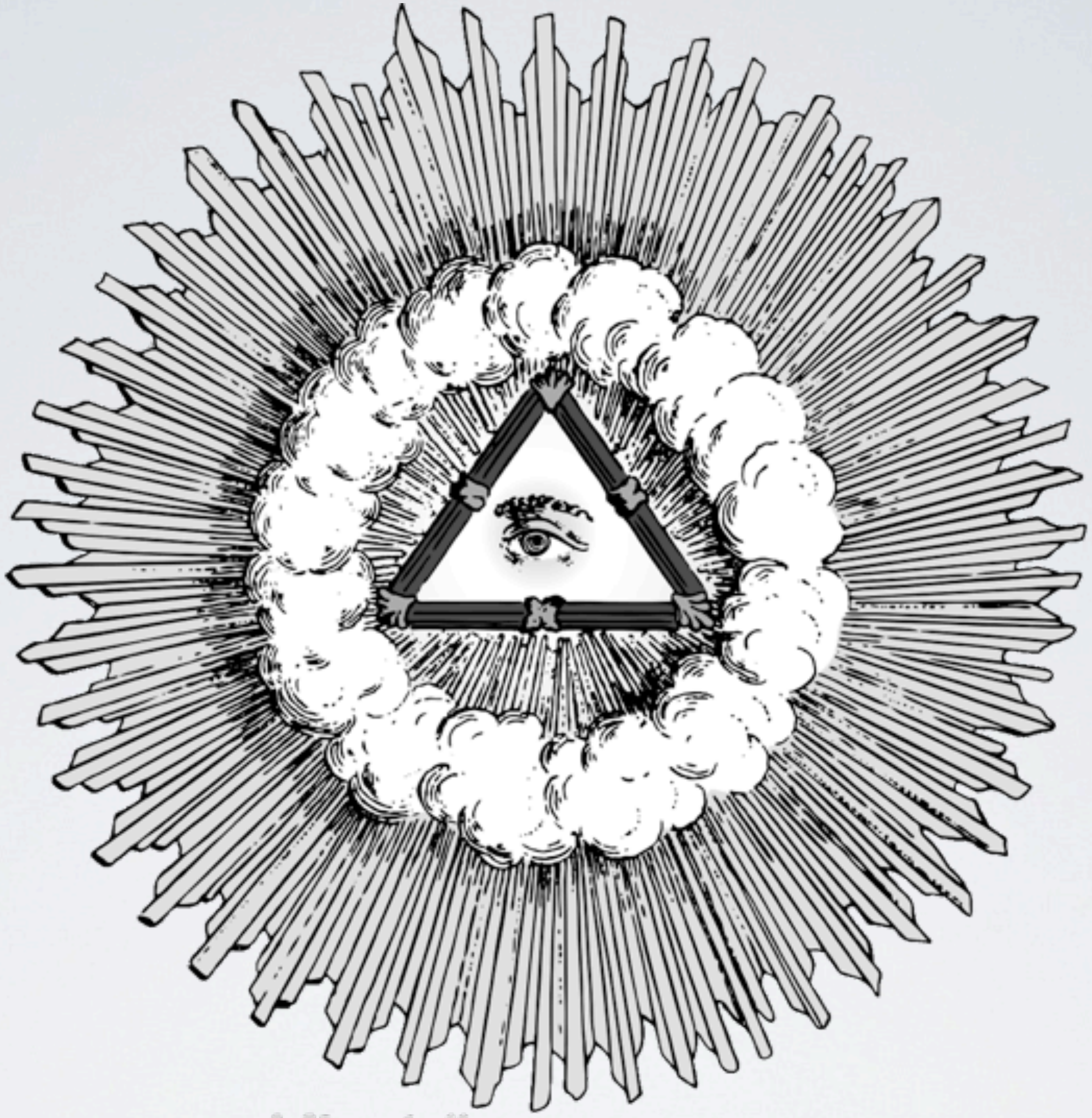
- Haven't figured out how certificates are delivered to vehicle
- Proposals include cellular, wifi, infrastructure links
- So many opportunities for failure

WORRISOME NOISE

- Manufacturers using this system for commercial applications
- Advertising and other "fund raising" schemes
- Fixed infrastructure potentially operated by data brokers

WHAT YOU CAN DO

- Hack the radios
  - Commercially available now
- Hack the protocols
- Become politically engaged
  - Most decisions are not being made by elected officials
  - Help them find a way to fund it without selling out!



THANK YOU

ACKNOWLEDGEMENTS

- Professor Dorothy Glancy, who requested my help on this project
- DC 650 (especially Charles Blas) who gave me a reality check with current security and privacy capabilities

CONTACT

- Christie Dudley
- @longobord
- c.dudley@ieee.org

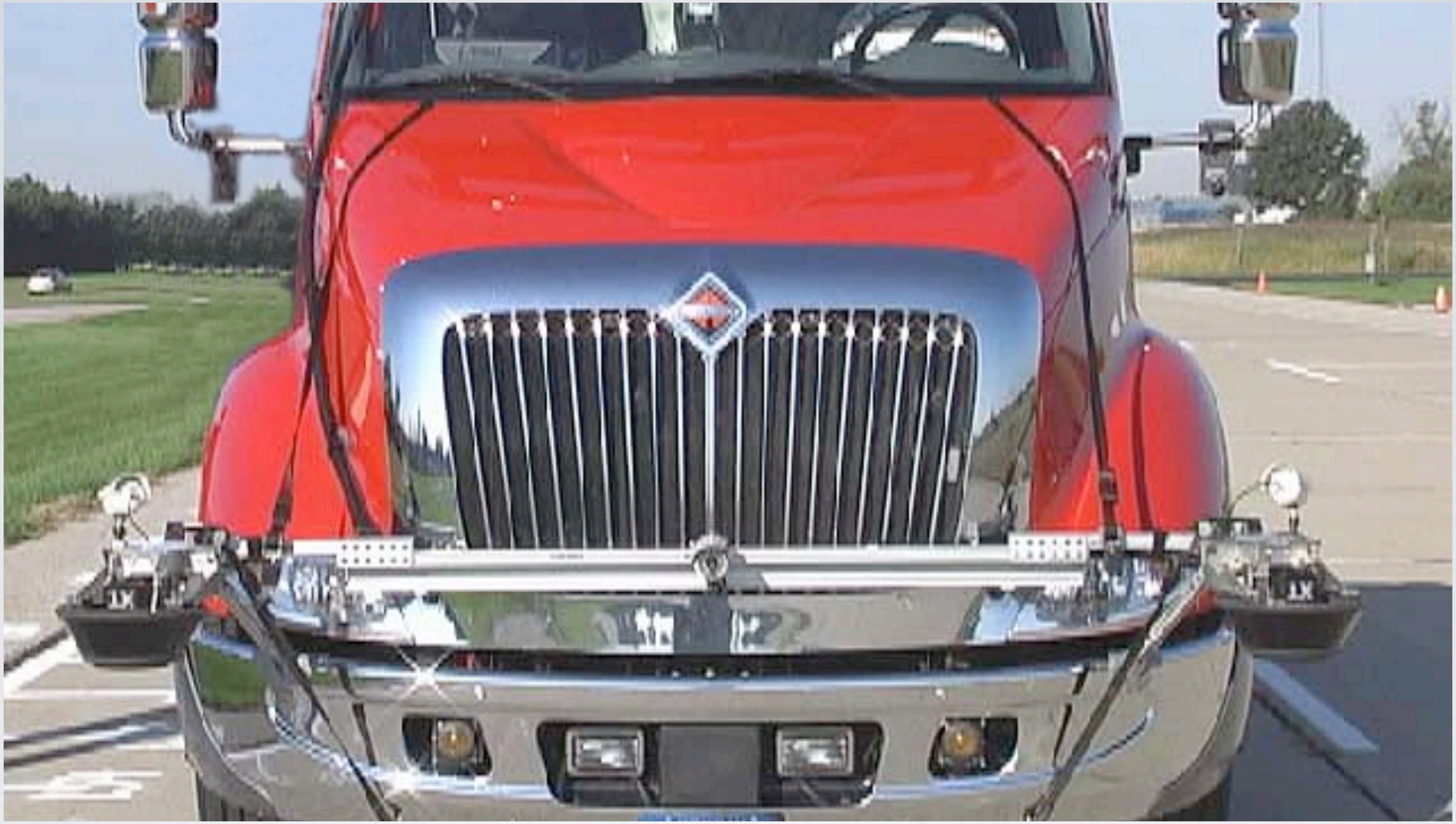


Photo Credit: NIST

AFTERMARKET INSTALLATION

A little cumbersome