STANDARDS ITS TRAINING

WELCOME

U.S. Department of Transportation

Office of the Assistant Secretary for
Research and Technology

Welcome

Ken Leonard, Director
ITS Joint Program Office
Ken.Leonard@dot.gov

www.pcb.its.dot.gov

Module CSE 201:

Introduction to Security Credential Management System (SCMS) Part 1 of 2

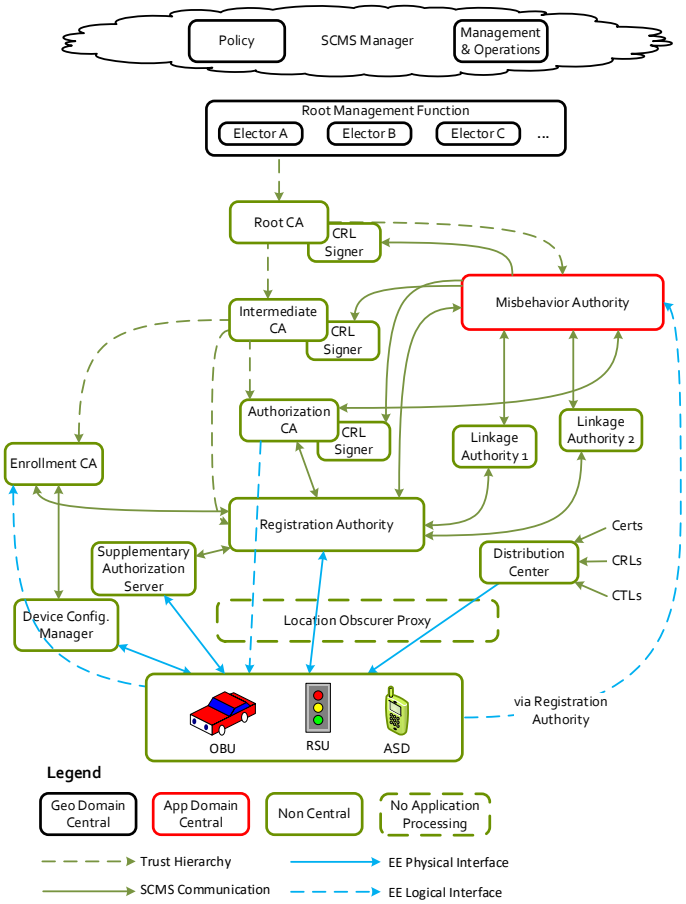


Image source: IEEE P1609.2.1

Instructors

Dr. William Whyte

Senior Director, Technical Standards

Qualcomm Technologies, Inc.

Dr. Virendra Kumar

Senior Staff Engineer, Technical Standards

Qualcomm Technologies, Inc.

Learning Objectives

Define communications security requirements in the Connected Vehicle (CV) environment

Describe how the Security Credential Management System (SCMS) uses cryptographic building blocks to provide trust

Understand how to get devices interacting with the SCMS in a deployment

Identify the Vehicle-to-Everything (V2X) certification process for a device to enroll in the SCMS

Illustrate how to make a deployment plan that uses SCMS services

Learning Objectives - Part 1 of 2

Define communications security requirements in the Connected Vehicle (CV) environment

Describe how the Security Credential Management System (SCMS) uses cryptographic building blocks to provide trust

Understand how to get devices interacting with the SCMS in a deployment

Learning Objective 1

Define communications security requirements in the Connected Vehicle (CV) environment

Security of deployments and the role the SCMS plays in that security

- The security of Connected Vehicle deployments depends on the security of many different aspects of the system
  - Support networks must be secure against cyber attack
  - Stored data must be managed in an appropriate way with suitable access control
  - Each individual component or subsystem within the overall system must also be secure
  - Communications between components must be secure
- The SCMS helps with
  - Communications security – by providing certificates that allow devices to communicate securely
  - Security of individual components – by checking that certificates are only provided to components that are secure
- Having access to an SCMS is a vital part of a secure deployment, but other security issues must also be addressed
  - See CSE202, Cybersecurity!

Need for Trust

- Electronic communications can be intercepted, read, and altered
- Secure communications mechanisms allow us to protect against this
- Cryptographic algorithms are mechanisms we use to meet security goals for protecting data in transit
- These goals are:
  - Confidentiality
  - Integrity
  - Authenticity

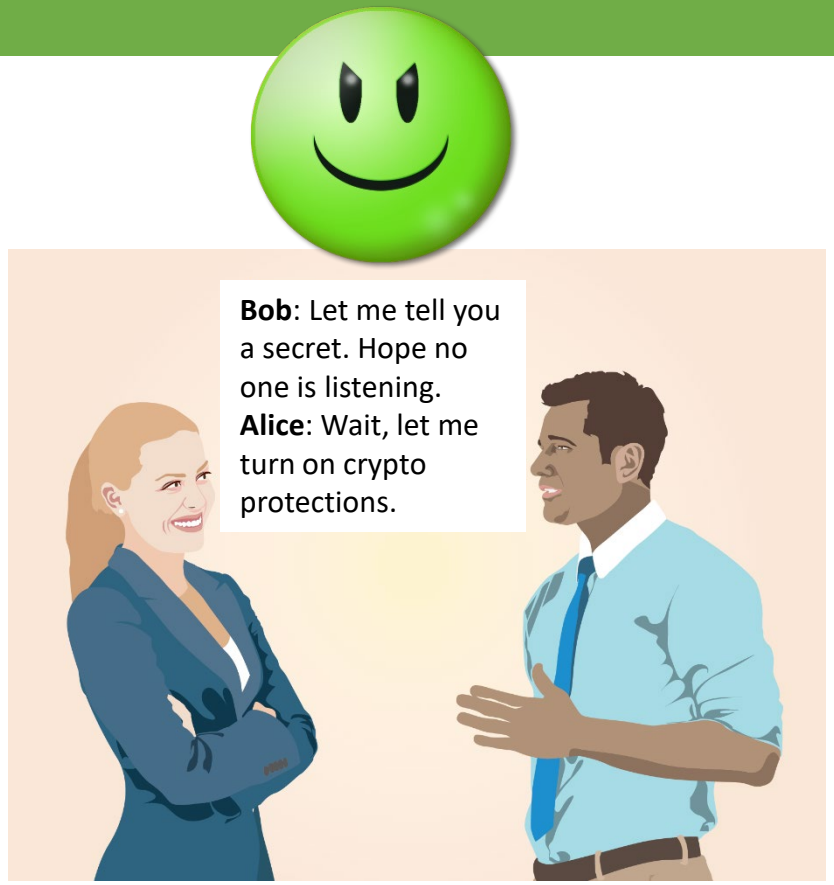


Image source: USDOT

Need for Trust contd.

- With the security mechanisms, the receiver can trust that
  - The message received is the same as the message sent
  - The sender was legitimate
  - The message has not been read by anyone who shouldn't read it
- Without trust, there would be no point sending messages
  - Receivers could not be sure they were correct
  - The system could be flooded with false messages
  - Receivers would not be able to act on received messages
- In any communication system, including Connected Vehicle, trust in received messages is vital for the system to achieve its goals

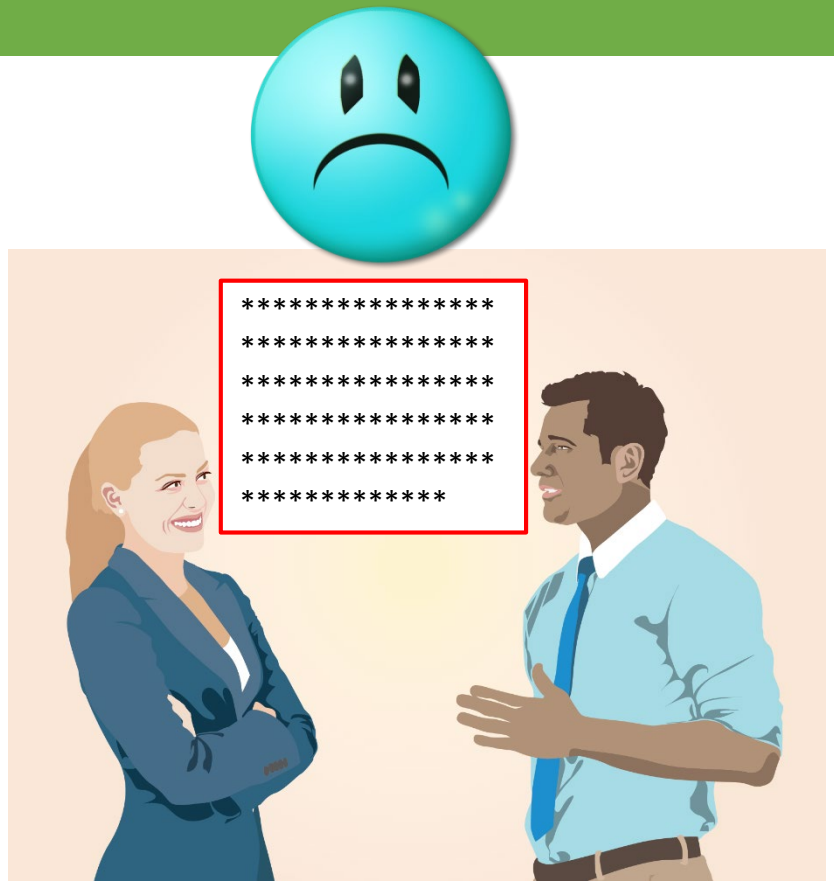


Image source: USDOT

What's Unique about Connected Vehicle (CV)?

- Trusted communications in the context of the Web
  - If I go to eCommerceGiant.com, my browser makes sure that the server is actually owned by that e-commerce company
  - It does this using Transport Layer Security and X.509 certificates – digital documents that attest identity or ownership of a specific resource
- What's special about the CV system requirements compared to online shopping?
  - Many-to-many communications
  - Need to be able to make real-time decisions
    - Limited bandwidth
    - Low-latency network connectivity not assured
  - Different actors in different roles but the identity of the actor isn't important, the role is
  - Concern about privacy
  - Limited connectivity for security updates

Many-to-many communications

Image source: USDOT

Need for local, real-time decisions

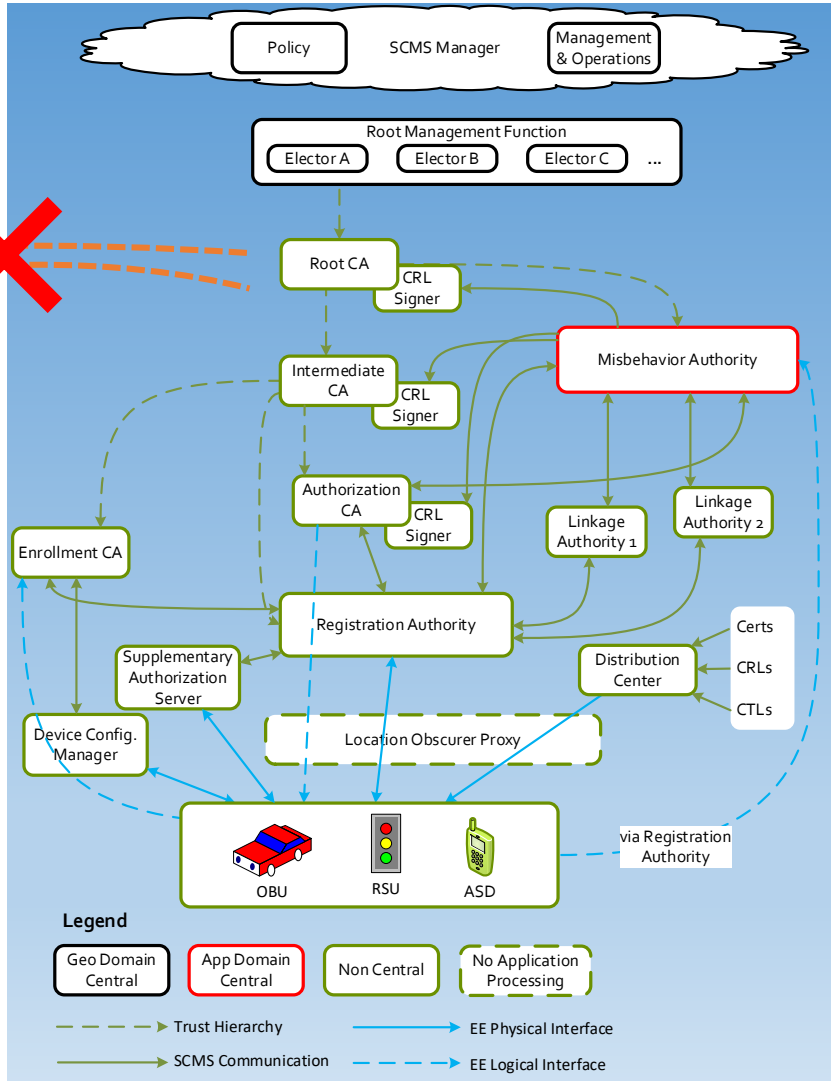


Image source: USDOT

Identity v. Role

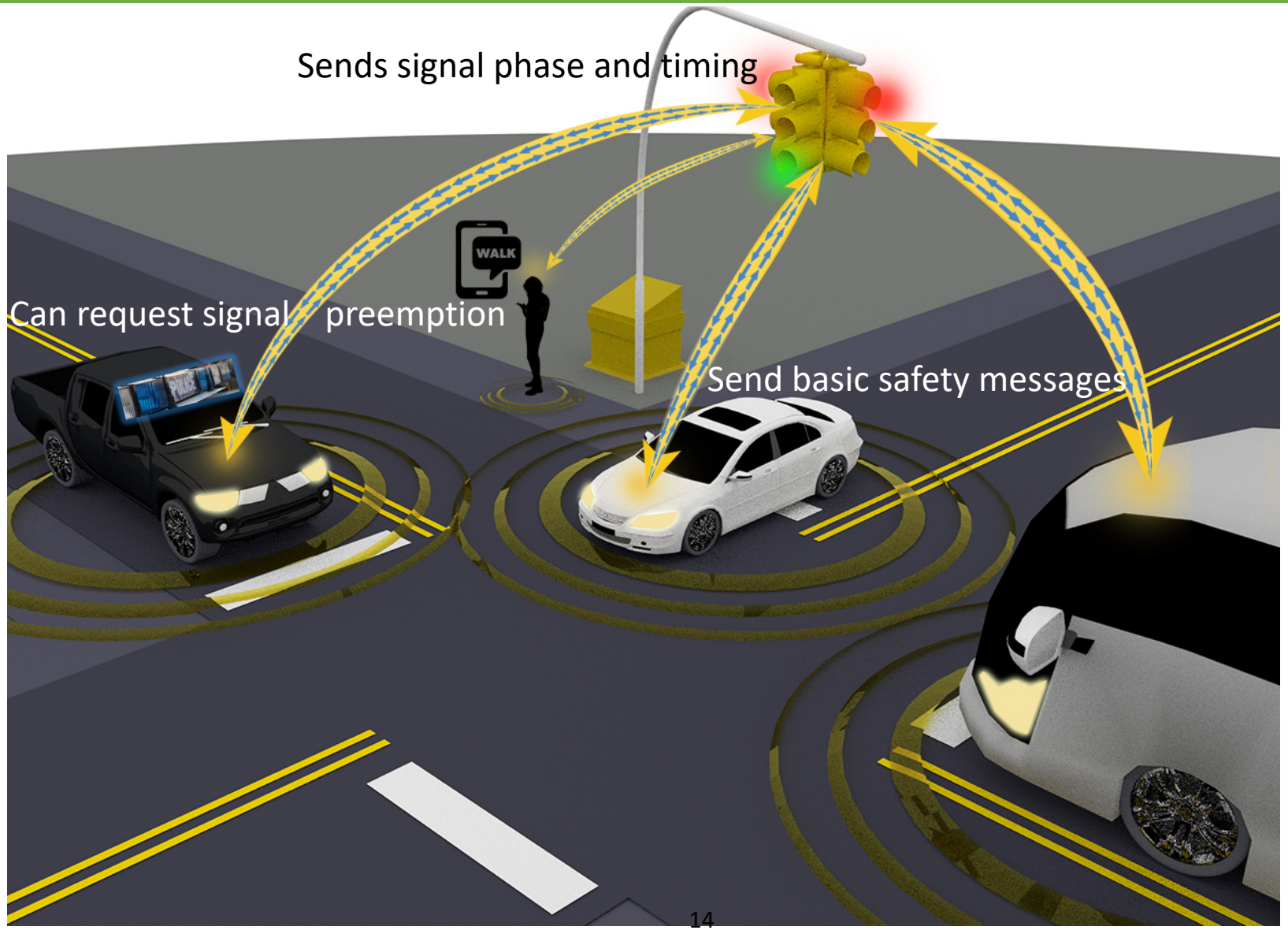


Image source: USDOT

Concern about Privacy

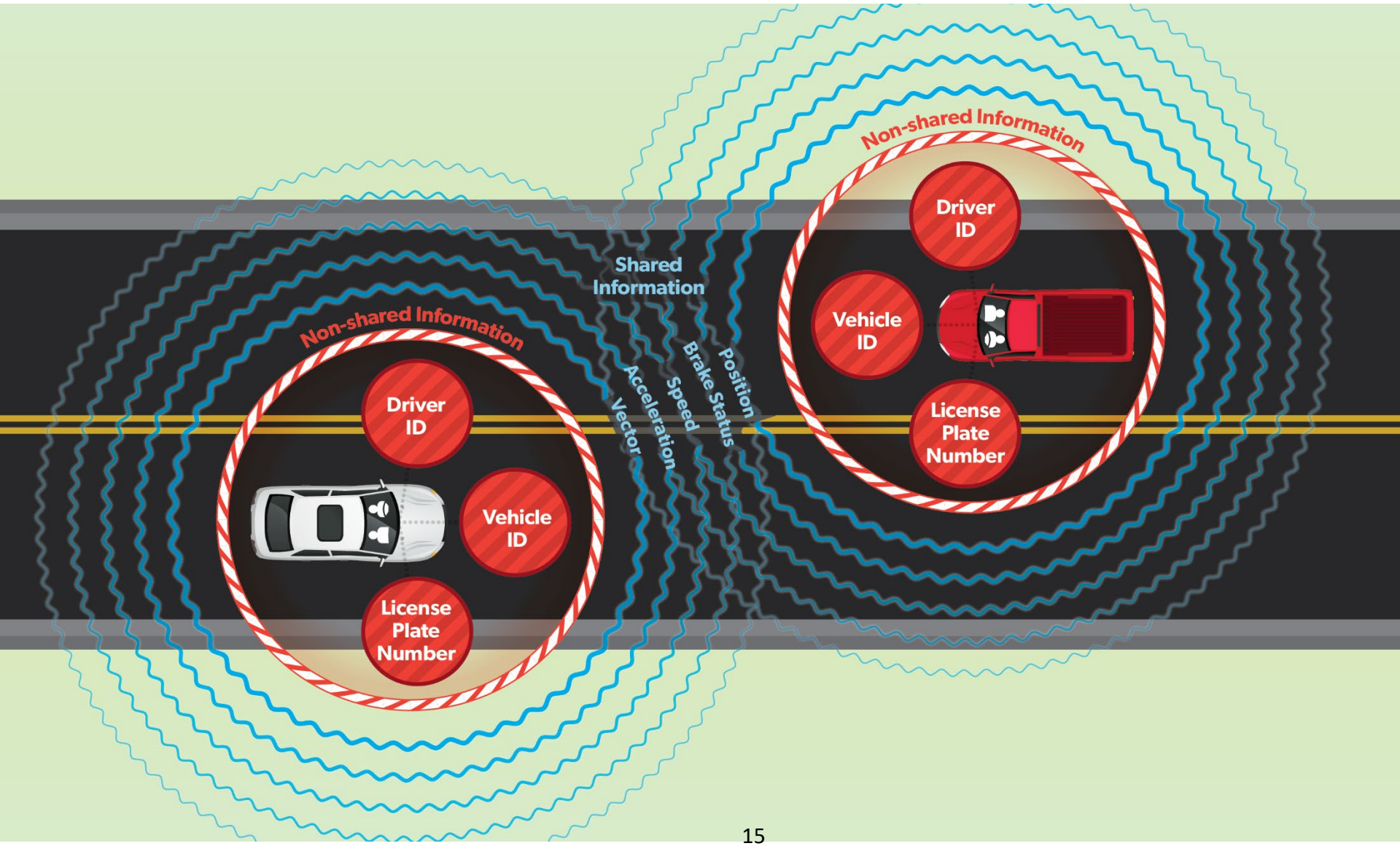


Image source: USDOT

Limited connectivity for security updates for vehicles

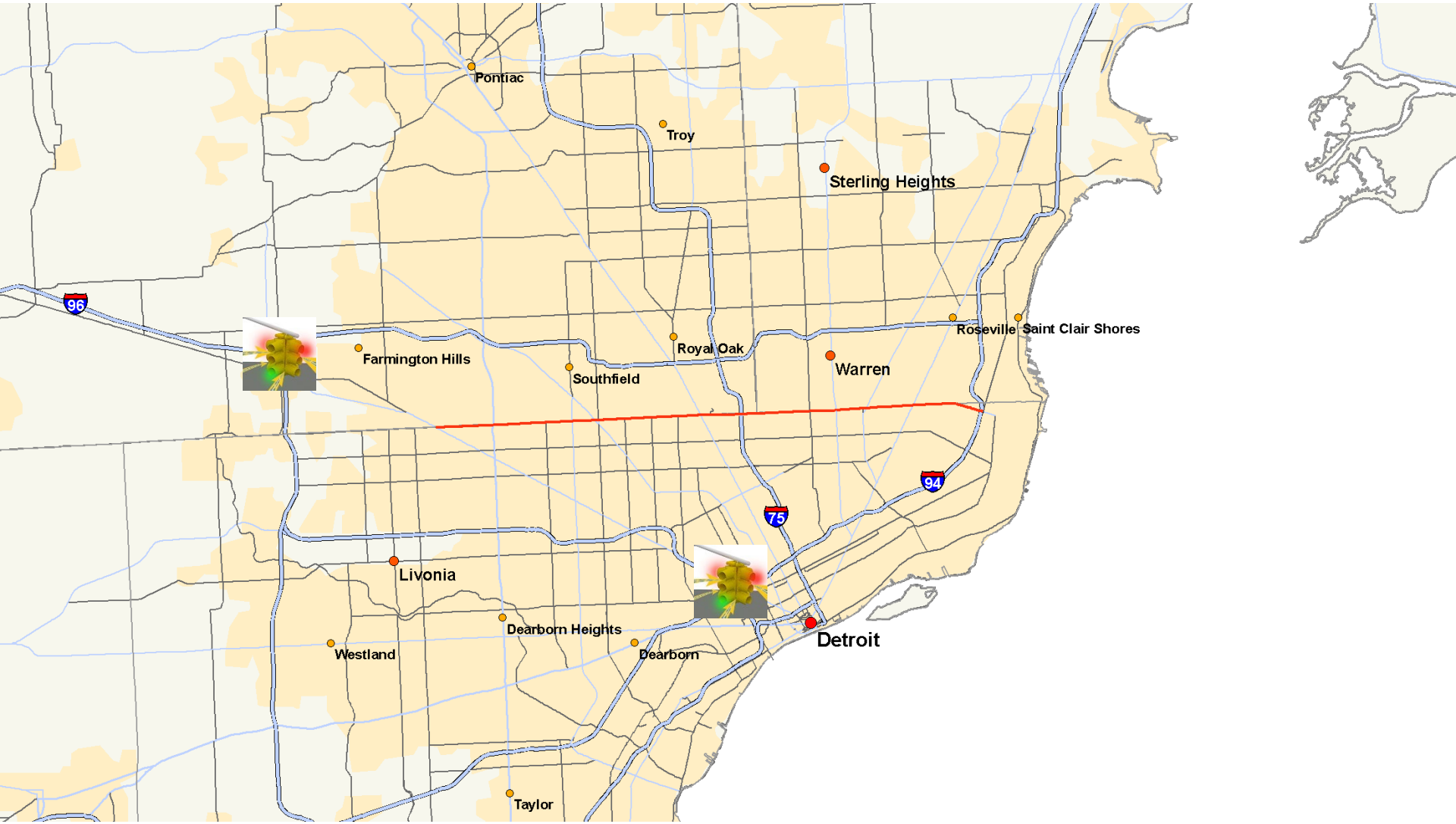


Image source: wikimedia.org

Functional Requirements

- Devices get issued with credentials that state their properties / permissions
  - Credentials state everything that the receiver needs to know about the sender to decide whether to trust its messages.
  - We use cryptography to make sure that only the credential owner can use it
    - Credential issuer and receiver cannot use the credential
- A Credential Issuer makes sure that the device is entitled to the credentials
- The system recovers from compromise
  - Misbehaving devices (sending bad data or otherwise harming the system) are detected and removed or fixed
  - Bad actors on the system management side (e.g. bad credential issuers) are detected and credentials they issued removed from circulation

Image source: wikimedia.org

System Security Requirements

- System properties and requirements drove the development of a different certificate format than is used on the Internet
  - Internet: X.509
  - Vehicle-to-Everything (V2X) : 1609.2
- Limited capacity channels
- Role-based Access Control

  - Many-to-many communications
  - Need to be able to make real-time decisions
    - Limited bandwidth
    - Low-latency network connectivity not assured
  - Different actors in different roles but the identity of the actor isn't important, the role is
  - Concern about privacy
  - Limited connectivity for security updates

System Security Requirements

- System properties and requirements drove the development of a different certificate format than is used on the internet
  - Internet: X.509
  - Vehicle-to-Everything (V2X) : 1609.2
- Limited capacity channels
- Role-based Access Control

- DSRC supports 10 MHz, 6Mbps channels – can be saturated if too many vehicles present
- C-V2X with 20 MHz channels has higher capacity but can still become saturated, especially if security overhead is excessive
- Small certificate format is necessary
- 1609.2 is smaller by design than X.509

System Security Requirements

- System properties and requirements drove the development of a different certificate format than is used on the internet
  - Internet: X.509
  - Vehicle-to-Everything (V2X) : 1609.2
- Limited capacity channels
- Role-based Access Control

- 1609.2 certificates naturally identify participants by role
  - Role is identified by Provider Service Identifier (PSID), an identifier managed by IEEE to ensure each use of that PSID means the same thing
- X.509 certificates naturally identify participants by identity
  - In the V2X system, a receiver **might** need to know identity, but certainly **does** need to know if the sender is a traffic signal or an ordinary car
- 1609.2 certificates meet system requirements

System Security Requirements

- System properties and requirements drove the development of a different certificate format than is used on the internet
  - Internet: X.509
  - Vehicle-to-Everything (V2X) : 1609.2
- Limited capacity channels
- Role-based Access Control
- New certificate format = new certificate management protocols ==> SCMS

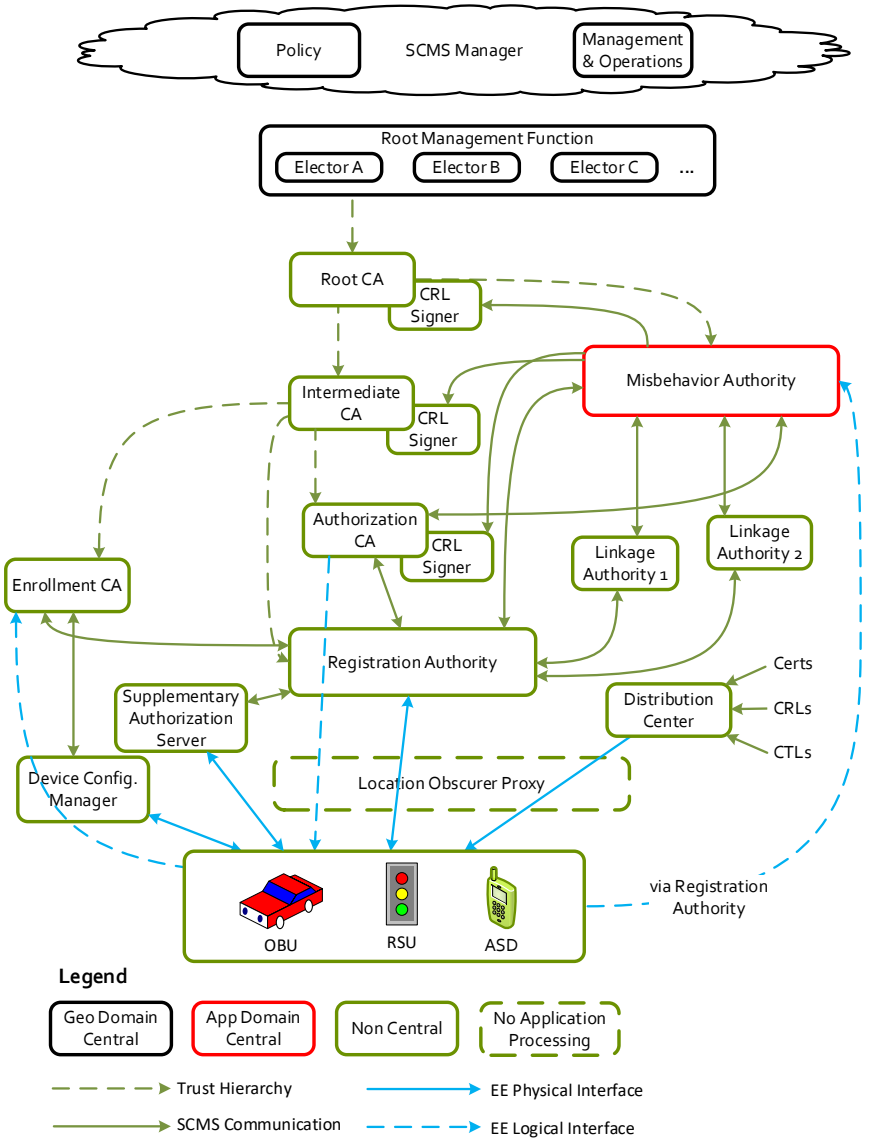


Image source: IEEE P1609.2.1

Privacy Requirements

- Privacy means you have a right to go about your business without other people knowing what you're doing
- … with some exceptions
  - If they need to know what you're doing to provide a service
  - If there's a public safety reason for them to know what you're doing
  - If you give your active consent
  - Depending on local privacy regulations
- Even in these cases, others should not get more information than they need

Privacy Requirements

- Privacy means you have a right to go about your business without other people knowing what you're doing
- BUT V2X data potentially leaks information about your movements
  - You can be identified with a vehicle (e.g., through a crash report)
  - If vehicle's movements are known without there being a good reason or need for it, this means your privacy has been violated
- **Design goal for V2X**: Ensure that V2X communications are never the cheapest way to track you
- Note: there are lots of other ways you can be tracked in real life
  - License plate and toll tags
  - Shops track your visits; your cellphone is somewhat trackable
  - Tire pressure sensors in your car give out low-power unique identifiers
  - MAC address readers
- So "not the cheapest way" is an appropriate goal

Privacy Requirements: Data management

- The V2X system generates a huge amount of data
  - Vehicles send 10 Basic Safety Messages / second
    - Application payload ~ 30 bytes
    - Total size ~ 150-250 bytes
    - In one hour's driving generate ~ 9 MB per car
    - One day of 2 hours' driving each by 300m cars = 5.4 x 10^{15} bytes
- Must ensure that the data is appropriately managed, and gathered only when necessary
- Data management isn't really an SCMS issue, but it must be addressed for deployment

How Does the SCMS Address All This?

- IEEE 1609.2 specifies security services – cryptography and data validation services that can be used to protect data in transit
- In the 1609.2 system, a receiver knows a sender is trusted to send a message (or command) of a particular type because the sender has a certificate that says they are entitled to do so and the 1609.2 processing cryptographically links the certificate to the message to show that only that certificate holder could have generated that message
- The SCMS is in charge of issuing certificates to actors in the system. Its primary responsibility is to make sure that certificates are issued to actors who are entitled to them by carrying out checks that
  - The actor was entitled to the certificate in the first place
  - The actor has not become malicious, untrustworthy, or otherwise unreliable since the certificate was issued
- The SCMS and the 1609.2 certificate system is designed to preserve privacy from eavesdroppers in the field and from insiders at the SCMS

How Does the SCMS Address All This?

- Major challenges in SCMS deployment include:
  - Enrollment: establishing that devices are entitled to certificates, especially for specialized applications
  - Provisioning: keeping devices provisioned with certificates – this requires regular access to the Internet
  - Revocation: understanding which devices should have their certificates withdrawn

ACTIVITY

Question 1

Which of the following statements about privacy is not true?

Answer Choices

a) There are many ways to track drivers on the road.

b) To preserve privacy, consideration must be given both to how data is created and transmitted, and also to how it is stored and managed.

c) Protecting privacy uses both technological and policy approaches.

d) The V2X system must always completely protect the anonymity of drivers.

Review of Answers

a) There are many ways to track drivers on the road.

Incorrect. Drivers can be tracked by cellphones, toll tags, license plates read by cameras, and many other means.

b) To preserve privacy, consideration must be given both to how data is created and transmitted, and also to how it is stored and managed.

Incorrect. Data at any stage of its lifecycle may be personal identifiable information and must be protected.

c) Protecting privacy uses both technological and policy approaches.

Incorrect. Technology can prevent data from being used by unauthorized users, but policy is necessary to ensure that authorized users do not use data in ways that were not intended.

d) The V2X system must always completely protect the anonymity of drivers.

Correct! Driver privacy is important but cannot be fully guaranteed by V2X as it is somewhat compromised by many other mechanisms. The V2X system design aims to ensure that V2X is not the cheapest method available to an attacker to compromise privacy.

Learning Objective 2

Describe how the Security Credential Management System (SCMS) uses cryptographic building blocks to provide trust

Digital Signature

- **Trust is essential to CV system: if receivers can't trust the messages, they are useless**
  - Digital signatures are the cryptographic building block that we use to construct systems of trust
- Senders sign messages with digital signatures and receivers verify the digital signatures
  - For verification receivers use the sender's certificate (sent with every message or periodically)
  - Certificate is issued by the SCMS
  - Message signers for applications are called "end entities"
- End entity certificate shows
  - Sender is a correctly implemented application
  - Sender is running on a properly secure device
  - Sender is allowed to send a message of that type.

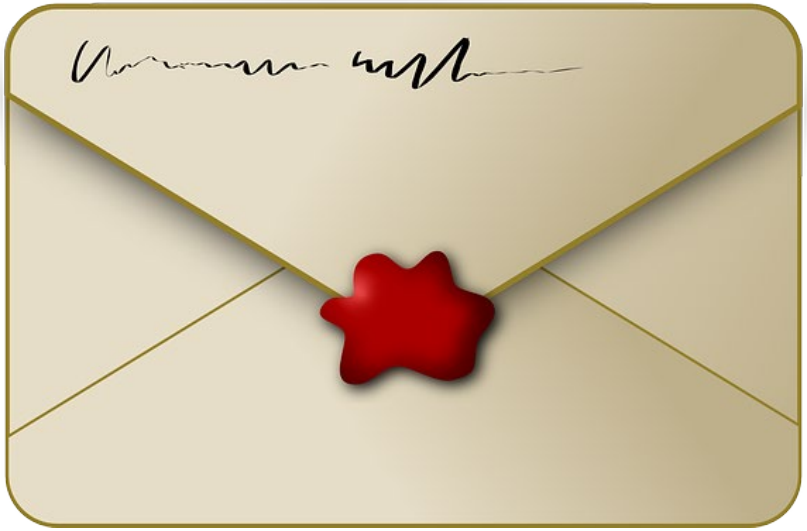
Image source: wikimedia.org

Digital Signature contd.

- The fundamental cryptographic mechanism used in these secure communications is known as digital signatures
- Signatures provide the communications security services
  - Authenticity: message came from the stated sender
  - Integrity: message wasn't modified on the way
  - Non-repudiation: message sender can't deny creating the signature
- Before generating any signatures, the sender generates a pair of mathematically related keys
  - Public key: can be distributed widely, and are used to verify the signature
  - Private key: hard to derive from the corresponding public key, and are used to create the signature
- Algorithm used in Connected Vehicle is based on elliptic curves, called the Elliptic Curve Digital Signature Algorithm (ECDSA)

Encryption

- Encryption ensures message can't be read by an outsider
- Encryption scheme examples
  - Symmetric: AES, DES
  - Asymmetric: RSA OAEP, ECIES
- Standard V2X messages are not encrypted, only used in special use cases
  - Secret data exchange between end entities and the SCMS
  - Protection of financial information, for example in tolling
- Hybrid encryption is used in CV
  - Asymmetric algorithm is used to exchange a symmetric key
  - Efficient symmetric algorithm is used to encrypt the data



In this presentation we focus on **asymmetric** (or **"public-key"**) cryptography as this enables digital signatures and asymmetric encryption, which in turn enable secure ad hoc networking

Image source: pixabay.com

Certificate Authorities

- Certificate Authorities (CAs) are essential for asymmetric crypto
  - Establish trust between two previously unknown users
- CAs issue certificates (using their private keys) to qualified users
- CAs are trusted to
  - Keep their private keys secure
  - Ensure that users are entitled to the requested certificate, often delegated to a Registration Authority (RA)

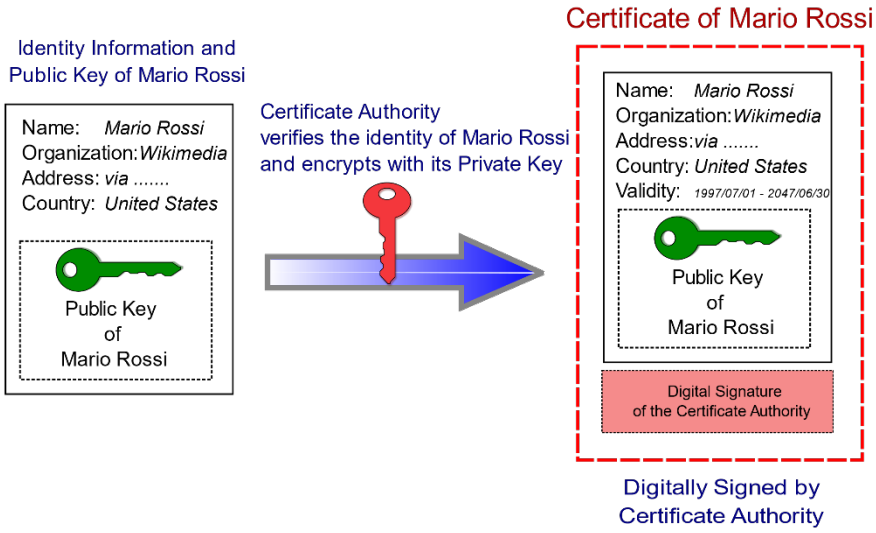
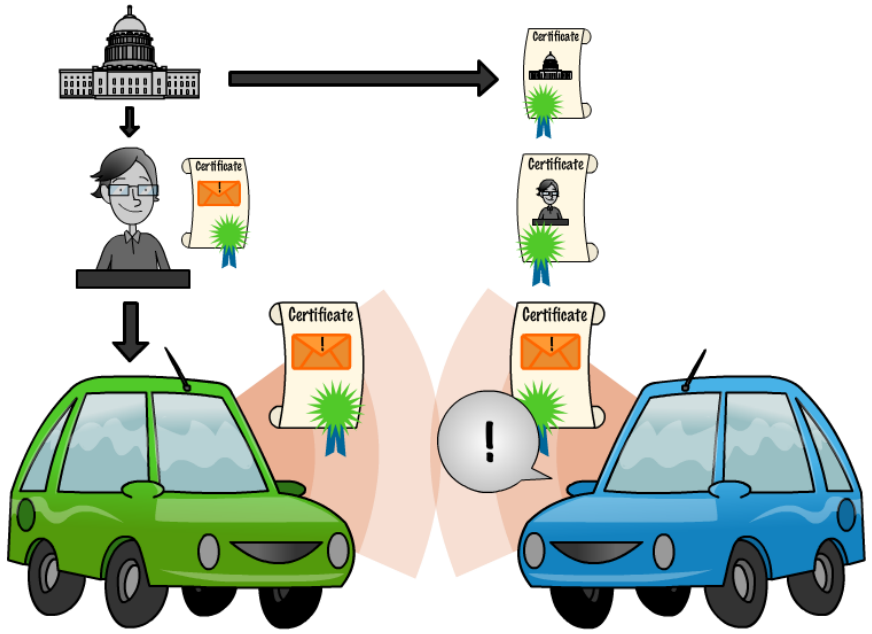


Image source: wikimedia.org

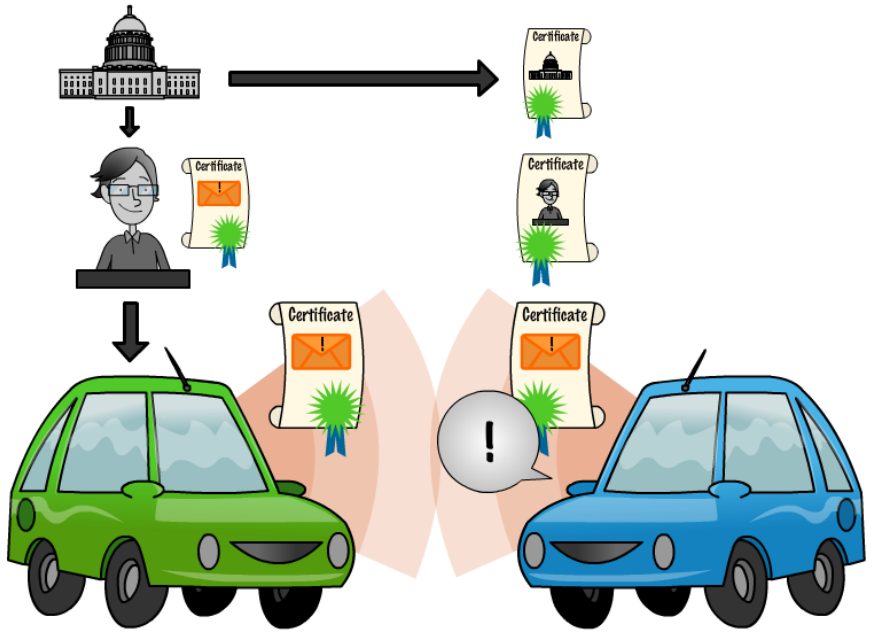
Chain of Trust

- Bob gets a certificate from a CA
  - Bob's certificate is signed by his CA's certificate
  - Bob's CA's certificate comes from another CA
  - …and back to a CA that issued its own certificate, called a "root CA"
  - Root CA certificate management is complex and will be dealt with later



Chain of Trust

- Bob gets a certificate from a CA
  - … which is part of a chain of trust
- When Alice receives a signed message from Bob, in order to trust it, she must:
  - Already trust Bob's certificate, or…
  - Already trust Bob's CA's certificate, and have Bob's certificate, or…
  - Already trust the Intermediate CA certificate that issued Bob's Authorization CA certificate and have the certificates below it, or…
  - Already trust the Root CA certificate at the top of the chain, and have the other certificates



IEEE 1609.2 Certificate

- Main features of IEEE 1609.2 certificates
  - Smaller size
  - Suitable for machine-to-machine communications
  - Allows pseudonym certificates
  - Allows the SCMS to issue certificates for all types of CV applications
    - Use of PSID to identify applications allows new applications to be added
      - Including drones, autonomous delivery robot identification, …

```
ToBeSignedCertificate ::= SEQUENCE  {
    id                      CertificateId,
    cracaId                 HashedId3,
    crlSeries               CrlSeries,
    validityPeriod          ValidityPeriod,
    region                  GeographicRegion OPTIONAL,
    assuranceLevel          SubjectAssurance OPTIONAL,
    appPermissions          SequenceOfPsidSsp OPTIONAL,
    certIssuePermissions    SequenceOfPsidGroupPermissions OPTIONAL,
    certRequestPermissions SequenceOfPsidGroupPermissions OPTIONAL,
    canRequestRollover      NULL OPTIONAL,
    encryptionKey           PublicEncryptionKey OPTIONAL,
    verifyKeyIndicator      VerificationKeyIndicator,
    ...
}
(WITH COMPONENTS { ..., appPermissions PRESENT} |
 WITH COMPONENTS { ..., certIssuePermissions PRESENT} |
 WITH COMPONENTS { ..., certRequestPermissions PRESENT})
```


Image source: IEEE P1609.2.1

SCMS Design

- At the core, SCMS is a standard PKI with Root CAs, Intermediate CAs, and end-user (authorization) CAs
- Diagram shows that standard PKI chain of trust running up the middle
  - There may be a different number of Intermediate CAs – 0, 1, or more
    - In Europe the convention is 0, in the US the convention is 1
- Participating devices need:
  - Root CA management to know which incoming messages to trust
  - Authorization CA interaction to obtain certificates to sign messages

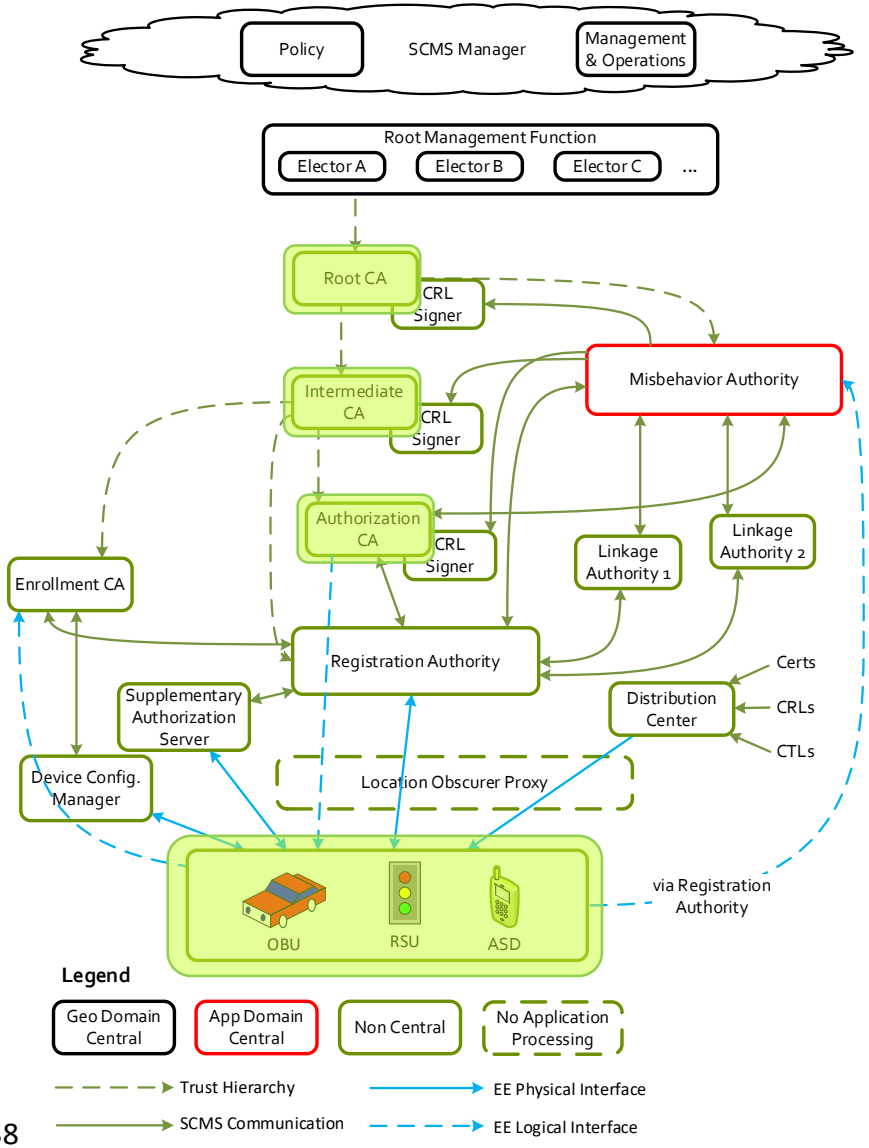


Image source: IEEE P1609.2.1

SCMS Design

- The SCMS has a lot of different components
  - More details on the next slides
- In principle each component could be run by a different company
  - Design is modular and internal interfaces are documented though not formally standardized
    - Root CA by Alice's SCMS Services
    - Intermediate CA by Bob's SCMS Services
    - Authorization CA by SCMS-R-Us, …
  - In this case, a deployer would engage with a Registration Authority operator who would interface to the rest of the SCMS operators
- In practice, currently a deployer will engage with a single SCMS provider who runs everything from the Root CA down
  - If different deployers use different SCMS providers, their devices can still trust each other – see later discussion of root CA management

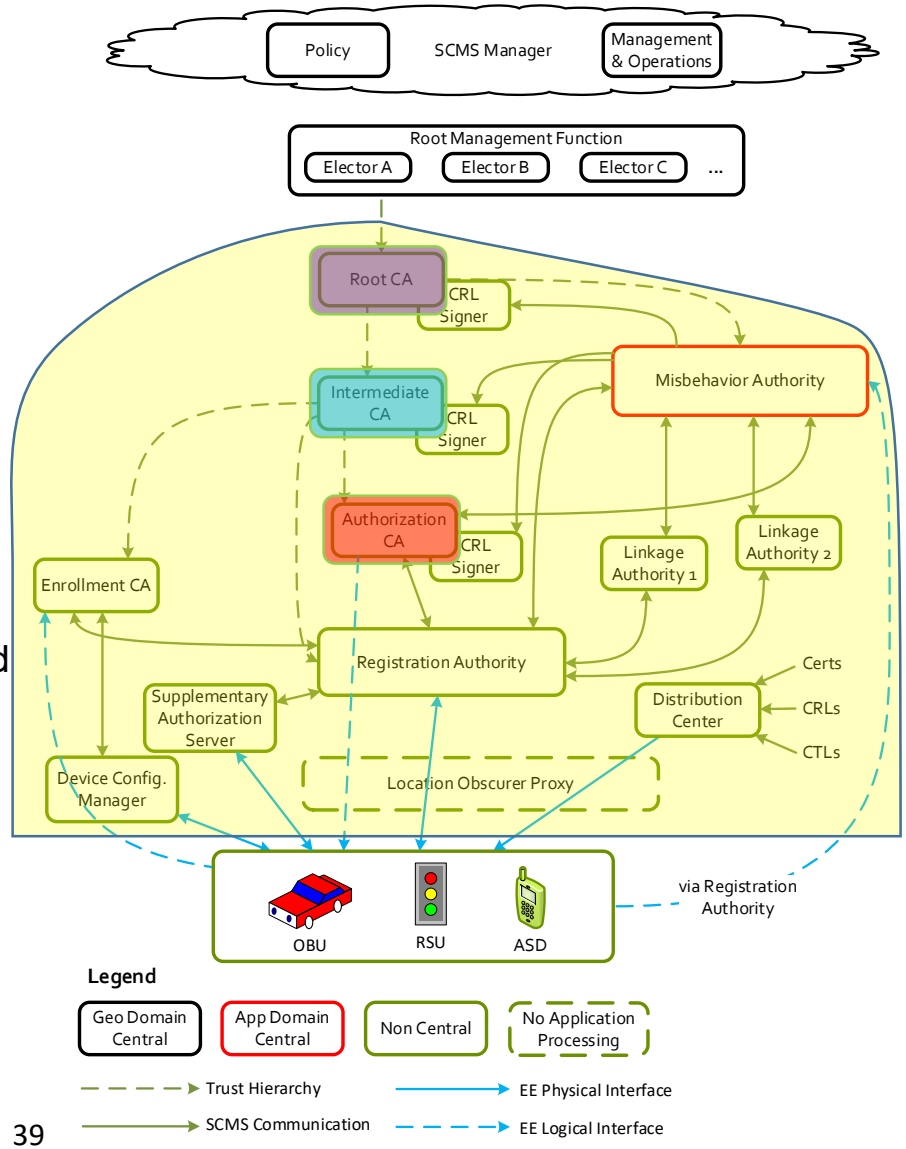


Image source: IEEE P1609.2.1

SCMS Design: Two types of certificates

- Authorization certificates
  - Used for application interactions with other end-entities
  - Specify the application activities that the holder is entitled to
- Enrollment certificates
  - Used for certificate management interactions
  - Authorize authorization certificate request and download
  - Long-term “identity”, used by SCMS component as a key for metadata
    - What permissions can go in the authorization certificate
    - Whether the enrollment certificate holder is entitled to auth certificates at all
- Separating Enrollment CA (ECA) and Authorization CA (ACA) improves robustness and privacy

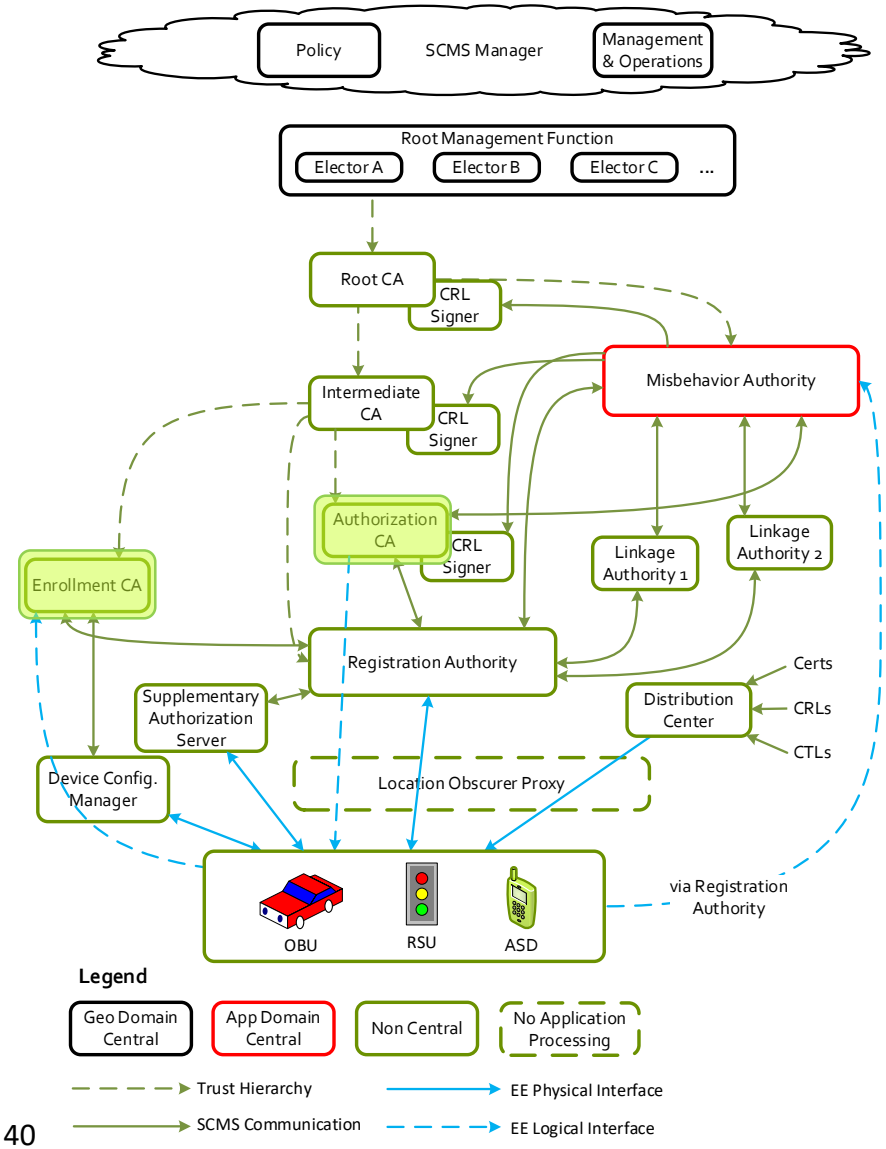


Image source: IEEE P1609.2.1

SCMS Design: Contact points with the SCMS

- End entities directly contact only three components of the SCMS
- Enrollment Certificate Authority (ECA) – enrollment certificates
- Registration Authority (RA) – gateway for SCMS interactions while in the field
  - Authorization certificate provisioning – gateway to authorization CA
  - Misbehavior report upload – gateway to MA
  - Security management info download
    - Certificate revocation list
    - New Root CA information
- Distribution Center (DC) – alternative path to download security management info
  - RAs provide security info only to devices that they also provide cert management services to – DC may provide security info to wider population

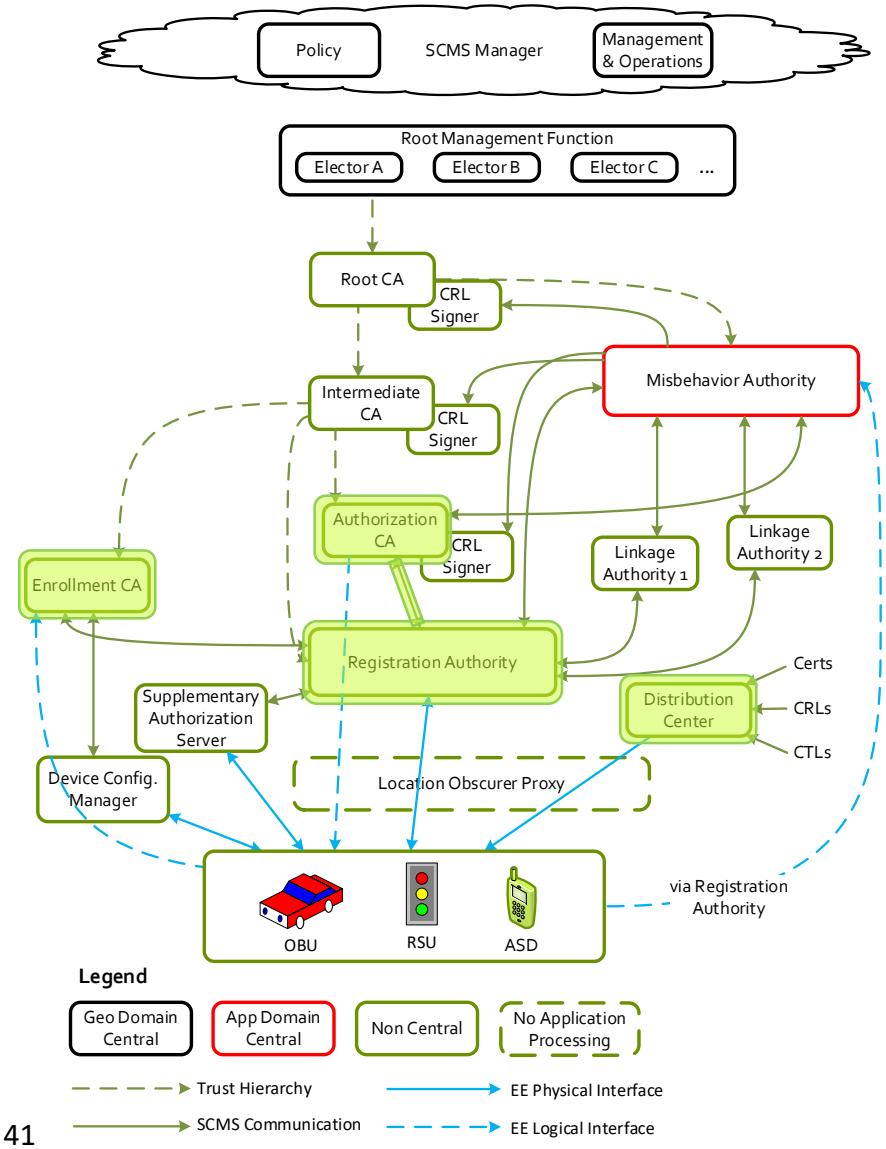


Image source: IEEE P1609.2.1

SCMS Design: Contact points with the SCMS contd.

- Contacting the ECA: happens at start of EE lifetime, can be proprietary interface
  - 1609.2.1 provides standardized interface but this is not required
- Contacting the RA:
  - Each EE has a single “home” RA which it is hard-wired to use
  - The RA is identified by a URL, has a certificate including that URL
- Contacting the DC:
  - DC accessed by URL
  - There may be multiple DCs
  - Standards do not address how EEs are configured with DC URLs
- Interfaces are standardized in IEEE 1609.2.1 (pub. 2020-12)
  - Connected Vehicle Pilot Deployments used a previous interface, the “CAMP Interface”
  - The CAMP interface is still widely supported but deployments are migrating to 1609.2.1

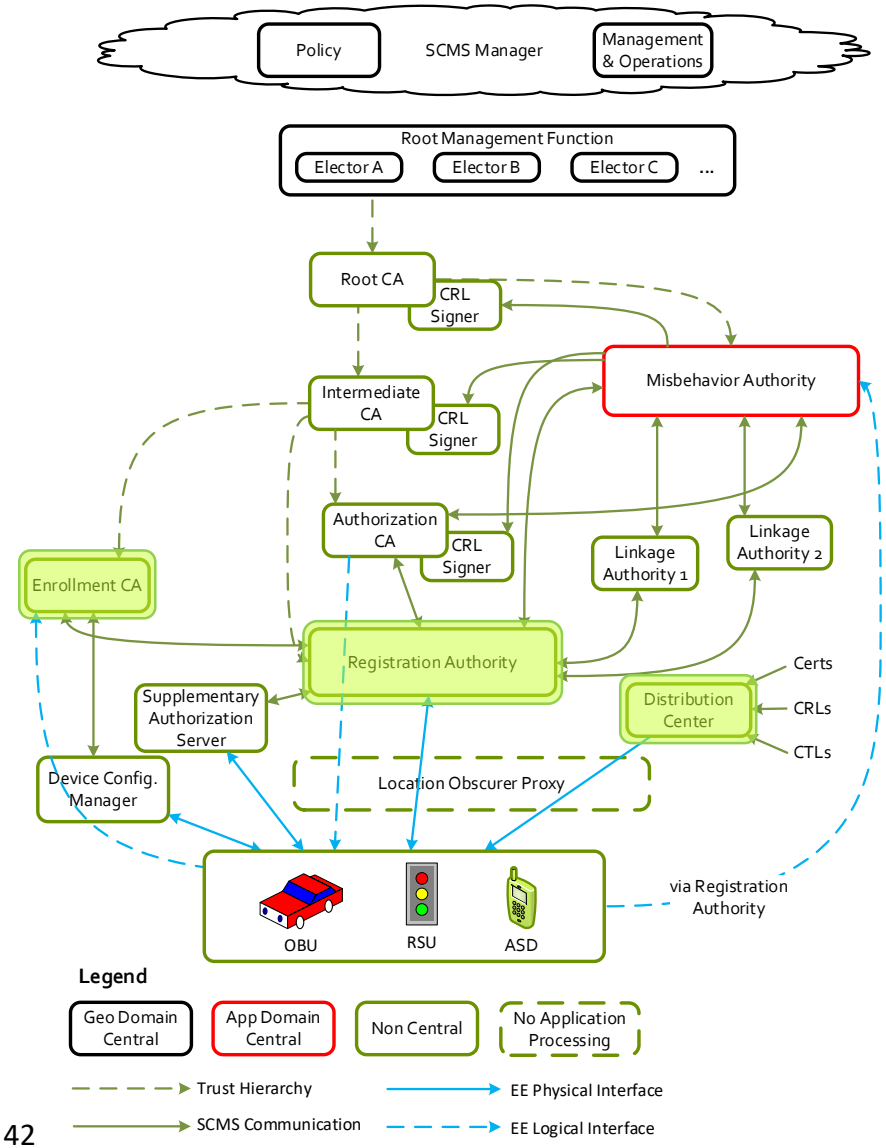


Image source: IEEE P1609.2.1

SCMS Design: Pseudonym certificate request

- To preserve privacy, Basic Safety Message (BSM) senders use a special type of authorization certificate: pseudonym certificate
  - Pseudonym certificates don't contain any identifying information about the sender
  - A BSM sender has multiple pseudonym certificates all valid at the same time and can change from using one to using a different one at will
  - This makes it hard to track vehicles
  - Typically, pseudonym certificates are valid for a week
- Revocation of pseudonym certificates is complicated

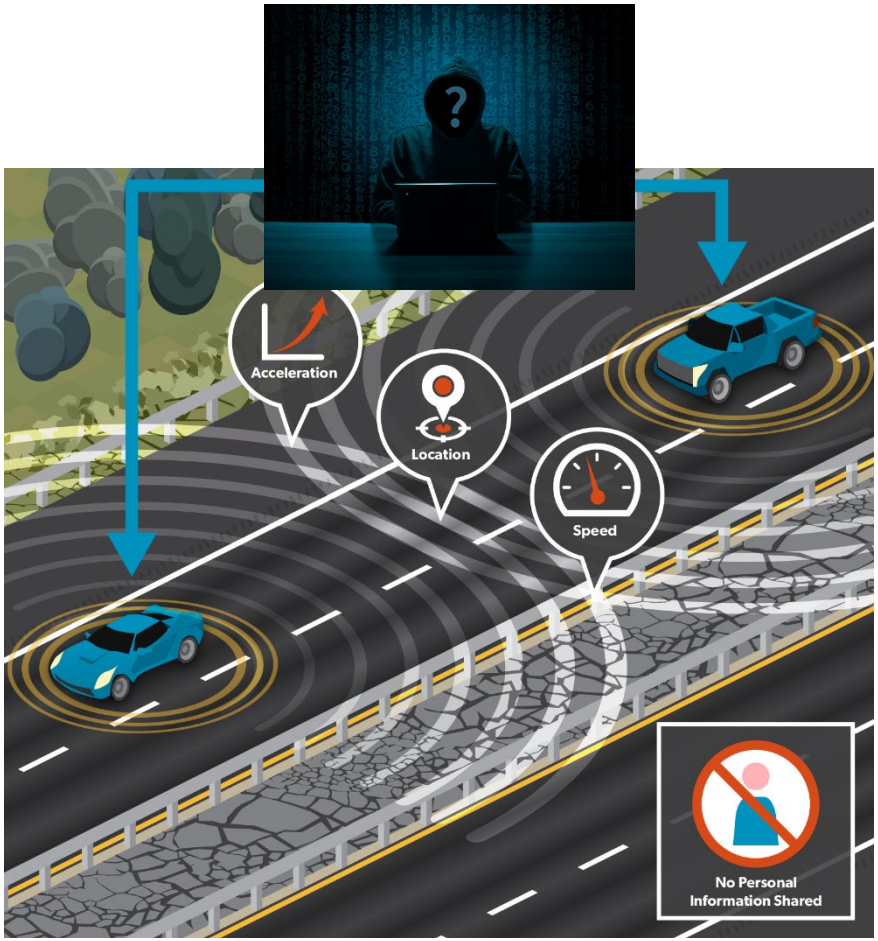
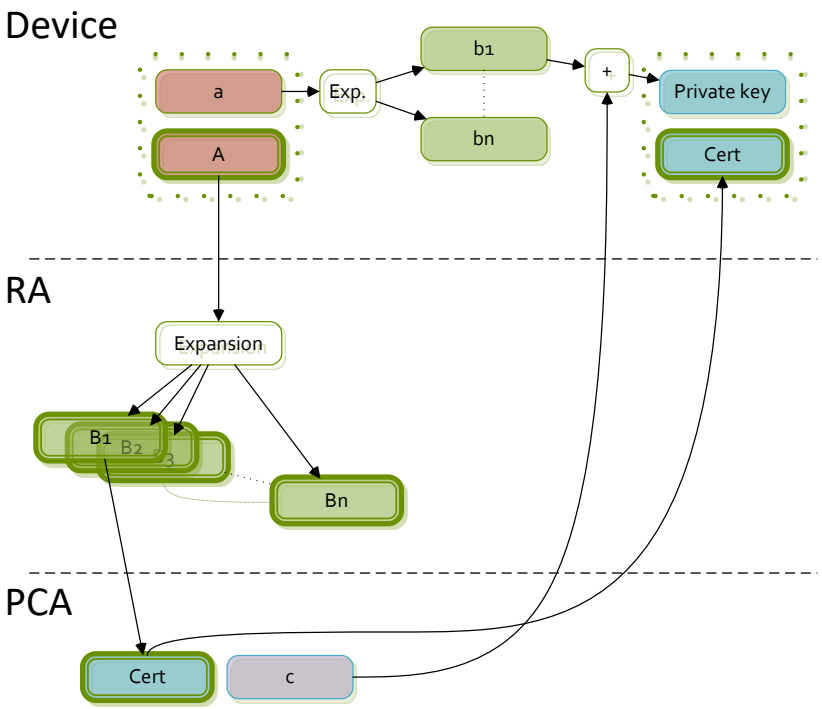


Image source: USDOT, wikimedia.org

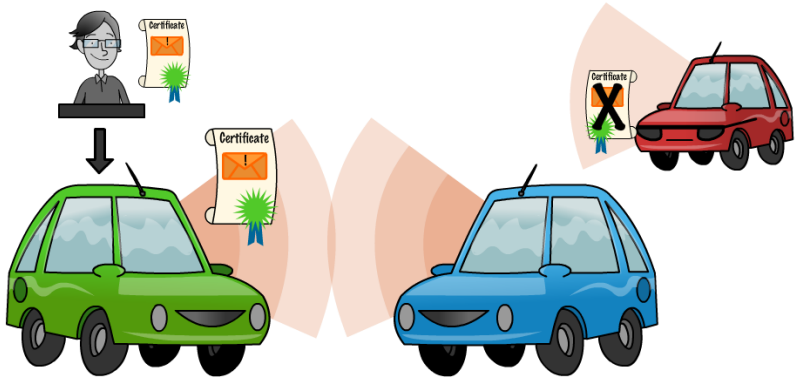
SCMS Design: Authorization certificate request contd.

- Authorization cert request optionally uses a technique called butterfly keys
  - This allows the end entity to send a single request and all of its certificates for the rest of its operating life can be generated using that request as a seed
  - A single request generates all 20+ certificates for a given week, and also the certificates for all future weeks
- Greater efficiency: allows the certificates to be generated at the time that makes most sense within the SCMS, not tied to the time of request
- Better privacy: decouples the time of generation from the time of request, so the ACA can't link different requests together as they were received at the same time



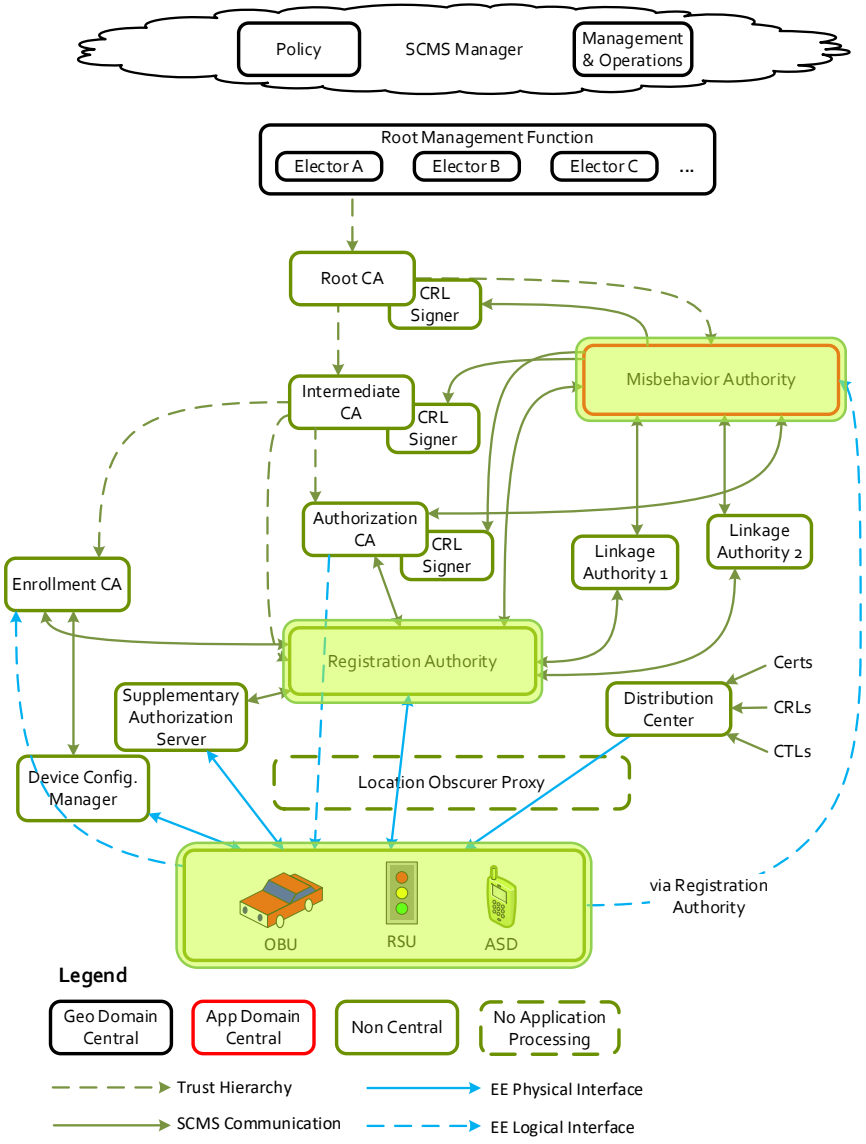
SCMS Design: Authorization certificate request contd.

- An end entity device can run any number of applications.
  - For example, RSU running WSA and SPaT
- Applications can share a certificate (one cert authorizes messages for multiple applications) or have distinct certificates (one cert per application)
  - Tradeoff: storage space v authorization complexity
- The SCMS may make policy about which applications can share a certificate
  - In principle the SCMS may make policy about which applications can share a device, but this is currently not a subject of SCMS policy
- Unless there is a good reason to couple applications, it is often easier to have separate certificates for separate applications



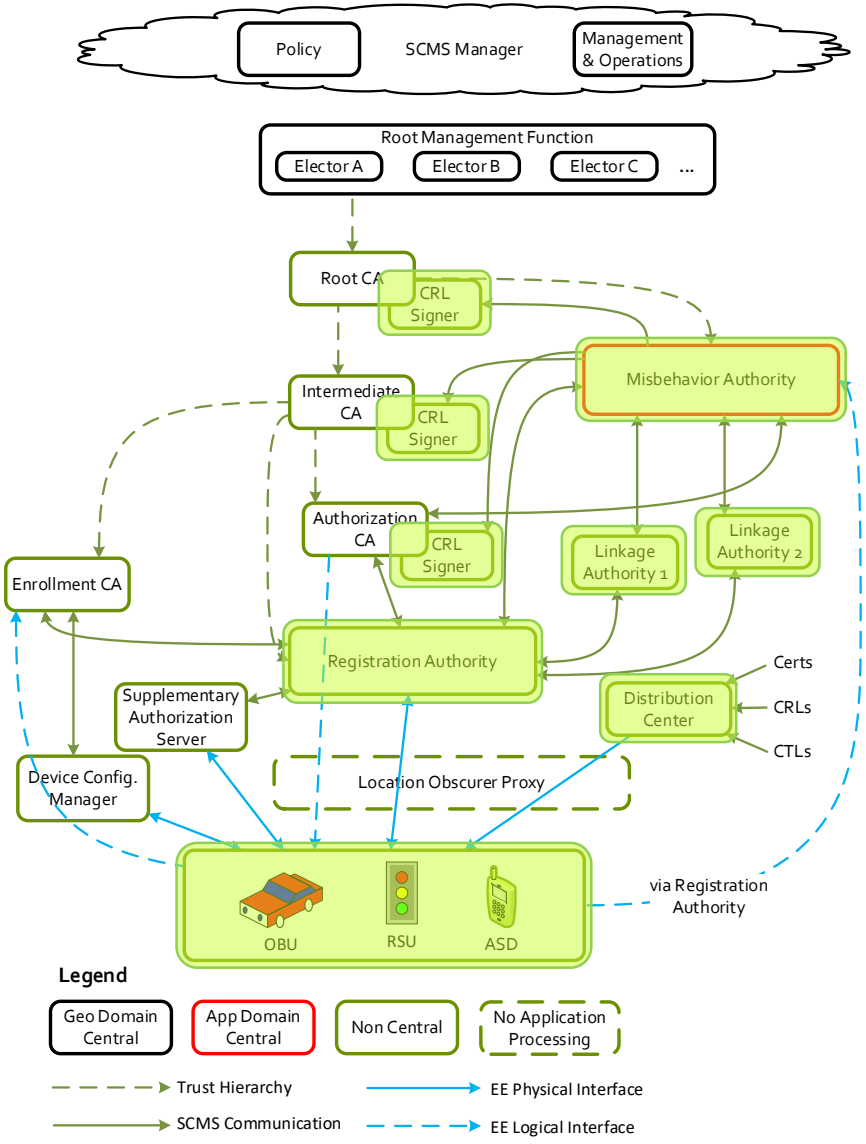
SCMS Design: Misbehavior management

- The system allows for devices that send bad data to be removed
  - Examples: Cars in mid-air, two cars in the same place, cars that say they're braking but speed up
- End entities report misbehavior to their RA
- The RA passes the reports to a central Misbehavior Authority (MA)
- The MA analyses the reports and decides whether the bad data an end entity is sending is having a significant effect on the system



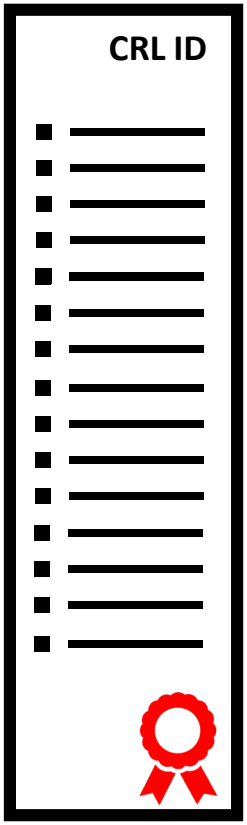
SCMS Design: Misbehavior management contd.

- If the bad data is sufficiently impactful, the MA *revokes* the end entity
- A Certificate Revocation List (CRL) is issued telling other end entities not to trust the revoked end entity
- The end entity's RA is told not to let it have any more certificates
- The CRL is distributed via the RAs and distribution centers



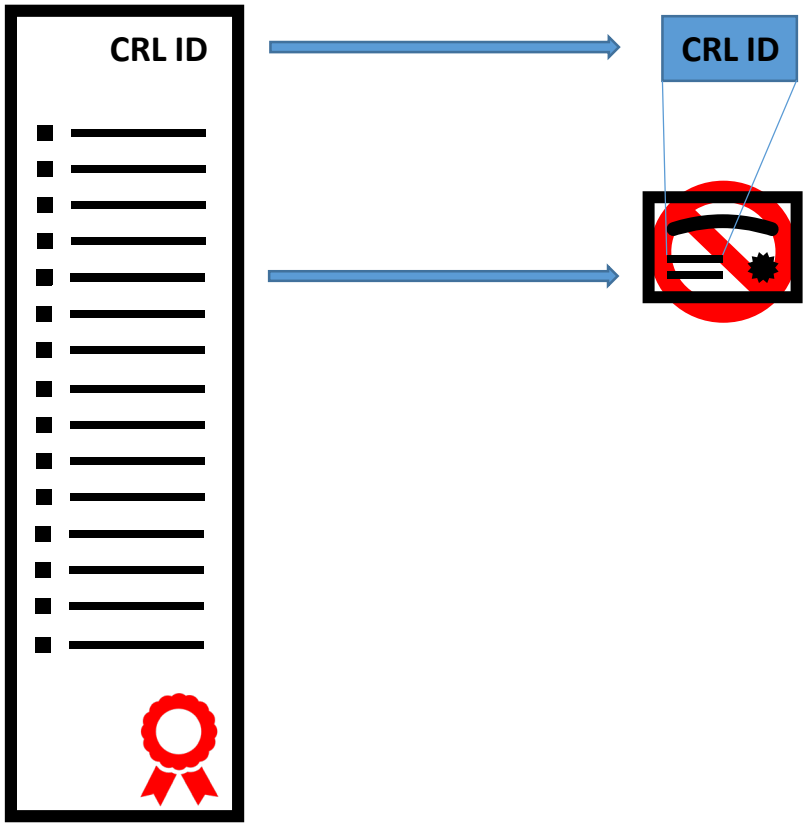
SCMS Design: Misbehavior management details – Certificate Revocation List (CRL)

- The CRL is a list of revoked certificates
  - When a receiver gets a signed message, it checks to see if the signing certificate is on the CRL
  - If the signing certificate is revoked, the receiver considers the message invalid
- The CRL only revokes currently valid certificates – expired certificates are automatically not trusted
  - If a device's certificate(s) will expire in the near future relative to when misbehavior is detected, it may not be necessary to revoke it depending on policy



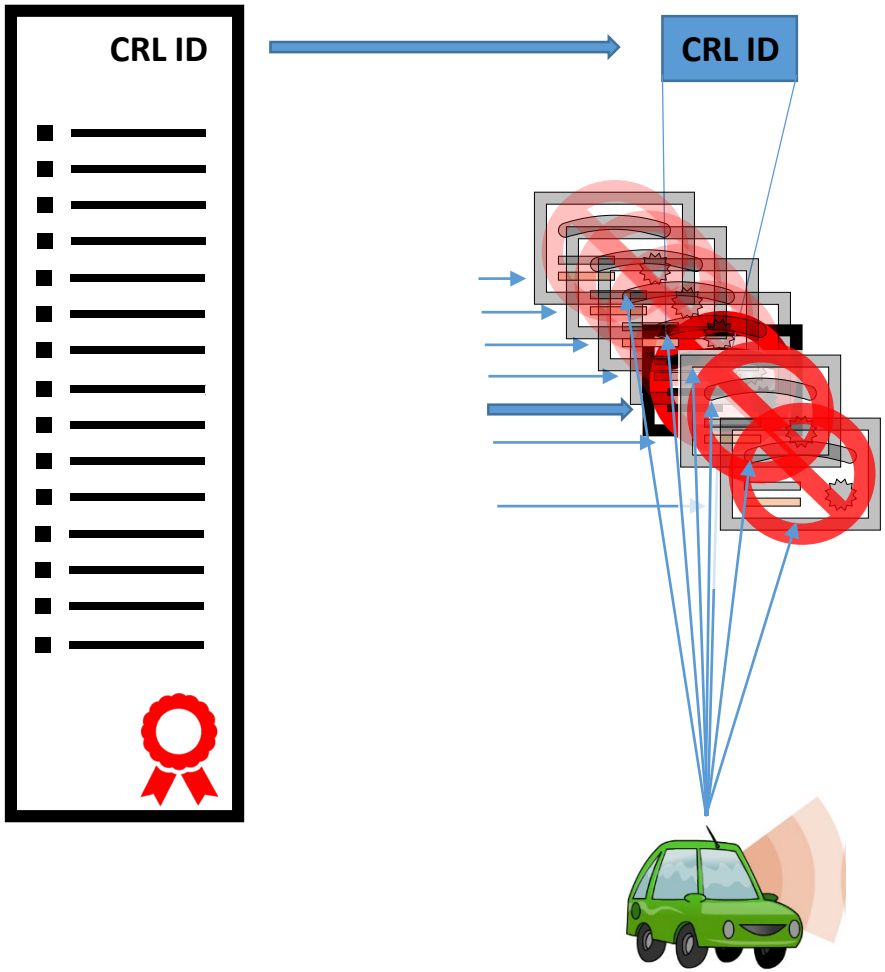
SCMS Design: Misbehavior management details – Certificate Revocation List (CRL)

- Each CRL signer can only revoke a particular set of devices, and each device can only be revoked by one CRL Signer
  - This limits the damage that a "rogue" CRL signer can do



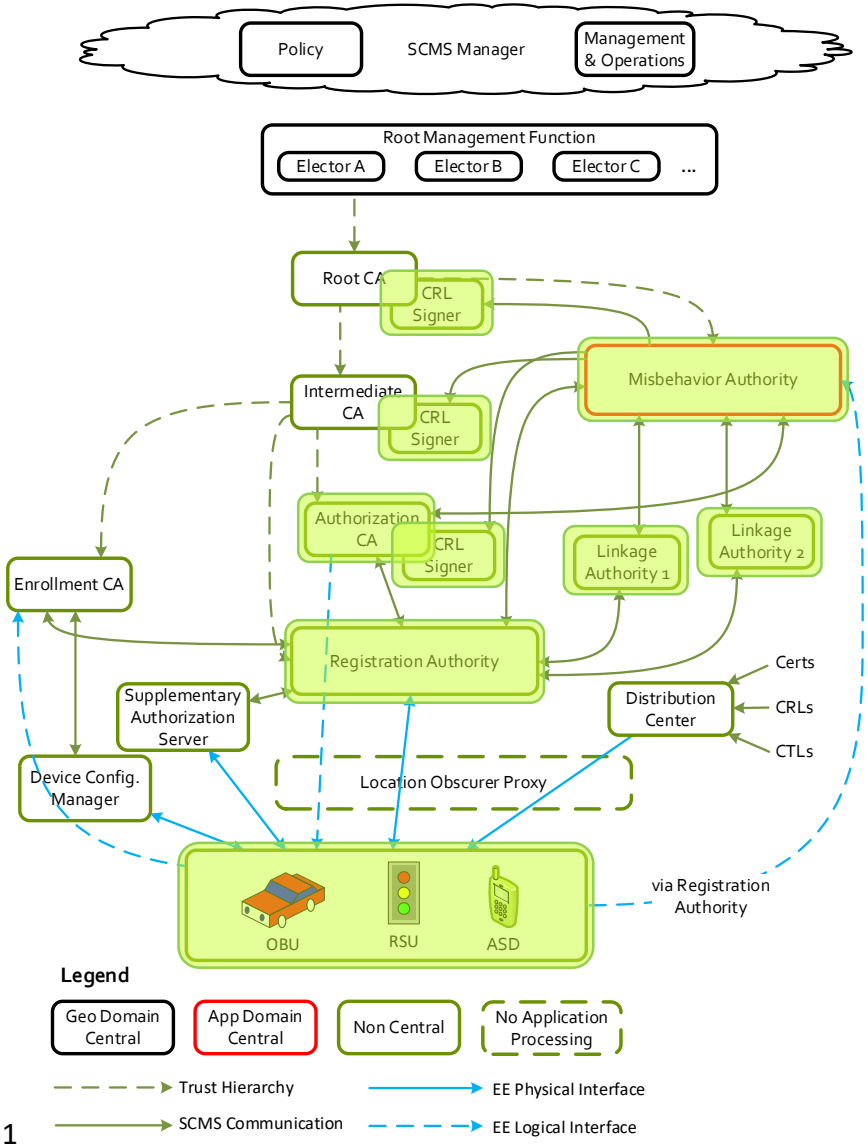
SCMS Design: Misbehavior management details – CRL contd.

- Pseudonym certificates are revoked using a field called a linkage value that appears in the certificate
  - This allows a single CRL entry to efficiently revoke all of that vehicle's pseudonym certificates



SCMS Design: Misbehavior management and privacy

- To investigate misbehavior, the MA may need to work out which certificates belong to the same EE
- For privacy, the SCMS builds in a complex set of components
- Misbehavior investigation and revocation involve: ACA, CRL signer, Linkage Authorities (LA1, LA2), MA, RA
- The components interact through standardized, auditable processes to ensure that privacy-breaching requests cannot be made
  - These processes are not complete but the principles behind them are well understood

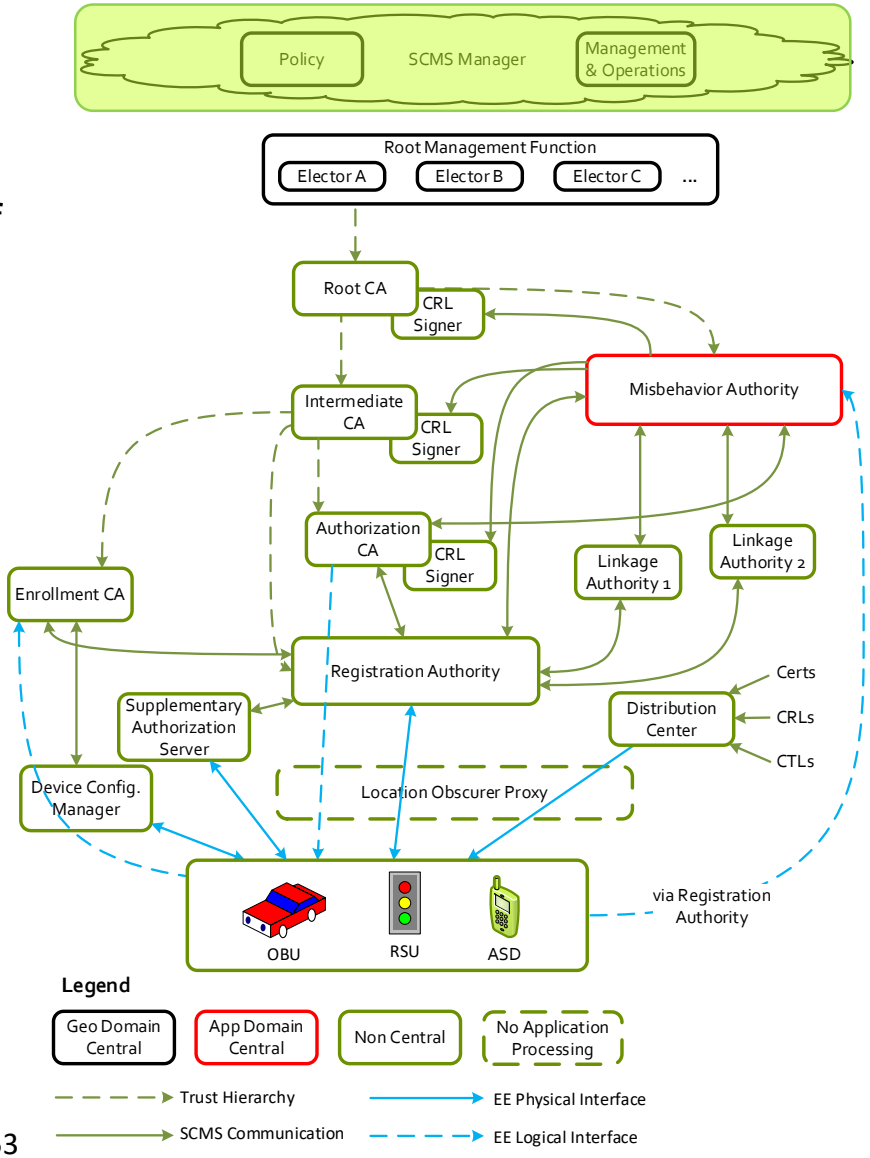


SCMS Design: Misbehavior management – current status

- CRL generation and distribution is fully standardized but the rest of the misbehavior management system is not complete (as of Dec 2020)
- No standards for misbehavior reporting by end entities
  - ETSI is producing a survey of proposals and options in TR 103 460
  - Pilot Deployments have defined baseline misbehavior detection and reporting algorithms
  - University of Michigan is doing more advanced research
  - It's unlikely that there will be standardized mechanisms before 2021
- No systematic process for detecting misbehavior by SCMS entities
  - The assumption is that if there is significant bad issuing of certs, it will be caught by noting high levels of misbehavior by those end entities

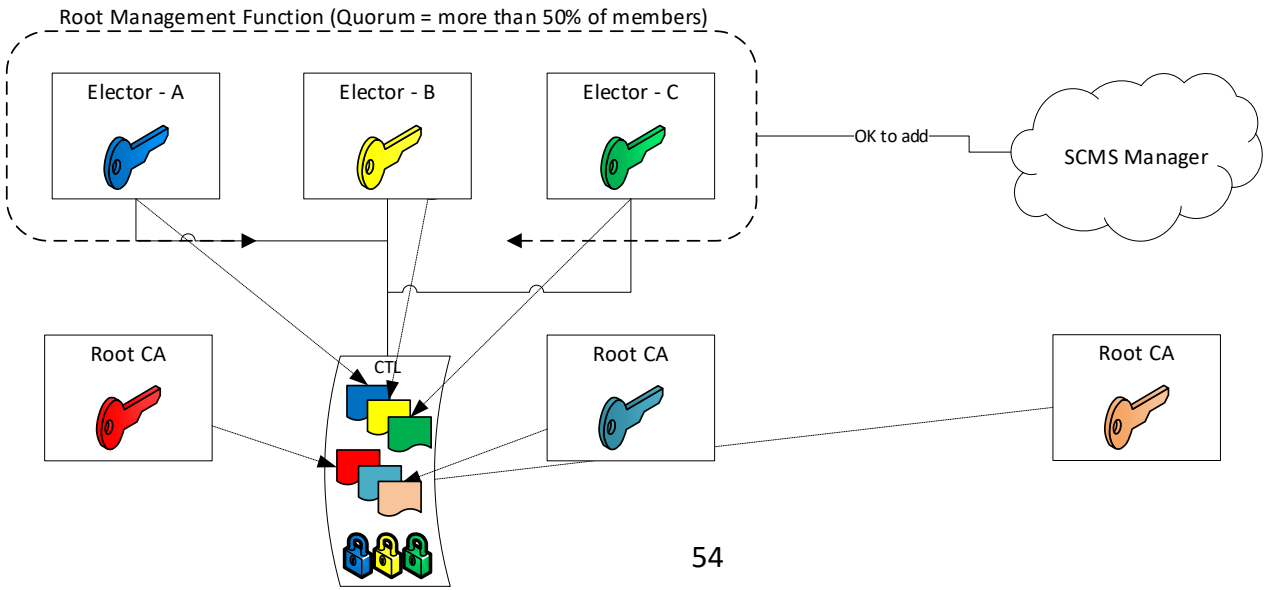
SCMS Design: SCMS Manager

- SCMS Manager
  - Sets overall SCMS policies
  - Coordinates the approval or removal of an elector or a root CA
  - Examples: security and certificate policy from the EU and the DG GROW
- As of 2020, a US SCMS Manager has been established as an industry organization with observer participation from USDOT
- For deployments in the near future, there will probably be a single SCMS provider who will effectively act as the SCMS Manager



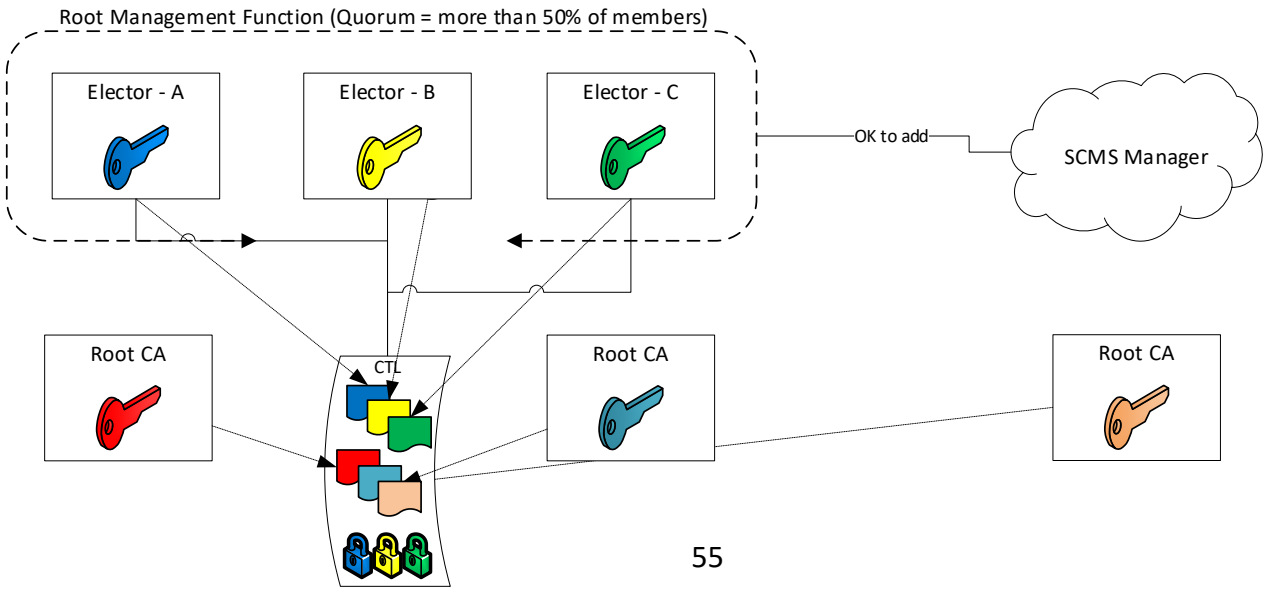
Multiple Root CAs

- Devices usually get certs that chain back to a single Root CA
- Different devices could chain back to different Root CAs
  - For interoperability, devices must trust each other's Root CAs
  - At the time of writing only one Root CA is widely used in the US but there are multiple Root CA suppliers
- Deployment managers determine if support for multiple Root CAs is required
  - Client software supports installing multiple root CA certificates in a "trust store" – if this is a requirement for the deployment, it can be supported
- Future: Elector system, standardized in 1609.2.1



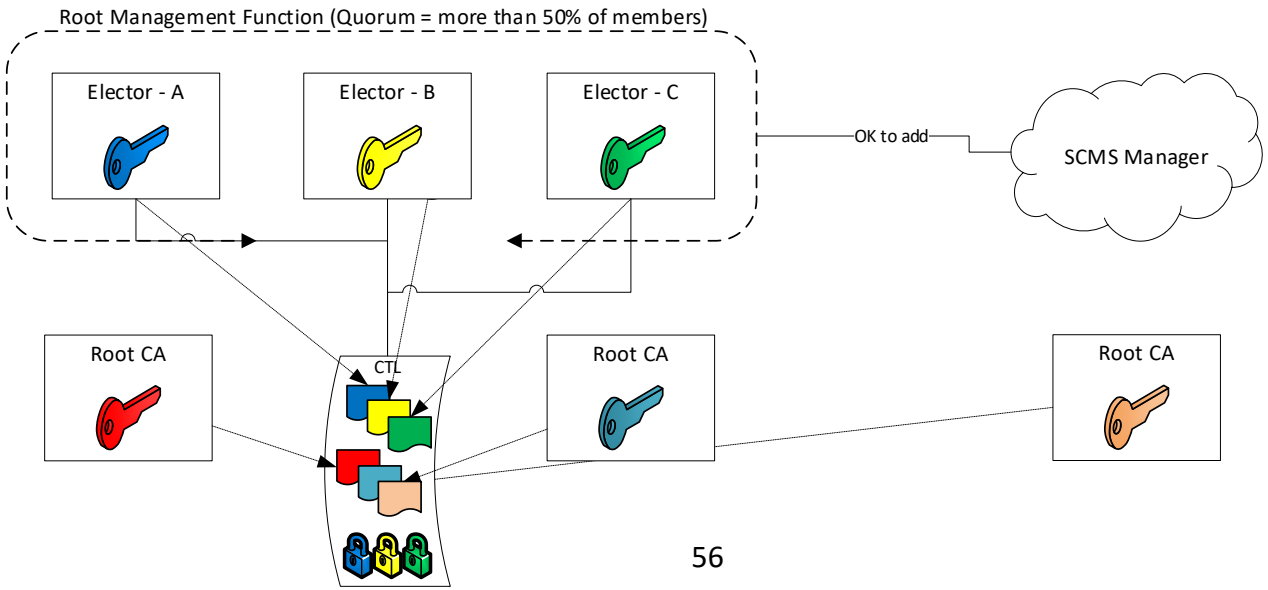
Electors

- Electors are entities that sign Certificate Trust Lists (CTLs)
  - CTLs are trust statements about Root CAs and other electors
  - The trust decisions are made by the SCMS Manager – Electors act effectively as notaries for those decisions
    - The end entities trust the Electors as a matter of crypto, but the Electors are just validating the SCMS Manager's decision



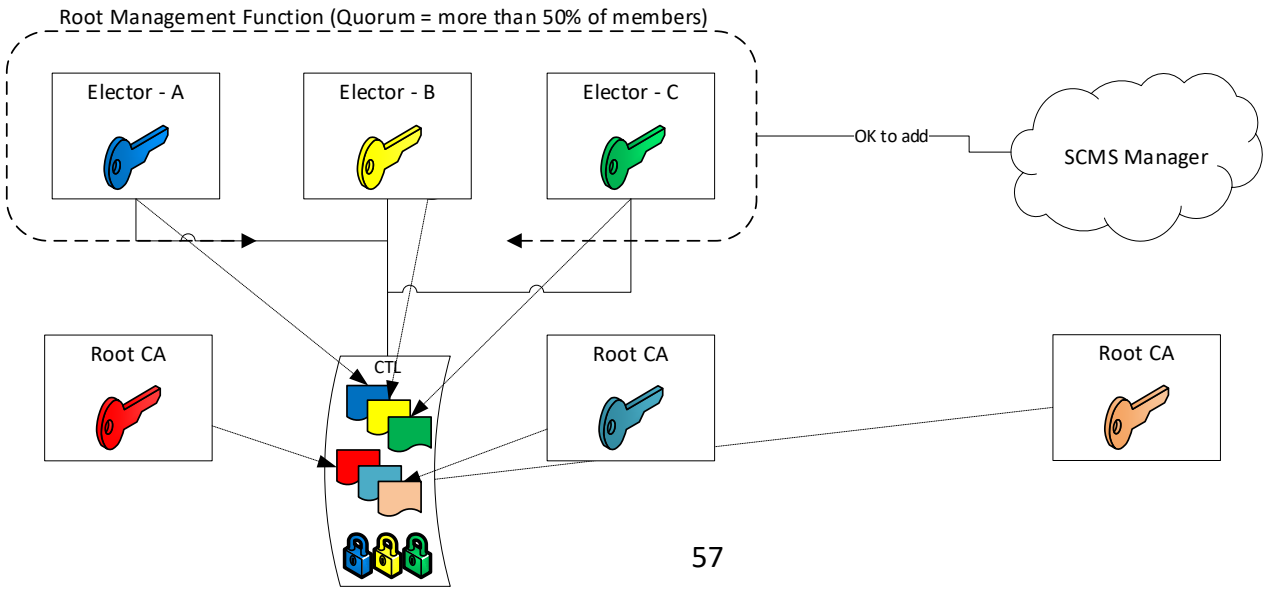
Electors contd.

- Electors are entities that sign Certificate Trust Lists (CTLs)
- A CTL is trustworthy if it is signed by a quorum (“m of n”) Electors
  - The number of Electors and the quorum are system parameters selected by the SCMS Manager
  - Having multiple Electors gives robustness against compromise and smoother transitions when an Elector certificate is retired



Electors contd.

- Electors are entities that sign Certificate Trust Lists (CTLs)
- A CTL is trustworthy if it is signed by a quorum (“m of n”) Electors
- When the Elector system is rolled out, deployment managers will no longer have to be concerned with specifying which Root CA to trust – everything will be handled automatically and transparently
  - Electors currently exist under scmsmanager.org, client software support is under development



ACTIVITY

Question 2

Which of the following is good practice for a CA?

Answer Choices

a) Share its private key with the authorities to assist with legal investigations of hackers.

b) Issue certificates to anyone who pays a fee.

c) Require end entities to submit a copy of their private key before receiving a certificate.

d) Ensure that certificate requesters meet minimum standards for security and are entitled to the requested certificate.

Review of Answers

a) Share its private key with the authorities to assist with legal investigations of hackers.

Incorrect. If the CA shared its private key this would allow anyone who knew the private key to issue certificates.

b) Issue certificates to anyone who pays a fee.

Incorrect. The CA should ensure that requesters are entitled to the requested certificate, not just that they have paid a fee.

c) Require end entities to submit a copy of their private key before receiving a certificate.

Incorrect. End entity private keys should exist only on the end entity device to ensure that no-one can forge signatures from that end entity.

d) Ensure that certificate requesters meet minimum standards for security and are entitled to the requested certificate.

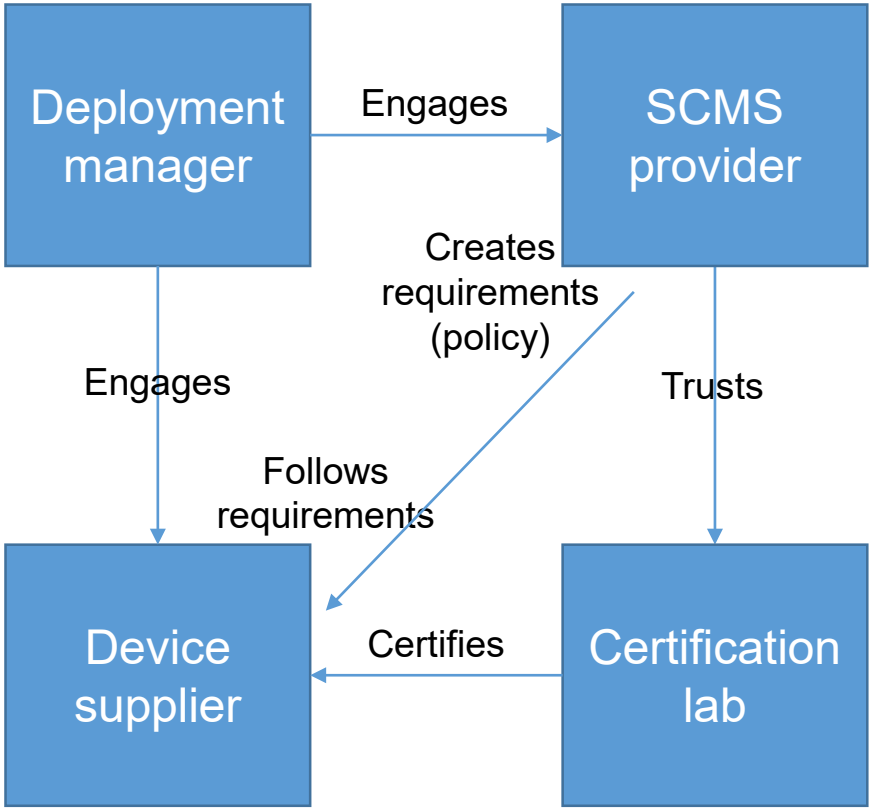
Correct!

Learning Objective 3

Understand how devices participate in the SCMS to get certificates

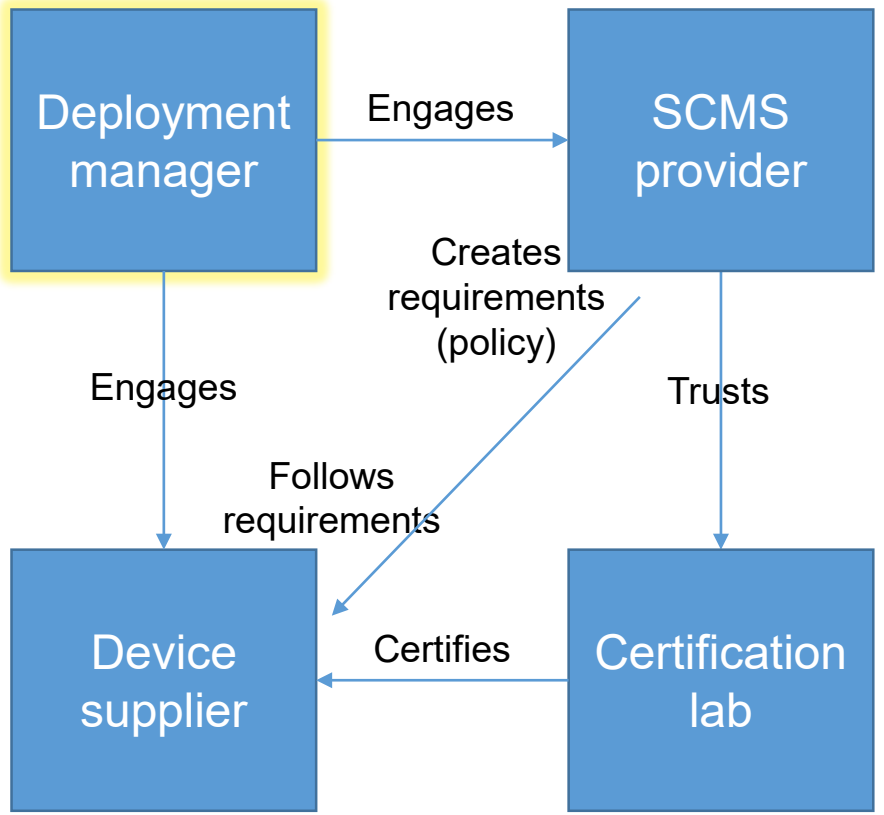
Parties Participating in the SCMS

- Deployment manager
- SCMS provider
- Device supplier
- Certification lab



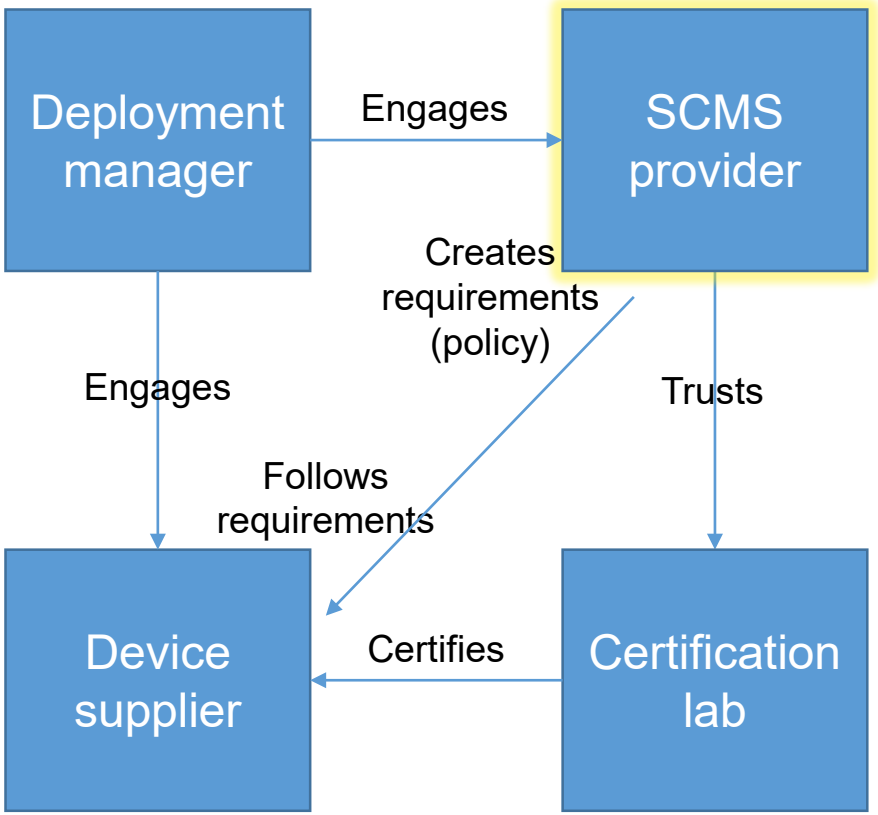
Deployment Manager Responsibilities

- Selecting and contracting with SCMS provider
- Determining device suppliers
- Determining which set of Root CA certificates should be trusted



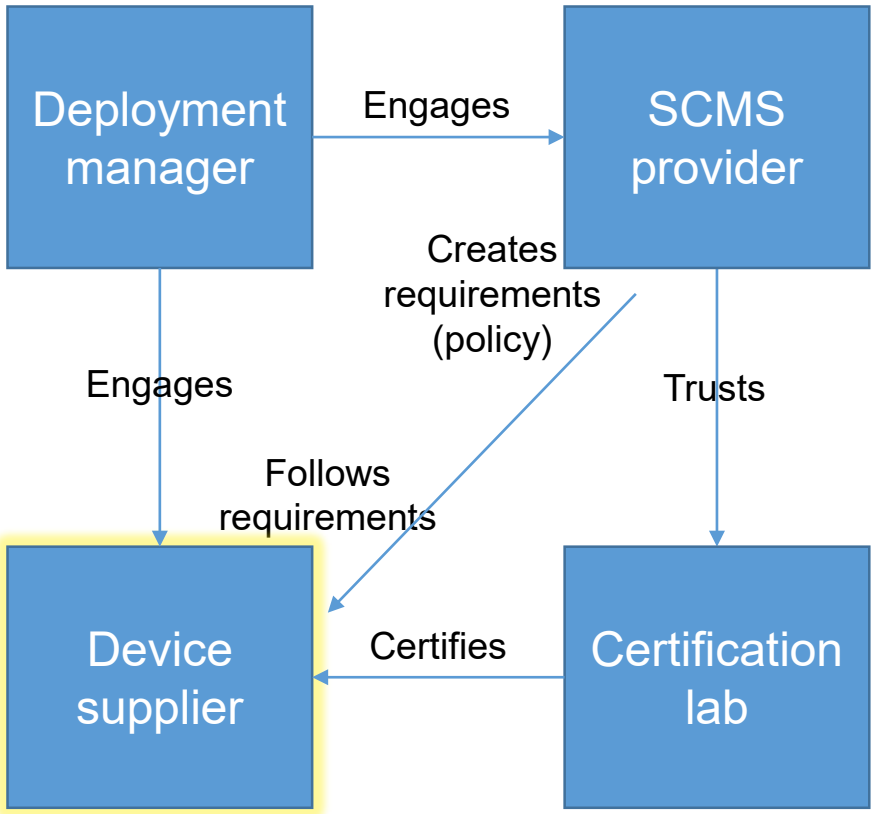
SCMS Provider Responsibilities

- States certificate and security policies for devices with "standard" applications
  - May include a requirement for third party type certification by certification labs – SCMS provider will indicate which certification labs are approved/accredited
- Works with deployment manager to specify certificate and security policies for deployment-specific applications
- Runs
  - Enrollment CA (ECA), Registration Authority (RA) (points of contact for devices as described in LO2)
  - Authorization CA (ACA)
  - In the future it will probably be possible to select ECA, RA, ACA from different providers



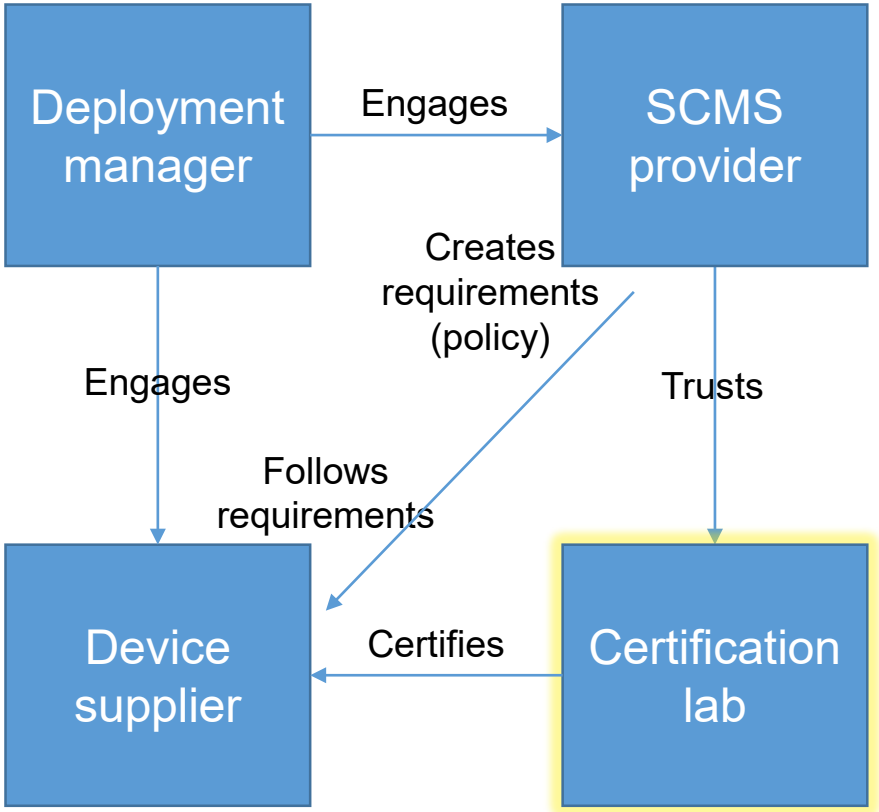
Device Supplier Responsibilities

- Provides deployment manager devices with 1609.2 and SCMS client software
- Responsible for meeting security and interoperability requirements
- May need to interact with certification lab



Certification Lab Responsibilities

- Works with device supplier to determine that device meets requirements
- Trusted by SCMS Manager
- Not necessarily directly engaged by deployment manager but may interact with deployment manager
- Currently some certification services are provided by OmniAir



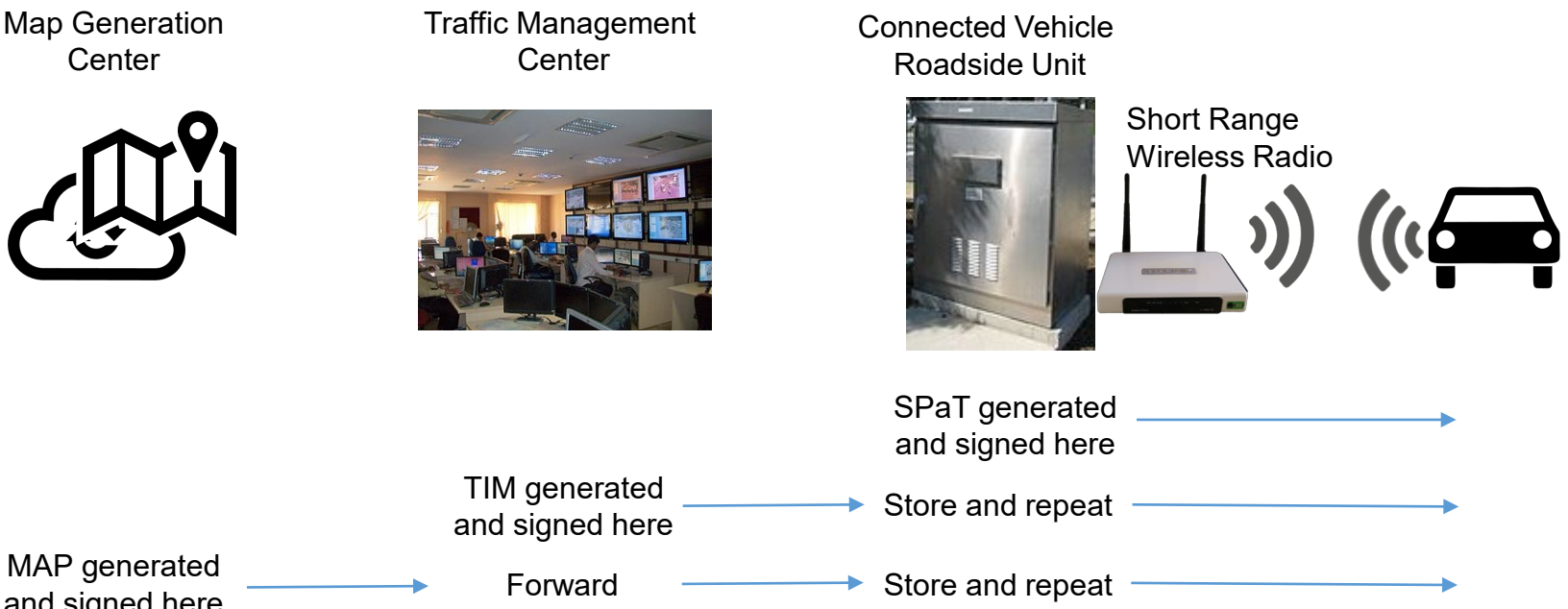
Third-party SCMS Providers

- It is recommended to use a third party SCMS provider
- Running SCMS components is not easy, specially Root CAs
  - Secure key storage
    - Some SCMS providers use a vault in a mountain!
  - Waking the CA up and using it
  - Enforcement of policy
  - Audit
  - Potential liability
- SCMS should be run internally only if the manager has significant experience running Public Key Infrastructure (PKI)

Image source: wikimedia.org

Interactions between devices and the SCMS

- All devices that use certificates should come fully equipped with certificate management software
- Deployment sites may also want centrally generated messages, e.g., map messages or traveler information messages



Interactions between devices and the SCMS contd.

- These should be signed centrally rather than at RSUs
  - Messages should be signed at the point of generation not distribution
  - If all RSUs can sign a “centrally generated” message, then a compromised RSU allows the system to be (temporarily) flooded with fake messages
- This will require negotiation with the SCMS provider to set the security requirements
  - Is it enough to generate the message on a box at the Traffic Management Center (TMC) with a smartcard or is an appliance with heightened security needed?
  - What are network security requirements to ensure correct operation on the box at the TMC?
- Existing deployments have successfully used certificates for centrally generated messages, so the problem can be addressed
- If centrally generated messages will be part of a deployment, then security requirements should be addressed early in the process

ACTIVITY

Question 3

What is the minimum number of Root CAs that must be supported in a deployment?

Answer Choices

a) Zero.

b) One.

c) Two.

d) All existing Root CAs.

Review of Answers

a) Zero.

Incorrect. If no Root CAs are trusted, the system cannot operate.

b) One.

Correct!

c) Two.

Incorrect. A system can operate correctly with only one trusted Root CA.

d) All existing Root CAs.

Incorrect. When the Elector system is stood up, devices will automatically trust all Root CAs, but this is not necessary for a deployment.

Module Summary

Define communications security requirements in the Connected Vehicle (CV) environment

Describe how the Security Credential Management System (SCMS) uses cryptographic building blocks to provide trust

Understand how to get devices interacting with the SCMS in a deployment

Next Course Module

Module CSE 201:
Introduction to SCMS Part 2 of 2

Concepts taught in next module (Learning Objectives):

4) Identify the Vehicle-to-Everything (V2X) certification process for a device to enroll in the SCMS

5) Illustrate how to make a deployment plan that uses SCMS services

Next SCMS Module

- **CSE 201**: Introduction to Security Credential Management System Part 1 of 2

- **CSE 201**: Introduction to Security Credential Management System Part 2 of 2

Thank you for completing this module.

Feedback

Please use the Feedback link below to provide us with your thoughts and comments about the value of the training.

Thank you!