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

Free ITS Standards Training

Over 70 web modules on how to evaluate, procure, and deploy standards-based highway and transit technologies.

Learn More ➔

www.pcb.its.dot.gov

Module CSE201:

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

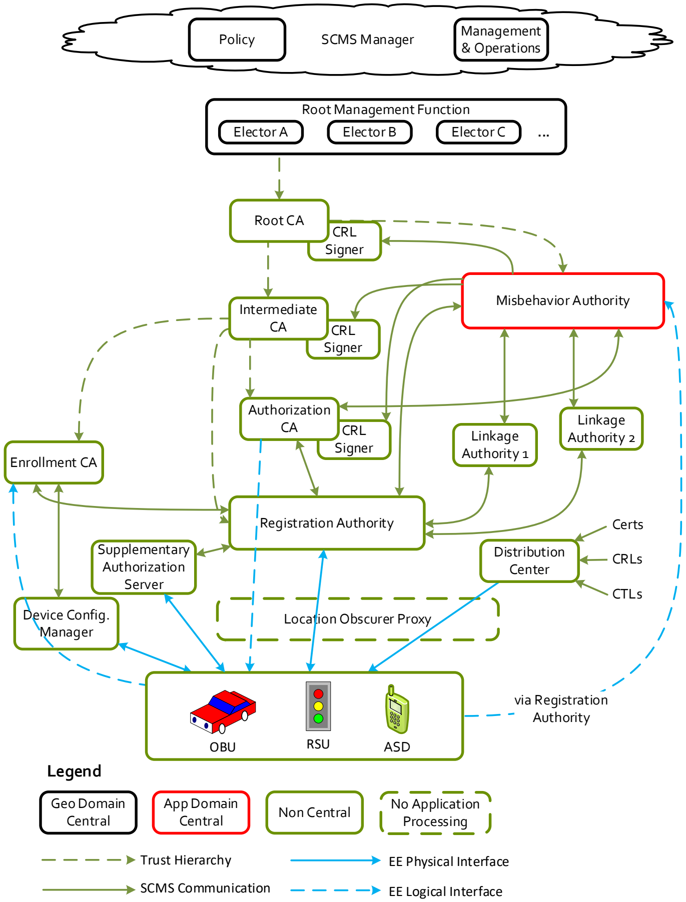


Image source: IEEE P1609.2.1

Instructors

Dr. William Whyte

Senior Director, Technical Standards

Qualcomm Technologies, Inc.

Dr. Virendra Kumar

Senior Staff Engineer,
Technical Standards

Qualcomm Technologies, Inc.

Learning Objectives-Part 2 of 2

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

Recap of Learning Objectives 1-3

- 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
- Major challenges in SCMS deployment include
  - Enrolling devices – establishing that they are entitled to certificates, especially for specialized applications
  - Keeping devices provisioned with certificates – this requires regular access to the Internet
  - Understanding which devices should have their certificates withdrawn (*revocation*)
- It is recommended that deployers work with an SCMS service provider rather than trying to run SCMS Services themselves

LO 4

LO 5

Learning Objective 4

Identify the Vehicle-to-Everything (V2X) Certification Process for a device to enroll in the SCMS

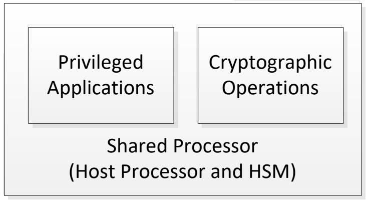
Security Requirements for Devices

- The security requirements on a device are the security requirements for all the application activities that device is carrying out
  - To determine the security requirements for a device, work out the requirements for each application it runs, and aggregate them
    - The NIST Cybersecurity framework (PCB Course CSE202, Intro to Cybersecurity for Agencies) provides a way for the deployment manager to analyze the security requirements of devices in a deployment
    - Determine the sensitivity of each “information flow” starting or ending at a given device to confidentiality, integrity and availability
  - For many applications, this work has already been done
    - ARC-IT contains security analysis for all applications
- Four device security classes have been defined and can be referenced in procurement documents
  - Classes refer to different combinations of confidentiality / integrity / availability capabilities
  - Definitions are in CV Pilot Deployment documents

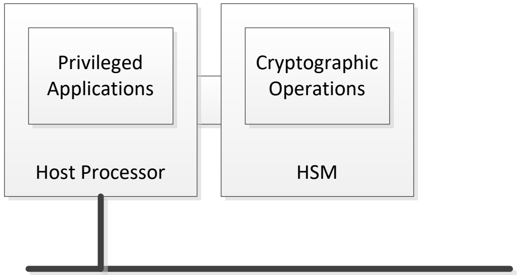
SUPPLEMENT

Baseline Security Requirements

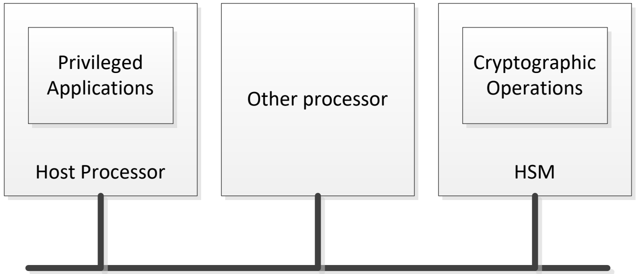
- For a device to be trusted to run a particular application, it must meet
  - General security requirement common to all devices
  - Application-specific requirements.
- Devices need to protect key material against being revealed
  - Integrated / Connected / Networked architectures all possible
    - "Architecture" refers to connection/link between application processor and Hardware Security Module (HSM)
  - HSM protection is specified by standards such as Federal Information Processing Standard (FIPS) 140



Integrated architecture



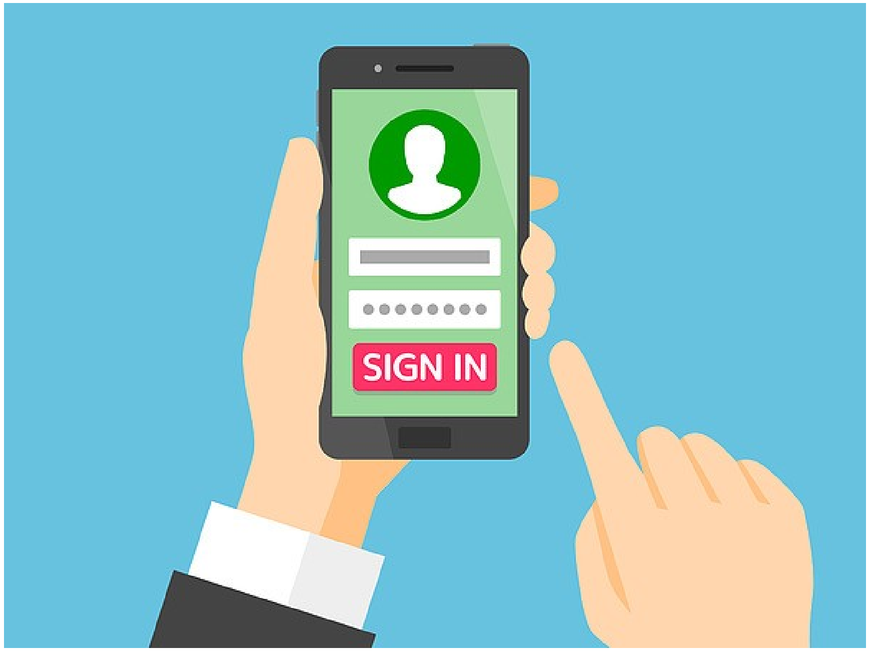
Connected architecture



Networked architecture

Baselines Security Requirements (2)

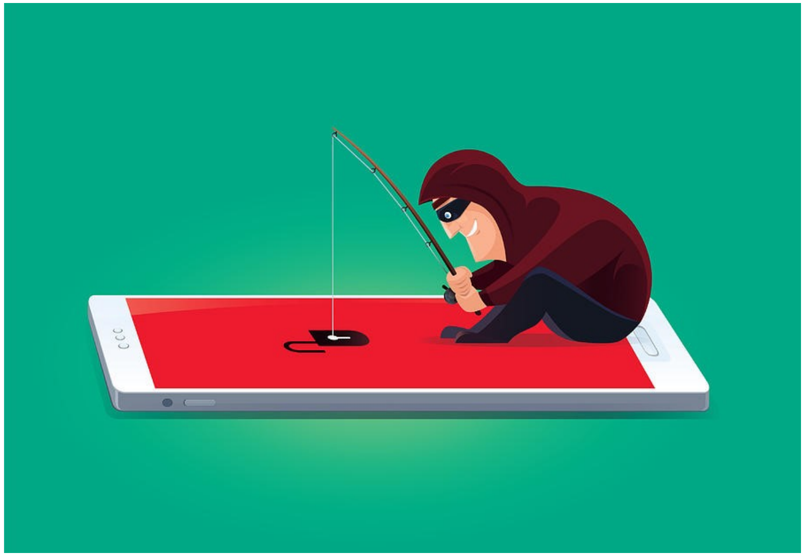
- Devices need to enforce secure update mechanisms
  - Ensure that all changes to software, firmware, or configuration are made by an authorized party
- For higher security levels, operator authentication may be needed
- Different requirement documents exist
  - OmniAIr Hardware/Software/OS Security Guidelines
  - Car2Car Communications Consortium Protection Profiles
- It is up to the SCMS to say exactly which requirements apply – all sets of requirements are broadly similar, but details may differ



SUPPLEMENT

Baseline Security Requirements (3)

- Devices need to protect against key material being used by illegitimate users
  - Malware protection
  - Ensure a key can be used only by approved processes on the devices
- Devices need to enforce secure boot
  - Secure boot ensures that if a device is tampered with, this will be detected by the boot mechanism and access to sensitive or security-critical data can be cut off
  - It is a local activity that does not need intervention from a network entity



Security Certification via OmniAir

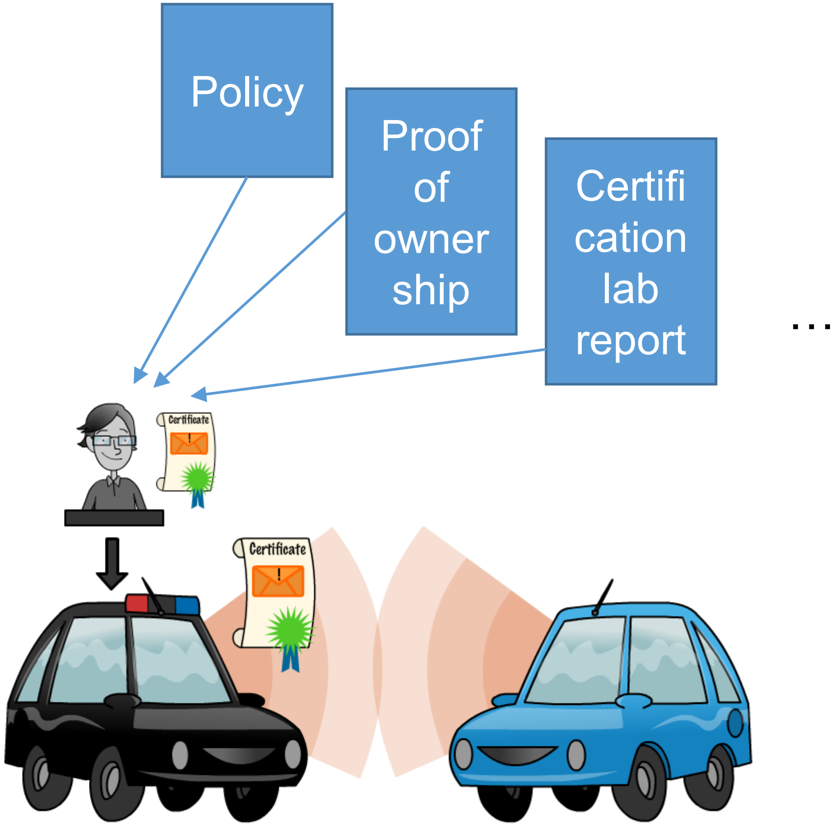
- The OmniAir testing consortium is defining formalized security requirements for V2X devices
- There is no formal, national policy that an SCMS operator requires OmniAir certification, but in practice existing SCMS operators respect OmniAir certification
- OmniAir runs several PlugFests a year where interoperability can be tested; full conformance testing for security is likely to be available by early 2021

OMNIAIR®

CONSORTIUM

Special Permissions

- Conditions for certificate issuance are application-specific
- Some applications can be issued with certificates at the factory
  - BSM signing
- Other applications need assertion from a real-world authority that certificates can be issued
  - Police car certificates
- Different applications may need devices with different properties
  - Devices that can do signal preemption may need the driver to sign in
- For a lot of applications, the conditions are still being worked out – talk to your SCMS provider



Policy

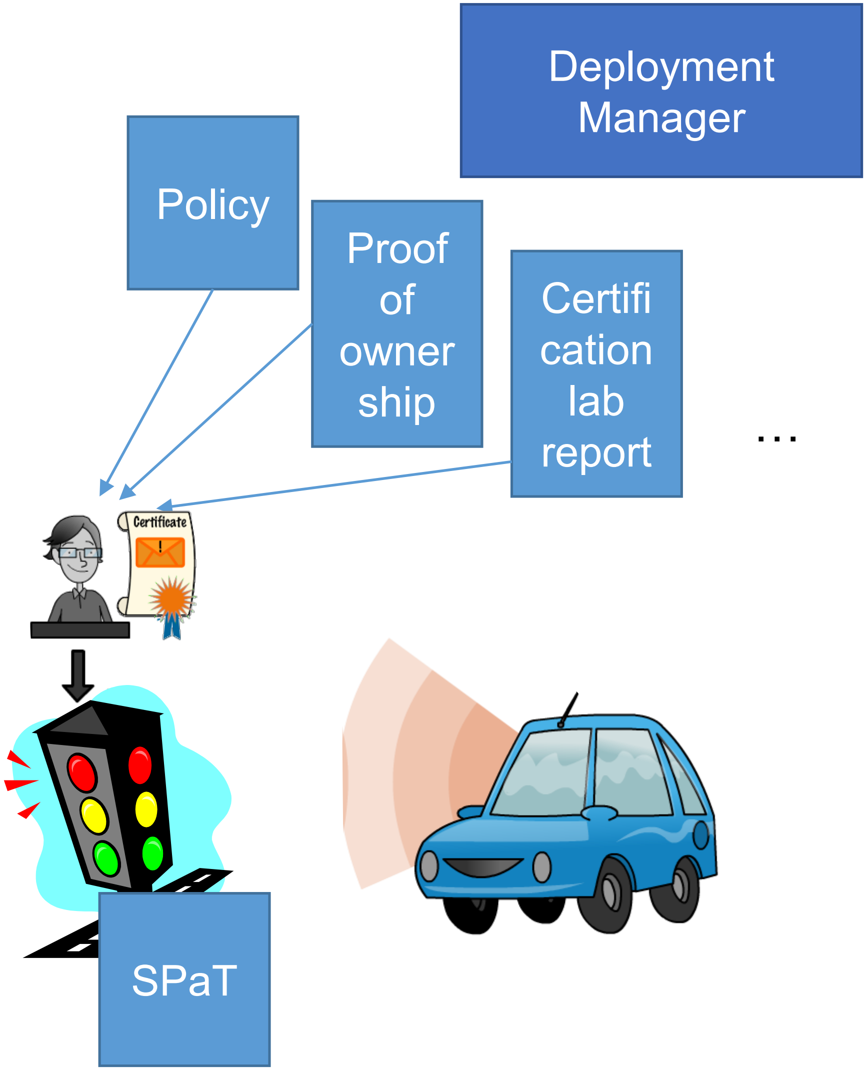
Proof of owner ship

Certifi cation lab report

…

Additional Functionality via New Software

- A device may in principle be deployed with an initial set of applications and later have new applications added
  - In this picture, an RSU is deployed with SPaT, and later upgraded to support Signal Request / Status Message (SRM / SSM)
- In the original CAMP interface, the device would need a new enrollment certificate
- In the new interface defined in 1609.2.1, the SCMS can update the permissions associated with the enrollment certificate
  - In order for it to do this, the deployment manager will have to demonstrate that the new application was valid and was validly installed
  - Processes for doing this are still manual
    - If you're a deployment manager, discuss this with your SCMS provider before deploying new applications



ACTIVITY

Question 4

Which of these is required for a device to be secure enough to run V2X applications?

Answer Choices

a) The device requires a user to log in before it will send any V2X messages.

b) The device requires user permission for updates.

c) The device supports virtualization.

d) The device protects its keys with a hardware security module.

Review of Answers

✗ a) The device requires a user to log in before it will send any V2X messages.

Incorrect. Many types of devices, such as standard on-board units in cars, are expected to start broadcasting without requiring the user to log in.

✗ b) The device requires user permission for updates.

Incorrect. Updates must be secured, meaning that they must be authenticated as coming from a trusted source, but they do not need the user’s explicit permission. It is a courtesy to inform the user that an update is taking place, but user permission is not required so long as the device can ensure that the update is taking place under safe conditions.

✗ c) The device supports virtualization

Incorrect. Virtualization can improve security by sandboxing different applications, preventing one application from interfering with another’s operations, but it is not a requirement – especially for devices like standard on-board units that only send one type of message.

✓ d) The device protects its keys with a hardware security module.

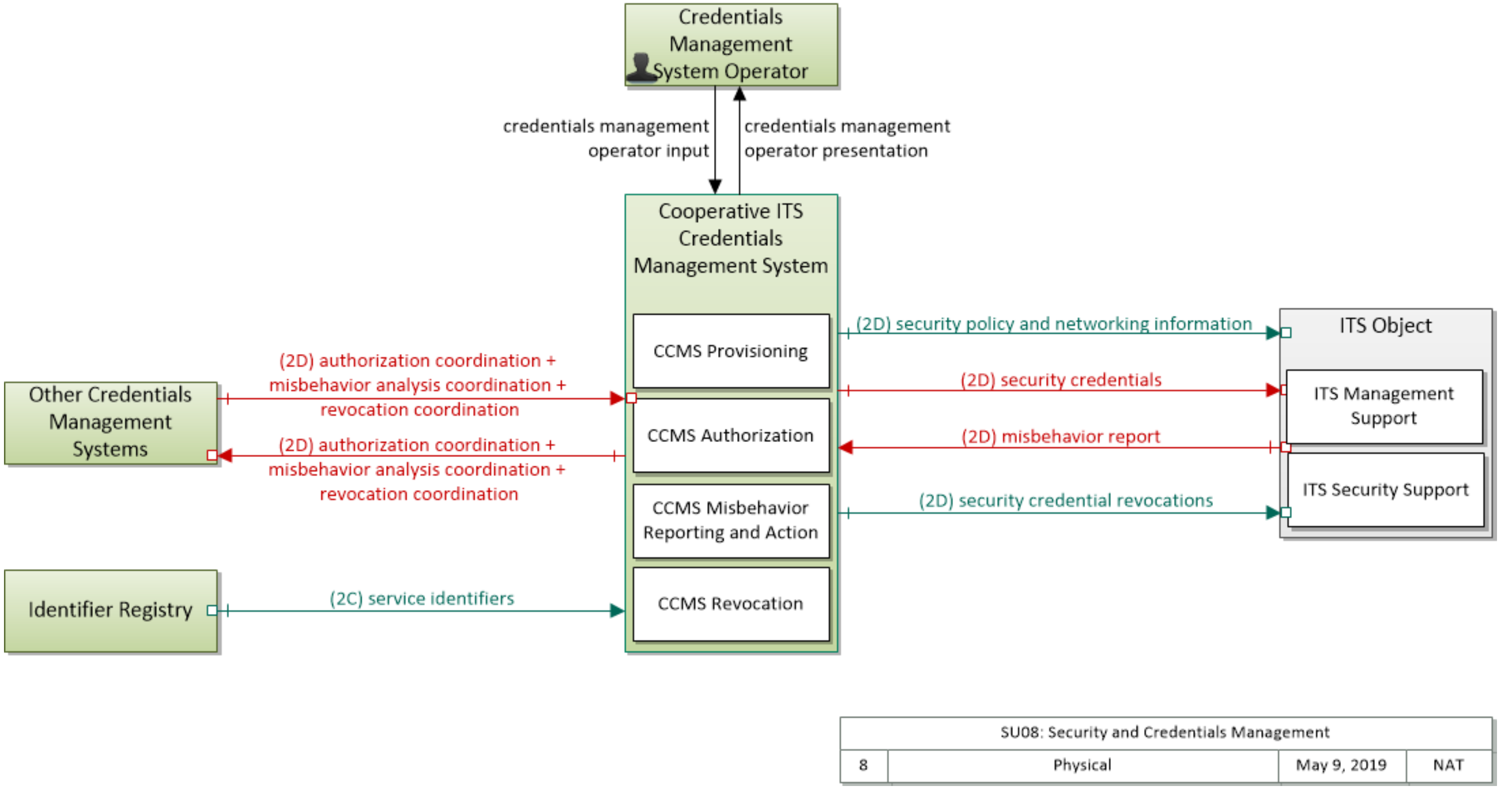
Correct! If the keys are not protected with a hardware security module, an attacker who gets access to the device can potentially obtain a copy of the keys and use them to forge messages.

Learning Objective 5

Illustrate how to make a deployment plan that uses SCMS services.

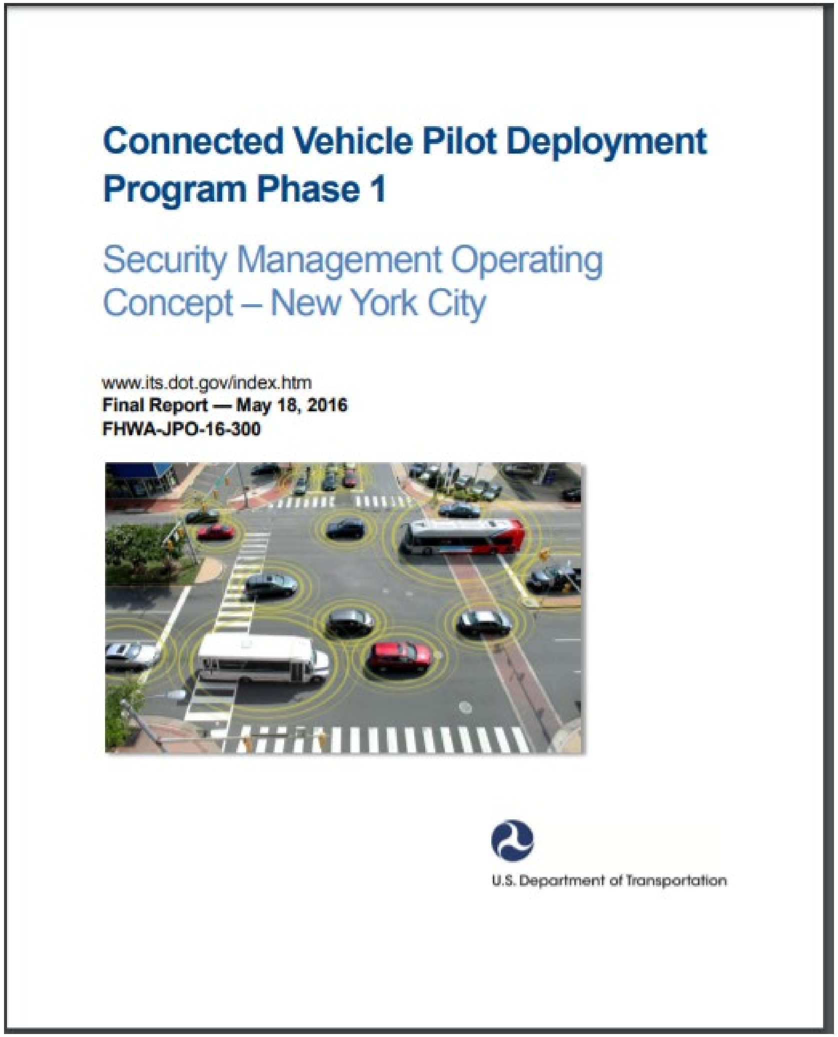
SCMS Design: SCMS In ARC-IT

SCMS services are fully described in ARC-IT and their deployment can be planned using the same tools that are used to plan the deployment of other Connected Vehicle services.


Credentials Management System Operator
credentials management operator input
credentials management operator presentation
Cooperative ITS Credentials Management System
CCMS Provisioning
CCMS Authorization
CCMS Misbehavior Reporting and Action
CCMS Revocation
Other Credentials Management Systems
(2D) authorization coordination + misbehavior analysis coordination + revocation coordination
(2D) authorization coordination + misbehavior analysis coordination + revocation coordination
Identifier Registry
(2C) service identifiers
ITS Object
ITS Management Support
ITS Security Support
(2D) security policy and networking information
(2D) security credentials
(2D) misbehavior report
(2D) security credential revocations
SU08: Security and Credentials Management
8
Physical
May 9, 2019
NAT

Security Management Operating Concept

- Deployments should develop a Security Management Operating Concept that
  - Identifies security requirements on each information flow
  - Uses this to determine device security requirements
  - Uses this to identify security mechanisms for information flows
    - 1609.2 certificates and signing may not necessarily be the correct security mechanism for each flow
- For information flows that use 1609.2 certificates
  - Specify the “security profile” (basic profile already part of the standard)
  - Identify the PSID to use
  - Determine certificate issuance policy



Connected Vehicle Pilot Deployment Program Phase 1

Security Management Operating Concept – New York City

www.its.dot.gov/index.htm

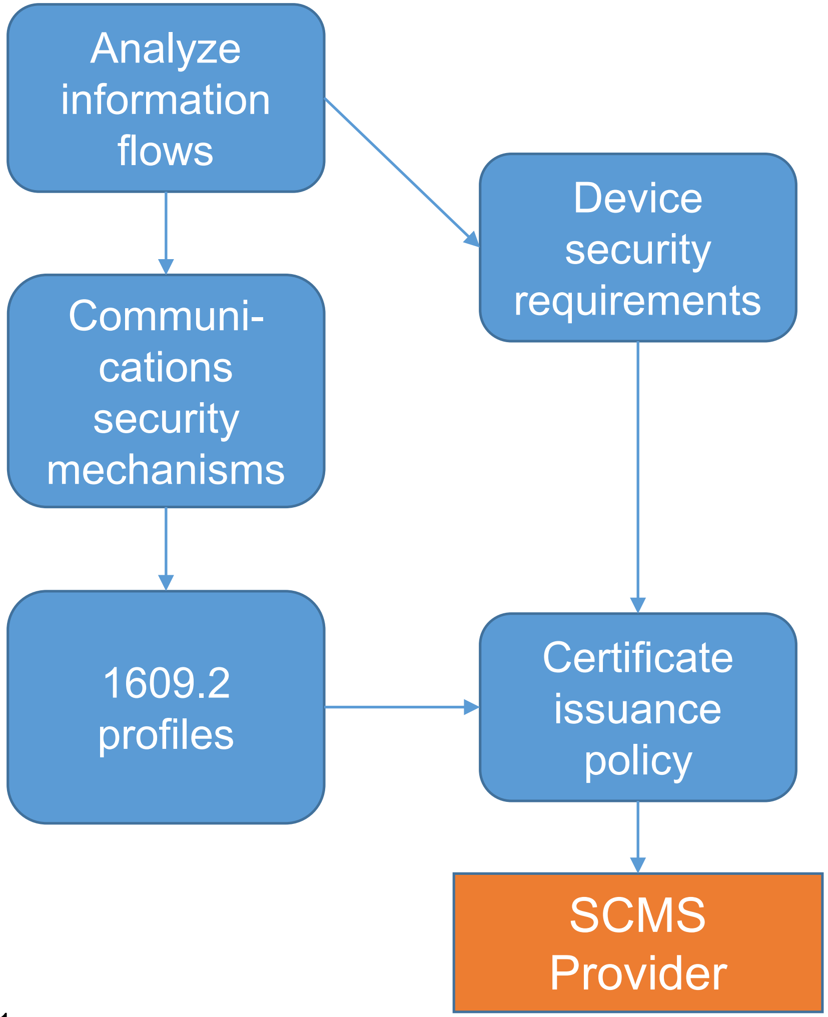
Final Report — May 18, 2016

FHWA-JPO-16-300

U.S. Department of Transportation

Security Management Operating Concept

- Deployments should develop a Security Management Operating Concept that
  - Identifies security requirements on each information flow
  - Uses this to determine device security requirements
  - Uses this to identify security mechanisms for information flows
    - 1609.2 certificates and signing may not necessarily be the correct security mechanism for each flow
- For information flows that use 1609.2 certificates
  - Specify the “security profile” (basic profile already part of the standard)
  - Identify the PSID to use
  - Determine certificate issuance policy


Analyze information flows
Device security requirements
Communi-cations security mechanisms
1609.2 profiles
Certificate issuance policy
SCMS Provider

CASE STUDY

U.S. Department of Transportation
ITS Joint Program Office
Image Source: Thinkstock USDOT

Case Studies

- New York City Pilot Deployment:
  - Central generation of TIMs and MAPs
    - Generated centrally at the TMC
      - Need a “security appliance” to generate the signatures – to protect keys and ensure messages are correct
  - SPaTs generated at RSU
    - RSUs certified as appropriately secure

- Tampa: Roadside generation and signing of SPaT and MAP
  - Need to get devices approved for certificates before installation

- Minneapolis: Allow snowplows to request signal prioritization
  - Devices are issued with certificates when they are provided to the site

Lessons Learned

- Production SCMS is needed for RSU certificate updates
  - RSUs need to be able to access the SCMS at least once a week
- Production SCMS is needed for certificate top-off for the OBUs
  - OBUs need to be able to access the SCMS at least once a week
  - Test all connections, especially if OBUs are connecting through RSUs and especially if IPv6-to-IPv4 translation is to be carried out
  - Test correct operation if the first certificate download fails; i.e., repeat download request
- Test that the system behaves correctly when devices transition between certificates, i.e., when one certificate expires and a new one is expected to be used
  - Devices attempt to update certificates in a timely manner
  - Devices stop using the old certificates and start using the new certificates at the appropriate time, i.e., before expiration of the old and after start-validity of the new
  - If there are conditions that inhibit certificate change (e.g.. alert state per J2945/1) test that system transitions correctly after condition stops holding

Lessons Learned Continued

- Integrate the CV needs into the agency’s cybersecurity program early on in the project
  - Network traffic necessary for SCMS operation will require various firewall settings, proxy servers, etc., that will need to meet the agency’s overall cybersecurity standards
- Maintain a secure, trusted network environment for the CV pilot deployment system
  - Try to isolate it from the general traffic management network
- Test the OTA download and upload mechanisms before extensive installation of the ASDs and RSUs
- For multi-application devices, understand whether there will be one certificate per application, one certificate per device, or something else
  - Some RSU vendors only support a single application certificate covering all PSIDs.
- Ensure that the RSU firmware permits sending pre-signed messages (MAP, TIM).

Other Lessons Learned

1. Ensure certificate top-off is robust against losing connectivity mid-top-off
   - Protocols are meant to give robustness, but implementations need to be tested
2. Ensure certificate top-off succeeds even if a device has not successfully topped off for some time
   - If certificate lifetime is a week and devices top-off up to 2 weeks in advance, make sure that a device that has been out of contact for a month can connect
3. Ensure that repeated requests for a certificate for a particular time period cause only a single certificate to be generated, not one certificate per request
   - Provides protection against “sybil attacks”
4. Test enrollment certificate expiry and rollover

Other Lessons Learned

5. Test that certificate management software works across expiry of an ACA certificate or an ECA certificate
   - Both for devices that get certs from that ACA/ECA, and for devices that trust them.
6. Ensure that new CA certificates can be distributed in a timely way
   - If there is a new ACA, ensure that trust of the new ACA certificate does not act as a gatekeeper for access to certificate updates.
   - For example, in one case, network connectivity was provided by RSUs that started to use a certificate from a new ACA to advertise that connectivity: OBUs that did not already have the new ACA certificate could not trust the advertisement, and so could not connect to update the ACA certificate.
7. Ensure there is a good way to get feedback to SCMS Manager and other governance bodies

Misbehavior Reporting and CRL Download

- Messages with bad data / that will cause bad outcomes
- CV Pilot Deployments have implemented baseline misbehavior reporting mechanisms and some SCMS providers have implemented misbehavior investigation and revocation
- Deployments may want to implement additional revocation conditions
  - For example, if a pilot deployment device is stolen, it may be easier to revoke it to prevent misuse
- SCMS Providers should be asked about performance metrics – the time between a report being submitted that leads to revocation and the CRL being issued
- Deployments may want to support other means of CRL distribution beyond direct download from the RA, such as broadcast by RSUs
  - There is currently no standard that supports this, so this would be a custom development

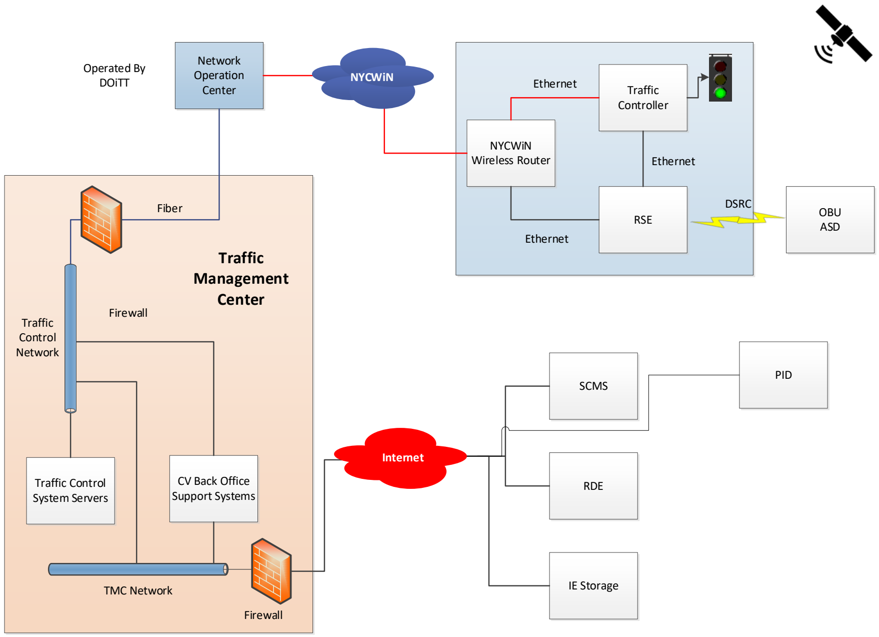
SCMS Design: Misbehavior Management – open questions

- Questions for SCMS provider
  - … that affect operational interactions with the SCMS
    - Is there another way to report devices that need to be revoked; for example, devices that have had their private keys extracted?
  - … that provide information about expected system behavior
    - What's the "threshold" of bad behavior that a device must pass to be revoked?
    - How many different reporters must report a device before it's revoked? Are there different levels of trust in reporters?
    - How quickly should it be possible to revoke a misbehaving device?
    - How often do we create new CRLs?
    - Is there any process of appeal against revocation?
- Questions for device supplier and SCMS provider together
  - How can a revoked device be trusted again?
  - Is there any process of appeal against revocation?
  - If a device is producing bad data because of bad configuration, can we notify and fix the device rather than reporting it?

Traffic on the Infrastructure Owners and Operators (IOO) Network

- Most interactions between mobile devices and infrastructure in the V2X setting can naturally be confined to the traffic management network as they are primarily about exchanging local information
- SCMS network traffic is different as its natural endpoint is outside the Infrastructure Owners and Operators (IOO) network and remote on the Internet
    - Contact RA to download certificates
    - Contract RA to upload misbehavior reports

Network Connectivity Architecture



Traffic on the IOO Network contd.

- Many mobile devices will have cellular connectivity to enable SCMS communications but for some devices it may be necessary to provide Internet access via the IOO network
    - RSUs could potentially *only* be on the IOO network and will need specific consideration if so
    - Network connectivity is required for certificate update, so even mobile devices may require connectivity through the IOO network to avoid the risk that connectivity is not available due to, for example, cellular subscription expiring and/or Wi-Fi not being available
- SCMS architecture makes hosting SCMS components within the IOO network problematic – this needs to be reconciled with firewall rules for ingress/egress to the IOO network
- Each IOO network will address this question in their own way depending on local network configuration but implications need to be thought through early in the process

Incident Detection and Response

- In addition to misbehavior reporting, which is purely an SCMS activity leading to revocation, a deployment must be aware of other possible threats within the system

- These include various forms of denial of service as well as standard network cyberattacks

- IOO networks should already have network monitoring and other security mechanisms in place, but should review those to determine if a V2X deployment introduces new threats and, if so, whether the current security measures are adequate to defend against them

Data Management

- Many instances of Connected Vehicle applications result in the generation and potential collection of large amounts of data that could be personally identifying

- Deployment should not happen without a site data management plan to ensure proper handling of data

- This is not an SCMS concern, but it is conceivable that future certificate policies could make issuance of certs dependent on having a data management plan

- NIST and DOT have created a privacy analysis process for use with Connected Vehicle deployments

SUPPLEMENT

ACTIVITY

Question 5

Which of these is a correct statement about data collection and management?

Answer Choices

a) Only vehicles can produce personally identifying information.

b) Individuals must give consent to their data being collected.

c) If there is concern that data may reveal driver behavior that violates the law, it should be immediately shared with law enforcement.

d) Data must be managed in a manner consistent with local data protection regulations.

Review of Answers

✗ a) Only vehicles can produce personally-identifying information.

Incorrect. A deployment might include pedestrian devices which directly generate personally-identifying information. Additionally, fixed devices like cameras can generate information that might be linked to individuals.

✗ b) Individuals must give consent to their data being collected.

Incorrect. This depends on the applicable local data protection regulation.

✗ c) If there is concern that data may reveal driver behavior that violates the law, it should be immediately shared with law enforcement.

Incorrect. This will depend on the applicable local data protection regulation and other laws, but there is, in general, no requirement to be proactive about sharing data with law enforcement.

✓ d) Data must be managed in a manner consistent with local data protection regulations.

Correct! A deployer must be aware of local data protection regulations and ensure that they are complied with.

Module Summary Part 2 of 2

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

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

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

Introduction to SCMS Curriculum

✓
- **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!