ITU-T X.509 use case for V2X security credential management system

… or, how X.509 and other certificate types can play nicely together

William Whyte, Qualcomm Technologies Inc., 2022-05-09

Motivation

- 2.8 trillion vehicle miles traveled in 2001 in the US
- Nearly 43,000 deaths per year from automobile accidents
  - 1.59 per 100 million vehicle miles traveled
  - Leading cause of death for ages 4 to 34
- 3 million people injured
- 6 million crashes
- Automobile accidents cost $230B

- What to do?
  - Improved survivability
  - Short-range radar
  - **Improved data connections to vehicle**

Motivation

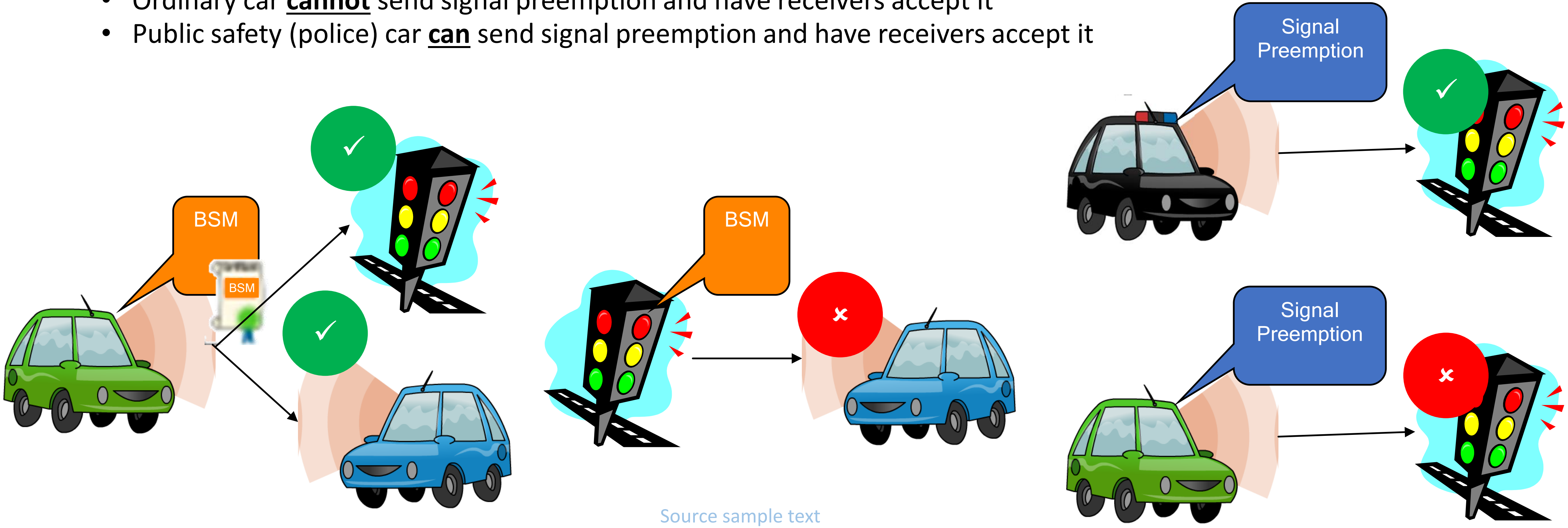
- 2.8 trillion vehicle miles traveled in 2001 in the US
- Nearly 43,000 deaths per year from automobile accidents
  - 1.59 per 100 million vehicle miles traveled
  - Leading cause of death for ages 4 to 34
- 3 million people injured
- 6 million crashes
- Automobile accidents cost $230B

- What to do?
  - Improved survivability
  - Short-range radar
  - **Improved data connections to vehicle**

Must be trustworthy!

Security goal

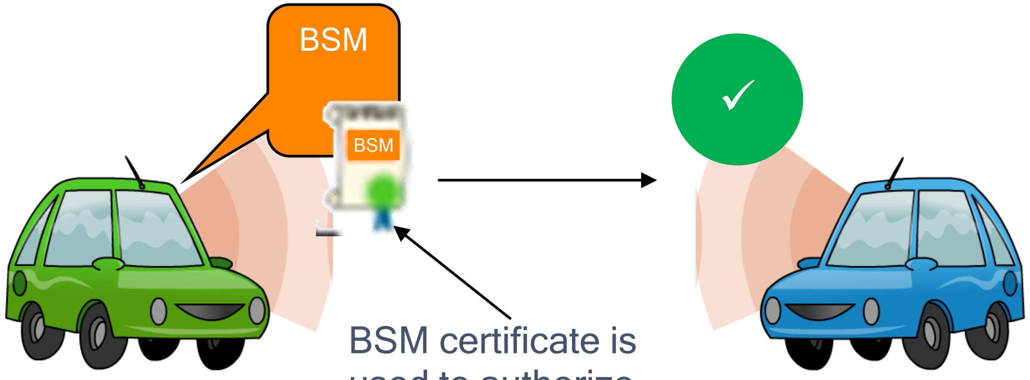
- Allow receivers to make trust decisions about received messages in real time with minimal increase in packet size
  - Ordinary car **can** send Basic Safety Message / Cooperative Awareness Message and have receivers accept it
  - RSU **cannot** send BSM / CAM and have receivers accept it
  - Ordinary car **cannot** send signal preemption and have receivers accept it
  - Public safety (police) car **can** send signal preemption and have receivers accept it



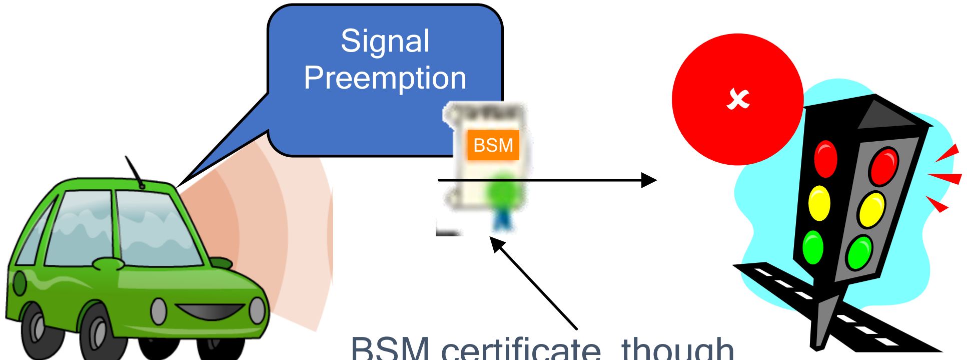
Source sample text

Approach: IEEE 1609.2 certificates

- Certificate states permissions; receiver checks that sender has the permissions they need to carry out the actions
- ITS-AID-based system is extensible to support arbitrarily many future applications
  - ITS-AIDs available from IEEE or from ISO to identify applications
- IEEE 1609.2 certificates are used in US, Europe (ETSI profile), China (CCSA harmonized standard), Korea, Australia, …
- Differences with X.509:
  - Smaller (due to use of OER v BER)
  - More optimized to be used as attribute certificates



BSM certificate is used to authorize BSM

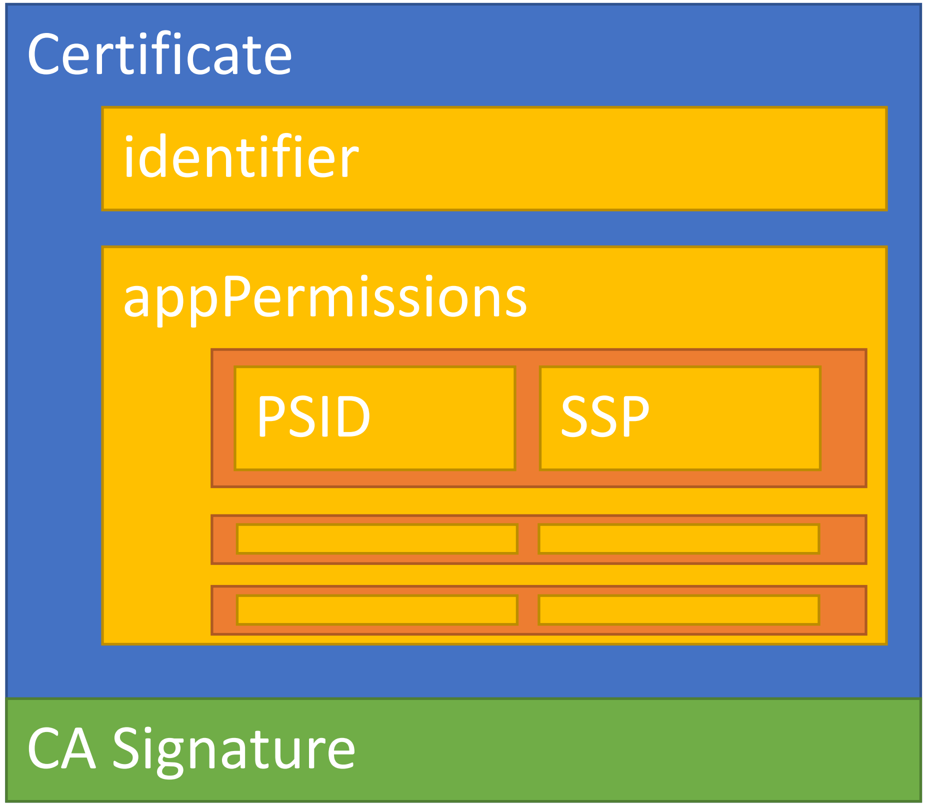


BSM certificate, though valid for BSM, cannot be used to authorize signal preemption message

Source sample text

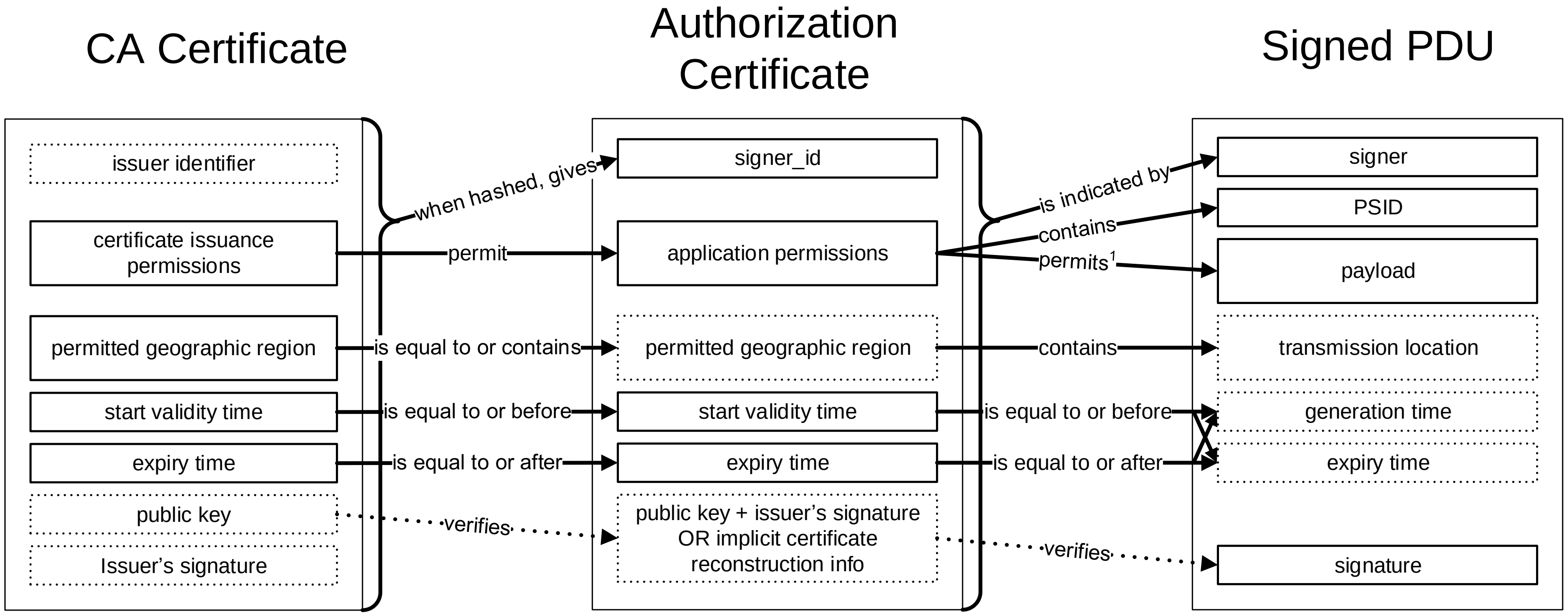
IEEE 1609.2 Certificates

- "Attribute certificates" – transmit authorizations, not identities
- Authorizations are indicated by Provider Service Identifier (PSID) and Service Specific Permissions (SSP)
  - PSID identifies the "application domain"
    - Send Basic Safety Message
    - Tolling
    - Signal Phase and Timing
    - Advertise other services
    - Weather reporting
    - …
  - SSP: additional PSID-specific authorization statements
    - Roles within application
    - Weather-related road management: center / vehicle
- Managed by IEEE and ISO, jointly

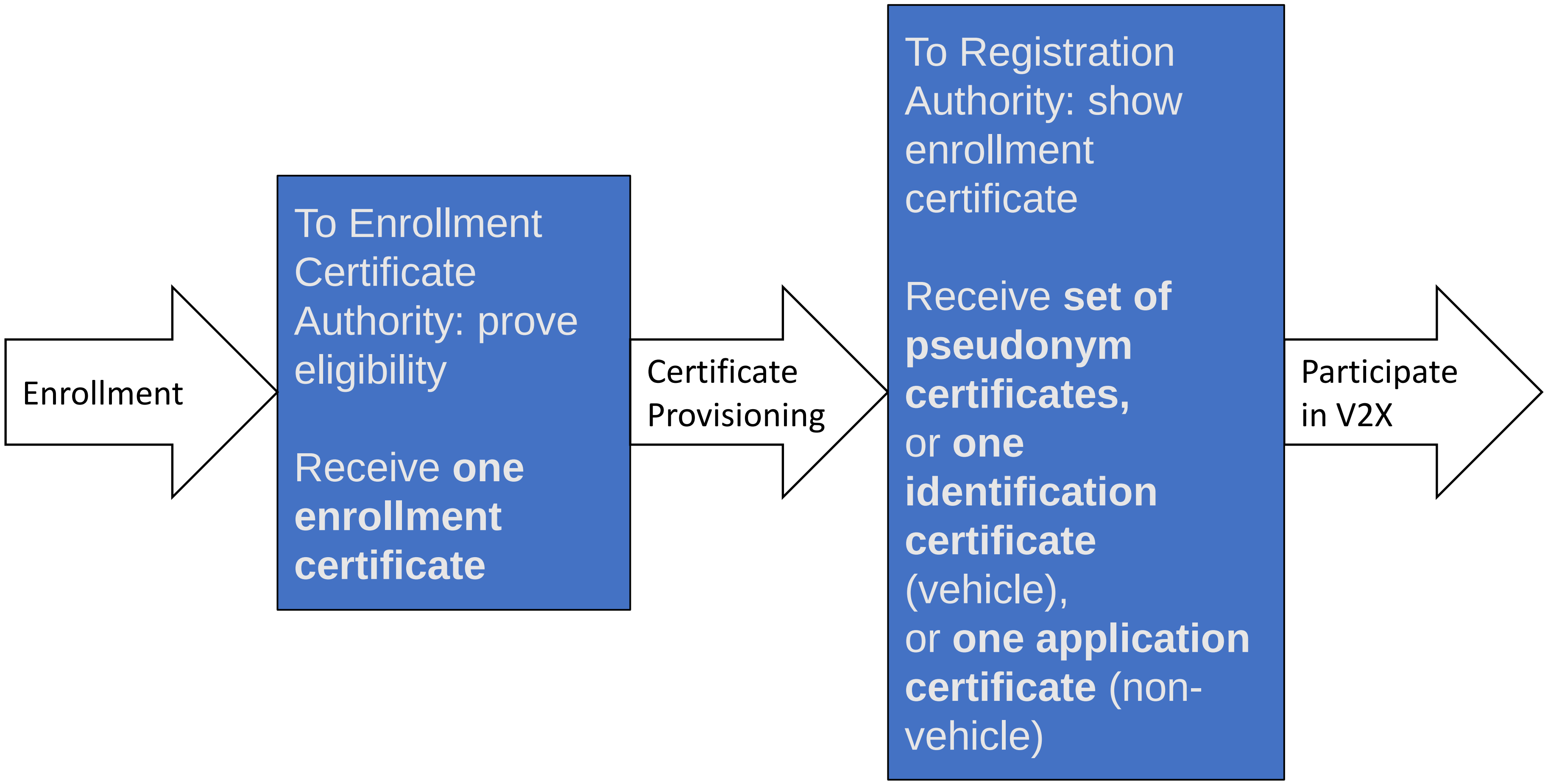


Consistency

- 1609.2 completely defines consistency conditions between certificates and messages, and between a CA certificate and a certificate that CA issued
- A message is only valid if all consistency checks are passed
    - Dotted boxes = optional fields; if present, they too must be consistent



Enrollment and authorization certificates



Enrollment

To Enrollment Certificate Authority: prove eligibility

Receive **one enrollment certificate**

Certificate Provisioning

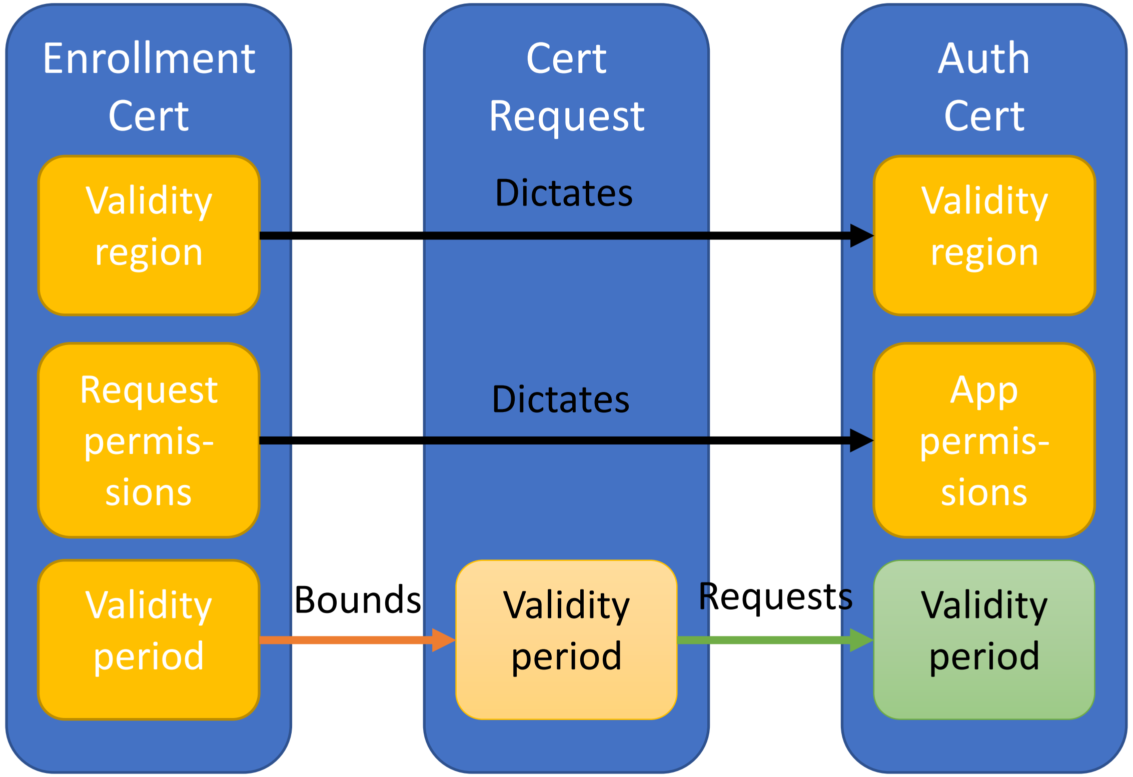
To Registration Authority: show enrollment certificate

Receive **set of pseudonym certificates,** or **one identification certificate** (vehicle), or **one application certificate** (non-vehicle)

Participate in V2X

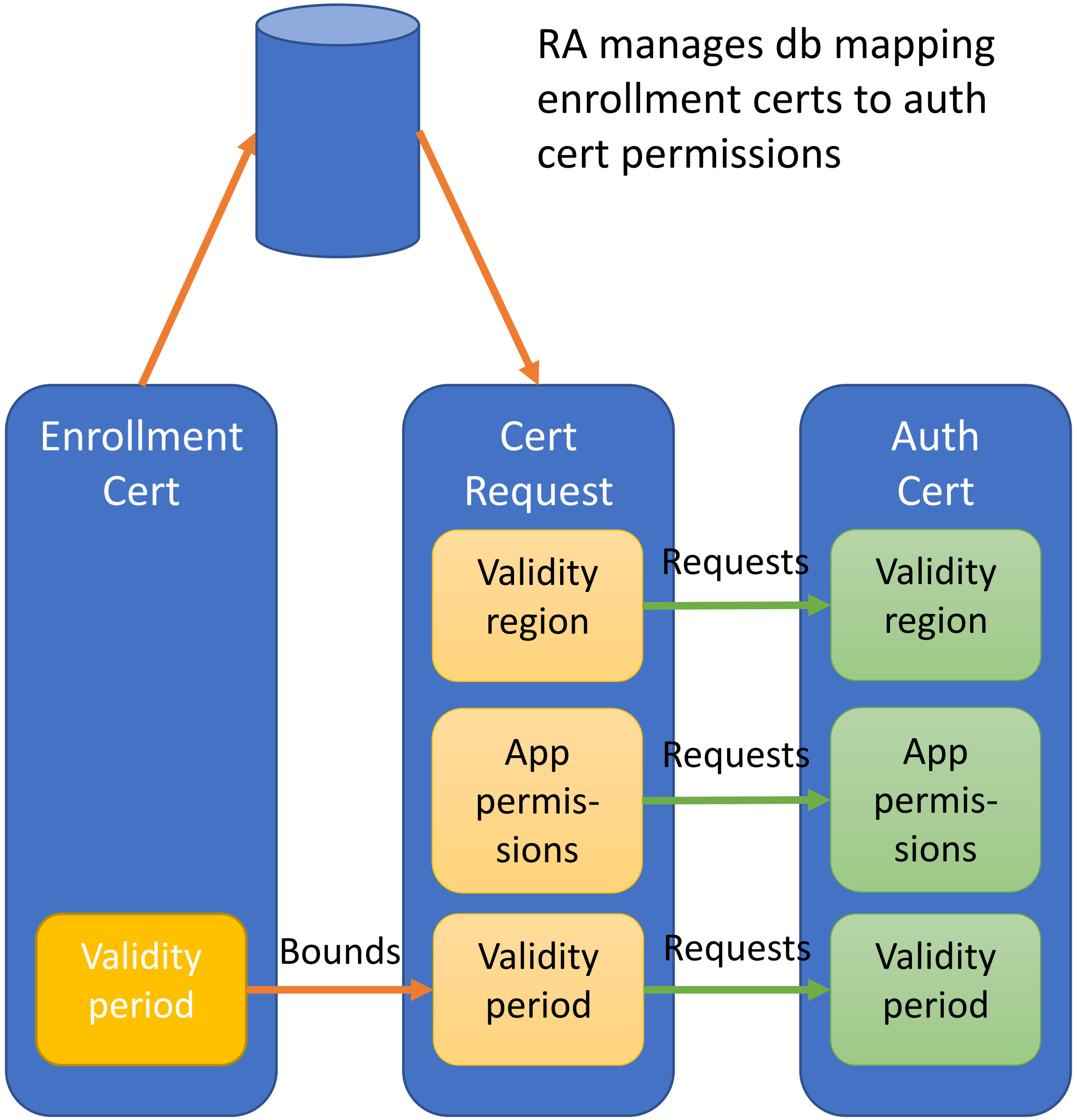
Enrollment certificate permissions: original model

- SCMS design: enrollment certificates and authorization certificates requested using them have one-to-one mapping of permissions
    - PSID: If the enrollment cert has PSID 23 then so do the authorization certs
    - Geographic Permissions: If the enrollment cert is bound to Times Square, then so are the authorization certs
    - No need to include permissions explicitly in request, they are dictated by enrollment cert
- Drawbacks
    - PSID:
        - Either, include all the permissions in one enrollment cert and risk getting fully revoked, even if only one of them needed to be actually revoked
            - Re-enrollment can be expensive and inconvenient
        - Or, spread out the permissions over multiple enrollment certs and increase the enrollment overheads including EE storage and communication
    - Geographic Permissions:
        - Either, include a large enough area to cover all use case scenario
        - Or, go through enrollment process for every new use case
- One-to-one mapping of permissions is not sustainable



Current model

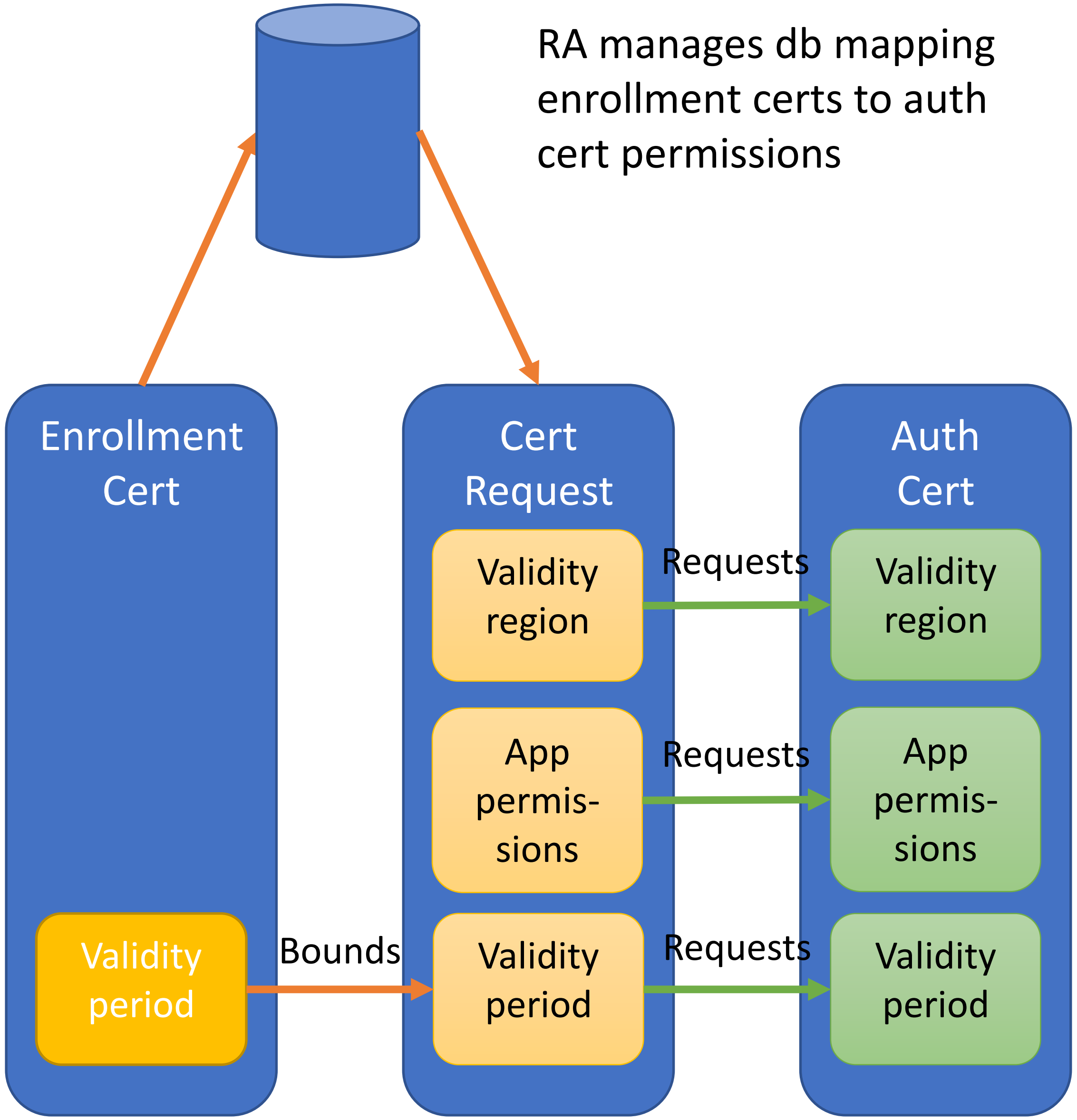
- Constraints on auth certs are managed out of band
  - One enrollment cert per EE: `certRequestPermissions.subjectPermissions` is set to `all`
  - Authorization cert permissions are handled by the RA
    - Enrollment certs are sent to the RA
    - Permissions associated with the enrollment cert are managed by the RA
      - Mechanism --> out of scope for 1609.2.1
    - EEs can request any subset of the allowed permissions



RA manages db mapping enrollment certs to auth cert permissions

Current model

- Constraints on auth certs are managed out of band
  - One enrollment cert per EE: `certRequestPermissions.subjectPermissions` is set to `all`
  - Authorization cert permissions are handled by the RA
    - Enrollment certs are sent to the RA
    - Permissions associated with the enrollment cert are managed by the RA
      - Mechanism --> out of scope for 1609.2.1
    - EEs can request any subset of the allowed permissions
- **… but if we do this, enrollment certs can be X.509**
  - Easy to manage with off-the-shelf systems
  - Fit with existing provisioning systems



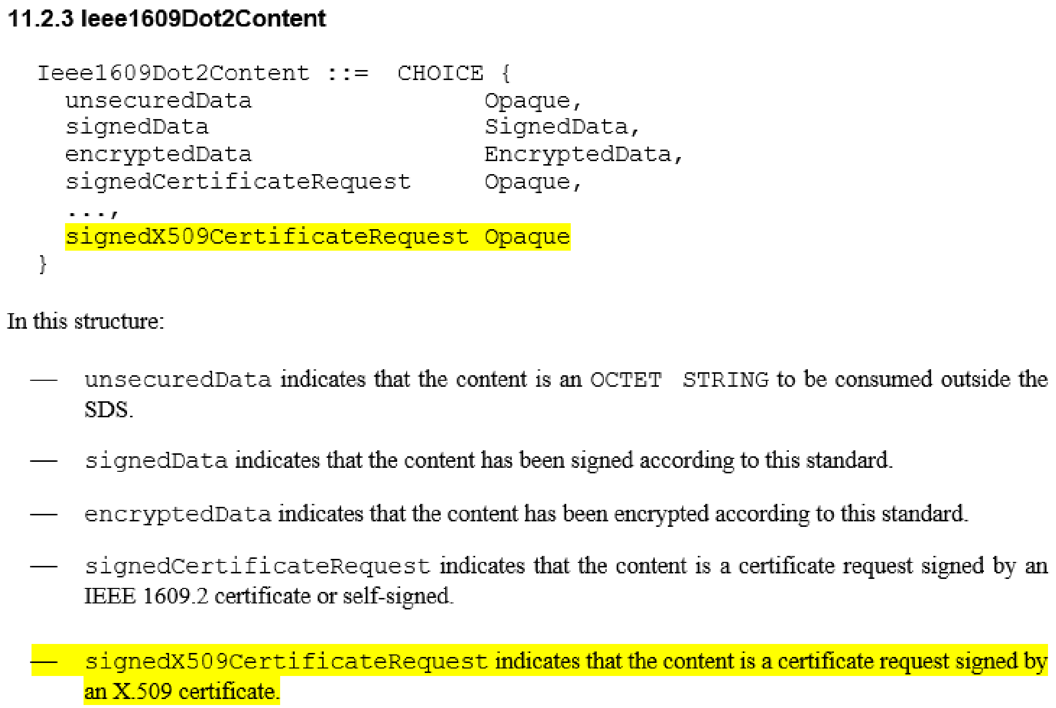
RA manages db mapping enrollment certs to auth cert permissions

X.509 “enrollment” certs: technical integration

- Requires change only to authorization cert request
    - Other use cases that use enrollment certs – for example, for auth cert download – also support alternative authorization mechanisms like Oauth
    - Other use cases for direct enrollment cert management (request, rollover) have existing X.509 mechanisms (specified via PKIX group in IETF) and do not need 1609.2 to specify mechanisms

Overview of changes: clause 11

- Ieee1609Dot2Content
  - Add signedX509CertificateRequest
  - Note: this is opaque so doesn't directly contain the SignedX509CertificateRequest from 1609.2.1
  - Also note: content type isn't part of the 1609.2 hash input – this is baked into 1609.2 now but is unfortunate



11.2.3 Ieee1609Dot2Content

```
Ieee1609Dot2Content ::=  CHOICE {
  unsecuredData                Opaque,
  signedData                   SignedData,
  encryptedData                EncryptedData,
  signedCertificateRequest     Opaque,
  ...,
  signedX509CertificateRequest Opaque
}
```

In this structure:

— unsecuredData indicates that the content is an OCTET STRING to be consumed outside the SDS.

— signedData indicates that the content has been signed according to this standard.

— encryptedData indicates that the content has been encrypted according to this standard.

— signedCertificateRequest indicates that the content is a certificate request signed by an IEEE 1609.2 certificate or self-signed.

— signedX509CertificateRequest indicates that the content is a certificate request signed by an X.509 certificate.

Lesson

- Even in settings where non-X.509 certificates have advantages for applications…
  - Bandwidth-constrained
  - Attribute certs favored
  - No use of technologies that X.509 is optimized for
- … using X.509 for certificate management is attractive
  - Integration with existing systems
  - Identity-based authorizatoin