Qualcomm

V2X IEEE 1609.2.1: Status and Deployment

William Whyte

Outline

- 1609.2.1 status
  - Publication
  - Adoption / interop
  - Profiling
  - Deployment
  - Other considerations around certificate management
- 1609.2 status
  - Revision timeline
  - New features (general)
  - Extensibility and potential use in Korean market
- Misbehavior detection and reporting
  - ETSI standard
    - Architecture
    - Report design philosophy
    - Adoption in other regions
  - Policy for revocation / remediation - 5GAA work item

1609.2.1 overview

Overall goals

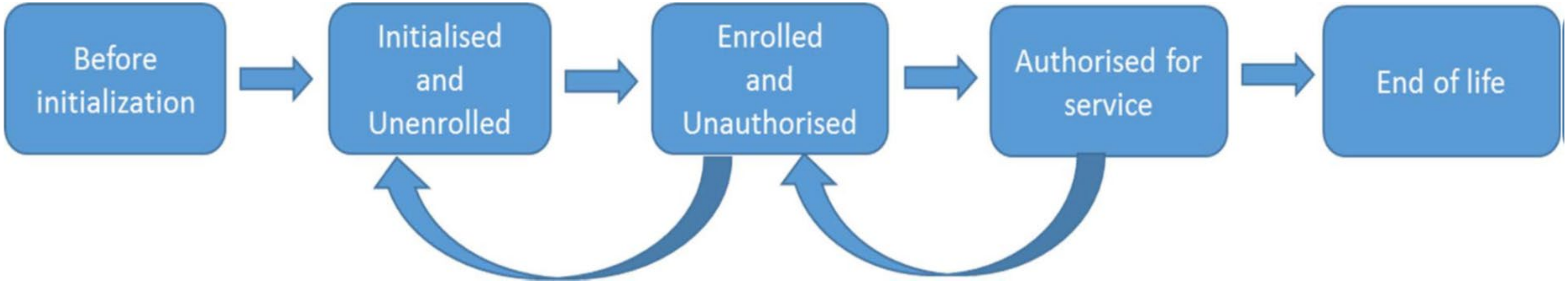
Primary use cases

- Authorization certificate request and download by end entities
  - For multiple different applications
  - For pseudonym / non-pseudonym certificates
- Certificate revocation for pseudonym / non-pseudonym certificates
- Root certificate / trust management

Support use cases

- Obtain / renew enrollment certificates (certificates used for authentication of end entities in SCMS communications)
- Distribution of sets of trusted CA certificates so they don't have to be received within application exchanges
- Misbehavior report upload
- Support multiple certificates per device for pseudonymity
  - Butterfly keys
  - Linkage values

Basic overview



- End Entity is provisioned to become initialized (non-SCMS activity)
- EE interacts with ECA to become enrolled – obtains enrollment certificate
- EE interacts with RA to become authorized – authorization cert requests are signed by enrollment certificate
- While authorized, EE interacts with RA / DC to
  - Request new certificates (RA only)
  - Update system information (RA/DC)
  - Submit misbehavior reports (RA only)
- At end of life, EE may be revoked by CRL signer

1609.2.1 Status: publication

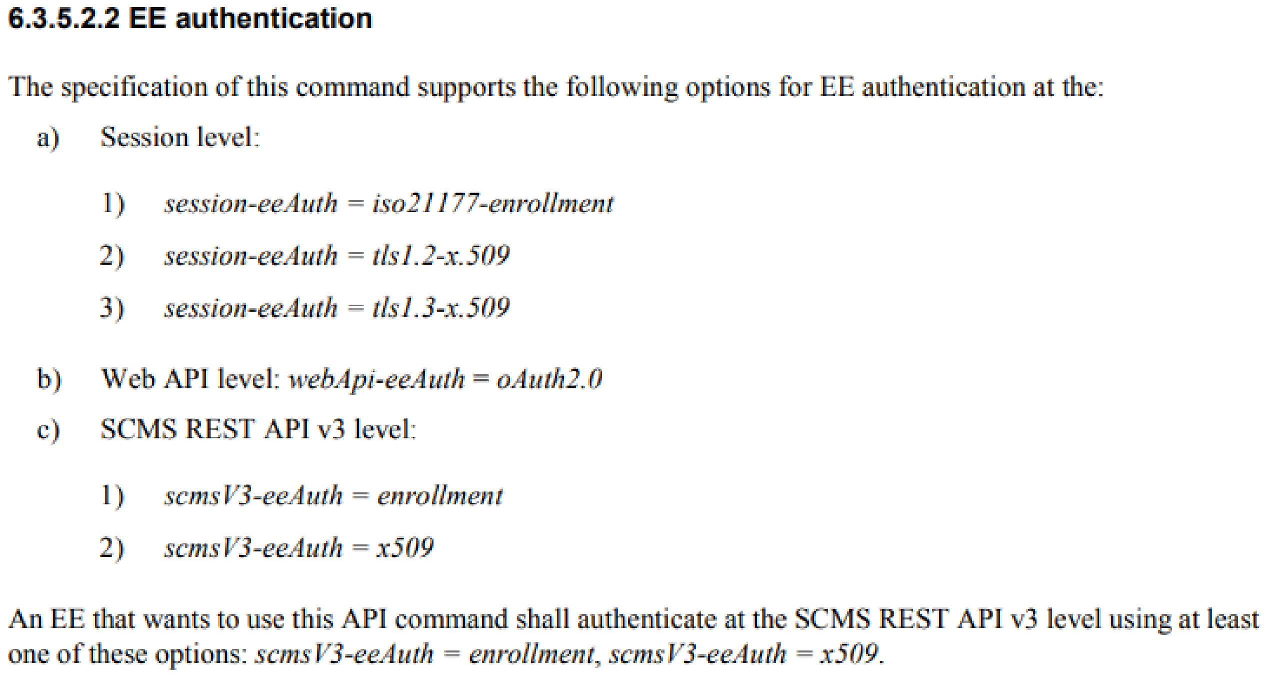
- IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities
- Initially published: December 30th, 2020
- Revision published: June 30th, 2022
- Changes between first publication and revision:
  - Minor but include some non-backwards compatible changes so structure version number was incremented
  - Treatment of generation time in payload / security headers of SCMS PDUs was not uniform → fixed
    - Coordinated this change with the Chinese transposition of 1609.2.1
  - Corrected certificate profile for Enrollment CA, enrollment certificate; added profile for intermediate certificate
  - Clarified format of plaintext within1609.2 Encrypted Data – this was correct but had been misinterpreted by some implementers
  - Clarify what authentication mechanisms are optional v mandatory for (a) use (b) support
  - Clarify that 1609.2 “canonicalization” feature does not apply to 1609.2.1 PDUs
  - Provide complete specification of “validity” for cert request SPDUs
  - Added material to baseline SCMS diagram (Figure 1)
  - Reviewed ASN.1 structure naming for consistency and for compatibility with ETSI use (affects backwards-compatibility of ASN.1 files but not of PDUs over the air)
- All US and Chinese deployments will be based on -2022

1609.2.1 status: interop, availability, deployment

- Two SCMS providers (ISS, Blackberry) have made SCMS implementations available for 1609.2.1 interop testing at OmniAir plugtests
  - OmniAir = US V2X testing organization
- Other SCMS providers have stated that they have implementations
- No public statements of client support – no interop testing actually took place at OmniAir plugtest
  - Next opportunity is Malaga, end of October 2022
- Schedule for Qualcomm support not formally announced

1609.2.1 status: profile

- 1609.2.1 architecture supports multiple options
  - Use of OAuth or other Supplementary Authorization Services
  - Use of ACPC
- 1609.2.1 commands support multiple options
  - See illustration
- SCMS Manager LLC is proposing a profile of 1609.2 that downselects options for initial support
  - Planned publication September 2022
  - Will likely be used by OmniAir as basis for testing



6.3.5.2.2 EE authentication

The specification of this command supports the following options for EE authentication at the:

a) Session level:

1) *session-eeAuth = iso21177-enrollment*

2) *session-eeAuth = tls1.2-x.509*

3) *session-eeAuth = tls1.3-x.509*

b) Web API level: *webApi-eeAuth = oAuth2.0*

c) SCMS REST API v3 level:

1) *scmsV3-eeAuth = enrollment*

2) *scmsV3-eeAuth = x509*

An EE that wants to use this API command shall authenticate at the SCMS REST API v3 level using at least one of these options: *scmsV3-eeAuth = enrollment*, *scmsV3-eeAuth = x509*.

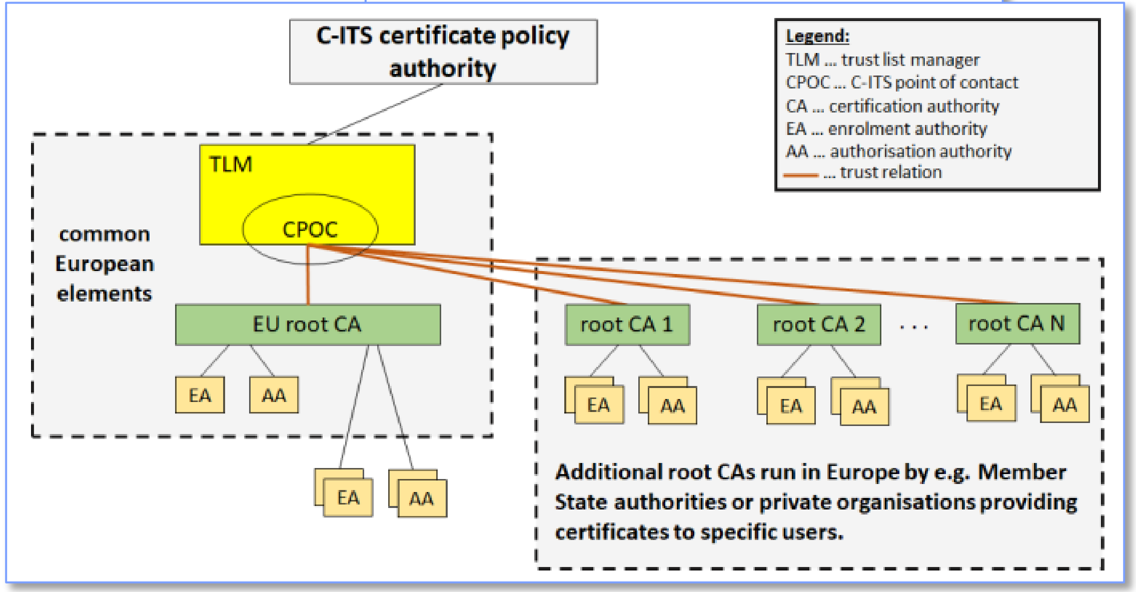
Governance and trust management -- EU

- Based on TS 102 941 rather than 1609.2.1
- Trust List Manager issues Certificate Trust Lists (CTLs) of CAs that follow the Certificate and Security Policies
- DG MOVE organizes the operation of the Trust List Manager and the Common EU Root CA
  - Three different “levels” - 0, 1, 2 - to allow development / experimental deployment units to get certificates
  - Common EU Root issues certs to CAs for Road Operators, etc
  - Other root CA operators, e.g. OEMs, are included on the CTL
- DG MOVE sponsors C-ITS Expert Group tasked with maintaining / updating Certificate and Security Policy

EUROPEAN COMMISSION

Security Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)

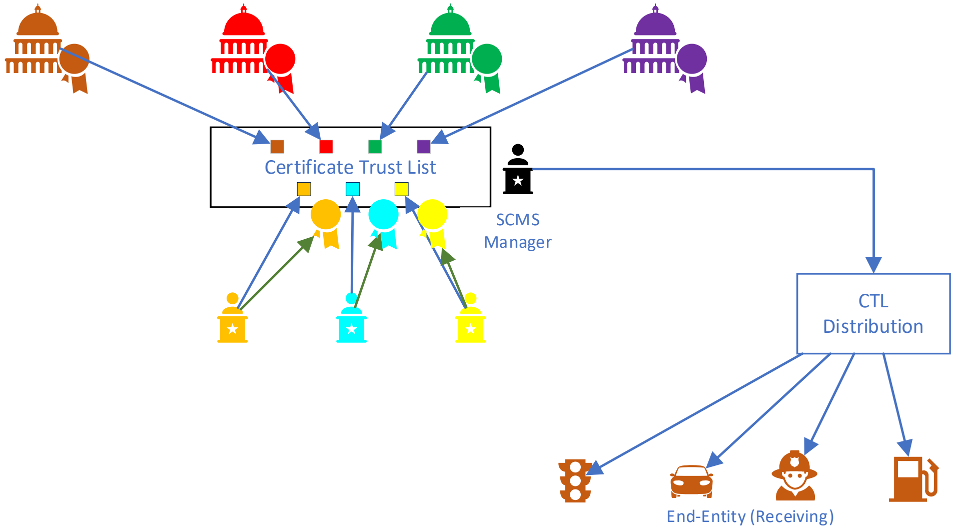
Release 2.1, Draft 28 June 2022



C-ITS certificate policy authority
Legend:
TLM ... trust list manager
CPOC ... C-ITS point of contact
CA ... certification authority
EA ... enrolment authority
AA ... authorisation authority
... trust relation
TLM
CPOC
common European elements
EU root CA
EA
AA
EA
AA
root CA 1
root CA 2
. . .
root CA N
EA
AA
EA
AA
EA
AA
Additional root CAs run in Europe by e.g. Member State authorities or private organisations providing certificates to specific users.

Governance and trust management – US

- Trust management model from 1609.2.1
  - SCMS Manager issues certificate policy and identifies root CAs that meet the policy
  - Multiple Electors “notarize” SCMS Manager policy decisions by signing CTL
  - CTL includes root CAs and also Elector certificates, allowing for robust rollover of Elector certificates
- In US, industry organization “SCMS Manager LLC (https://www.scmsmanager.org/) has created Electors and Certificate Policy, and is developing other technical documents to support certificate issuance
  - Voluntary organization, not “sponsored” by governments
    - US and Canadian transport departments are involved as observers (https://tc.canada.ca/sites/default/files/2021-08/transport-canada-vehicle-cyber-security-strategy.PDF)
  - Activities mainly driven by one SCMS provider, ISS
- “SCMS Manager LLC” is currently the only candidate “SCMS Manager” but widespread acceptance may require participation by more SCMS providers



1609.2 overview

1609.2 Change Topics

1 Canonicalization

2 Enrollment CA Permissions

3 Issues around validity due to overdue CRLs

4 Security Profile Update

5 Future Information

6 Security Profile for Non-Broadcast Applications

7 Security Considerations for Applications Using Service Advertisement

8 Guidance for permissions encoding in CA certificates

9 Alternative Revocation Mechanisms

10 Trust management

11 Geographic Relevance Conditions

12 Omitted Payload

13 Peer-to-peer distribution for large security management messages

14 Peer-to-peer cert distribution for non-peer application instances

15 HeaderInfo extension mechanism

16 Extend PduFunctionalType to cover session extension

17 Russian algorithm support

18 Chinese algorithm support

19 Extending the set of region identifiers

20 Sending standalone certificates

21 Rationale / FAQ

22 CRL Design Review

23 Hash-Based Signature Support

24 Asserted Encrypted Data

25 Sharing CRLs

26 Empty CRL

27 Best practices for multi-message applications

28 Clarify encryption process

29 Best practices for referring to 1609.2

30 OperatingOrganizationId

31 Unlinkability

99 Misc

1609.2 Change Topics by category

🟨 Significant new feature
🟦 Extensibility
🟩 Important clarification

1	🟩	Canonicalization
2		Enrollment CA Permissions
3		Issues around validity due to overdue CRLs
4	🟧	Security Profile Update
5	🟧	Future Information
6	🟧	Security Profile for Non-Broadcast Applications
7	🟨	Security Considerations for Applications Using Service Advertisement
8		Guidance for permissions encoding in CA certificates
9	🟧	Alternative Revocation Mechanisms
10		Trust management
11	🟧	Geographic Relevance Conditions
12	🟨	Omitted Payload
13		Peer-to-peer distribution for large security management messages
14	🟨	Peer-to-peer cert distribution for non-peer application instances
15	🟦	HeaderInfo extension mechanism
16	🟧	Extend PduFunctionalType to cover session extension
17		Russian algorithm support
18	🟨	Chinese algorithm support
19		Extending the set of region identifiers
20		Sending standalone certificates
21		Rationale / FAQ
22		CRL Design Review
23		Hash-Based Signature Support
24		Asserted Encrypted Data
25		Sharing CRLs
26	🟩	Empty CRL
27		Best practices for multi-message applications
28	🟩	Clarify encryption process
29		Best practices for referring to 1609.2
30	🟨	OperatingOrganizationId
31	🟧	Unlinkability
99	🟧	Misc

1609.2 Change Topics: Significant new features (1)

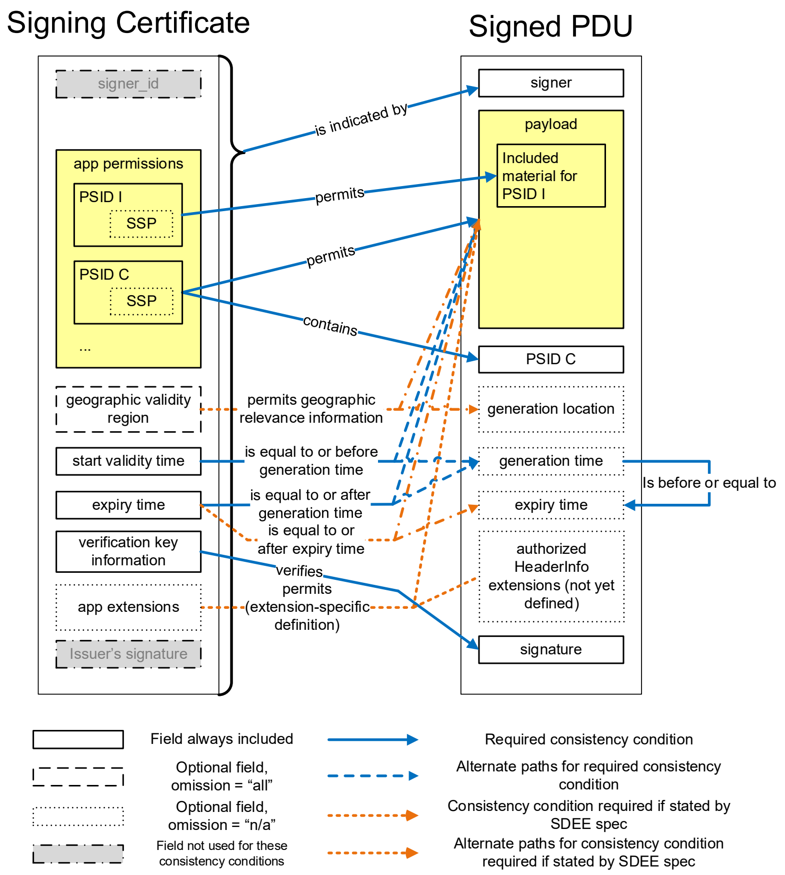
- CR7: Security Considerations for Applications Using Service Advertisement
  - Allows application A to carry authenticated information for application B and indicate that it is authenticated
  - Allows fast initiation of sessions with application B
  - Currently used with WSA (1609.3) carrying information for tolling (SAE J3217) but applicable to any case where it is useful for one application to provide information to initiate a session involving another application
- CR12: Omitted payload
  - Allows signature to be generated over payload obtained from another source
  - Supports UAV communications standards defined in ASTM where UAV messages are limited to 125 bytes – enables peer-to-peer identification
    - Work on defining RemoteID functionality using this feature is starting in ASTM
- CR14: Extended P2PCD
  - Baseline P2PCD: If a receiver doesn’t know a BSM sender’s CA certificate, it can send a request in its own BSM
  - Extended P2PCD: If a receiver doesn’t know the CA certificate for any sender, the receiver can send a request in any message of its own
  - Uses the extensibility mechanism defined in CR 15

1609.2 Change Topics: Significant New Features (2)

- CR18: Chinese algorithm support
  - Adds support for Chinese national algorithms SM2, SM3, SM4
  - This makes support for other national algorithms easy to add – specification is generally modular and all points that might be affected by addition of a new algorithm have been identified
- CR30: Operating Organization Id
  - Defines a new authenticated property of the certificate holder, the Operating Organization responsible for the end entity
  - Can be used to support access control policies that depend on the operator
    - For example, Signal Prioritization/Preemption
      - Signal operator maintains a list of Operating Organization Ids and the types of operating organization (e.g. ID A is a police department, ID B is an ambulance operator)
      - Access control policy lists all operating organizations for which the signal operator will grant a preemption request
      - Example “normal conditions” policy: allow preemption by police cars from that county or state police cars but not by other police cars:
      - Example “exception conditions” policy: allow preemption by all police cars and all public transit vehicles to assist evacuation
  - Extension to certificate, not to security headers

1609.2 extensibility

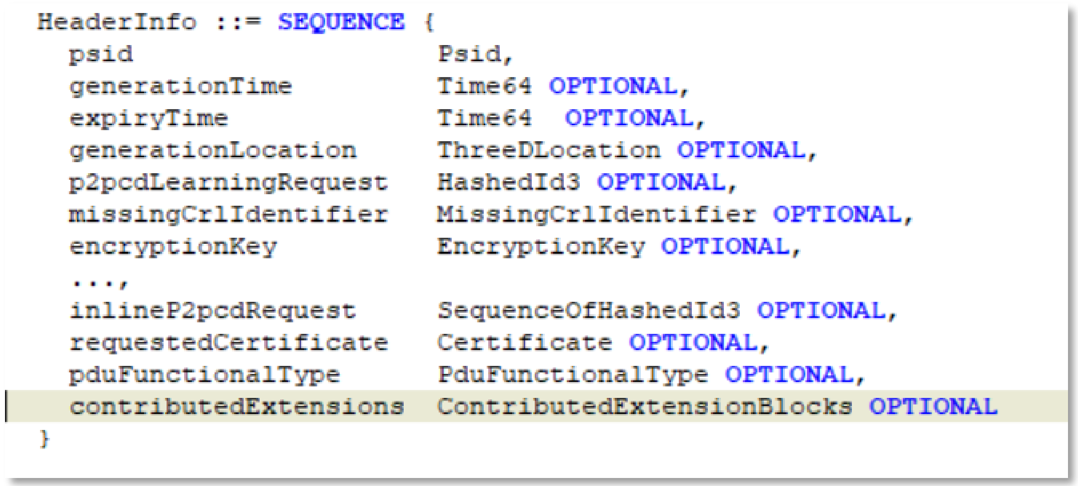
- 1609.2 defines extensions to both HeaderInfo (the signed PDU security envelop) and certificates



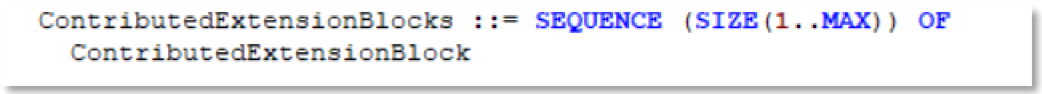
Signing Certificate
Signed PDU
signer_id
app permissions
PSID I
SSP
PSID C
SSP
...
geographic validity region
start validity time
expiry time
verification key information
app extensions
Issuer's signature
signer
payload
Included material for PSID I
PSID C
generation location
generation time
expiry time
authorized HeaderInfo extensions (not yet defined)
signature
is indicated by
permits
permits
contains
permits geographic relevance information
is equal to or before generation time
is equal to or after generation time
is equal to or after expiry time
verifies
permits (extension-specific definition)
Is before or equal to
Field always included
Optional field, omission = "all"
Optional field, omission = "n/a"
Field not used for these consistency conditions
Required consistency condition
Alternate paths for required consistency condition
Consistency condition required if stated by SDEE spec
Alternate paths for consistency condition required if stated by SDEE spec

1609.2 extensibility

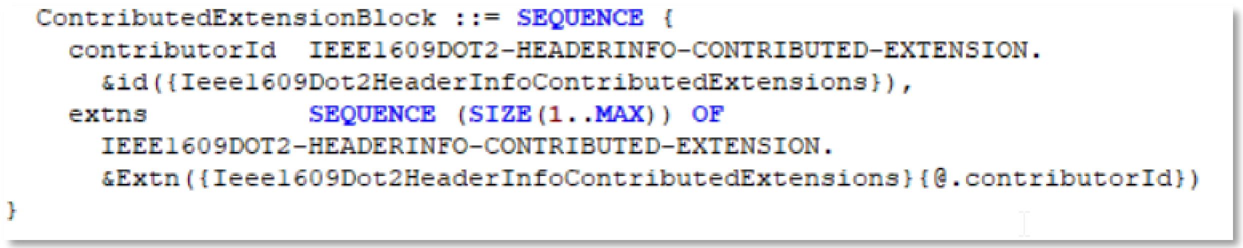
- 1609.2 defines extensions to both HeaderInfo (the signed PDU security envelop) and certificates
- Within HeaderInfo definition, Contributed Extensions are identified by contributorId
  - 1-byte integer
- Any SDO that wishes to extend 1609.2 HeaderInfo can request a contributorId from the Working Group and develop a specification with assurance that there will be no identifier value collisions
- Currently made use of by:
  - ETSI - CRL and CTL request for peer to peer distribution
  - IEEE - Extended P2PCD request



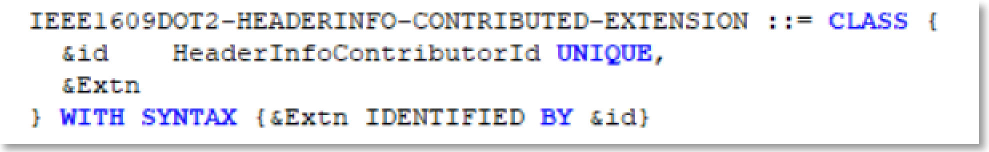
```
HeaderInfo ::= SEQUENCE {
  psid                      Psid,
  generationTime            Time64 OPTIONAL,
  expiryTime                Time64  OPTIONAL,
  generationLocation        ThreeDLocation OPTIONAL,
  p2pcdLearningRequest      HashedId3 OPTIONAL,
  missingCrlIdentifier      MissingCrlIdentifier OPTIONAL,
  encryptionKey             EncryptionKey OPTIONAL,
  ...,
  inlineP2pcdRequest        SequenceOfHashedId3 OPTIONAL,
  requestedCertificate      Certificate OPTIONAL,
  pduFunctionalType         PduFunctionalType OPTIONAL,
  contributedExtensions     ContributedExtensionBlocks OPTIONAL
}
```



```
ContributedExtensionBlocks ::= SEQUENCE (SIZE(1..MAX)) OF
  ContributedExtensionBlock
```



```
ContributedExtensionBlock ::= SEQUENCE {
  contributorId  IEEE1609DOT2-HEADERINFO-CONTRIBUTED-EXTENSION.
    &id({Ieee1609Dot2HeaderInfoContributedExtensions}),
  extns          SEQUENCE (SIZE(1..MAX)) OF
    IEEE1609DOT2-HEADERINFO-CONTRIBUTED-EXTENSION.
    &Extn({Ieee1609Dot2HeaderInfoContributedExtensions}{@.contributorId})
}
```



```
IEEE1609DOT2-HEADERINFO-CONTRIBUTED-EXTENSION ::= CLASS {
  &id    HeaderInfoContributorId UNIQUE,
  &Extn
} WITH SYNTAX {&Extn IDENTIFIED BY &id}
```

1609.2 status

- Currently in IEEE-SA ballot
- Met approval conditions in first ballot but WG decided to implement some changes as a result of comments so recirculation ballot underway, closing 2022-09-03
- Next steps:
  - Submit to IEEE RevCom (verifies that process was correctly followed)
    - Submission deadline: 2022-09-15
    - RevCom consideration: 2022-10-25
  - IEEE-SA Board approval (by email, usually a day or so after RevCom approval)
  - Publication editing (typically 30-60 days)
- Publication date likely end December 2022 or early January 2023
- Implementation status:
  - ETSI implementations are already using extensibility
  - Chinese implementations are already using Chinese algorithms
  - Support for other new features is not widespread

Misbehavior reporting and management

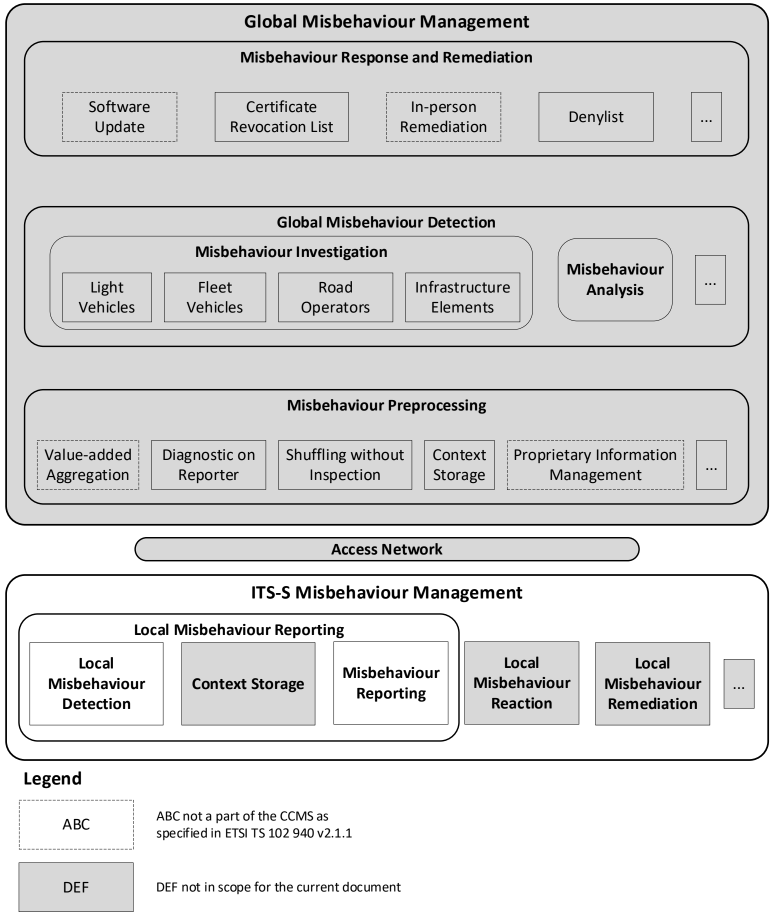
Introduction

- ETSI TS 103 759
  - Intelligent Transport Systems (ITS); Security; misbehavior Reporting service; Release 2
  - Scope: To specify the misbehavior Reporting Service (MRS) in support of trusted ITS stations for the reporting of locally misbehavior detections to a central authority (misbehavior Authority) which collects misbehavior reports on different ITS messages for global analysis and reaction.
  - Close to publication: will be publicly available and free when published
  - Designed to be modular and extensible
- Uses similar principles to the MBR design in https://scmsmanager.org/wp-content/uploads/2020/01/Misbehavior-Report-and-Application-Specification-v1.0.pdf but not bytewise compatible
  - Informal coordination has been carried out with SCMS Manager throughout the ETSI TS development process: expectation is that SCMS Manager will update ASN.1 to be consistent with ETSI TS
  - SCMS Manager doc provides more information about prioritization of reports for storage and upload compared to ETSI TS, which is mainly an interoperability specification
- Goal of this presentation:
  - Provide overview of 103 759 design
  - Discussion of how it can be used as a framework for SAE work in misbehavior specification

Misbehavior management system

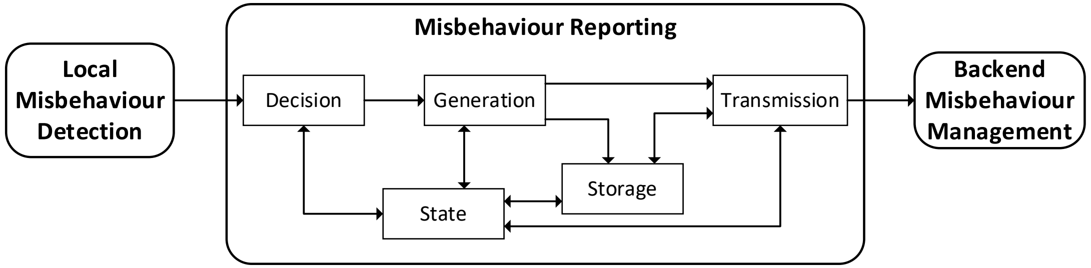
Four different stages in misbehavior detection and management:

- ITS station locally detects and reports misbehavior to the MA
- Misbehavior preprocessing component validates / aggregates / shuffles misbehavior reports before passing them on
- Global misbehavior detection component determines
  - whether misbehavior has taken place
  - who is responsible
  - what response to take
    - Responses can in principle include revocation, suspension, forced software update, physical intervention, …
    - 5GAA project starting to investigate appropriate responses
- Misbehavior response and remediation component implements the response decided by GMBD


Global Misbehaviour Management
Misbehaviour Response and Remediation
Software Update
Certificate Revocation List
In-person Remediation
Denylist
...
Global Misbehaviour Detection
Misbehaviour Investigation
Light Vehicles
Fleet Vehicles
Road Operators
Infrastructure Elements
Misbehaviour Analysis
...
Misbehaviour Preprocessing
Value-added Aggregation
Diagnostic on Reporter
Shuffling without Inspection
Context Storage
Proprietary Information Management
...
Access Network
ITS-S Misbehaviour Management
Local Misbehaviour Reporting
Local Misbehaviour Detection
Context Storage
Misbehaviour Reporting
Local Misbehaviour Reaction
Local Misbehaviour Remediation
...
Legend
ABC
ABC not a part of the CCMS as specified in ETSI TS 102 940 v2.1.1
DEF
DEF not in scope for the current document

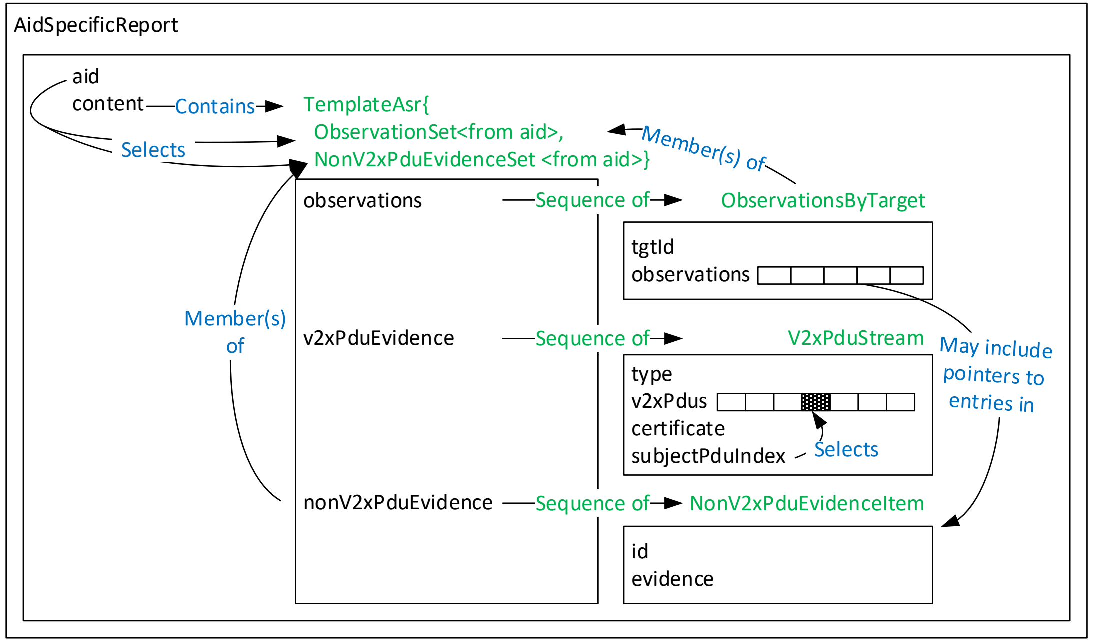
Local misbehavior detection and reporting

- Decompose local misbehavior management into detection and reporting
- Goal of local misbehavior detection: identify messages that do not correspond to ground truth
  - Incoming messages are checked for physical plausibility, security consistency, etc
  - Messages are compared to:
    - Other V2X messages from the same sender
    - Other V2X messages
    - Other external data (e.g. maps),
    - Sensor and other locally-obtained data (e.g. RF RSSI)
- If bad data is identified:
  - Alert system is notified and can decide to suppress alerts that the message would have caused
  - Reporting subsystem is notified and can decide to create report
- The misbehavior reporting system may have to manage three distinct "budgets"
  - Report creation – managed by Decision block
    - How many MBRs can be generated a second? Which observed misbehaviors lead to a report?
  - Storage
    - If connectivity is intermittent, how many reports are stored and which are deleted to make space?
  - Transmission
    - Which reports are prioritized for upload when connectivity becomes available?



Report format

- Modular and extensible – different SDOs can define their own Observations with minimal coordination with ETSI
- Observations identifies which detectors were triggered and why
  - Can include cross-references to the PDUs and evidence fields.
  - Observations are drawn from a supplied application-specific observation Information Object Set.
- v2xPduEvidence contains PDUs that triggered the detectors reported in the observations field
  - An array of sequences of PDUs
  - Each sequence of PDUs is the sequence sent by a single sending application instance
  - One PDU in each sequence is identified as the “target” PDU, the rest are context
- nonV2xPduEvidence is any information that was used by the detectors other than the V2X PDUs.
  - E.g., maps, sensor data, …
  - Drawn from a supplied application-specific evidence Information Object Set.
  - Not required to be used and not defined for any currently defined observations



Defined observations: “classes” and principles for inclusion in v1

- Class 1: Individual V2X messages that are incorrect
- Class 2: V2X messages for the same application from the same sender that are inconsistent with each other
- Class 3: V2X messages that are inconsistent with trusted external data, e.g., maps
- Class 4: V2X messages that are inconsistent with information known to reporter, e.g., reporter’s sensor data
- Class 5: V2X messages from different senders that conflict with each other
- Focus is on detectors that are easy to specify and have low chances of false positives
  - Reduce schedule risk due to specification complexity
  - Reduce implementation risk
  - Reduce risk that use of these detectors causes large amounts of low-quality reports to be sent to MA

CAM detectors for v1 (following WG discussion)

- Class 1: (all with hard-wired thresholds)
  - Speed too large for a vehicle type
  - Speed too large for reverse drive direction
  - Longitudinal acceleration too large
- Class 1 / Security:
  - messageID inconsistent with headerInfo
  - headerInfo inconsistent with security profile
  - psid in headerInfo inconsistent with that in certificate
  - message inconsistent with SSP in certificate
  - generationTime in headerInfo outside validity period of certificate
  - message location outside validity region in certificate
  - generationLocation in headerInfo outside validity region in certificate

- Class 2:
  - With threshold defined by CAM spec
    - Beacon interval too small
  - With hard-wired threshold
    - Change in static fields
    - Change in position too large
    - Change in speed too large
- Class 3: No detectors
- Class 4: No detectors
- Class 5: No detectors

Next steps

- ETSI publication for 103 759 is imminent
  - Requires resolution of some document referencing issues, but doc is technically complete and stable
- ETSI has started Testing Task Force (TTF) to specify tests for 103 759
- SCMS Manager has defined some MBR observations consistent with this framework
  - SAE will move forward with a formal standard once 103 759 is issued
- Chinese standards under development, will be compatible with 103 759
- Initial informal discussions of holding plugtests, nothing scheduled as of 2022-08

- Outstanding issues:
  - Who will actually run the Misbehavior Authorities?
    - How will reporting work across borders? E.g. American car in Canda notices another American car misbehaving – if separate US and Canadian MAs, who is responsible for receiving / processing report?
  - What are actual criteria for revocation? What are other possible mitigations for persistent misbehavior?
    - 5GAA project about to kick off on this topic

Questions?

Qualcomm

Thank you

Follow us on: f 🐦 in ◎

For more information, visit us at:

www.qualcomm.com & www.qualcomm.com/blog

Nothing in these materials is an offer to sell any of the components or devices referenced herein.

References in this presentation to “Qualcomm” may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes our licensing business, QTL, and the vast majority of our patent portfolio. Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of our engineering, research and development functions, and substantially all of our products and services businesses, including our QCT semiconductor business.