ISAIC2020: Privacy Enhancement for Vehicle's Long Term Credential in V2X using Direct Anonymous Attestation

Pan Lanlan (潘蓝兰)

abbypan@gmail.com

Guangdong OPPO Mobile Telecommunications Corp. Ltd., China

2020.10

1. **Background**
   - Connected Car
   - V2X Communication
   - Personally Identifiable Information (PII)
   - Privacy in V2X Communication
2. **Related Work**
   - Direct Anonymous Attestation (DAA) Scheme
   - V2X DAA
   - Problem
3. **Our Proposal**
   - Overview
   - Issue Short-Term Pseudonymous Certificate
   - Conclusion

Connected Car

https://www.qorvo.com/design-hub/blog/v2x-in-the-connected-car-of-the-future

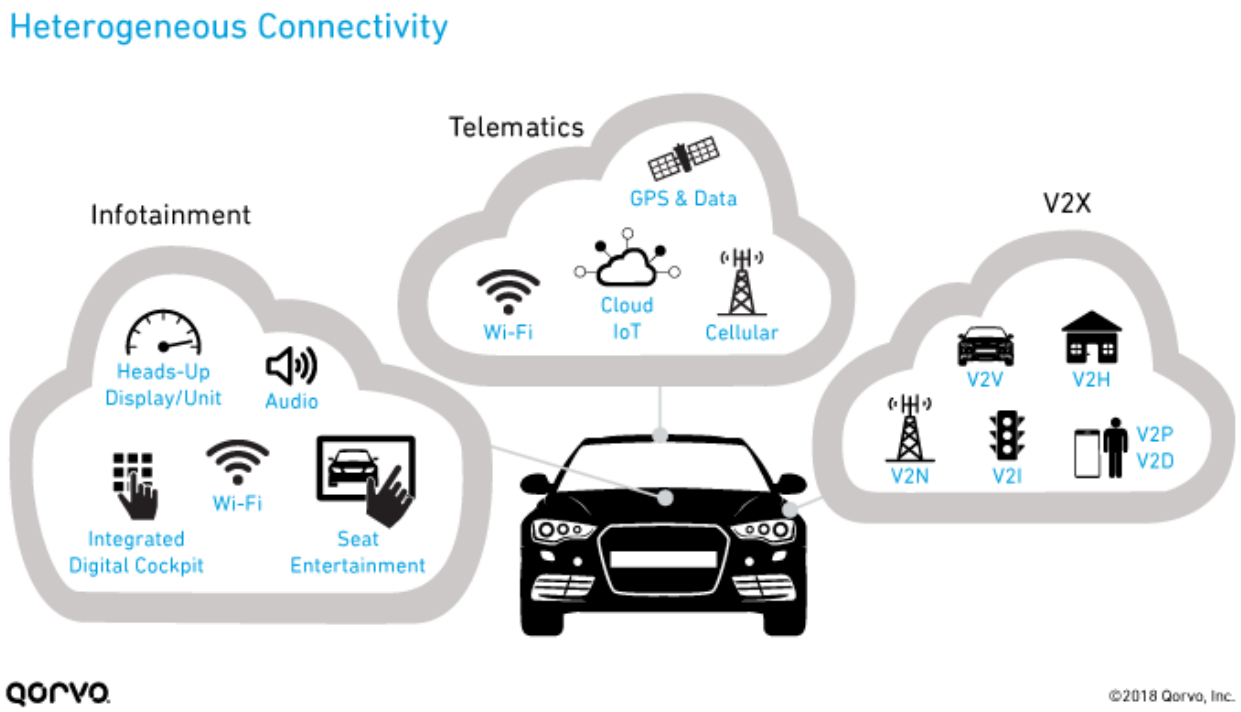


Fig: Connectivity

V2X Communication

https://www.researchgate.net/publication/331676083_Software-Defined_Heterogeneous_Vehicular_Networking_The_Architectural_Design_and_Open_Challenges/

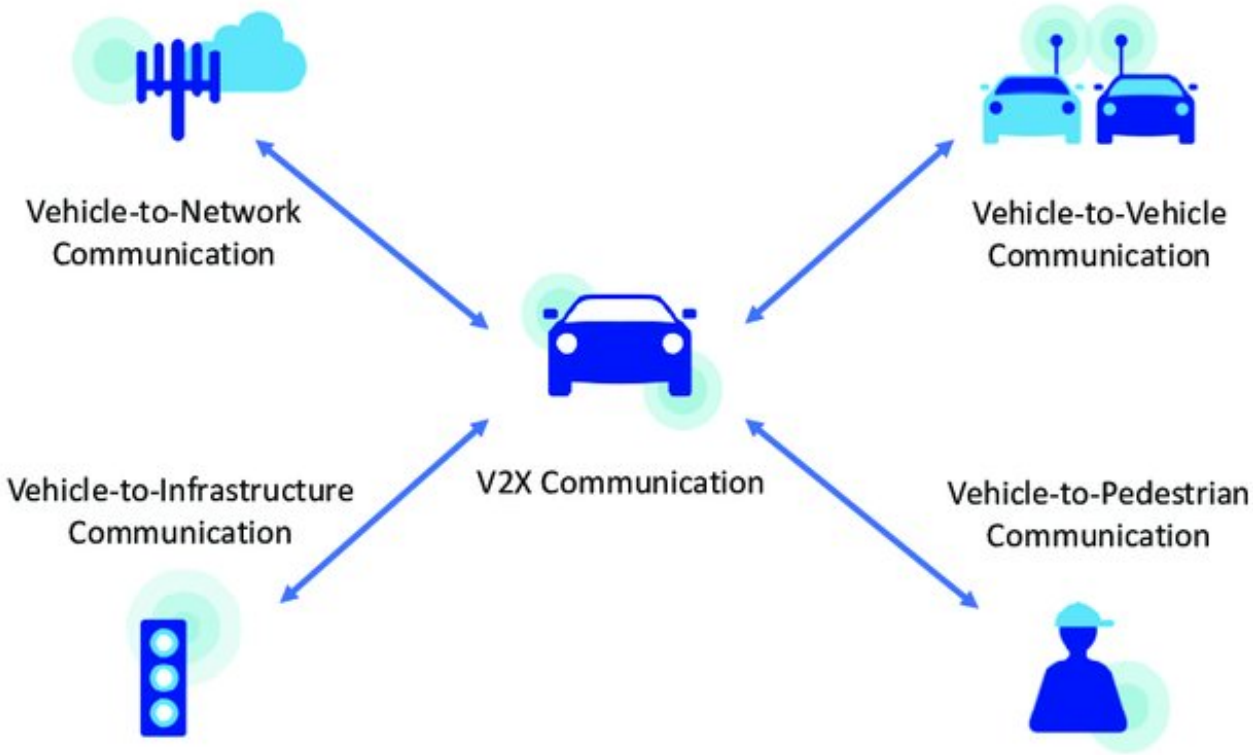
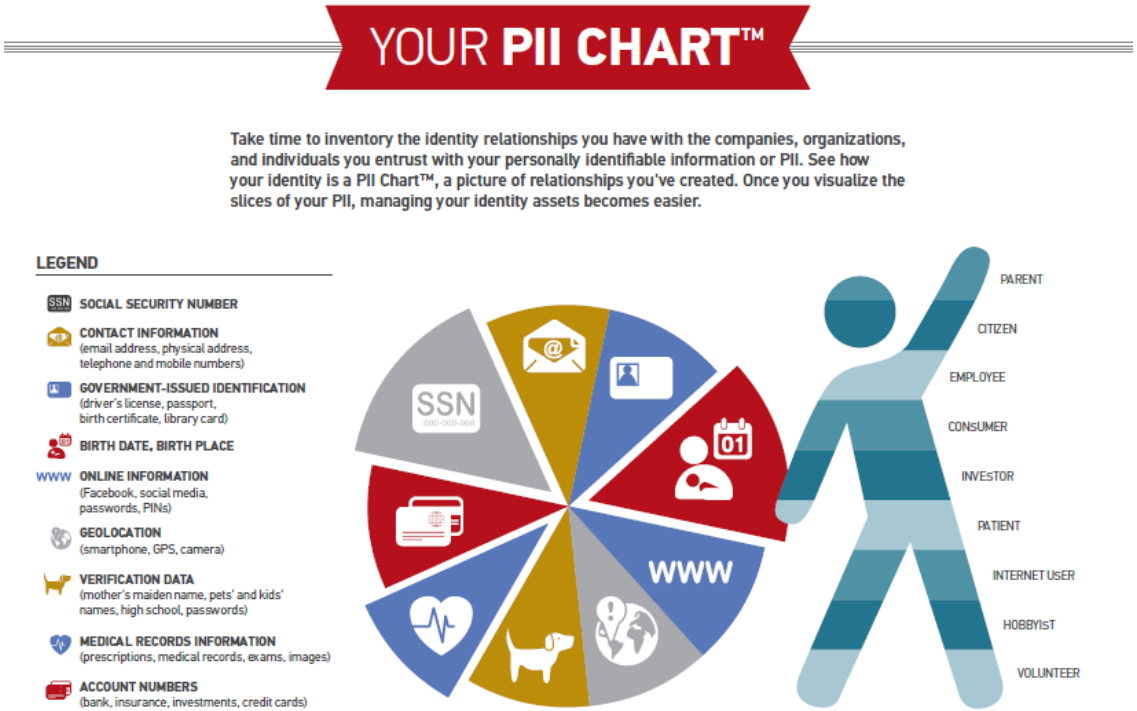


Fig: V2X Communication

Personally Identifiable Information (PII)

Avoid tracking.
GDPR: Prevent attackers or insiders from collecting Personally Identifiable Information (PII).
`https://cyberscout.com/nl/blog/recipe-for-a-safer-identity-is-as-easy-as-pii`



Privacy in V2X Communication

- Confidential
- Anonymous
- Pseudonymous
- Conditional Traceable, Protect PII

Direct Anonymous Attestation (DAA) Scheme

https://www.researchgate.net/publication/225162761_On_a_Possible_Privacy_Flaw_in_Direct_Anonymous_Attestation_DAA

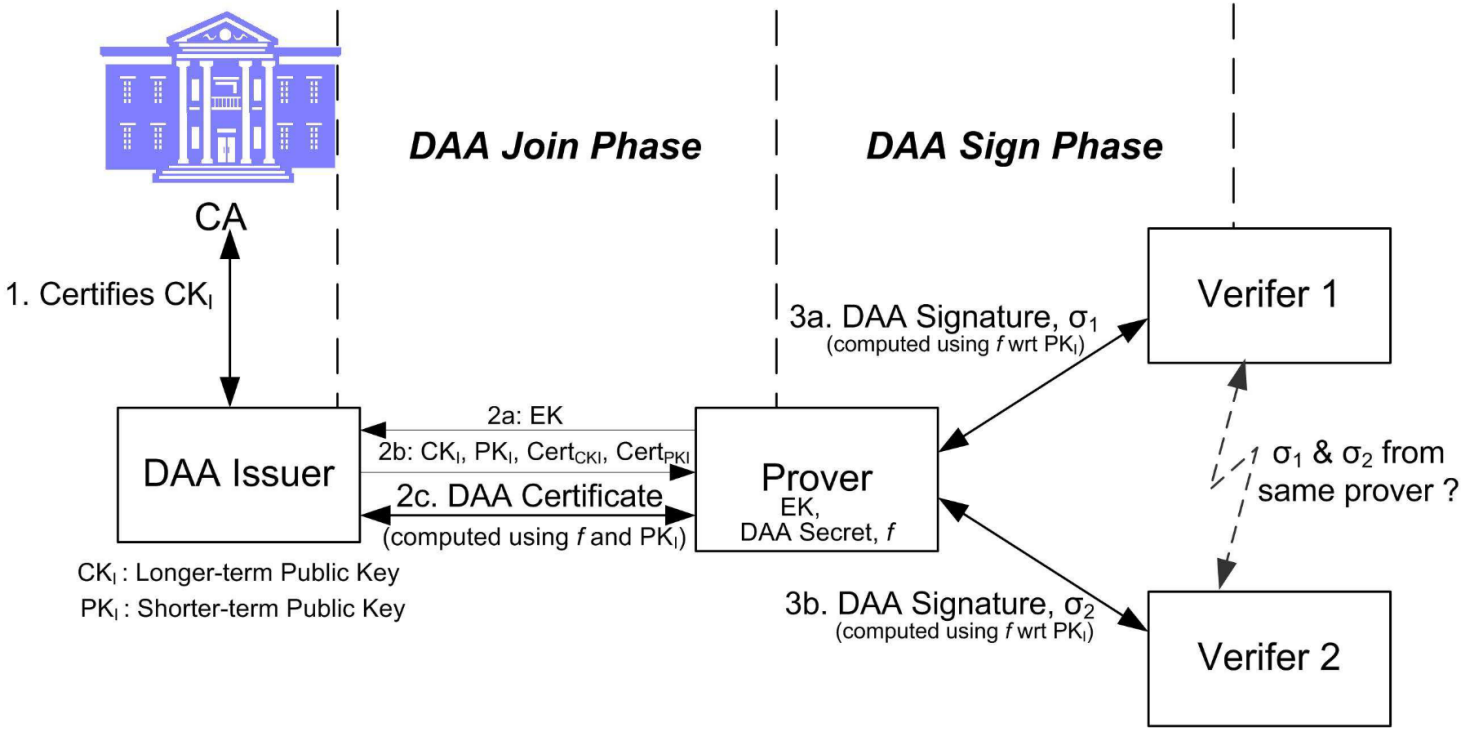


Fig: DAA

Privacy-Enhanced Capabilities for VANETs using Direct Anonymous Attestation

https://www.researchgate.net/publication/321422009_Privacy-Enhanced_Capabilities_for_VANETs_using_Direct_Anonymous_Attestation

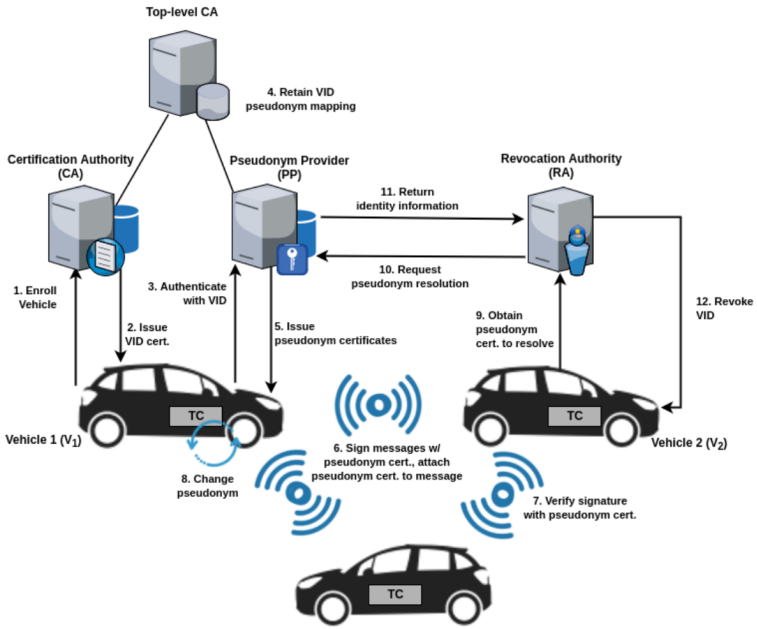


Fig: V2X PKI

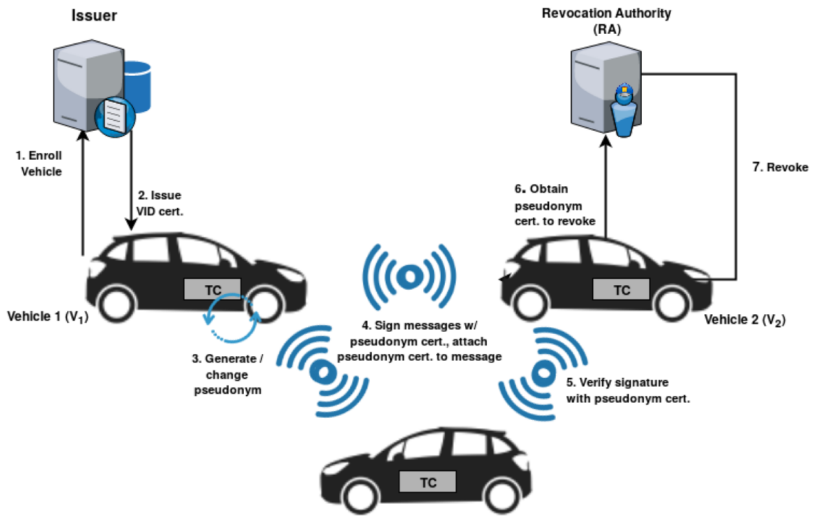


Fig: V2X DAA

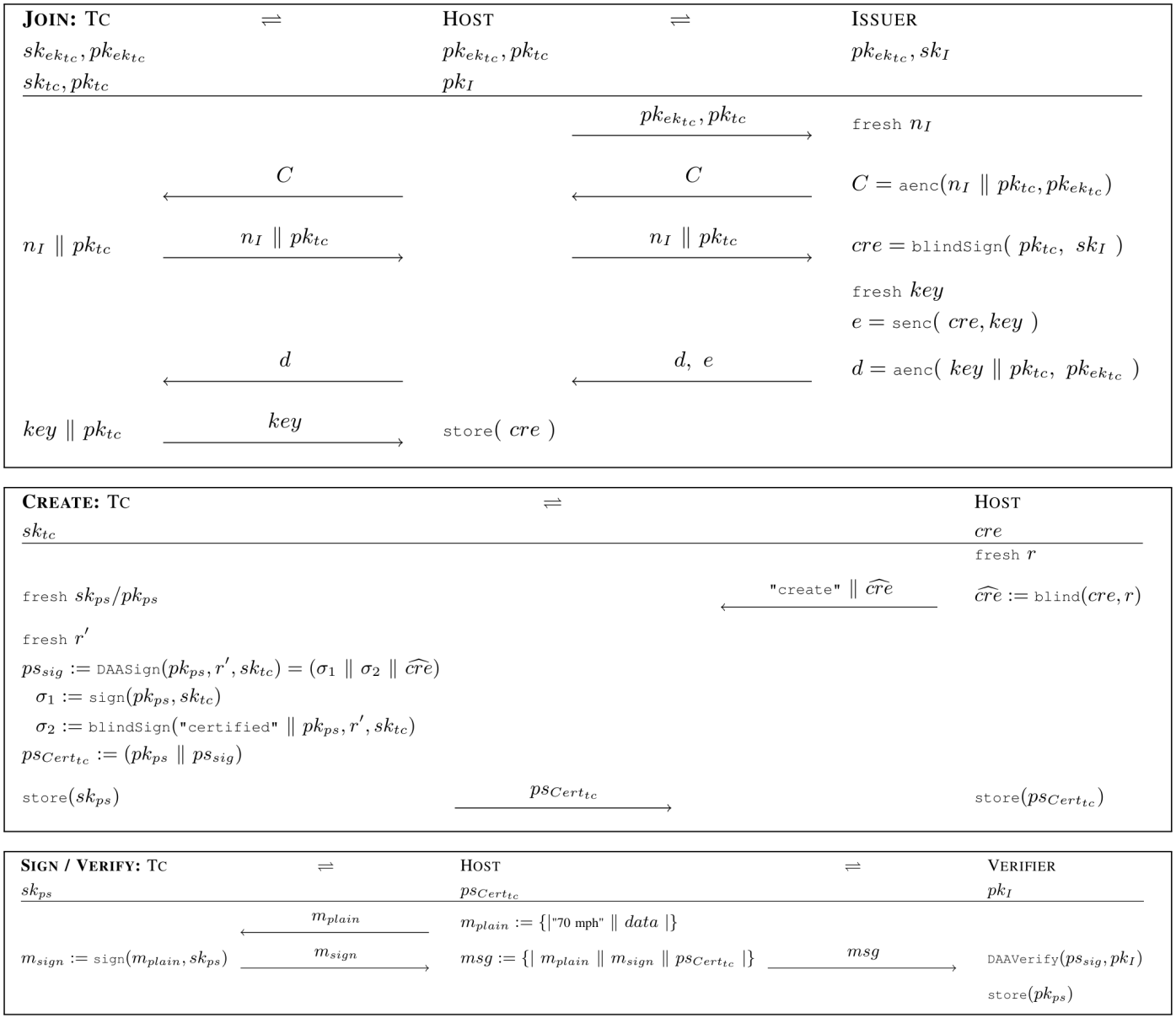


Fig: V2X DAA protocol

Securing V2X Communications for the Future

https://www.researchgate.net/publication/335089342_Securing_V2X_Communications_for_the_Future_Can_PKI_Systems_offer_the_answer

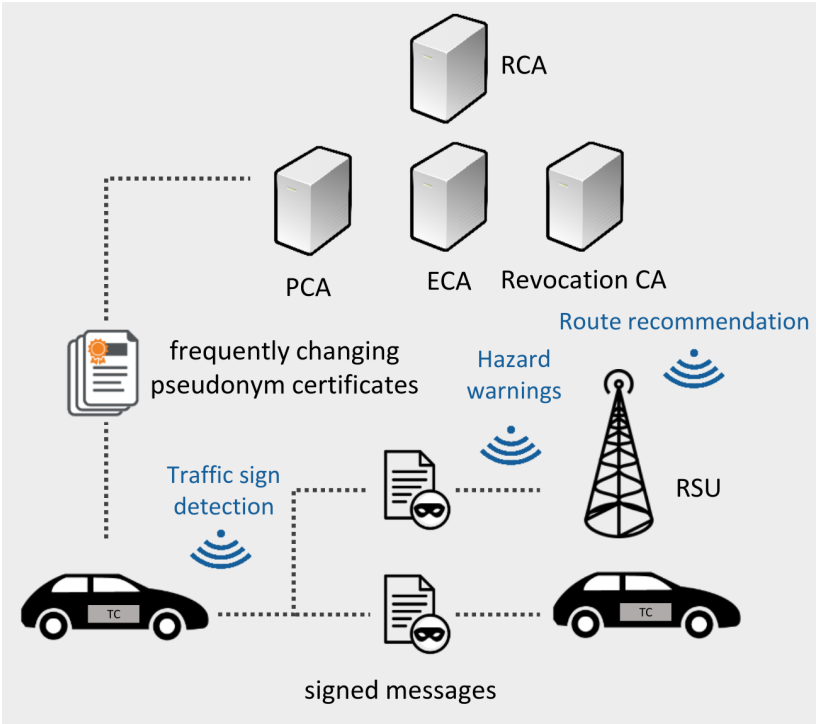


Fig: V2X PKI

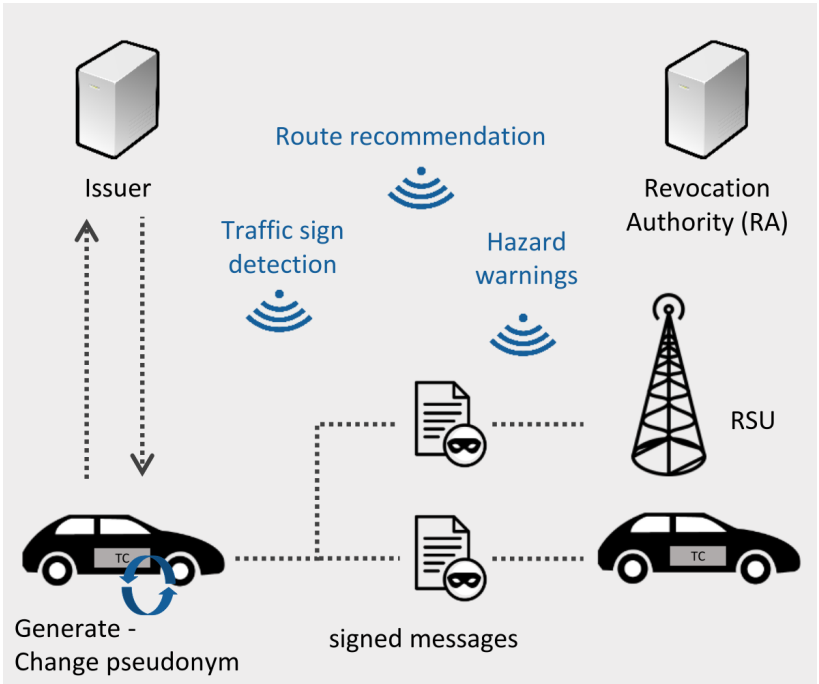


Fig: V2X DAA

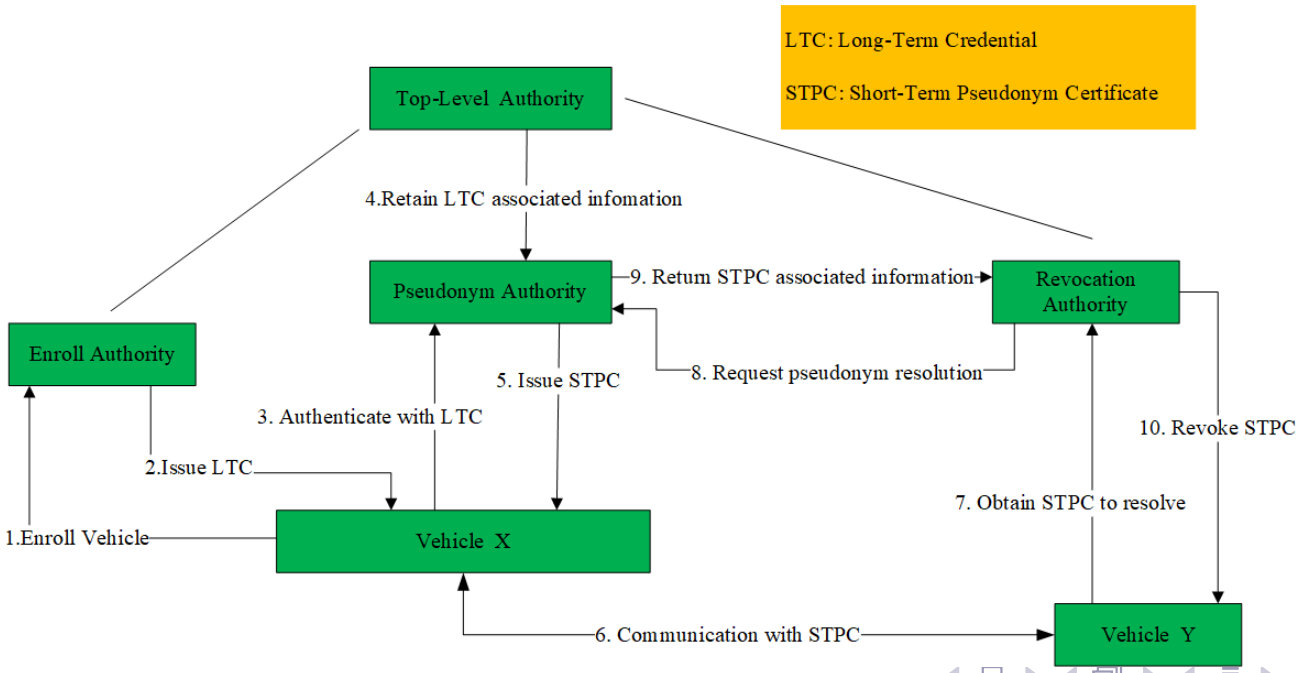
Problem

Traditional VID Certificate is a long-term credential, it is traceable by Pseudonymous CA.
Therefore, it is hard to scale if
we want to enhance the privacy protection from Pseudonymous CA insiders.

Above DAA schemes make the enrollment authority write long-term pseudonymous certificate into vehicle, remove short-term pseudonymous certificate.
It is simpler than traditional V2X solution. However, the trust is mostly shift to vehicle.

Privacy Enhancement for Vehicle's Long Term Credential in V2X using Direct Anonymous Attestation

Enrollment authority writes long-term pseudonymous credential into vehicle.
Reserve the Pseudonymous Authority to issue short-term pseudonymous credential for vehicle.



Issue Short-Term Pseudonymous Certificate

Vehicle' s long-term pseudonymous credential is used to authenticate the request for short-term pseudonymous credential.

The verifier is Pseudonymous Authority.

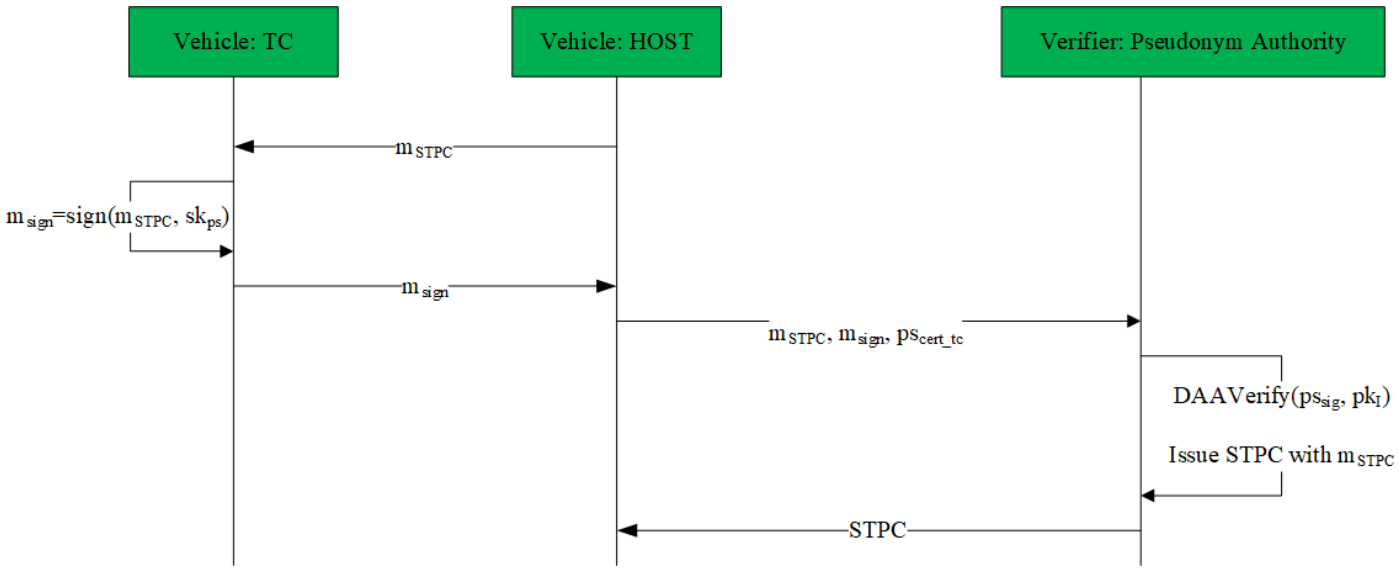


Fig: Issue Short-Term Pseudonymous Certificate

Conclusion

Privacy enhancement is critical for person in V2X scenario.

We should build up the future V2X ecosystem with the principles of 'privacy by design' and 'privacy by default'.