MMLAB Main Seminar

Decentralized Public-Key Infrastructure With Blockchain in V2X Communications

Edy Kristianto, Van-Linh Nguyen, and Po-Ching Lin
National Chung Cheng University

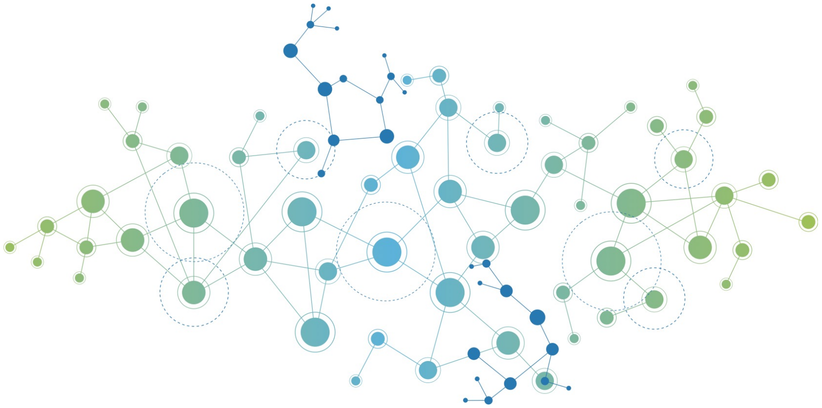
IEEE Security & Privacy, July-August 2022

Hyunsoo Kim (hskim@mmlab.snu.ac.kr)

2022. 08. 24

서울대학교
SEOUL NATIONAL UNIVERSITY

MMLab
Network Convergence & Security Lab



Contents

Vehicle-to-Everything (V2X) Communications

- Overview
- Security and Pseudonym Certificates

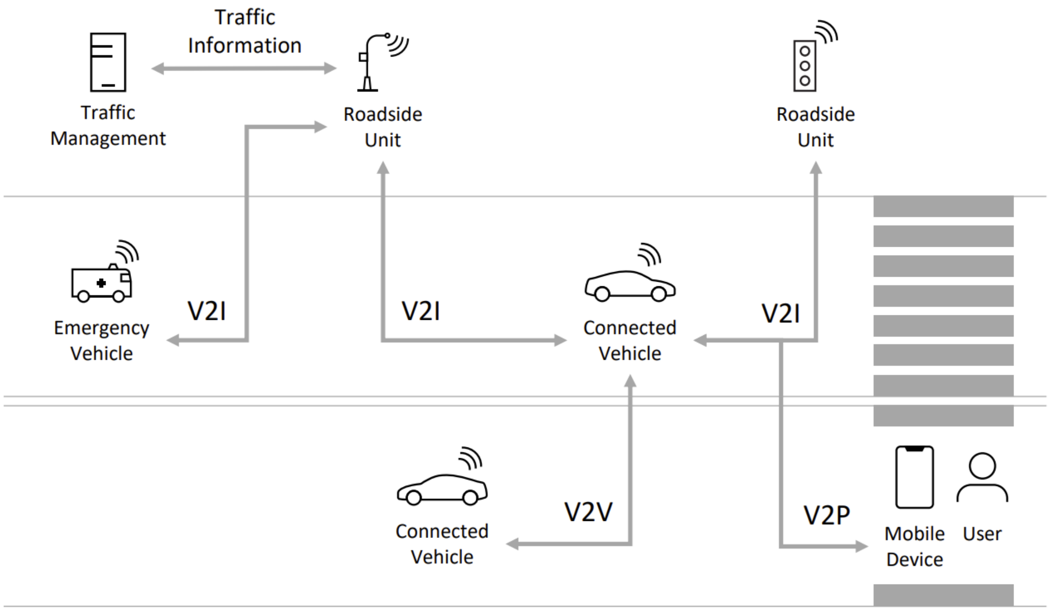
C-PKI / B-PKI for V2X Authentication

- Workflow Comparison
- Advantages and Disadvantages

Conclusion & Critique

V2X Communications

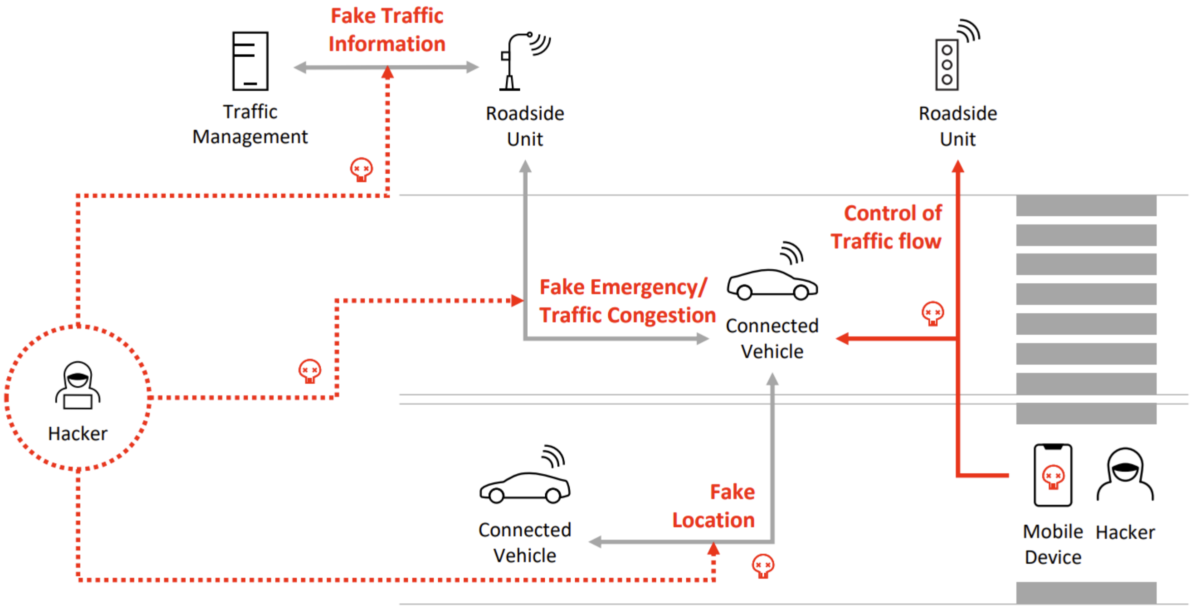
- Enables vehicles and roadside equipment to send and receive messages
- Data associated with vehicle, road or traffic status
  - Real-time traffic updates, vehicle collision alerts, pedestrian alerts
- Vehicle ⇔ Vehicle (V2V), Vehicle ⇔ Infrastructure (V2I), …



V2X Communications Security

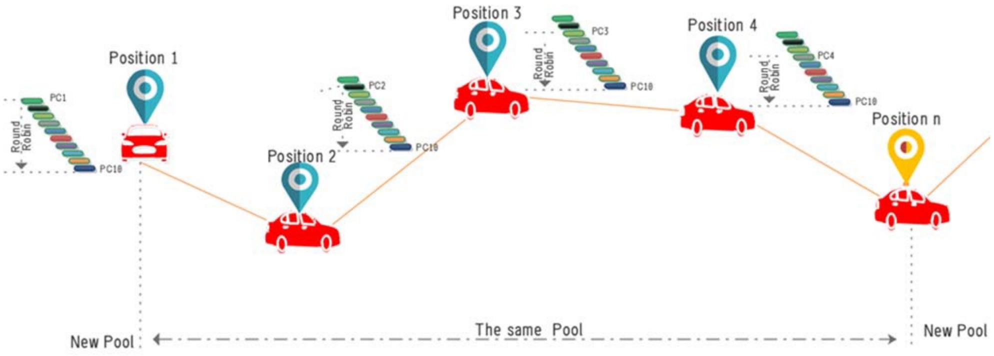
- Without security, a malicious actor may gain access to critical functionality and manipulate information transferred between entities
  - Vehicle accidents/pedestrian accidents due to false signals, traffic congestions

➔ Vehicles must be **authenticated** before joining V2X communications



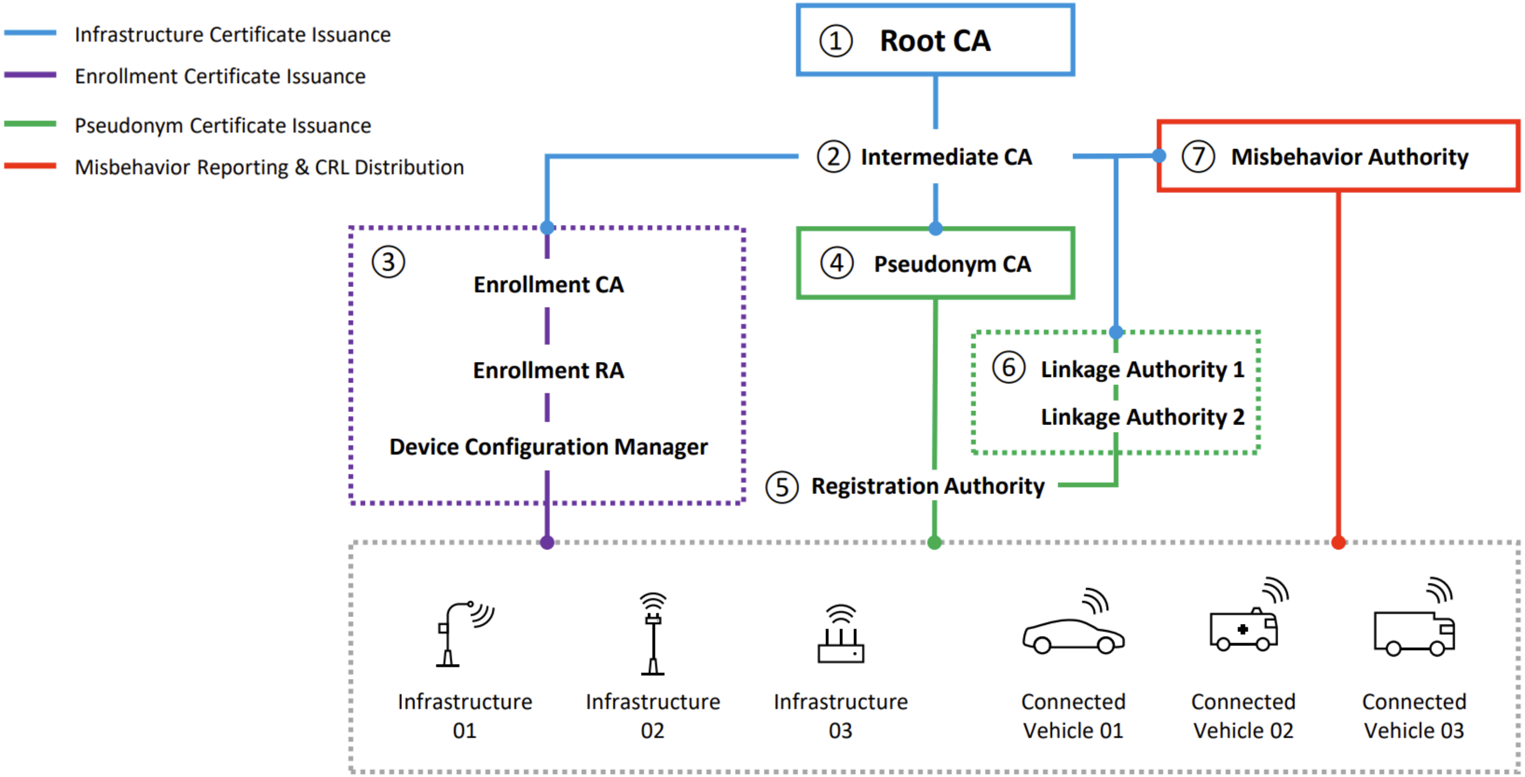
Pseudonym Certificates in V2X

- V2X security systems implement large scale PKI for authentication
- Digital certificates are **privacy-intrusive**
  - Owners/vehicles can be linked and traced (current location, trip history, etc.)
- Pseudonym certificate
  - Used in authenticating V2X messages
  - Preserves privacy by hiding vehicle/module identity, reducing user linkage
  - Short-term (up to 3 months), multiple concurrent certificates per vehicle
    - ✓ 20 per week → hundreds of billions of pseudonyms required



Current Developments

- C-PKI based V2X authentication architecture
  - US – Security Credentials Management System (SCMS)
  - EU – Cooperative ITS Credentials Management System (CCMS)

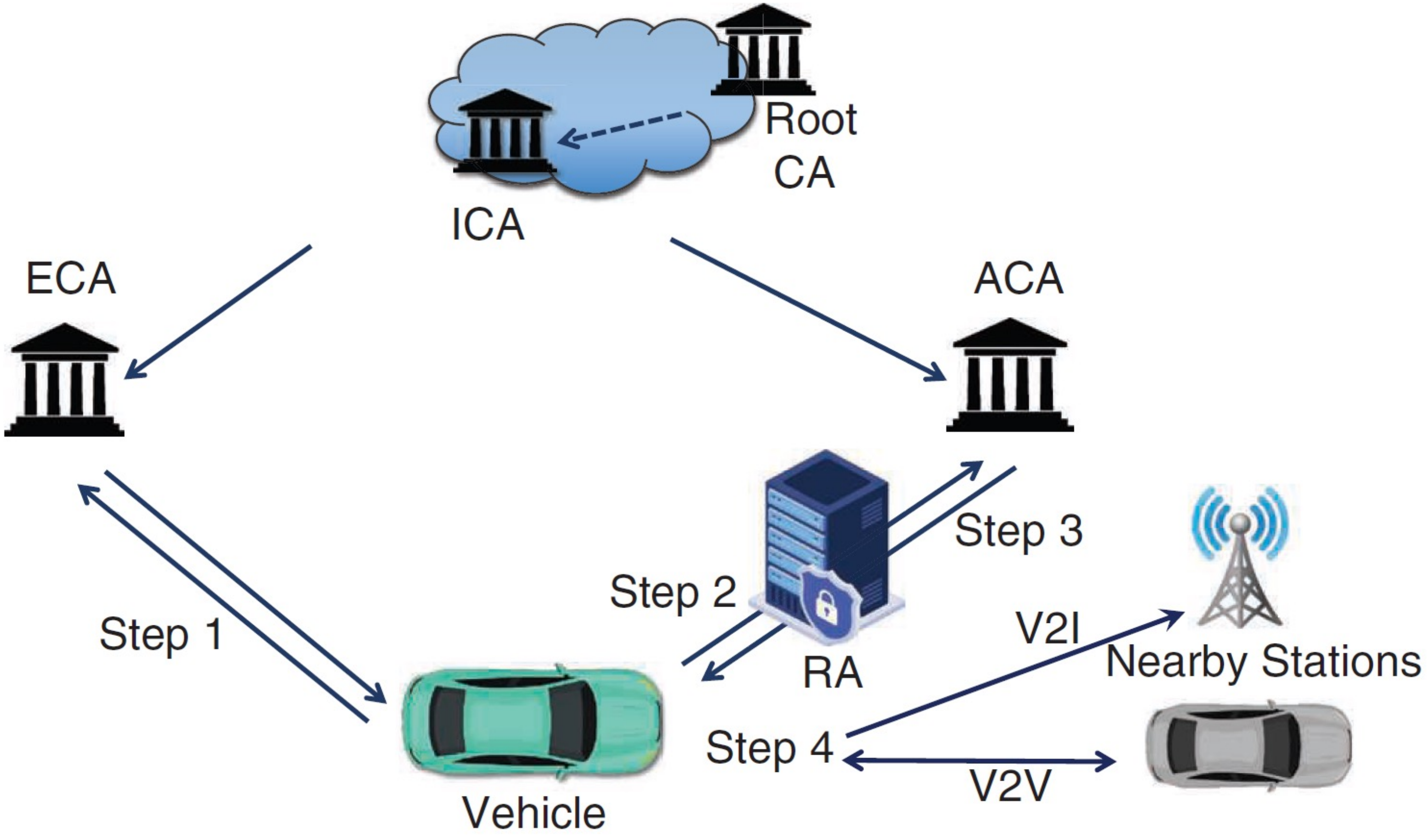


🟦 Infrastructure Certificate Issuance
🟪 Enrollment Certificate Issuance
🟩 Pseudonym Certificate Issuance
🟥 Misbehavior Reporting & CRL Distribution

① Root CA
② Intermediate CA
⑦ Misbehavior Authority
③ Enrollment CA
Enrollment RA
Device Configuration Manager
④ Pseudonym CA
⑥ Linkage Authority 1
Linkage Authority 2
⑤ Registration Authority

Infrastructure 01
Infrastructure 02
Infrastructure 03
Connected Vehicle 01
Connected Vehicle 02
Connected Vehicle 03

C-PKI Workflow



Problems of C-PKI for V2X Authentication

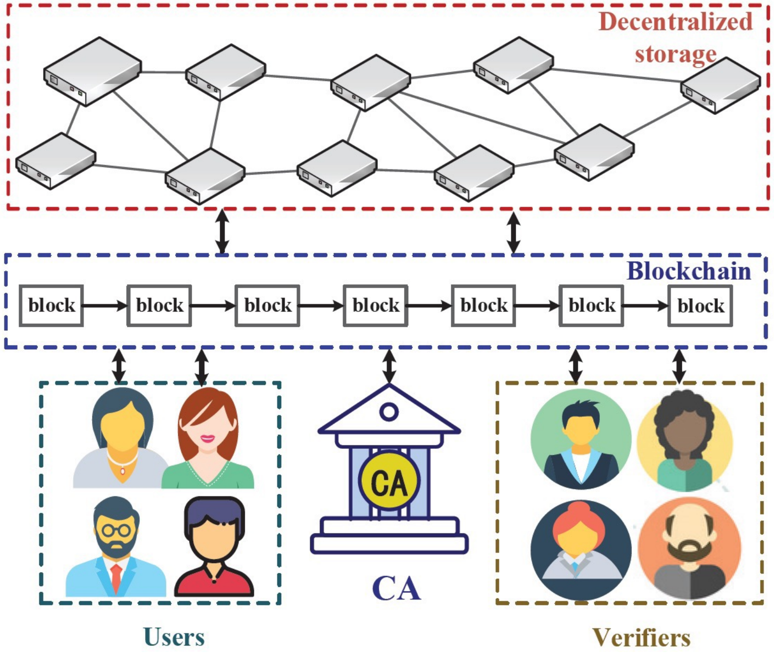
- Bottleneck issues from the heavy authorization, registration, verification requests traffic

- Short comings

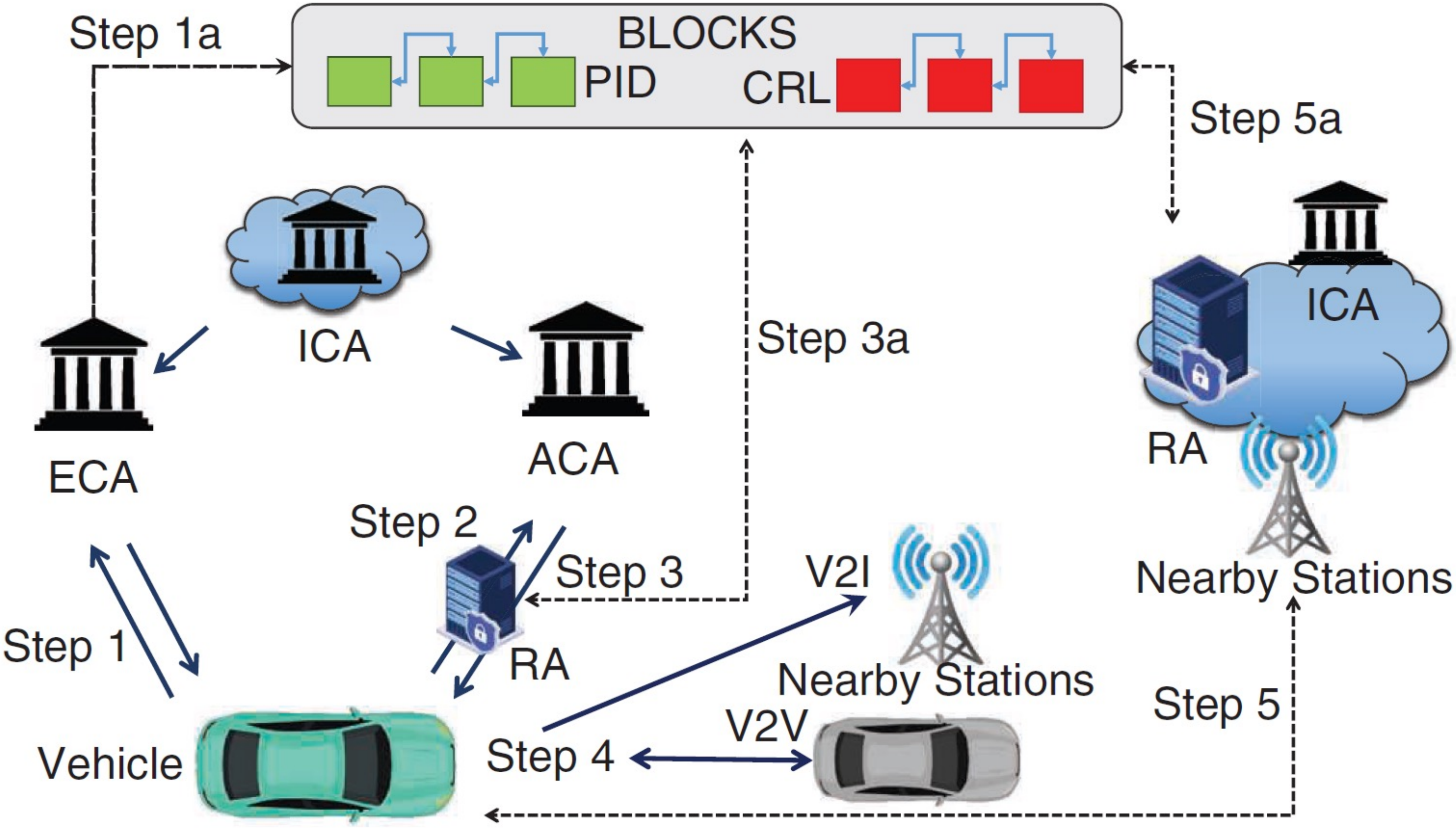
1. Trust maintenance among the PKI entities
   - Misbehaving CAs, rogue CAs
2. Scalability to serve a massive number of vehicles
   - Issuance/distribution/verification of hundreds of billions of pseudonym keys
3. An efficient mechanism for certificate revocation in terms of time, cost, and security
   - Renewing CRLs or revoking certificates in a timely manner

B-PKI for V2X Authentication

- B-PKI with CA (Semi-centralized)
  - Blockchain acts as the communication layer + public log to record certificate operations to support public and verifiable search
  - CA operations are identical as that in C-PKI
  - Decentralized storage = off-chain storage of certificates



B-PKI Workflow



ADVANTAGES OF B-PKI

- Public and transparent log eliminates the trust problem on CA's actions
  - Reduce dependency on a centralized CA (single point of failure)
- Certificate transparency and revocation transparency are already provided by the chain
- Distributed architecture + fast consesnsus algorithm ensures scalability

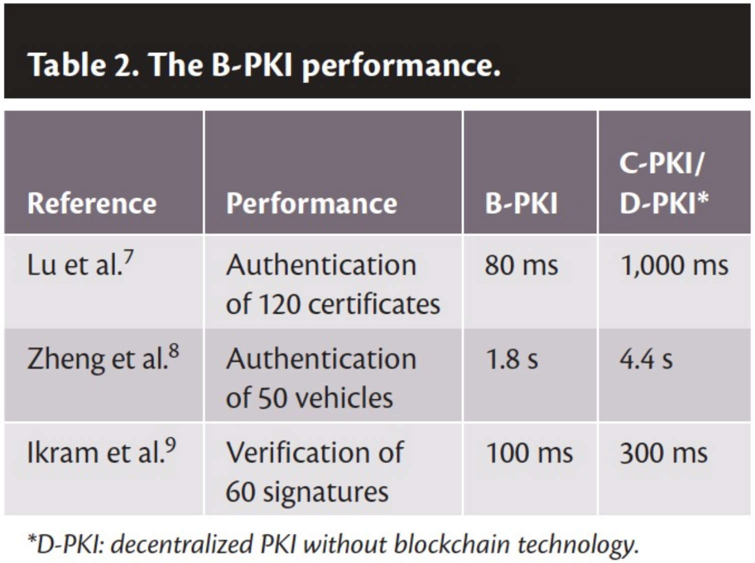


Table 2. The B-PKI performance.

Reference	Performance	B-PKI	C-PKI/ D-PKI*
Lu et al.[7]	Authentication of 120 certificates	80 ms	1,000 ms
Zheng et al.[8]	Authentication of 50 vehicles	1.8 s	4.4 s
Ikram et al.[9]	Verification of 60 signatures	100 ms	300 ms

**D-PKI: decentralized PKI without blockchain technology.*

- Security Advantages
  - Resistance against DDoS attacks
  - Resistance against impersonation, MitM attacks
  - Resistance against replay attacks
  - Resistance against tampering attacks

WEAKNESS AND CHALLENGES OF B-PKI

- Communication security among CAs and participating blockchain nodes
- Real time processing for massive requests
- Vulnerability of the underlying blockchain technology
  - Smart contract vulnerabilities
  - Attack on the blockchain
- Public, transparent logs may allow big data analysis and AI to undermine user privacy

CONCLUSION

- Proposed blockchain technology as the key enabler of V2X PKI
  - Scalable, secure, and efficient authentication
  - Partial integration (B-PKI with CA) supporting interoperability
  - Strong resistance against DDoS attacks and misbehaving CAs

- Critique
  - Storing and maintaining pseudonym certifiactes and CRL require large amount of storage on participating nodes
  - Unclear on some operation and usage of smart contracts
  - No implementation and evaluation (results from other literatures)

감사합니다

Thank you~!