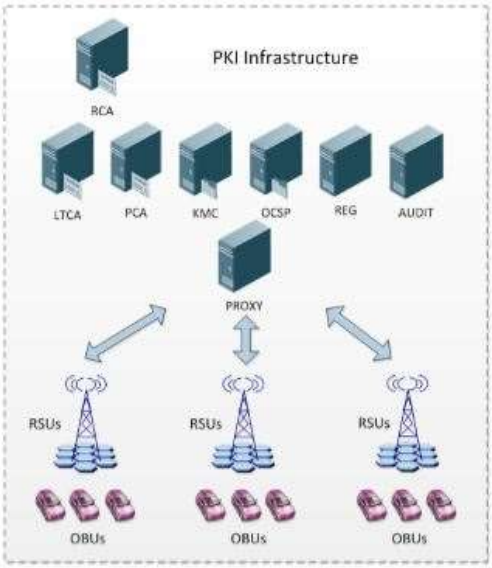
Security Enhanced Technologies for IEEE 802.11p

According to the dedicated short-range communications (DSRC) in road safety-related applications, each vehicle equipped with onboard units (OBUs) will broadcast routine traffic messages with the information of position, current time, direction, speed, acceleration/deceleration, and traffic events, etc. With the information, drivers can be better aware of their driving environment and take early action to respond to an abnormal situation, such as a traffic accident.

However, before putting this attractive application into practice, the security challenges of 802.11p must be resolved. Without security guarantees, an adversary can either forge bogus information to mislead other drivers, and even cause a deliberate traffic accident. Therefore, how to secure 802.11p has become a fundamental requirement for vehicle-to-x (V2X) communications. In the latest approved IEEE Std 1609.2, a complete framework for security has already been proposed, where the Elliptic Curve Integrated Encryption Scheme (ECIES) algorithm is used to achieve the confidentiality in V2X communications, while the Elliptic Curve Digital Signature Algorithm (ECDSA) signature algorithm is suggested to ensure authentication and non-repudiation. However, both of them are only efficient in one to one communication. Once a group of vehicles communicate simultaneously, pure ECIES and ECDSA cannot handle secure multicast/broadcast communications. Furthermore, more complexity security requirements like user privacy and revocation should also be met in the V2X communication.

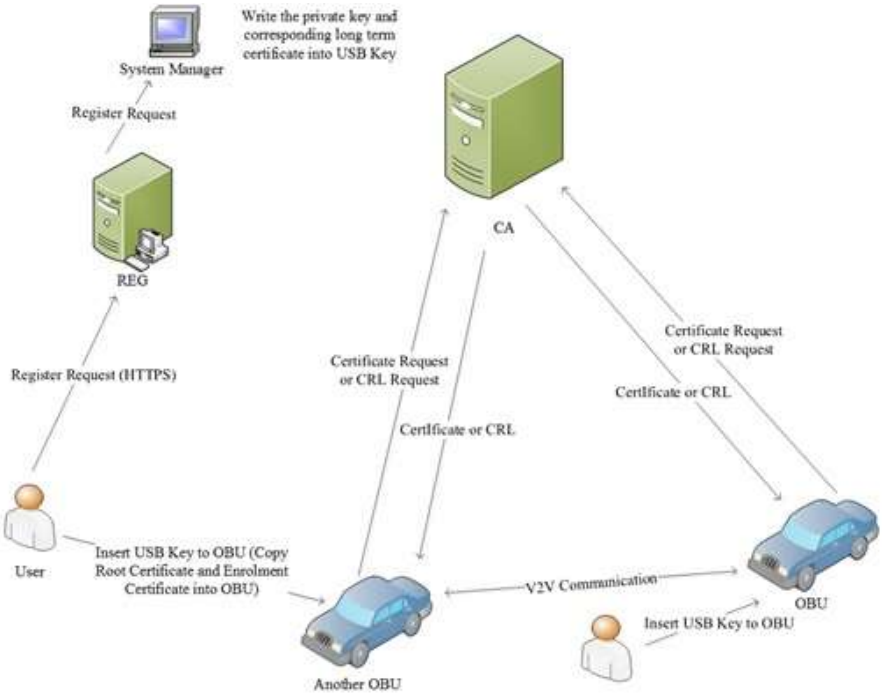
As the major work in the project, we aim to investigate PKI-certificate management, dynamic group key management, forgery detection and trust evaluation of vehicles to make V2X communication secure and efficient. Different from other similar research projects around the world, our project is to develop and implement a test-bed to test various security schemes on the security functionality. We have put our efforts to investigate various theoretical research issues and will test the solutions to examine their effectiveness and efficiency including the issues of pseudonyms changing mechanism for privacy, efficient revocation mechanism, and dynamic group key management, in real environment, thus to narrow down the gap between theory and practice of security enhanced technologies for IEEE 802.11p. The long term goal of this project is to provide a secure and trustworthy vehicular communication environment, making V2X technologies really benefit our daily life, not only in Singapore but also around the world. In addition, students in this project will have sufficient opportunities to interact with industry. The knowledge and skills acquired through the project, on both theoretical and practical fronts aspects, will prepare them well in a competitive job market with a strong demand from equipment and software vendors, service providers, and research labs.

1. PKI Infrastructure



- RCA (Root Certificate Authority)
- LTCA (Long Term Certificate Authority),
- PCA (Pseudonym Certificate Authority),
- OCSP (Online Certificate Status Inquiry System),
- KMC (Key Management Centre),
- REG (Registration Server),
- AUDIT (Audit Server),
- PROXY (Proxy Server).
- RSU (Roadside Unit)
- OBU (On-board Units on Cars)

2. System Overview



Principal Investigators	Assoc. Prof. Maode Ma *(EEE)*
Researchers	Dr. Hao Hu Mr. Chunpeng Liu Mr. Heng Chuan Tan
Student	Ms. Qinglei Kong
School / Dept	School of Electrical and Electronic Engineering / Infinitus
Collaborator	NXP Semiconductors Singapore Pte. Ltd.
Source of Funding	Economic Development Board, Singapore