TEST Engineering & Management

March - April 2020
ISSN: 0193-4120 Page No. 4186 - 4194

Certificate Management Scheme for IoT Services

Seung-hwan Ju[1], Hee-suk Seo[*2]

[1]Senior Research Engineer, Electrical Standards Center, Korea Testing Laboratory, Republic of Korea
[*2]Professor, Dept. of Computer Engineering, Koreatech, Republic of Korea
seunghwan@ktl.re.kr[1], histone@koreatech.ac.kr[*2]

Article Info
Volume 83
Page Number: 4186 - 4194
Publication Issue:
March - April 2020

Abstract

Industrial IoT services such as inter-vehicle communication systems, electric vehicle charging infrastructure, and advanced metering infrastructure provide security requirements. They use public key-based PKI, which leads to common requirements.

Using the results of the C-ITS vehicle authentication system and the mutual authentication system in the smart metering environment, this study analyzed the security requirements of the IoT environment and proposed a framework for designing the certificate management system of the IoT service. We analyzed the certification schemes of international standards such as IEEE 1609.2 of C-ITS, ISO/ EC 15118 of EV charging infrastructure, and IEC 62056 of smart metering.

At the manufacturing stage, the certificate is installed on the device. When the device is delivered to the user, the certificate is delivered to the user. This is a certificate for user verification that is used almost permanently unless the user of the device changes. The service participation certificate is managed separately. It has an authentication scheme with a short lifespan for privacy protection and security of service operations.

Many IoT services will launch in the future. It is expected to have a clearer security system by applying the certificate management system for credential management and service participation.

Keywords: *Privacy, IoT-Services, PKI, Bootstrapping, Certificate for service, Certificate Management Scheme.*

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 26 March 2020*

1. Introduction

IoT services with limited resources and networks using low-power communication technologies pose risks to various threats of the existing Internet. Therefore, embedded security technologies such as secure S/W coding technology and low power Crypto S/W implementation technology for resources with limited computing resources and storage space are required. Security threats in the Internet of Things can occur in the form of data forgery and alteration, unauthorized service and user access, authentication interference, confidentiality/integrity violations of signals and data, information leakage, replication attacks, etc. Design a PKI certification scheme to solve the problem. This paper generalizes the PKI certification system of IoT service through PKI system of V2X environment, vehicle-to-vehicle communication, PKI scheme of electric vehicle charging infrastructure ISO/IEC 15118.

2. PKI Management System of Industrial IoT Service

2.1. Cooperative Intelligent Transport System

Automobiles are developing as information and communication technology convergence devices as intelligent and autonomous vehicles. The

American Society of Automotive Engineers (SAE) predicts that by 2040, 75% of cars will be autonomous [1]. With the development of these vehicles, the ITS technology linked with the road is developing, and recently, the ITS technology in which the vehicle and the road infrastructure are converged is actively studied. In the field of intelligent transportation systems, the connection between roads, vehicles and drivers has become more closely known as the Cooperative Intelligent Transport System (C-ITS). Vehicles can receive information directly from the center or check traffic conditions through base stations or CCTVs on the roadside.

The vehicle communication technology used herein may be classified into in-vehicle communication, inter-vehicle communication, and communication between the vehicle and the infrastructure. Requirements for securing vehicle safety driving and eliminating traffic jams using such vehicle communication technology are increasing. The vehicle communication system is largely composed of a vehicle terminal unit (OBU), a roadside unit (RSU), a service infrastructure, and the like. The vehicle terminal device is a system installed inside the vehicle to support vehicle communication. The vehicle terminal device collects information on driving of the vehicle and communicates with the external device for communication. Wireless networking in C-ITS can be classified into vehicle to center (V2C), vehicle to infrastructure (V2I), vehicle to vehicle (V2V), vehicle to nomadic device (V2N), and we can describe them as V2X.

2.1.1. IEEE 1609.2

The IEEE 1609.2[2] is a standard related to Wireless Access in Vehicular Environments (WAVE), which is a wireless communication standard in the automotive environment. The IEEE 1609.2 standard for Wireless Access in Vehicular Environments (WAVE) defines the security message format as a standard for Security Services for Applications and Management Messages. This standard also defines an environment for using secure message exchange. Application service using WAVE communication technology is directly related to the safety of vehicle driving [2,3]. Therefore, it is essential to protect the message from eavesdropping, spoofing, tampering, and reply attack. In addition, since the WAVE technology is applied to individual vehicles, the driver's privacy guarantee must also be provided.

- **Hardware based high speed encryption technology**

In a vehicle-to-vehicle communication environment, messages such as speed and direction of a vehicle are exchanged between vehicles that are driving at high speed. According to the WAVE technical specification, the vehicle status information message is exchanged every 100 msec. Therefore, a hardware-based fast encryption technique is required to minimize the time required to encrypt a message.

- **Elliptic Curve Password based Message Authentication Technology**

The IEEE 1609.2 standard defines digital signature technology to identify whether messages between vehicles are tampered with, and whether the message sender is a suitable entity. In particular, since the digital signature technology based on elliptic curve cryptography (ECC) is defined, an elliptic curve cryptography authentication system suitable for a vehicle communication environment is required.

- **Privacy protection authentication technology**

In a vehicle communication environment, a technology for protecting the privacy of the vehicle's location information should be provided. In the field of privacy-protected authentication

March - April 2020
ISSN: 0193-4120 Page No. 4186 - 4194

technology, research is being conducted on authentication technology using pseudonym and authentication technology using group signature. In particular, since IEEE 1609.2 does not define an authentication technology for privacy protection, research on a privacy protection authentication technology suitable for a vehicle communication environment is required.

2.1.2. PKI for V2X (CAMP VSC3)

In a traditional system where a certificate is used, it is essential to verify who owns the certificate. For example, if a financial institution uses an accredited certificate to use Internet banking, the financial institution must be able to verify who the user is, so that authentication and authorization can be performed, and the transaction is performed through a signature. However, in the case of V2V, it is more important that "the message was sent from a trusted entity" rather than "from which vehicle." In other words, the relative vehicle is not an object of identification but an object of trust. In addition, if you identify the other person's vehicle, you face a privacy problem [4,5]. If the vehicle can be identified, in connection with the owner of the vehicle, personal information such as location information and driving features is known, which causes a legal problem. Therefore, it is necessary to make sure that only a legitimate entity that has obtained a certificate from a trusted CA and grant anonymity so that the vehicle cannot be identified through the DN (Distinguished Name) of the certificate as shown in Figure 2.

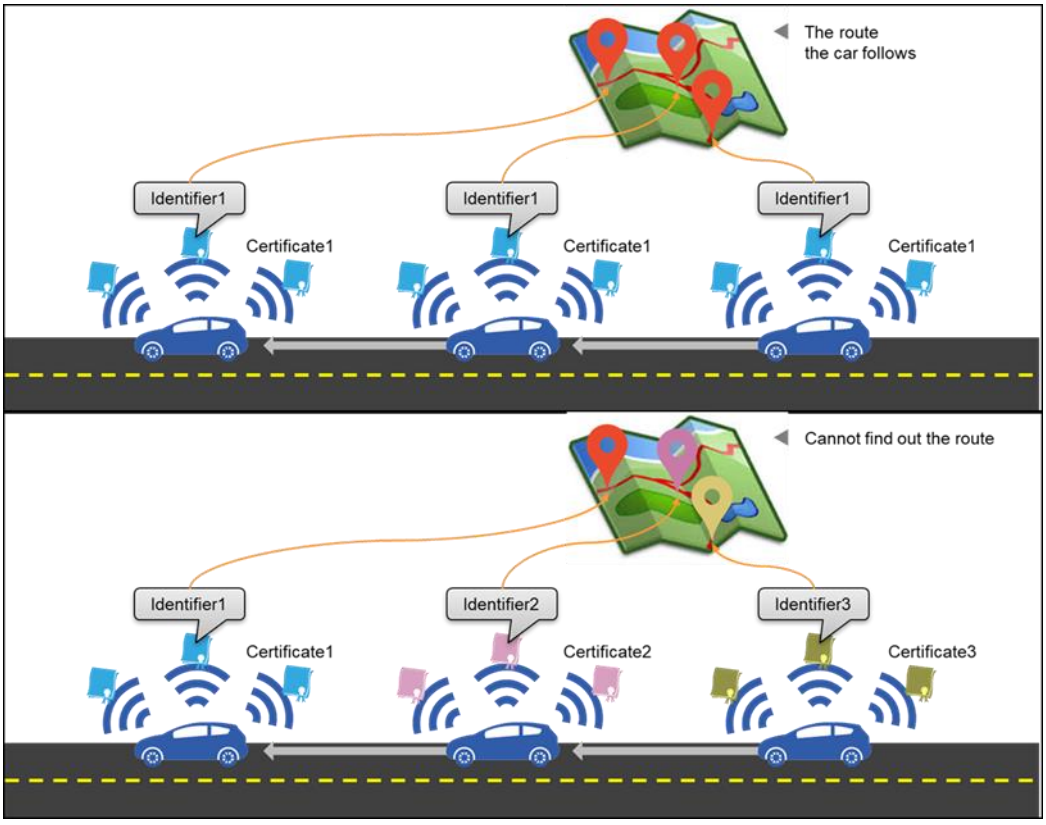

Figure 1. Privacy protection of location information using pseudonym certificate for short-term use.

The special feature of V2X is the use of anonymous certificates. Anonymous certificates require a different procedure than issuance of certificates in order to ensure anonymity [4-6]. The pseudonym certificate is a certificate that guarantees the anonymity of the vehicle. The certificate does not specify the owner of the CertID of the certificate. To ensure anonymity, the

March - April 2020
ISSN: 0193-4120 Page No. 4186 - 4194

LA that creates Linkage Value, which is the Seed value of the CertID, is also separated into two so that a single LA alone cannot infer the CertID. The CA authority that issues the certificate does not know its owner information and is provided in an environment structure where other RAs and LAs can collaborate and track that information.

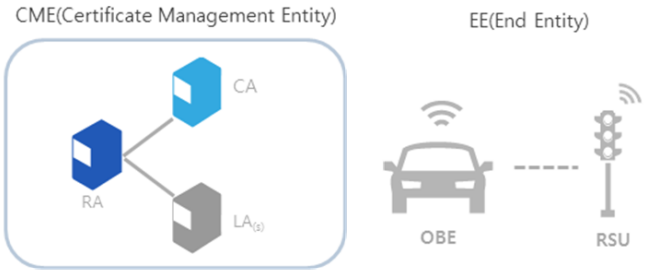

Figure 2. Certificate management system components

Therefore, as shown in Figure 2, a certificate management system is established and certificates are used in vehicles and RSUs.

2.1.3. Certificate Management Scheme

The vehicle (OBU) and the roadside unit (RSU) can issue a credential certificate through the bootstrapping process in order to issue the necessary certificates for V2X secure communication [7]. Afterwards, each vehicle and roadside toilet station establishes a vehicle certificate issuing system that can issue their own certificate using a credential certificate at the time of operation.

In addition, the issued certificate is revoked and each vehicle is configured with a management environment of the vehicle to which the revoked information can be applied in Table 1.

The vehicle (OBU) and the roadside unit (RSU) can issue a credential certificate through the bootstrapping process in order to issue the necessary certificates for V2X secure communication.

Table 1: Certificate scheme for Cooperative Intelligent Transport System (C-ITS)

Certificate Type	Description
Enrollment Certificate	- Certificate with information necessary for issuing V2X service certificate - Certificate that proves the qualification of the device by issuing it before applying it to the actual environment - A certificate containing the requestor's information in order to issue a certificate
Identified Certificate	Issued mainly to RSU, used for V2I application authorization
Anonymous Certificate	Certificates used to sign BSMs (Basic Safety Messages) on vehicles that need to be anonymous

Afterwards, each vehicle and roadside station establishes a vehicle certificate issuing system that can issue their own certificate using a credential certificate at the time of operation.

• Bootstrapping Procedure

The vehicle should have a CA certificate, RA certificate, and RootCA certificate for bootstrap. The bootstrapping procedure can be divided into initialization and registration as follows and Figure 3:

March - April 2020
ISSN: 0193-4120 Page No. 4186 - 4194

- Initialization: Process of delivering SCMS configuration certificates and access information to the device
- Enrolment: The process of issuing an Enrolment Certificate that has authority to communicate with the SCMS on the device.

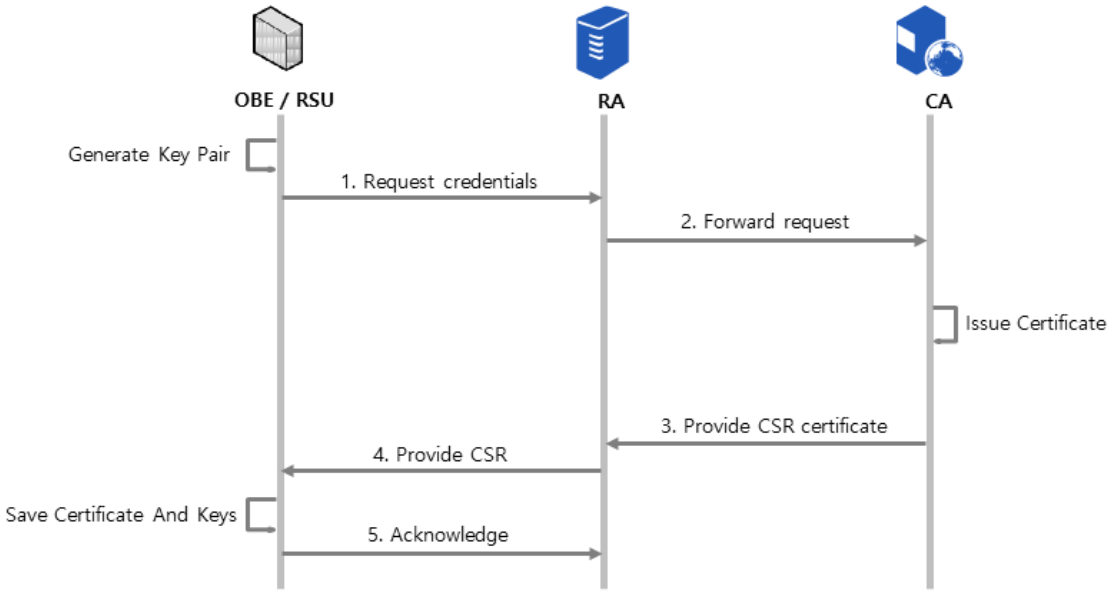

Figure 3. Sequence Diagram for Bootstrap

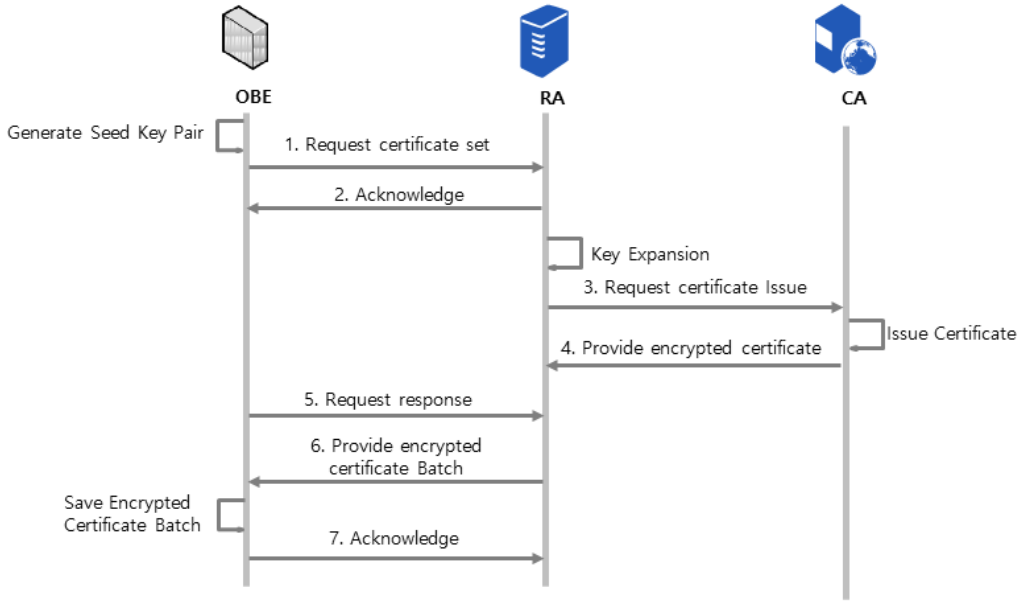

Figure 4. Sequence diagram of request-response for issuing pseudonym certificate

• Anonymous Certificate Issuance Procedure

In order to request a pseudonym certificate [8], the vehicle must complete the bootstrapping procedure and have an enrolment certificate like Figure 4. The vehicle gets a certificate batch, which can vary from policy to policy, but usually contains 20 pseudonym certificates in a batch. The vehicle can only use one certificate batch for a week and must reacquire it upon expiry.

March - April 2020
ISSN: 0193-4120 Page No. 4186 - 4194

2. 2. EV Charging Infrastructure

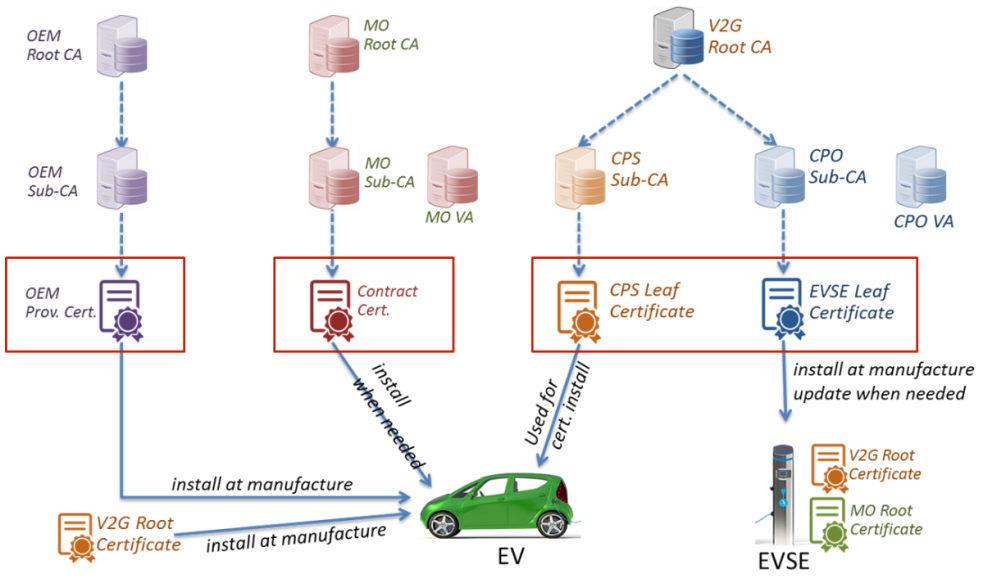

Figure 5. Certificate types used in EV charging infrastructure standards (ISO/IEC 15118)

The EV charging infrastructure uses the following certificates like Figure 5. When a vehicle is produced, the OEM Provisioning Certificate is generated. This is unique for each vehicle. When the vehicle is delivered to the customer, the CertID of the OEM Provisioning Certificate is delivered to the customer in the form of an information sheet or a delivery contract [8]. When a customer first initiates a transaction with a utility or EV charging provider, they use the OEM Provisioning Certificate to prove themselves and request the Contract Certificate. After the OEM Provisioning Certificate is verified, the Contract Certificate is issued, which is a short term certificate that can be used for a relatively short period of time [9]. (Availability may vary by policy) If a V2G service is used to transfer electricity from electric vehicles to utilities, a certificate for participation in supplementary services is required, and the CPS (EVSE) Leaf Certificate has a role

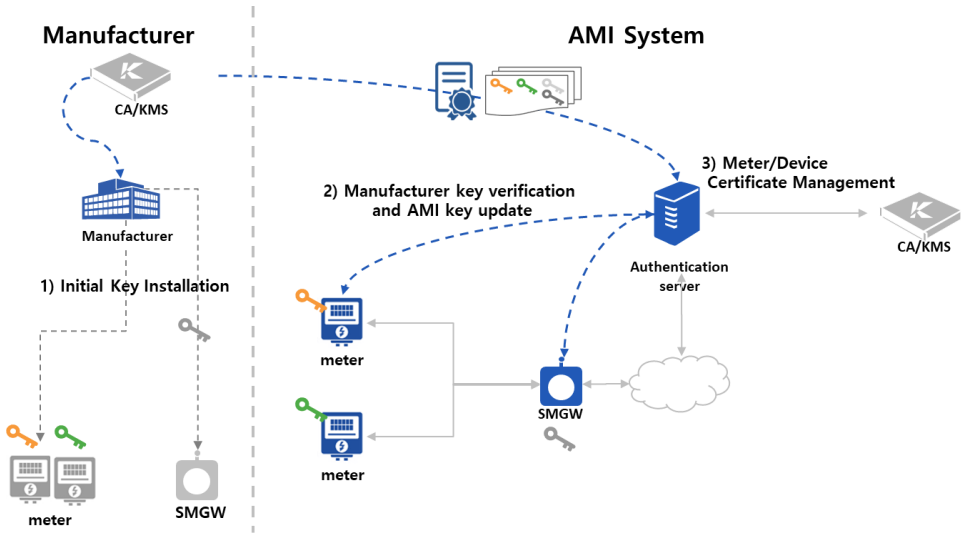

Figure 6. Reorganize certificate management system of IEC 62056 smart metering standard

2.3. Smart-Metering

Smart metering is a system for automatically and remotely acquiring measuring data [10]. Although Figure 6 shows the manufacturer's CA and the operator's CA separately, a CA may play both roles depending on the application. Importantly, there is a manufacturer's certificate that is injected at the device manufacturing stage, and the device is authenticated based on the manufacturer's certificate and subsequently issued a certificate for service participation. This service participation certificate will be available for a relatively short period of time and will require a new issue if the owner of the device changes and the provisioning information changes [11].

3. PKI System for IoT Services

In addition, several IoT services also require various necessary certificates. At this time, we can classify using the features of the certificate like Table 2 required by the IoT service.

Table 2: IoT Certificate Schemes as Certificates of Industry

Classification	EV Charging Infra	V2X vehicle communication
Bootstrapping	OEM Provisioning Certificate	CSR Certificate
Certificate for participation in service	Contract Certificate	Enrollment Certificate
Certificate for Additional Service	CPS(EVSE) Leaf Certificate	Pseudonym Certificate

3.1. Bootstrapping certificate

Bootstrapping certificates are installed for the certification of the device itself during the vehicle production phase. In the case of automobiles, certificates can be issued from the vehicle of the vehicle manufacturer or from the transportation system operator. When a device wants to participate in IoT services, it validates device suitability with a Bootstrapping certificate. This certificate is used to guarantee the producer of the device. Chain verification of the device manufacturer's certificate confirms that the device was produced from the correct subject.

3.2. Certificate for participation in service

After verifying the bootstrapping certificate, a certificate to participate in the service is issued. This is a certificate for authenticating the user of the device. In the automobile industry, for example, certificate information is composed of user information of purchasing a car. If the owner of the car changes, this certificate will be issued. This certificate proves the ownership of the device. When operating a vehicle or IoT device, it is used to distinguish the person in charge and the management of the device.

3.3. Certificate for Added-value Service

This is a certificate for the added value of the service. Certificates for added value in vehicle-to-vehicle communications are updated with short expiration dates to protect user privacy. The privacy problem is that it is possible to infer who the corresponding communication participant is by location information due to the communication between the vehicles. To solve this, the car exchanges an anonymous certificate with no name on a short cycle. The core security requirements of IoT services can be accommodated using value-added certificates.

4. Conclusion

The security certificate scheme is defined by analyzing the international standard Security Suite. It targeted communication between vehicles, charging infrastructure for EVs, and smart metering standards. These services used certificates at the stage of production of the device. Later, the device needed other certificate to access the service, and then the other certificate was needed for the actual service. This paper proposes a security authentication system for IoT services based on these characteristics. Standards of various IoT services include service requirements and security schemes. ISO/IEC 15118, the international standard for EV charging infrastructure, includes cryptographic communications and security certification systems for information protection. Communication Standard between Vehicles SCMS describes an authentication scheme for privacy protection. Smart metering's IEC 62056 defines security schemes, including the DLMS/COSEM Security Suite. I analyzed the security schemes of the IoT services and found that certificates could eventually be classified into three levels.

In the C-ITS vehicle certification system, the mobility of the vehicle was taken into consideration. Therefore, privacy protection, physical safety of the vehicle, verification of credentials and network connection protection were important. The main feature is the use of a pseudonym certificate to protect personal information in the vehicle, and to shorten the expiration date of the pseudonym certificate so that it can be periodically certified and receive a new pseudonym certificate. The smart metering mutual authentication system tried to establish a secure AMI communication by using PKI technology and digital signature to authenticate communication participants and distribute keys for communication. Since the meter has low-performance computing power, it established a secure communication environment through pre-authentication, and it was important to prepare a secure communication method in the smart metering IoT service.

This paper has established a certificate management scheme for IoT services and will be used as a research for interoperability in a certificate management system for new services.

Acknowledgment

This paper was supported by Education and Research promotion program in 2020.

References

[1] Litman, Todd. Autonomous vehicle implementation predictions. Victoria, Canada: Victoria Transport Policy Institute, 2017:32

[2] DEMBA, Albert, MÖLLER, Dietmar PF: Vehicle-to-Vehicle Communication Technology. 2018 IEEE International Conference on Electro/Information Technology (EIT) IEEE; 2018:459-464.

[3] KIM, Eun-Gi; CHO, Hanbyeog. SW Implementation on Security Algorithms in IEEE 1609.2, 18th ITS World CongressTransCoreITS AmericaERTICO-ITS EuropeITS Asia-Pacific. 2011.

[4] Whyte, W., Weimerskirch, A., Kumar, V., Hehn, T. A security credential management system for V2V communications. In 2013 IEEE Vehicular Networking Conference, 2013: 1-8.

[5] Höfer, C., Petit, J., Schmidt, R., Kargl, F. POPCORN: privacy-preserving charging for eMobility. In Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles. 2013:37-48.

[6] Rabadi, N. M. Implicit certificates support in IEEE 1609 security services for Wireless Access in Vehicular Environment (WAVE), The 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2010). 2010:531-537.

[7] Brecht, Benedikt, and Thorsten Hehn. A security credential management system for V2X communications. Connected Vehicles. Springer. 2019:83-115.
[8] Yang, Y. Wei, Z. Zhang, Y. Lu, H. Choo, K. Cai, H. V2X security: A case study of anonymous authentication. Pervasive and Mobile Computing. 2017(41):259-269.
[9] Haas, J. J. Hu, Y. C. Laberteaux, K. P. Efficient certificate revocation list organization and distribution. IEEE Journal on Selected Areas in Communications, 2011(29):595-604.
[10] Falk, Rainer, and Steffen Fries. Electric vehicle charging infrastructure security considerations and approaches. Proc. of INTERNET. 2012:58-64.
[11] Ju SH, Seo HS. Design Key Management System for DLMS/COSEM Standard-based Smart Metering. International Journal of Engineering & Technology. 2018(7):554-557.