차량통신보안을 위한 IEEE 1609.2 표준 인증서 뷰어 구현

정한균, 진성근

전자부품연구원

junghg@keti.re.kr, skjin@keti.re.kr

Implementation of IEEE 1609.2 Certificate Viewer for V2X Communication Security

Jung Han Gyun, Jin Seong Keun

Korea Electronics Technology Institute

요 약

본 논문은 C-ITS 및 자율협력주행 기술에 적용되는 V2X 통신의 보안성을 확보하기 위해 사용되는 IEEE 1609.2 표준 인증서 뷰어의 구현에 대해 소개한다. IEEE 1609.2 표준은 전자서명 또는 암호화 기술을 통해 V2X 통신의 보안성을 지원하기 위한 기능들을 정의하고 있으며, 이러한 기능들은 자체 형식으로 정의된 인증서를 통해 사용된다. 해당 인증서는 표준에 정의된 자체 형식으로 정의된 ASN.1 형식으로 인코딩되어 있으므로 그 내용을 쉽게 확인할 수 없는 특성을 가지고 있어 사용하기에 일부 불편함이 존재한다. 본 논문에서는 이러한 불편함을 개선하기 위해 구현된 인증서 뷰어 프로그램에 대해 소개한다.

Ⅰ. 서 론

V2X(Vehicle-to-Everything) 통신에 관련된 표준 중 하나인 IEEE(Institute of Electrical and Electronics Engineers) 1609.2 표준은 차량무선통신 링크에서 교환되는 메시지에 대한 보안성을 높일 수 있는 기능들에 대해 정의하고 있다[1]. IEEE 1609.2 표준은 비대칭 암호화 기법인 ECC(Elliptic Curve Cryptography) 암호화 기법을 이용한 전자서명 기능과 대칭 암호화 기법인 AES(Advanced Encryption Standard) 암호화 기법을 이용한 암호화 기능을 정의하고 있다[2,3]. 이와 더불어 비대칭 암호화 기법에서 사용되는 공개키를 담아 교환하기 위한 표준 인증서의 기능과 형식을 정의하고 있다.

해당 표준에서는 ECC 암호화용 공개키를 수납하는 인증서의 형식을 ASN.1(Abstract Syntax Notation One) 기반으로 자체 정의하고 있으며, 인코딩 방식은 COER(Canonical Octet Encoding Rule)을 따르고 있다.

IEEE 1609.2 표준 인증서는 자체적으로 정의된 형식이 COER로 인코딩되어 있기 때문에, 일반적인 사용자가 그 내용을 직접 읽거나, 일반적인 범용 툴을 이용하여 그 내용을 확인하는 것이 불가능하다. 또한 해당 인증서는 보안성을 강화하기 위해 인증서 수명을 매우 짧게 설정하여 사용하고 있으며, 이로 인해 각 인증서를 사용할 수 있는 시점을 파악하기가 쉽지 않다.

본 논문에서는 이러한 문제점을 해결하고 인증서 관리의 효율성을 높이기 위해 인증서의 내용과 부가정보를 쉽게 확인할 수 있는 IEEE 1609.2 표준 인증서 뷰어 프로그램의 구현에 대해 소개한다.

Ⅱ. 본론

IEEE 1609.2 표준 인증서 뷰어는 GUI(Graphic User Interface) 형태로 구현되어 있으며 윈도우즈 운영체제 상에서 실행된다. 뷰어 프로그램은 크게 5가지 영역으로 구성되며, 각각 ① 인증서 파일 또는 디렉토리 로딩 및 인증서 목록 표시 영역, ② 인증서 부가정보 표시 영역, ③ 인증서 유효지역 표시 영역, ④ 인증서 내용 표시 영역, ⑤ 단말기 인증서를 위한 주(Week) 값 표시 영역으로 구성된다.

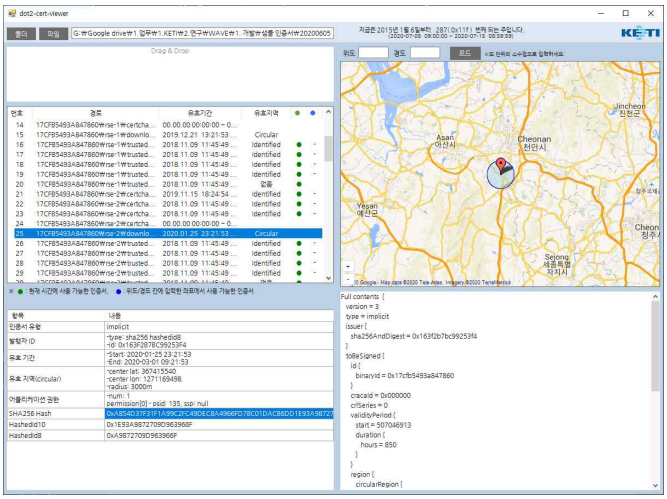

그림 1. IEEE 1609.2 표준 인증서 뷰어 프로그램 실행 화면

사용자는 “인증서 파일 또는 디렉토리 로딩 및 인증서 목록 표시 영역”에 각 인증서 개별 파일 또는 인증서파일이 포함된 디렉토리를 드래그 앤 드롭 함으로써 확인하고자 하는 인증서들을 뷰어 프로그램에 로딩할 수 있다. 로딩된 인증서들은 목록으로 표시되며, 인증서 유효기간과 유효지역 유형에 관련된 정보와 함께 각 인증서가 현재의 시점 및 지리적 위치에서 사용 가능한지 여부를 표시해 준다. 사용자는 이를 통해 현재 사용 가능한 인증서들을 파악할 수 있다.

“인증서 부가정보 표시 영역”에는 인증서 내용에 대한 요약과 사람이 읽을 수 있는 형태의 유효기간 등이 표시되고, 인증서간 관계를 파악하는 데 필요한 인증서 해시값이 표시된다.

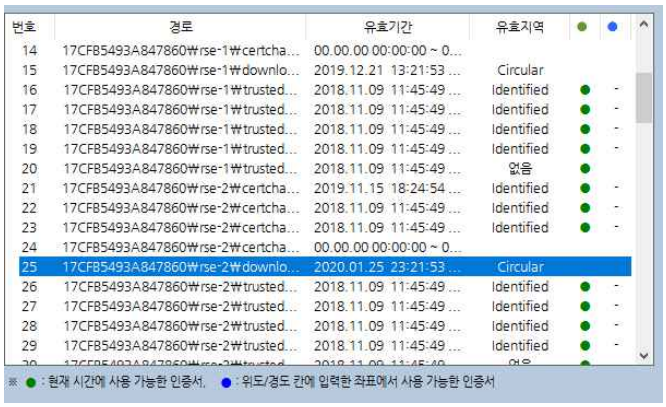

그림 2. 인증서 목록 표시 영역

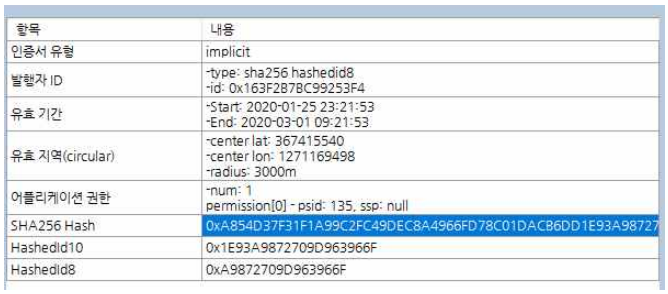

그림 3. 인증서 부가정보 표시 영역

인증서 내에 포함된 유효지역 정보가 식별자 기반이 아닌 지리적 영역 기반으로 구성되어 있을 경우(예: 원형, 사각형), 해당 인증서의 유효지역 정보가 “인증서 유효지역 표시 영역”에 표시된다. 또한 위도와 경도를 직접 입력하여 입력된 위도, 경도 상에서 해당 인증서가 사용 가능한지 여부를 확인할 수 있다.

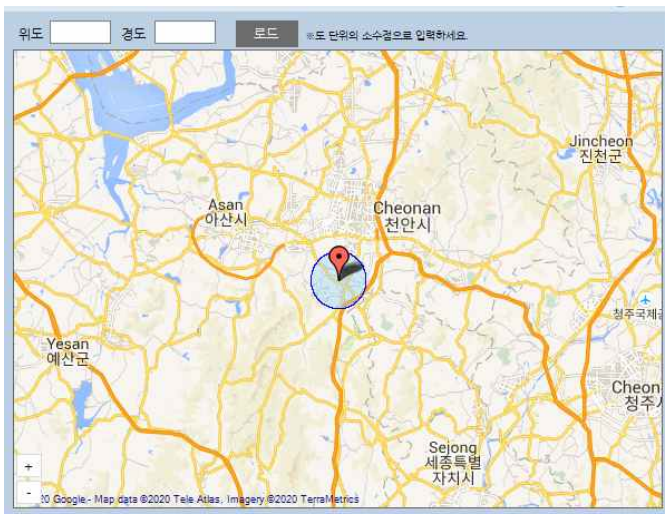

그림 4. 인증서 유효지역 표시 영역

“인증서 내용 표시 영역”에는 ASN.1 OER로 인코딩된 인증서의 내용이 사람이 읽을 수 있는 형태로 표시된다. 사용자는 이 정보를 통해 인증서를 구성하고 있는 정보를 모두 확인할 수 있다.

마지막으로 “주(Week) 값 표시 영역”에는 현재 시점이 2015년 1월 6일로부터 몇 번째 주인지가 표시된다. 이는 인증서를 구성하는 항목 중 iValue와 동일하며 또한 1주일을 유효기간으로 갖는 단말기 인증서들이 저장된 디렉토리 및 파일 이름과 동일하다. 본 정보를 통해 현재 주간에 사용 가능한 단말기 인증서 또는 인증서들이 저장된 디렉토리를 파악할 수 있다.

그림 5. 인증서 내용 표시 영역

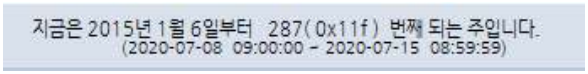

그림 6. 주(Week) 값 표시 영역

Ⅲ. 결론

본 논문에서는 IEEE 1609.2 표준 인증서의 내용과 부가정보를 쉽게 확인할 수 있는 인증서 뷰어의 구현에 대해 소개하였다. 해당 뷰어 프로그램은 범용 툴을 이용하여 그 내용을 확인할 수 없는 인증서의 내용을 쉽게 파악할 수 있도록 해 줌으로써, 개발 단계에서의 효율성을 증대시킬 수 있을 뿐만 아니라, 실제 제품 또는 시스템 레벨에서 인증서를 사용하고 관리하는데 있어서 편의성을 증대시킬 수 있다.

참 고 문 헌

[1] IEEE 1609.2, “IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages”, 2016.

[2] Elliptic Curve Cryptography, https://en.wikipedia.org/wiki/Elliptic-curve_cryptography.

[3] Adavanced Encryption Standard, https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.