정 보 보 호 학 회 지
제27권 제2호, 2017. 4

스마트그리드 기기 보안인증 운영시스템의 구현 및 현장 실증

현 무 용*, 최 연 주*, 김 진 철*

요 약

전력망과 IT의 융합으로 구현되는 스마트그리드가 IT 보안의 위협을 갖게 됨에 따라 스마트그리드에서의 안전한 통신을 보장하기 위한 수단 중 하나로 스마트그리드 기기 인증 운영 시스템을 운영한다. 이는 스마트그리드에서 운영되는 기기에 대한 인증서 발급, 등록, 관리 및 검증 서비스를 제공하여 기기인증서를 기반으로 신뢰성 높은 네트워크 환경을 구축한다. 본 논문에서는 스마트그리드 환경 하에서 동작하는 다양한 기기들이 신뢰성이 높은 네트워크 환경구축을 통해 안전한 통신이 가능하도록 지원하는 PKI 기반 기기 보안인증 운영시스템의 구현 결과를 설명하고, 제안된 시스템의 신뢰성, 현장적용성 검증을 위한 실증 테스트베드 구축 및 실증실험에 따른 결과를 제시한다.

Ⅰ. 서 론

스마트그리드는 기존 전력망에 ICT기술이 접목된 지능형 전력망으로 방향 정보교환이라는 편의성을 제공한다. 반면, ICT기술은 기존 통신망과의 연계하여 양방향 통신이 이루어지기 때문에 메인 시스템까지의 악의적 접근이 매우 용이해짐으로써 보안 취약성을 그대로 가지고 있다. 스마트그리드 환경 하에서 동작하는 기기들 간에는 광범위한 데이터 전송이 발생하며, 이러한 데이터 전송들은 기존의 폐쇄된 전력망이 아닌 통합된 광대역 전력 통신망을 통해 이루어지므로, 스마트그리드 통신환경을 안전하게 운영하기 위한 보안기술에 대한 요구사항이 급증하고 있다[1,2].

본 논문에서는 공개키 기반 구조(PKI:Public Key Infrastrucrutr) 기반의 스마트그리드 기기 보안인증 운영 시스템을 구현하고 실증하였다. 기기 보안인증 운영 시스템은 스마트그리드에서 운영되는 기기에 대한 인증서 발급, 등록, 관리 및 검증 서비스를 제공한다. 또한 저전력 특성을 반영한 경량한 암호 알고리즘 및 대규모 인증운영기술 적용으로 스마트그리드 전 분야에 도입이 가능하여, 스마트그리드 네트워크에 대한 보안 위협 대응 및 신뢰성 있는 통신환경을 지원한다.

Ⅱ. PKI 기반 스마트그리드 기기인증 개념

표 1은 스마트그리드 기기인증과 사용자 인증에 대한 비교분석 결과를 예시하고 있다. 사용자 인증은 인증대상이 사용자 본인인 반면, 기기인증은 스마트그리드 기기이다. 따라서 사용자 인증은 발급주체가 사용자 본인이 되지만, 기기인증의 경우 기기를 제조하는 기기제조사 혹은 기기를 운영하는 유틸리티 사업자가 된다. 인증서 발급유형의 경우 사용자 인증은 건별 발급이 주된 형태이지만, 기기인증의 경우 기기 제조사에 의한 대량 동시발급이 지원된다.

사용자 인증의 인증서 유효기간은 보통 1년에서 2년 3개월인 반면, 기기인증은 최소 5년에서 기기의 수명주기(10년 이상)와 일치하게 된다. 인증서 프로파일의 경우 둘 다 국제표준규격(X.509)에 기반을 두어 설계가 되었으며, 기기인증의 경우 소유자 정보내에 기기정보가 추가된다. 한편, 사용자 인증의 경우 공개키 알고리즘으로 RSA 알고리즘을 주로 사용하지만, 기기 인증의 경우 기기의 특성(저전력, 저사양)을 고려한 ECC 기반의 경량화 알고리즘이 적용된다.

사용자 인증서를 발급받기 위한 인증서처리 프로토콜의 경우 인증서발급요청, 표준인가코드생성, 패스워드 입력 등의 절차를 수반되지만, 기기인증서 발급의 경

* 한전KDN 전력IT연구원 전력보안연구팀 (my_hyun05@kdn.com, yeonju.12@kdn.com, shine_1991@kdn.com)

〔표 1〕 사용자 인증 VS 기기인증 비교분석

구 분	사용자 인증	기기인증	비고
인증 대상	사용자 본인	스마트기기	
인증서 발급주체	사용자 본인	기기제조사/유틸리티	
인증서 발급방법	건별 발급	대량 동시발급	
유효기간	1년(NPKI)/ 2년3개월(GPKI)	5년/기기 사용연한	
인증서 프로파일	X.509 v3	X.509 v3 기반 기기정보 추가	
공개키 알고리즘	RSA(2048 bit)	ECC (256 bit)	
인증서 처리 프로토콜	RFC 2510	PKCS #10	

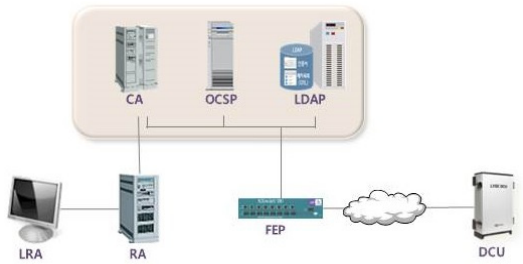
우에는 기기정보를 포함한 인증서 발급요청으로 단순화 된다.

Ⅲ. 스마트그리드 기기 보안인증 운영시스템 설계 및 구현

제안된 시스템은 인증서 발급, 등록, 검증시스템으로 구성되며, 저전력·저사양 및 대량성을 고려하여 설계되었으며, 관련 보안 가이드라인 및 표준이 반영하여 설계하고 구현되었다. 확장필드에 기기정보가 포함된 X.509 기반의 인증서 표준을 적용하고 사용자 인증에 사용되는 RSA 알고리즘에 비해 경량화 설계가 반영된 ECC 암호알고리즘과 Delta CRL이 적용되었다.

3.1. 시스템 구성

그림 1은 제안된 시스템의 구성을 보여주고 있다. 인증서 발급시스템(CA)은 기기 제조사의 기기인증서 발급요청을 수신하여, 인증서를 발급하는 기능을 수행한다. 인증서 등록시스템(RA)은 기기 제조사에 의한 인증서 발급요청양식 생성 및 인증서 발급시스템으로 인증서 발급요청을 수행한다. 기기 제조사는 인증서 등록시스템에서 제공하는 웹화면(LRA)을 통해 인증서 발급신청 및 발급된 인증서를 다운로드 한 뒤, 현장에 설치된 기기에 주입하게 된다. 인증서 검증시스템(OCSP)은 스

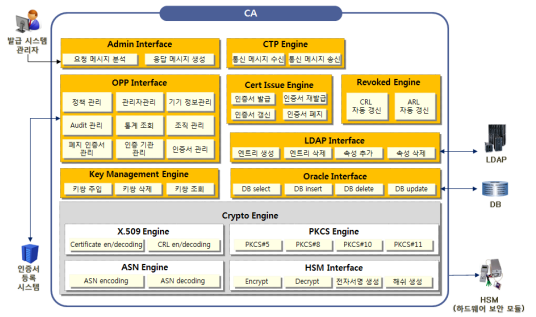


〔그림 1〕 SG기기 보안인증시스템 구성

마트그리드 운영시스템, 기기들로부터 인증서 검증요청을 접수하고, 접수된 인증서에 대한 유효성 검증을 수행한다.

3.2. 인증서 발급 시스템

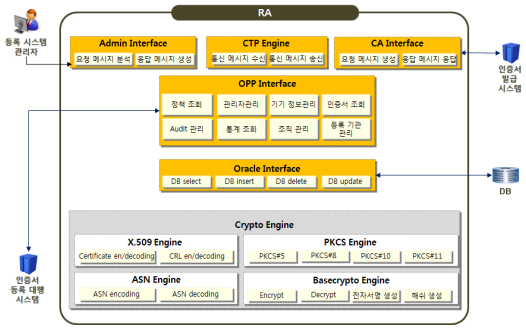
인증서 발급시스템은 크게 암·복호화 엔진과 인증서 발급 서버로 분류되고 9개의 세부기능으로 나누어진다. 세부기능은 암호화 관련된 Cryto Engine, 키쌍과 관련되 Key Management Engine, DB와의 인터페이스를 정의한 Oracle Interface, LDAP, 인터페이스, 인증서 발급과 관련된 Cert Issue Engine, CRL/ARL 관련 Revoked Engine, 정책/감사/인증서 등을 관리하는 OPP Interface, 관리자 프로그램과 관련된 Admin Interface, 통신관련 CTP Engine으로 구성된다. 발급시스템의 기능 및 역할은 그림 2와 같다.



〔그림 2〕 인증서 발급시스템

3.3. 인증서 등록 시스템

인증서 등록 시스템은 크게 인증서 등록 서버와 암·복호화 엔진으로 나누어지며, 세분화하면 그림 3과 같

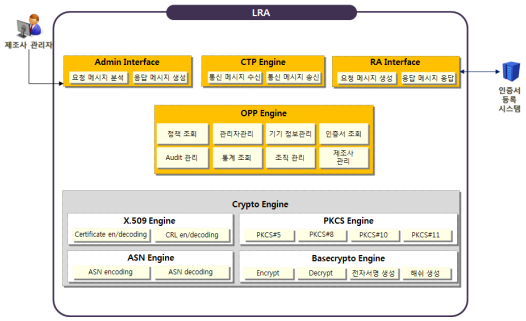


〔그림 3〕 인증서 등록시스템

이 암·복호화와 관련된 Ctypto Engine, DB와의 인터페이스를 정의한 Oracle Interface, 인증서 등록시스템 기능을 관리하는 OPP Interface, 인증서 발급 시스템과 통신하기 위한 CA Intrerface, 통신관련 CTP Engine과 관리자 프로그램 관련 Admin Interface의 6개의 기능으로 구성된다. 각 기능 및 역할은 아래 그림 3에서 보는 바와 같다.

3.4. 인증서 검증 시스템

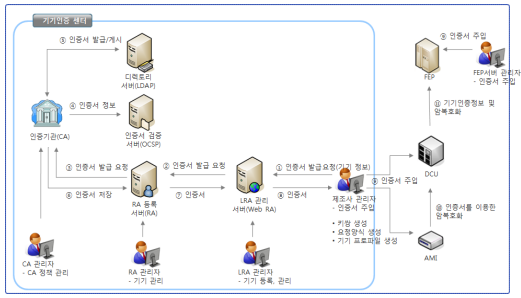
스마트그리드는 인증서 검증 시스템은 크게 인증서 검증 서버와 AMI프로그램 API로 나누어지고, 인증서 검증 서버를 기능별로 세분화하면 그림 4와 같이 7개의 세부기능으로 분류된다. 세부기능은 암·복호화와 관련된 Crypto Engine, DB와의 인터페이스를 제공하는 Oracle Interface, 인증서 검증 관리 기능인 OPP Interface, 인증서 검증 기능인 Verify Process Engine, 업무서버와 통신하기 위한 Verify Interface, 통신관련 CTP Engine과 관리자 기능을 갖는 Admin Interface으로 구성된다.



〔그림 4〕 인증서 검증시스템

3.5. 기기인증서 발급 및 주입 프로세스

그림 5는 기기인증서 발급 및 주입 프로세스를 예시하고 있다. 제조사 관리자는 기기인증서를 발급받기 위해 로컬 인증서 등록서버(LRA)에 접속하여 키쌍(개인키, 공개키), 기기정보, 인증서 요청양식(PKCS#10)등을 생성한 뒤 인증서 발급을 신청한다. 접수된 인증서 발급요청은 인증서 등록서버를 통해 인증서 발급서버로 전달되어 인증서 발급이 진행된다. 발급된 인증서는 인증서 등록서버를 통해 제조사 관리자에 전송되며, 인증서를 전송받은 제조사 관리자는 키주입 시스템 등을 이용하여 대상기기에 주입하게 된다.



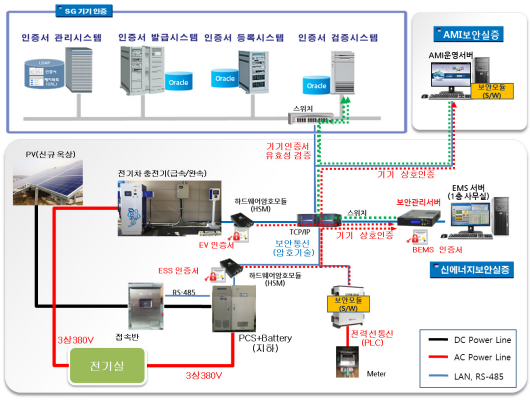
〔그림 5〕 기기인증서 발급 및 주입 프로세스

Ⅳ. 시스템 실증

미래창조과학부는 2015년부터 스마트그리드 보안기술의 신뢰성 검증 및 국내 스마트그리드의 안전한 확산에 기여하기 위해 “스마트그리드 보안 테스트베드 구축 및 실증”과제를 진행 중에 있다. 본 절에서는 제안된 시스템의 신뢰성 및 현장적용성 검증을 위해 상기 과제에 참여하여 수행한 PKI 기반 스마트그리드 기기 보안인증 실증 테스트베드 구축 및 실증 결과를 제시한다.

4.1. 실증 테스트베드 구축

그림 6은 스마트그리드 보안인증 기술실증을 위해 한전KDN 대전충남지역본부 사옥에 설치한 실증 테스트베드 구성도를 보여주고 있다. 에너지저장장치(ESS) 분야의 실증을 위해 태양광 패널, PCS, 베터리를 설치하였고, 단위모듈 간 보안통신을 위해 외장형 하드웨어 보안모듈을 적용하였다. 또한, 태양광 패널 및 배터리의



〔그림 6〕 현장 보안실증 구성도

효율적인 운영을 위한 에너지관리서버(BEMS)를 설치하였다. 전기차충전인프라(EVCI) 분야 실증을 위해서는 전기차충전기 및 관리서버를 설치하였고, 보안통신을 위해 ESS 분야와 동일하게 외장형 하드웨어 모듈을 적용하였다.

원격검침(AMI) 분야 보안기술 실증의 경우에는 S/W 보안모듈을 탑재한 DCU와 FEP을 설치하였고 한전의 원격검침프로토콜을 통해 교환되는 메시지의 안전한 전송 여부를 확인하기 위한 시험환경을 구축하였다. 마지막으로 상기의 하드웨어 및 S/W 보안모듈과 연동하여 PKI 기반 기기 보안인증 서비스를 위한 SG기기 보안인증 운영 시스템을 구축하였다.

4.2. 실증 결과

에너지저장장치 분야의 실증에서는 PCS 장비와 BEMS 서버 구간(TCP/IP)에 대한 PKI 기반 보안인증 통신 여부를 검증하였다. PCS와 BEMS 서버 구간에 설치된 외장형 하드웨어 보안모듈에 SG 기기 보안인증 운영시스템에서 발급된 기기인증서를 주입한 후, 하드웨어 보안모듈 간 보안채널 초기화시 인증서 검증서버와 연계한 인증서 실시간 유효성 검증을 포함한 기기인증서 기반의 상호인증이 성공적으로 진행됨을 확인하였다. 또한, 하드웨어 보안모듈 간 상호인증 절차가 성공적으로 수행된 후 키공유(Key Agreement) 절차에 따라 키공유가 진행되며 대칭키 기반의 보안통신(ARIA/AES 등)이 성공적으로 수행됨을 확인하였다.

전기차 충전 인프라 분야의 실증에서는 전기차 충전기와 BEMS 서버 구간(TCP/IP)에 대한 PKI 기반 보안인증 통신 여부를 검증하였다. 에너지저장장치 분야의 실증과 동일하게 외장형 하드웨어 보안모듈을 설치한 뒤 기기 인증서 기반의 상호 인증 및 보안통신 여부를 실증하였다. 시험 결과 전기차 충전기와 BEMS 서버 간 인증서 검증서버와 연계한 인증서 실시간 유효성 검증을 포함한 PKI 기반 보안인증 및 보안통신이 성공적으로 수행됨을 확인하였다.

AMI 분야의 실증에서는 DCU와 FEP 구간(TCP/IP)에 대한 S/W 보안모듈을 적용한 PKI 보안인증 통신시험을 시행하였다. DCU와 FEP에 SG 기기 보안인증 운영시스템에서 발급된 기기인증서가 주입된 뒤, DCU와 FEP에 탑재된 보안모듈에서 보안채널 초기화시 인증서 검증서버와 연계한 인증서 실시간 유효성 검증을 포함한인증서 기반의 상호인증이 성공적으로 수행됨을 확인하였고, ECDH 기반의 키공유 알고리즘을 통해 대칭키(ARIA)를 생성한 뒤 메시지 암복호화를 성공적으로 수행함을 확인하였다.

Ⅴ. 결론 및 향후 연구과제

지능화된 차세대 전력망인 스마트그리드의 보급이 가속화됨에 따라 스마트그리드 통신환경을 안전하게 운영하기 위한 보안 요구사항이 급증하고 있다. 스마트그리드 기기들은 넓은 공간에 산재되고 있어 공격자가 쉽게 접근하여 기기 및 네트워크에 장애를 유발할 뿐만 아니라 통신상의 주요 메시지에 대한 위변조 공격이 가능하며, 통신 객체 간 암호화 및 적법한 인증절차가 적용되지 않는다면 기기정보 유출은 물론 전체 스마트그리드 네트워크에 치명적인 피해를 야기할 수 있다.

본 논문에서는 적법한 인증과정을 거친 인가된 기기 및 서버 간 안전한 통신환경 구축을 위한 PKI 기반의 기기 보안인증 운영 시스템을 구현하고 실증하였다.

제안된 시스템은 스마트그리드에서 운영되는 기기에 대한 인증서 발급, 등록, 관리 및 검증 서비스를 제공함은 물론 저전력 특성을 반영한 경량화 암호 알고리즘 및 대규모 인증운영기술 적용으로 스마트그리드 전 분야에 도입이 가능하여, 스마트그리드 네트워크에 대한 보안 위협 대응 및 신뢰성 있는 통신환경을 지원한다.

또한, 시스템의 성능 및 현장적용성 검증을 위한 현장 실증시험을 수행하였고, 에너지저장장치, 전기차충전인프라, 원격검침 분야 스마트그리드 기기 간 인증서

기반의 상호인증 및 보안통신이 성공적으로 수행된 실증결과를 제시하였다.

향후에는 실증 테스트베드에서 장기간 다수의 기기를 대상으로 인증시스템 발급 및 검증 성능분석, 다양한 제조사들의 기기와 연계할 수 있는 표준화된 보안 모듈 적용 등의 실증을 통하여 보다 견고하고 신뢰성 높은 SG 기기 보안인증 운영 시스템이 될 수 있도록 지속적인 연구를 진행할 예정이다.

참 고 문 헌

[1] Yan, Y., Qian, and Y.,Sharif, H., "A Survey on Cyber Security for Smart Grid Communications", IEEE Communications Surveys & Tutorials, pp.998-1010, Jan. 2012.

[2] S. Lee, Y. Park, H. Lim, T. Shon, "Study on Analysis of Security Vulnerabilities and Countermeasures in ISO/IEC 15118 Based Electric Vehicle Charging Technology", ICIST 2014, pp1-4, 2014

[3] I.Karabey, G. Akman, "A cryptographic approach for secure client - server chat application using public key infrastructure (PKI)", ICIST 2016, 2016

〈저 자 소 개〉

현 무 용 (HYUN)
정회원
2003년 2월 : 충북대학교 대학원 박사졸업
2005년 7월~현재 : 한전 KDN 전력보안연구팀 근무
관심분야 : 정보보안, 정보통신, 분산시스템

최 연 주 (CHOI yeonju)
정회원
2009년 2월 : 서울산업대학교 매체공학과 졸업
2012년 6월~현재 : 한전 KDN 전력보안연구팀 근무
관심분야 : 통신공학, 정보보안

김 진 철 (KIM Jincheol)
정회원
2006년 8월 : 광운대학교 대학원 박사 졸업
1996년 12월~현재 : 한전 KDN 전력보안연구팀 근무, 팀장
관심분야 : 암호알고리즘, 정보보안