ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

지능형 전력량계 SW의 안전한 배포 및 업그레이드를 위한 스마트카드 기반 보안 메커니즘에 대한 연구☆

A Study on Smart card-based Security Mechanisms of upgrades Smart Meter SW for secure deployment in Smart Grid

양 인 석1 홍 석 희2*
Inseok Yang Seokhie Hong

요 약

최근 지능형 전력망 사업에서 가장 큰 이슈로 부각되고 있는 것이 지능형 전력량계의 보안과 미래 기능을 만족하기 위한 SW 업그레이드 기능이다. 그러나, 일반 기기와 달리 법정계량기에 속하는 지능형 전력량계는 공정한 상거래기반의 확립을 위해 그 기능 및 변경이 법으로 엄격히 제한되고 있다. 따라서 본 논문에서는 지능형 전력량계의 SW업그레이드와 관련된 요구사항을 분석하여, 법정계량기 요건에 준한 미래 지능형전력량계의 기능 개선을 위해 배포되는 SW이미지에 대한 인증을 통한 배포방안을 제시하고, 스마트카드를 이용한 지능형 전력량계의 보안기능을 구현하는 방법을 제안한다.

☞ 주제어 : 지능형 전력량계 SW 업데이트, 지능형 전력량계 보안, 스마트카드, 계량기 형식승인, 계량기 공인인증체계

ABSTRACT

Latest in Smart Grid projects are emerging as the biggest issue that smart meter should meet the security goal and the SW upgrade for compliance with future standard. However, unlike regular equipment, Smart meters should be designed in accordance with the regulation of legal metrology instrument in order to establish a fair trade-based business and unauthorized changes, it is not allowed and it is strictly limited by law. Therefore, this paper propose a new scheme of certification regarding type approval and verification for legal smart meter as analyzing the requirements of a smart meter regarding upgrade and security. This analysis shows that the proposed scheme comply with the regulation and the specification of smart meter by applying it to smart meter with smart card.

☞ keyword : SW Update of Smart meter, security of smart meter, smart card, Type approval, PKI for Legal Metrology instrument

1. 서 론

국내외 지능형전력망사업에서 지능형 전력량계는 양방향 전력거래, 에너지관리, 수요반응 등 부가적인 서비스를 제공하기 위한 중요한 기반이 된다. 국내 지능형 전력량계 보급계획에 따라 지능형 전력량계는 2020년까지 2000만대를 계획하고 있으나, 지능형 전력량계를 이용한 고객 서비스 개발의 지연 및 보안 등의 이유로 보급에 어려움을 겪고 있다. 이에 따라, 미국 NIST, SGIP(스마트그리드 상호운영성패널)에서 미국의 스마트그리드 도입을 위한 우선추진계획(PAP, Priority Action Plans) 중 미래 지능형 전력량계의 기능을 구현하기 위하여 최우선 과제인 - PAP 00 : Meter Upgradibility Standard, 전력량계 SW업그레이드를 최우선과제로 지정하여 추진하고 있다.

지능형 전력량계 관련 국내 지능형 전력망 표준 및 AMI 구축을 위한 보급 사업에서도 원격에서 전력량을 검침하고, 필요시 원격 통신을 통해 기능을 업그레이드 할 수 있도록 지능형 전력량계의 SW업그레이드 기능을 필수 요구사항을 반영하고 있으나, 아직 지능형 전력량계의 SW업데이트 절차와 통신 오류 시 복구절차, 다운로드 받은 SW에 대한 진위성(Authenticity) 및 무결성(Integrity) 검증 등 관련 규정 및 기준 제정이 시급한 상황이다. 또한, 지능형 전력량계는 국내 계량법에 의해 관리되는 법정계

1 Dept of Information Security, Korea University, Seoul, 133-713, Korea
* Corresponding author (shhong@korea.ac.kr)
[Received 28 October 2013, Reviewed 7 November 2013, Accepted 26 November 2013]
☆ 본 논문은 미래창조과학부 및 정보통신산업진흥원의 '지식정보보안인력양성 최고정보보안전문가과정' 사업(과제번호: NIPA-H2102-13-1002) 및 2013년도 지식경제부 기술료지원사업 '지능형 전력량계 기능개선을 위한 표준 및 평가방법 개발'((과제번호:10045649)의 연구결과로 수행되었음.

량기로써 국내외 모든 법정계량기는 국제법정계량기구(OIML)의 요구사항에 따른 규격을 준수하도록 설계 되어야 한다. 미래 지능형 전력량계의 주요 기능 중 하나인 수요반응, 실시간 요금제, 보안 등 여러 서비스를 통해 지능형 전력망 사업의 확대를 위해서는 국내 법정계량기의 요구사항을 만족하고, 나아가 지능형 전력량계의 SW업그레이드관련 보안 등 관련 규격을 만족할 수 있도록 설계되어야 한다.

본 논문에서는 위에서 제시된 고려사항을 만족하기 위하여, 현재 금융 및 신원인증카드에서 많이 사용되는 자바카드(Java Card)기반의 스마트카드를 지능형 전력량계에 적용하여 국내 지능형 전력량계에서 최소한의 보안을 구현할 수 있도록 하였고, 안전하게 SW를 배포 및 관리될 수 있도록 제안하여 계량기 제조회사 측면에서는 물리적 보안성이 확보된 보안에 대한 구현을 스마트카드로 분리하여 운영함으로써 키(Key)관리 및 저장에 대한 위험을 감소시키고, 전력량계를 이용한 유틸리티 및 부가서비스 사업자들에게는 SW업데이트를 통해 다양한 서비스를 구현하여 배포할 수 있도록 하여 보다 창조적인 새로운 서비스들의 창출과 관련 산업의 활성화될 것으로 기대 한다.

2. 지능형 전력량계 관련 주요 요구사항

본 장에서는 1장에서 제시한 목표를 달성하기 위한 주요 기준인 법정계량기의 요건과 지능형 전력량계 SW업그레이드 관련 요건에 대해서 분석한다.

2.1 법정계량기(OIML)의 주요 요구사항

국내 보급되는 지능형 전력량계는 공정한 상거래기반을 확립하기 위해 “계량에 관한 법률”에 따른 법정계량기로 분류되어 엄격히 관리되어 운영되고 있다.

최근 출시되는 계량기는 (그림 1)과 같이 전자식계량기로 원시데이터를 가공하여 처리하는 계량기의 SW는 계량기의 정량 및 성능을 좌우하는 아주 중요한 요소로 작용한다. 이런 흐름에 따라 국제법정계량기구(OIML)에서 “SW로 제어되는 계량기의 일반 요구사항”(OIML D 31 : 2008)을 참조표준으로 제정하고 지능형 전력량계의 형식승인기준(OIML R 46)인 강제인증기준에 적용하고 있다.

따라서 국내 지능형 전력량계는 법정 계량기로 다음의 요구사항이 고려된다.

2.1.1 OIML D-31:2008 주요 요구사항

- SW 식별 (Software Identification)
- 알고리즘 및 기능의 정확성 (Correctness of algorithms and functions)
- SW 보호 (Software protection)
- HW특성에 대한 지원 (Support of hardware feature)

이 중 SW식별에 대한 요구사항이 제일 중요하며, SW의 버전과 불가분의 관계를 형성하기 위하여 SW이미지 파일에 대하여 체크섬(Checksum)을 사용하도록 요구된다.

2.1.2 SW 업데이트관련 요구 사항

법정계량기의 SW업데이트는 현장에서 검정관이 입회하에 봉인을 해제하고 실시되는 ‘Verified Update’와 원격에서 통신으로 실시되는 ‘Traced Update’의 2종류로 분류된다.

(그림 1)의 Traced Update에서는 업데이트할 프로그램이 외부 통신을 통해 계량기에 다운로드되어 업데이트할 준비가 되면 수신 받은 프로그램 코드에 대한 무결성(Integrity) 검사를 실시한 후, 법정계량기 형식승인서(Type Approval Certificate)에 명시된 SW 유효성을 검증하는 진위성(Authenticity) 단계를 거쳐 새로운 SW로 설치되어 활성화 될 수 있다.

또한, SW업그레이드시 감사로그(Audit trail)를 남겨 SW업그레이드 절차에 대한 성공/실패 등 이벤트를 기록하도록 규정되어 있다.

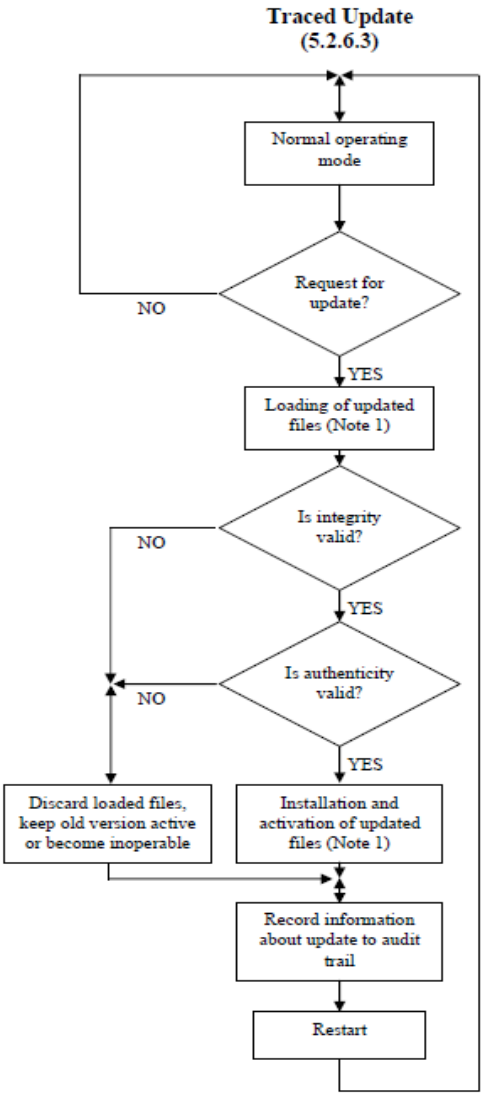
계량기 감사로그의 주요 내용은 다음과 같다.

- SW 업데이트 절차별 성공/실패
- 시점정보(Time stamp)를 기록한 이벤트 로그
- 설치된(이전) SW의 식별정보 및 관련 정보
- 형식승인 기관정보 및 계량기 모델 정보
- 다운로드 실시자 (공급처) 등

2.1.3 계량기 전자봉인(Electronic Seal) 요건

법정계량기의 정량에 대한 악영향을 미칠 수 있는 계량기 개조, 악의적인 SW변경, 파라미터 등의 무단 위변조를 차단하고, 관련 증거를 남기기 위한 주요 전자봉인 요건은 다음과 같다.

- 비인가된 신원의 접근을 막기 위한 신원인증
- 권한에 따른 접근제어 기능 (작업자, 감독관 등)



(그림 1) OIML기준 계량기 SW업그레이드 절차
(Figure 1) OIML SW Upgrade flow diagram

- SW변경을 막기 위한 암호학적 수단 (Hash, Signature 등)
- 계량기의 유지보수 또는 위변조시 증거 수집을 위한 이벤트 로그(감사 로그) 생성

2.2 SGIP PAP00-Meter Upgradability Standard

미국 NIST에서는 미래 지능형 전력량계의 표준과 상호운용성을 제공하기 위해 지능형 전력량계를 포함한 많은 디바이스들의 펌웨어는 업그레이드가 가능해야 한다는 이유로 2009년 6월 미국의 SGIP PAP00 최우선과제로 2009년 9월 주요 요구사항에 대한 표준이 완료되었다.

NEMA*에서 제시하고 있는 지능형 전력량계의 업그레이드 관련 기능요구사항들은 원격 업그레이드 및 보안에 대한 일반적인 지능형 전력량계의 요구사항을 다루고 있으며, 그에 대한 주요 내용은 다음과 같다.

- 지능형 전력량계 SW업그레이드 시 정의된 표준 적용 범위 및 운영 시스템 내에서 기능적 요구사항을 정의
- 지능형 전력량계 SW 업그레이드 시 제공되어야 할 보안 요구사항을 정의

위 표준에서도 지능형 전력량계 SW업그레이드시 개시되는 SW이미지가 신뢰할 수 있는 출처로부터 왔음을 확인해야 하며, 이를 위해 미국 정부에서 승인된 암호알고리즘을 적용할 것을 권고하고 있다.

3. 관련 연구

3.1 IEC 62056 : 2013 DLMS/COSEM

앞장에서 살펴본 요구사항을 적용하기 위하여, 국내외에서 지능형 전력량계 데이터 모델표준으로 적용되고 있는 IEC 62056시리즈[3-6]:2013, DLMS/COSEM에서는 지능형 전력량계의 SW를 업그레이드용 Image Transfer(Interface Class) 및 보안(Security)에 대하여 새롭게 정의하고 있다.

3.1.1 Image Transfer Interface Class

원격 통신을 통해 새로 업데이트 할 SW이미지의 다운로드 절차 및 무결성 검사, 설치 등 기기간 메시징에 대한 프로토콜을 세부적으로 다루고 있으며, 본 표준에서는 아래와 같이 7단계의 절차로 구성되어 있다.

1) Get ImageBlockSize supported by the servers
2) Initiate Image transfer
3) Transfer ImageBlocks
4) Check completeness of Image and transfer missing

* NEMA (미국 전기공업회, National Electric Manufacturers' Association)

blocks

5) Verify image*
6) Check Image before activation*
7) Activate Image

위 Image Tranfer의 1 ~ 4단계에 걸쳐 배포하려는 SW Image는 일정한 크기의 패킷에 나눠서 다운로드가 완료되며, 5, 6)의 2단계를 통해 다운로드 된 SW의 무결성 및 진위성을 통해 SW의 유효성이 검증된 후 활성화된다.

- Verify Image : 다운로드가 완료된 SW Image의 무결성을 검사하는 단계 (Integrity)
- Check Image before activation : image_to_activate_info 속성 확인/검사 (Authenticity)

image_to_activate_info 구조체

```
image_to_activate_info_element ::= structure
{
  image_size: double-long-unsigned,
  image_identification: octet-string,
  image_signature: octet-string
}
```

여기서, image_to_activate_info 구조체는 Image의 진위성을 확인할 수 있는 데이터로 분석이 되며, 위 구조체중 식별(identification)과 전자서명(signature)의 속성에 대해 표준[3-5]에서는 구체적인 내용이 정의가 안 되어 있다. 이는 각 국가별 고유한 계량법 및 전자서명체계에 따른 것으로 파악되며, 국내에서 이를 적용한 지능형 전력량계를 보급하기 위해서는 식별과 전자서명에 대한 구체적인 정의가 필요한 상황이다.

(표 1) Image_to_activate_info_element 구조체
(Table 1) structure of Image_to_activate_info_element

객 체	표시형식	비 고
image size	double long unsigned	이미지 사이즈
image_identification	octet-string	버전, 디바이스 타입, 제조자 등
image_signature	octet-string	활성화되기위한 전자서명 (인증기관 서명확인)

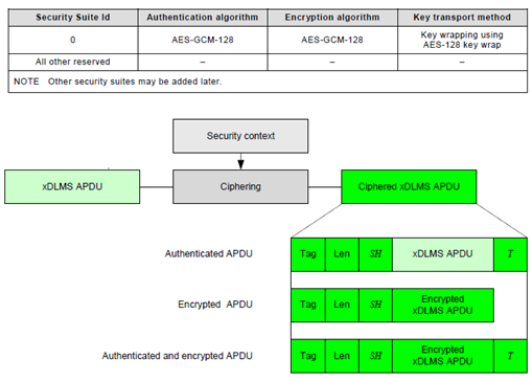
3.1.2 IEC 62056-53:2013 Security suite

DLMS/COSEM에 대한 새로운 표준[3]에서는 지능형 전력량계의 접근제어, 데이터 통신에 대한 보안을 다루고 있으며, 접근제어의 경우 기존 패스워드방식의 일방향인증인 LLS에서 AES-GCM-128 Security suite를 이용한 상호인증, HLS(High Level Security)를 (표 2)와 같이 제시하고 있다.

(표 2) IEC 62056:2013의 접근제어
(Table 2) Access Control in IEC 62056:2013

접근제어 방식	특 징
Lowest Level security (no security)	- 암호화, 인증 없음 - 기본적인 정보읽기에만 허용
Low Level Security (LLS)	- 비밀번호기반 일방향 인증 - 서버측 인증 없음
High Level Security (HLS)	- 클라이언트 서버간 양방향 인증 - 기기등록시 Challenge-Response 방식

(그림 2)의 표준에서 제시되는 데이터 접근제어 인증(Authentication) 및 데이터통신 보안(Encryption)을 위해 AES-GCM-128(= Security suite id:0)을 정의하고 있으며, AES128의 블럭암호 운영모드, GCM[3, 18]을 통해 접근제어에 대한 인증 및 3가지 유형의 데이터 암호에 대하여 적용할 수 있도록 제시되어 있다.



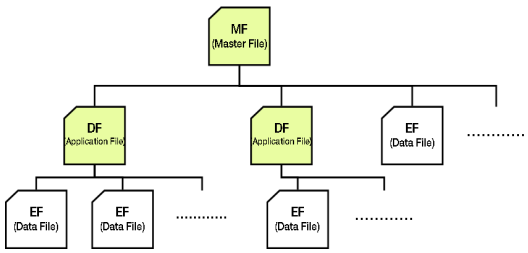
(그림 2) IEC 62056:2013의 Security Suite 및 데이터 보안
(Figure 2) Security Suite and Data security in IEC 62056:2013

3.2 Secure Network 구현을 위한 스마트카드

스마트카드는 종종 칩카드 또는 IC카드라고 불린다. 신용카드 크기만한 플라스틱판에 삽입된 IC는 데이터 전송, 저장, 처리를 위해 사용되는 기본요소를 포함하는 가장 작은 컴퓨팅 플랫폼으로 인식되고 있다. 최근에는 금융, 통신, 신원인증(ID), 교통 카드 등 다양한 분야에서 보안 솔루션으로 제안되고 있다.

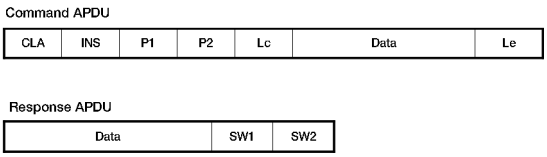
3.2.1 스마트카드의 표준 명령어 및 파일구조

ISO/IEC 7816 표준을 준수하는 스마트카드는 (그림 3)-(그림 4)와 같이 표준화된 화일시스템과 데이터 통신을 위한 명령어를 제공한다. NIST 등에서 권고하는 표준화된 암호연산을 위한 보조프로세서 및 각종 보안요소등을 통해 보안에 사용되는 키의 안전한 저장 및 비밀정보에 대한 암호연산을 통한 인증(authentication)결과에 따른 데이터 접근제어를 실현한다.



(그림 3) 스마트카드 화일시스템 (예)
(Figure 3) File system of Smart Card (example)

(그림 4)의 스마트카드는 ISO/IEC 7816에서 정의된 I/O 포트를 통해 카드단말기와 스마트카드 간 Command - Response 구조의 통신을 보여주고 있다. 카드 단말기로부터 제어되는 스마트카드는 특정 명령어에 대한 암호연산을 통한 암호화/복호화 및 서명 검증 등을 수행할 수 있는 표준화된 인터페이스를 갖고 있다.



(그림 4) 스마트카드 메시지 (Command - Response)
(Figure 4) Smart Card command and Response

3.2.2 자바카드 (Java Card)

자바카드(Java Card)는 스마트카드에 SUN(Oracle)사의 자바(Java) 기술을 적용하여, 자바 언어로 개발한 응용프로그램(이하 "애플릿")이 동작될 수 있도록 한 스마트카드이다.

스마트카드에서 지원되는 최소한의 리소스를 통해 자바 애플릿을 카드시스템에 적재하기 위한 가상 머신(Virtual Machine) SW가 내장되어 있어, 어느 HW에서도 독립적으로 실행이 가능한 개방형 플랫폼(Open Platform)을 갖고 있다.

자바카드 기술은 스마트카드 또는 다른 메모리 제약이 있는 장치에서 자바언어로 된 프로그램이 동작될 수 있는 플랫폼에 대한 정의를 하고 있으며, 자바카드 플랫폼에서 동작되는 응용프로그램을 "애플릿(Applet)"이라 부른다. 자바카드 애플릿은 어느 자바카드에서도 동작되는 확장성을 갖게 되었으며, 현재 가장 대중적인 스마트카드 운영체계 기술로 발전이 되었다. 자바카드 스펙은 다음 3개 부분으로 나뉘어 정의되고 있다.

- The Java Card Virtual Machine(JCVM) 스펙:
  - 자바 프로그램밍 언어 중 일부분으로 사용된 부분에 대한 정의, 스마트카드 응용프로그램에 부합하는 가상머신에 대한 정의
- The Java Card Runtime Environment(JCRE) 스펙:
  - 메모리 관리, 애플릿 관리, 그 밖의 runtime 특징에 대한 정의
- The Java Card Application Programming Interface(API) 스펙:
  - 스마트카드 어플리케이션을 프로그래밍 하는데 사용되는 핵심적인 자바 패키지/클래스와 확장 패키지/클래스에 대한 정의

4. 지능형 전력량계 SW의 안전한 배포방법 및 보안 구현

4.1 지능형 전력량계 관련 요구사항 분석

지능형 전력량계의 안전한 SW업그레이드 및 보안을 구현하기 위하여 지금까지 도출된 주요 요구사항을 (표 3)에서 보안을 기준으로 자바카드를 이용한 적용방안을 제시하였다.

(표 3)에서 제시된 적용방안은 현재 상용 자바카드 v2.2.2기준으로 도출된 요구사항을 만족하기 위한 공인인

(표 3) 안전한 SW업그레이드를 위한 지능형 전력량계의 주요 요구사항 분석
(Table 3) Analysis for the requirements of SW Upgrading safely in Smart Meter

구분	관련규격	보안 요구사항	기능 요구사항	적용 방안
1	OIML D 31 IEC 62056-53	진위성 (Authenticity)	SW이미지 제공 및 출처의 신뢰 (신뢰할 수 있는 가?)	공개키 인증서기반 전자서명체계 설계 및 어플리케이션 구현 (자바카드 애플릿)
2		무결성 (Integrity)	다운로드 된 SW이미지의 무결성	
3		기밀성 (Confidentiality)	원격 통신시 데이터의 기밀성	IEC 62056, AES-GCM-128 자바카드 표준 API 구현
4	OIML D31	감사로그 (Audit trail)	Event log (SW업데이트 등)	신원인증 및 데이터의 접근제어 (자바카드 애플릿)
5		전자봉인 (Electronic seal)	신원인증, 코드 및 데이터봉인	
6	OIML D 31 IEC 62056-53	암호기능 (암호연산/키관리)	Cryptographic primitive 제공 / 키배포(저장)	Cryptographic primitive 이용 (Javacard v2.2 이용)

증체계, IEC 62056 DLMS/COSEM AES128-GCM API개발, 자바카드의 표준 API 적용 등 지능형 전력량계의 SW를 안전하게 배포하기 위한 보안에 대한 목표제시 및 자바카드 애플릿 구현을 통해 본 논문에서 제안되는 방안에 대한 실제 구현에 대한 타당성을 제시하고자 한다.

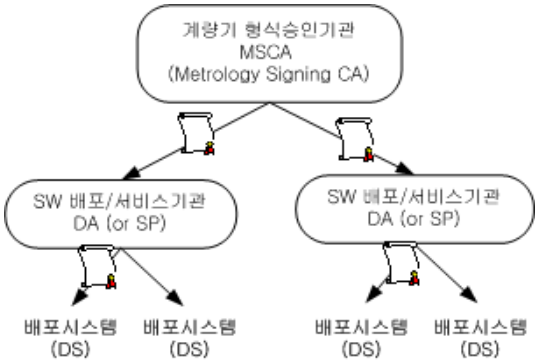
4.2 지능형 전력량계 SW 공인인증체계 설계

(표 3)의 요구사항을 만족하기 위해서는 PKI기반의 공인인증체계 도입이 필요하다. 지능형 전력량계의 형식승인(인증)에 대한 최상위 인증기관의 전자서명을 통해 각종 통신망을 통해 배포되는 SW의 진위성을 확보할 수 있으며, 데이터통신에 보안을 적용함으로써 무결성 및 기밀성을 확보할 수 있다.

국내 지능형 전력량계 형식승인기관(인증기관)을 최상위 인증기관(CA)로 두어, 형식승인기관에서 인증된 SW를 배포하는 기관인 한국전력, 에너지 서비스 사업자 등을 인증서배포기관(DA)로 (그림 5)와 같이 공개키 기반의 공인인증체계를 제시할 수 있다.

1) 계량기 형식승인기관 (Meter Signing CA)
- 지능형 전력량계 인증기관 (Certificate Authority)

2) 계량기 SW 배포 기관 (Distribute Agency)
- 지능형 전력량계 SW를 배포하는 기관 (예: 한전 등)



(그림 5) 지능형 전력량계 형식승인 공인인증 체계(PKI)
(Figure 5) PKI for Signing Type approval certificate of Smart Meter

3) 계량기 SW 배포 시스템 (Distribute System)
- SW를 배포하는 기관에서 운영하는 배포시스템

배포되는 계량기 형식승인 인증서는 법정계량기의 요건과 국제전기위원회(IEC) 표준에서 요구되는 기준들을 적용하도록 아래와 같이 인증서의 구조를 정의할 수 있다. 주요 특징은 지능형 전력량계의 SW인증을 담당하는 형식승인기관의 인증정보와 업데이트하려는 SW의 이미지 정보를 수록하도록 설계하였으며, 형식승인 인증서는 인증서의 본문을 다룬 Certification Body와 본문에 대한

서명(Signature)으로 구분된다.

계량기 형식승인 인증서

- 계량기 형식승인 인증서 Body [6]:
- CPI : 인증서 프로파일 식별자
- CAR : 인증기관 참조식별자 (예, KTC 등)
- SW Image of Meter : SW 크기, 식별, 모델 등
- Public Key : 서명검증을 위한 공개키 정보(RSA or ECC)
- CHR : 인증서 소지자 참조식별자 (예, KTC or KEPCO 등)
- 인증서유효기간 : 인증서의 유효기간
- 계량기 형식승인 인증서 Signature [6] :
- Signature : 인증서 Body에 대한 전자서명값

새롭게 정의된 인증서는 독일 BSI e-ID EAC용 인증서의 구조[6] 및 체계를 계량기 형식승인인증의 기준에 따라 표4와 같이 재정의 하였다. 인증서의 유효 기간, 참조자 권한 등은 공인인증체계에 대한 인증 정책에 따라 정의되어야 하며, 전자서명을 위한 공개키 알고리즘은 자바카드 표준에서 제시되는 RSA, ECC기반의 알고리즘을 사용한다(그림 10). 본 논문에서는 계량기의 SW를 안전하게 배포하고 이를 업데이트할 수 있는 인증체계에 대해서 제안한다.

새롭게 제시되는 계량기 형식승인 인증서(표 4)는 법정계량기인 지능형 전력량계에 배포하고자 하는 기관에서 SW업데이트를 개시하고자 할 때 통신구간에서 배포시스템을 통해 사용될 수 있다. 그리고, 지능형 전력량계는 계량기 형식승인이 완료된 이후, 루트 CA 형식승인기관의 공개키와 Reference 식별자가 자바카드에 발급되어, 지능형 전력량계의 검정(Verification)시 기기별로 배포가 된다. 인증서 내에는 인증기관의 참조식별자(CAR)외에도 전력량계를 관리하는 기관의 참조식별자(CHR) 템플릿 데이터에 따라 권한 별 데이터에 대한 접근에 대한 정의를 할 수 있다.

자바카드의 인증기관 참조식별자 정보는 형식승인 인증서의 전자서명을 검증하기 위한 공개키 사용을 식별하며, 전자서명을 통해 SW배포를 위한 SW Image정보에 대한 진위성이 검증된 후에는 SW업그레이드에 대한 통신구간에 대한 신뢰성이 확보되어, 안전하게 SW를 업그레이드할 수 있다.

4.3 자바카드를 이용한 지능형 전력량계 보안 설계

국내 주요 지능형 전력량계 적용되어 있는 IEC 62056 DLMS/COSEM [3-5]의 접근제어 및 데이터통신보안을 위해서는 AEM-GCM-128을 표준에 따라 구현해야 한다.

(표 4) 계량기 형식승인 인증서 정의

(Table 4) The definition of type approval certificate in Meter

데이터 객체	구분	비 고
MSCA Certificate	m	
Certificate Body	m	
Certificate Profile Identifier	m	1.0
Certification Authority Reference	m	형식승인기관의 정보
SW Image Information of Meter	m	
Image Size	m	Image Size
Image Identification	m	Image 정보
Device Type	m	계량기종류
Version	m	버전
Checksum	m	체크섬
Manufacturer code	m	제조사코드
Type approval Certification code	m	형식승인 일련번호
Certification Issuer	m	인증서발행사
Public Key	m	
Certificate Holder Reference	m	
Certificate Holder Access template	m	데이터 접근권한
Certificate effective date	m	
Certificate expiration date	m	
Signature	m	

자바카드 표준 API(V2.2.2기준)[15]에서는 블럭암호인 AES128은 지원하나, GCM 운용모드[18]는 지원하지 않는다. 따라서 이를 표준형 지능형 전력량계에 적용하기 위해서는 GCM을 지원하는 표준형 자바카드 클래스를 개발하여야 한다.

4.3.1 자바카드 클래스 개발시 주요 고려사항

표준형 자바카드에서 동작이 가능한 클래스를 개발하기 위해서는 자바카드표준개발가이드[17]를 참조해야 하며, 주요 제약사항 및 고려사항은 다음과 같다.

- 가비지 컬렉션 (Garbage Collection) 지원 안함
- 기본형(자료형) 지원: byte(8bits), short(16bits), boolean
- 지원하지 않는 자료형 : int, long, char, float, double
- 1차원 구조의 Array만 지원, 2차원 지원 안함
- JavaCard Class 상속/승계 가능, 예외처리 지원
- 스마트카드 표준 인터페이스 지원 : ISO/IEC 7816-4

- 제한된 표준 Crypto API만 지원함

4.3.2 IEC 62056 DLMS/COSEM GCM 설계

IEC 62056-53[3]의 5절 보안에서 정의된 AES-GCM-128 Security suite 개발시 주요 고려사항은 다음과 같다.

- AK, EK 키 길이 : len(Key) = 128bit
- IV (Inivial Vector) 길이 : len(IV) = 96bit
- Ciphered APDU의 최대 길이 : len(APDU) = 255

본 표준[3]의 5절 보안의 그림 6 “Figure 6 . Cryptographic protection of xDLMS APDUs using GCM”에서는 GCM을 사용하는 DLMS/COSEM APDU의 인증암호블럭을 잘 나타내고 있다. 위 그림에서는 기기간 HLS인증 및 데이터통신보안을 위하여 (표 5)의 Security Control값에 따라 3가지 유형의 인증암호 블럭으로 운영된다.

(표 5) DLMS/COSEM GCM 함수 적용 예
(Table 5) Example of GCM Function in DLMS/COSEM

Security Control	GCM Function()
SC-A (Authentication only)	(T) = GCM_AEk(IV, AAD) (Pass or Fail) = GCM_ADk(IV, AAD, T)
SC-E (Encryption only)	(C) = GCM_AEk(IV, P) (P) = GCM_ADk(IV, C)
SC-AE (Authenticated encryption)	(C, T) = GCM_AEk(IV, P, AAD) (P, Pass or Fail) = GCM_ADk(IV, C, AAD, T)

위 내용을 정리하면 DLMS/COSEM의 GCM함수는 아래와 같이 인증암호와 인증복호의 두가지 표준 함수로 정의될 수 있다.

- Output (C, T) = GCM-AEk(IV, P, AAD)
- Output (Pass or Fail, P) = GCM-ADk(IV, P, AAD, T)

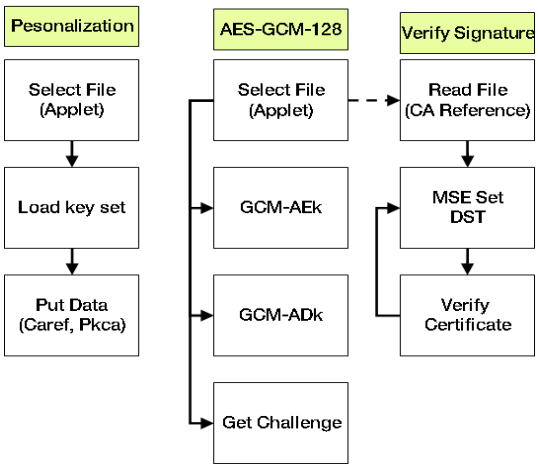
4.3.3 지능형 전력량계 인증 프로토콜 설계

지능형 전력량계 SW의 업그레이드를 위한 안전한 SW 배포 프로토콜은 자바카드를 이용하여 3가지 경우에 대한 명령어를 정의할 수 있다. (그림 6)

1) 지능형 전력량계용 자바카드 발급 (Personalization) :
   - 지능형 전력량계 형식승인 후 AES-GCM-128용 키의 발급과 형식승인인증서의 서명검증을 위한 인증기관의 공개키 및 참조식별자(CAR) 정보 발급

2) AES-GCM-128 for DLMS/COSEM (IEC 62056) :
   - HLS인증용 GMAC계산을 위한 Get Challenge
   - HLS인증용 GMAC계산을 위한 GCM-AEk
   - 데이터통신 보안을 위한 GCM-AEk/GCM-ADk

3) Verify Signature (형식승인인증서 유효성 검증) :
   - CAR정보 읽기 : Read Binary (EF File)
   - Make a trust point : MSE Set DST (CAR기준)
   - 인증서 검증 : Verify Certificate (Cert Body + Signature)



(그림 6) 지능형 전력량계용 자바카드의 명령어 흐름
(Figure 6) Command Flow of Smart Card

지능형 전력량계의 보안모듈로 제시되는 자바카드는 GCM-AES 연산 Key(AK, EK) 및 인증서 서명검증을 위한 루트 CA공개키(PKca)가 자바카드 파일시스템에 발급되어 지능형 전력량계에 탑재되어 운영되는 것을 가정하여 지능형 전력량계의 SW를 안전하게 배포하는 방안이 아래와 같이 제시된다. (그림 7)

1) DLMS/COSEM AA HLS인증(GMAC)을 통한 접근제어
2) 데이터 통신시 데이터 암·복호화 수행 (Secure채널)
3) Image Transfer를 통한 SW Image배포 및 다운로드
4) Image Transfer를 통한 계량기 형식승인 인증서 배포
5) 다운로드된 SW Image의 체크섬 계산후 인증서의 체크섬과 비교 (다르면 다운로드과정 취소후 재요청)

6) 배포하려는 SW 식별정보 확인 (버전정보, 계량기 종류, 제조사, 모델 등)을 통한 유효SW 확인
7) 다운로드 받은 형식승인 인증서를 스마트카드의 인증서 검증명령어를 수행하여 인증서 유효성 확인 (스마트카드에는 최초 SW인증기관의 공개키관련 정보가 발급되어 있음)
8) 인증서의 유효성 확인 후 정상적으로 SW인증기관으로부터 배포된 SW Image를 확인하고 정상적으로 설치후 새로운 SW로 재가동하여 운영함

지능형전력량계에서 보안 및 인증을 담당하는 보안모듈인 자바카드는 지능형 전력량계 SW의 안전한 배포외에도 DLMS/COSEM 통신간 Client-Server간 기기에 대한 상호인증 및 데이터 통신에 대한 암호화를 통해 지능형 전력량계의 데이터에 대한 접근제어 및 무결성, 기밀성을 달성할 수 있다. 또한 표준[3]의 5절 보안에서 제시된 AES-GCM-128용 Master Key의 배포에 대해서도 적용할 수 있다.

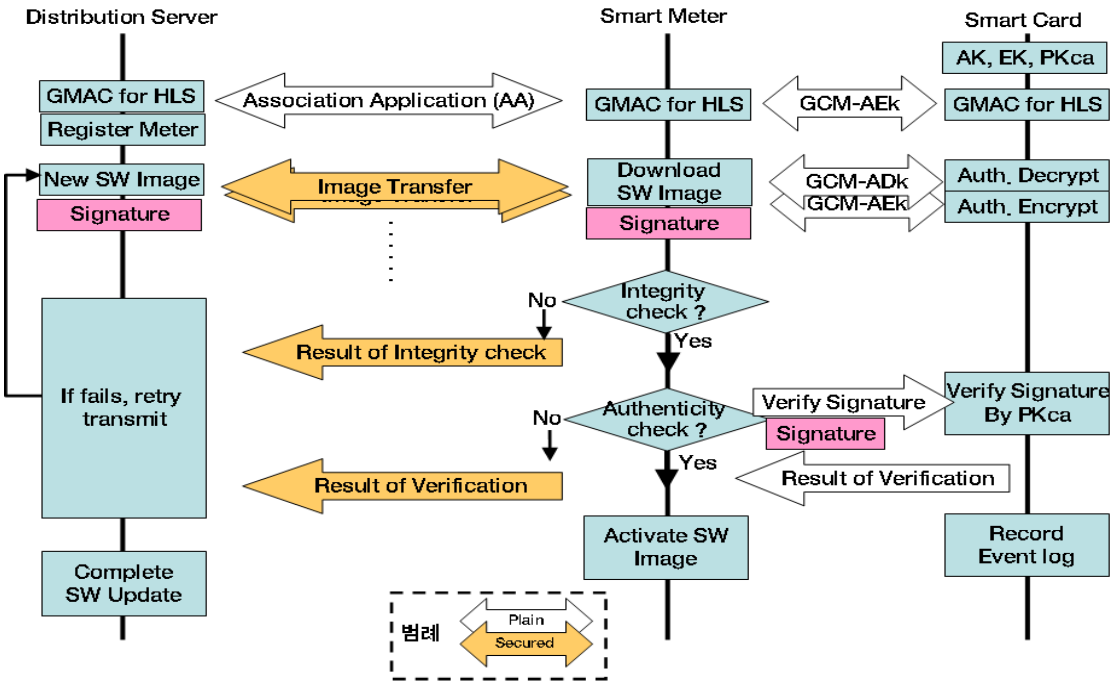
4.4 지능형 전력량계 보안 구현

4.4.1 AES-GCM-128 자바카드 표준 클래스 구현

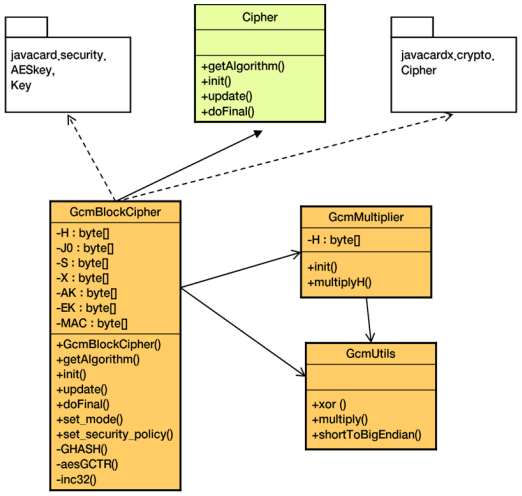
자바카드 표준API에서 제공되지 않는 AES-GCM-128을 지원하기 위하여, GcmBlockCipher 클래스를 이클립스 IDE와 NXP Toolkit을 이용하여 개발하였다. (그림 8, 9)

AES-GCM-128 표준 보안기능을 제공하기 위해 개발된 자바카드용 표준 GcmBlockCipher는 그림 8과 같이 자바카드의 Cipher 추상클래스를 상속받아, Cipher 추상클래스에서 제공하는 init(), update(), doFinal()의 method를 DLMS/COSEM용 GCM스펙[3, 18]에 따라 아래와 같이 구현하여 테스트 애플릿에 적용하여 표준에 맞는 결과를 확인하였다. (4.4.2절)

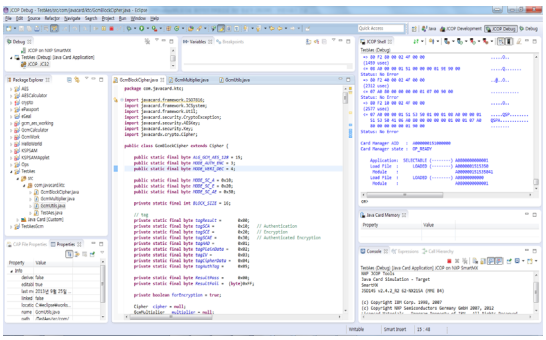
- GcmBlcokCipher Class Instance :
  - gcmCipher = new GcmBlockCipher();
- Encryption Key 등록 :
  - gcmCipher.init(key value);
- GCM-AEk : GCM AES128 Authentication Encrypt
  - gcmCipher.set_mode(MODE_AUTH_ENC);
  - gcmCipher.set_security_policy();
  - lenOutput = gcmCipher.doFinal(IV, P, AAD, Output)



(그림 7) 자바카드(스마트카드)를 이용한 지능형 전력량계 SW 배포 프로토콜
(Figure 7) Protocol for deploying sw of smart meter using smartcard



(그림 8) GCM-AES-128 표준 자바카드 API 구현
(Figure 8) Implementation of GCM-AES-128 API Class in JavaCar

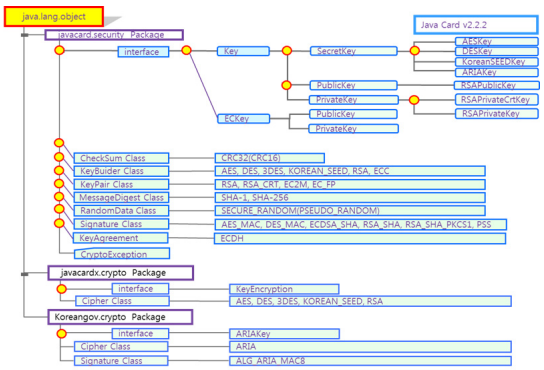


(그림 9) 이클립스(Kepler release)를 이용한 자바카드 애플릿 개발 환경
(Figure 9) The environment of Developing JavaCard Applet using Eclipse (Kepler release)

- GCM-ADk : GCM AES128 Authentication Decrypt
  - gcmCipher.set_mode(MODE_AUTH_DEC);
  - gcmCipher.set_security_policy();
  - lenOutput = gcmCipher.doFinal(IV, P, AAD, T, Output)

4.4.2 Verify Signature 구현

(그림 10)의 JavaCard v2.2.2에서 제공하는 표준 Cryptographic primitive로써 전자서명 검증을 위한 RSA, ECC, DSA, HASH 등 표준 API를 이용하여 구현한다.



(그림 10) 자바카드 v2.2.2에서 지원하는 Cryptographic Primitives
(Figure 10) Cryptographic primitives for JavaCard v2.2.2

4.4.3 지능형 전력량계 자바카드 Interface 구현

(그림 6)에서 제시된 지능형 전력량계용 자바카드 명령어를 참고하여, ISO/IEC 7816-4의 표준 스마트카드 명령어를 구현하기 위하여 지능형전력량계(카드단말기)와 자바카드의 인터페이스를 정의할 수 있다. (표 6)

(표 6) 지능형 전력량계용 스마트카드 명령어 정의
(Table 6) Define the commands of smart card for Smart Meter

Command	APDU (ISO/IEC 7816-4)
Select File	→ 00 A4 00 00 Lc AID
	← 90 00
Read Binary (CA Reference)	→ 00 B0 00 00 Le File_ID
	← CA Reference + 90 00
Put Data (Public Key)	→ 00 DA 01 00 Lc CA_Ref + PKca
	← 90 00
Load Key	→ 80 10 00 00 10 Key
	← 90 00
GCM-AEk	→ 80 20 P1 00 Lc + IV + AAD + P
	← C + T + 90 00
GCM-ADk	→ 80 30 P1 00 Lc + IV + AAD + C + T
	← Pass(or Fail) + P + 90 00
Get Challenge	→ 00 84 00 00 08
	← Random + 90 00
MSE Set DST	→ 00 22 00 00 Lc Public_Key_Reference
	← 90 00 or Error
Verify Certificate	→ 00 2A 00 00 Lc Cert_Body + Signature
	← 90 00 or Error

4.5 GcmBlocCipher 자바카드 표준 클래스 분석

본 논문에서는 지능형 전력량계의 접근제어 및 데이터 통신보안을 위해 AES-GCM-128 암호연산용 GcmBlockCipher 자바카드 표준 클래스를 제안하였다. 구현된 클래스에 대한 표준 및 성능에 대하여 검증하고자 한다.

4.5.1 표준 및 성능 검증용 시험 데이터

IEC 62056-53[3]:2013 'Table 6 - Example for ciphered APDUs' 의 Security Control 종류에 따라 Case 1에서 3까지 GCM-AEk, GCM-ADk 시험용 데이터를 (표 7)과 같이 정리할 수 있다.

(표 7) IEC 62056-53:2013, AES-GCM-128 시험 데이터
(Table 7) Test Vector of AES-GCM-128 for IEC 62056-53:2013

구분		Authentication	Encryption	Authenticated encryption
Security Material	IV	4D4D4D0000BC614E01234567		
	EK	000102030405060708090A0B0C0D0E0F		
	AK	D0D1D2D3D4D5D6D7D8D9DADBDCDDDEDF		
Security Control	SC	10 (SC-A)	20 (SC-E)	30 (SC-AE)
Input	P	-	C00100000800 00010000FF02 00	C00100000800 00010000FF02 00
	AAD	10D0D1D2D3D4 D5D6D7D8D9DA DBDCDDDEDFC0 010000080000 010000FF0200	-	30D0D1D2D3D4 D5D6D7D8D9DA DBDCDDDEDF
Output	C	-	411312FF935A 47566827C467 BC	411312FF935A 47566827C467 BC
	T	06725D910F92 21D263877516	-	7D825C3BE4A7 7C3FCC056B6B

4.5.2 GCM 검증용 APDU 명령어 및 응답 결과

(표 7)의 시험 데이터 분석을 통해 AES-GCM-128의 3가지 경우에 대하여 GCM-AEk, GCM-ADk의 기능시험을 위하여 스마트카드에서 수행 가능한 명령어 및 기대되는 응답값을 (표 8)에 정리하였다.

(표 8) AES-GCM-128 시험용 APDU 명령어 및 응답
(Table 8) The commands and response of APDU for testing AES-GCM-128

구분		Command data	Response data
Select Applet		00A4040007A0800 00000000100	9000
Key Load		80100000100001020 30405060708090A0B 0C0D0E0F00	9000
Case 1 SC-A	GCM-AEk	8020100030011E10D 0D1D2D3D4D5D6D7D8 D9DADBDCDDDEDFC00 10000080000010000 FF02000200030C4D4 D4D0000BC614E0123 456700	00021000050C24F 4D960E6F6E76C99 FCBA309000
	GCM-ADk	803010003E011E1 0D0D1D2D3D4D5 D6D7D8D9DADBD CDDDEDFC001000 0080000010000FF0 2000400030C4D4D 4D0000BC614E012 34567050C06725D 910F9221D263877 51600	000210009000
Case 2 SC-E	GCM-AEk	802020001F010000 20DC00100000800 00010000FF020003 0C4D4D4D0000BC 614E0123456700	00022000040D41 1312FF935A47566 827C467BC9000
	GCM-ADk	803020002101000 40D411312FF935A 47566827C467BC0 30C4D4D4D0000B C614E0123456705 0000	00022000020DC0 0100000800000010 000FF02009000
Case 3 SC-AE	GCM-AEk	802030003001113 0D0D1D2D3D4D5 D6D7D8D9DADBD CDDDEDF020DC00 1000008000001000 00FF0200030C4D4 D4D0000BC614E01 23456700	00023000040D41 1312FF935A47566 827C467BC050C7 D825C3BE4A77C3 FCC056B6B9000
	GCM-ADk	803030003E01113 0D0D1D2D3D4D5 D6D7D8D9DADBD CDDDEDF040D411 312FF935A475668 27C467BC030C4D4 D4D0000BC614E01 234567050C7D825 C3BE4A77C3FCC05 6B6B00	00023000020DC0 0100000800000010 000FF02009000

제시된 스마트카드 명령어는 ISOIEC 7816-4, (그림 4)의 APDU 표준 메시지 규격에 따라 표 6의 명령어 헤더를 사용하였으며, (표 8)의 각 유형에 따른 명령의 입력 데이터는 (표 7)의 시험 데이터를 참조하여 TLV (Tag-Length--Value)구조로 명령어에 포함하여, 자바카드 테스트 애플릿에서 명령어의 파싱(Parsing) 및 GcmBlockCipher클래스를 사용하여 AES-GCM-128 암호연산을 정상적으로 수행한 결과를 표시하였다. (표 8)

4.5.3 제안된 GcmBlockCipher의 성능 분석

이클립스용 NXP Tool의 JCOP Shell을 이용하여 (표 8)의 APDU 명령어를 전송하여 처리한 결과를 (표 9)에 표시하였다. NXP Tool에서는 기본적으로 JCOP, Smart MX 카드에 대한 시뮬레이션 환경을 제공한다. JCOP툴의 시뮬레이션과 ARM기반 자바카드에 대하여 동일한 GCM 시험용 애플릿을 탑재하여 성능시험을 수행하였다.

(표 9) GCM 자바카드 표준 클래스의 데이터 처리 응답 속도
(Table 9) Response rate of data processing for GCM Java card class

명령어 구분		JCOP_J5D145KB 시뮬레이션	ARM기반 자바카드
Select Applet		748us	4,812us
Key Load		425us	18,166us
Case 1:SC-A	GCM-AEK	228,349us	1,938,000us
	GCM-ADK	169,729us	1,905,000us
Case 2:SC-E	GCM-AEK	5,251us	119,493us
	GCM-ADK	5,985us	85,057us
Case 3:SC-AE	GCM-AEK	226,397us	2,587,000us
	GCM-ADK	224,049us	2,578,000us

성능분석 시험 환경

- JCOP Shell : 자바카드 APDU 명령어 수행
- Smart MX Simulation on PC
  - Model : J5D145KB_M62 v.2.4.2 R2
  - JavaCard 2.2.2, Global Platform 2.1.1
  - NXP JCOP Tool Plug in for Elipse
  - Eclipse SDK Kepler Release 64bit version
  - PC : Windows 7(64bit), Intel i7 1.90GHz, RAM 4GB
- ARM기반 자바카드 :
  - Core : ARM SC-100, RAM : 8KB, FLASH : 420KB
  - Clock : 3.56 MHz (스마트카드 표준 클럭)
  - JavaCard 2.2.2, Global Platform 2.1.1

5. 결 론

본 논문에서 제안하는 스마트카드를 이용한 '지능형 전력량계 SW의 안전한 배포방법 및 보안 구현'은 기존의 논문에서 제시하지 못했던 법정계량기의 요건에 대해서 분석하여, 현재 지능형 전력량계에 국내외에서 가장 많이 인용되는 IEC 62056 DLMS/COSEM : 2013 표준에 계량기 형식승인 인증서를 이용한 SW의 진위성을 검증할 수 있는 보안인증 스킴을 제안하였을 뿐 아니라, 지능형 전력량계의 보안을 위하여 표준형 자바카드에서 적용이 가능한 AES-GCM-128 암호연산용 GcmBlockCipher 클래스를 구현하여 지능형 전력량계의 안전한 SW업데이트를 위한 배포방법과 보안 구현에 대한 방안을 제시하였다.

스마트카드의 제한된 리소스를 활용하는 측면에서 본 논문에서 제시된 GCM기능은 일반 표준 자바카드에서 그 확장성 및 표준 호환성을 확보할 수 있으나, 현재 개발된 GCM 자바카드 애플릿의 성능 개선을 위하여 자바카드의 운영체제(OS)의 표준 API로 구현되어야 할 것이다.

또한, 본 논문에서는 물리적으로 보안성이 확보된 IC 카드 기술기반의 자바카드를 사용하여 계량기 형식승인 인증서 기반의 공인인증체계를 지능형 전력량계에 도입함으로써 지능형 전력량계의 SW업데이트 및 보안 요구사항을 만족하고, 지능형 전력량계의 보안 플랫폼으로써 자바카드를 제안하였다.

본 논문에서 제안된 형식승인 인증서 기반의 공인인증체계를 도입하기 위해서는 관련 시스템의 구성 및 운영 모델에 대한 연구가 필요하다. 현재 진행 중인 국내 지능형 전력량계 사업에서 미래 지능형 전력망 표준 및 부가서비스를 지속적으로 개발하고, 적용하기 위하여 법정계량기에서 요구되는 규정 및 기타 관련 표준들에 대한 종합적인 연구를 통해 이런 문제점들을 점차 해결하고 관련 기술들을 개발해야 할 것이다.

참 고 문 헌(References)

[1] NEMA, "REQUIREMENTS FOR SMART METER UPGRADEABILITY," September, 2009

[2] OIML D 31 - "General requirements for software controlled measuring instruments", 2008

[3] IEC 62056-5-3 Ed.1.0:2013, Electricity Metering Data Exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer

[4] IEC 62056-6-1 Ed.1.0:2013, Electricity Metering Data Exchange - The DLMS/COSEM SUITE - Part 6 - 1: COSEM Object Identification System (OBIS)
[5] IEC 62056-6-2 Ed.1.0:2013, Electricity Metering Data Exchange - The DLMS/COSEM suite - Part 6-2: COSEM interface classes
[6] BSI TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Version 1.11, 2008
[7] ITU-T. Information Technology . ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). X.690, 2002.
[8] RSA Laboratories. PKCS#1 v2.1: RSA cryptography standard. RSA Laboratories Technical Note, 2002.
[9] BSI. Technical Guideline: Elliptic Curve Cryptography (ECC) based on ISO 15946, Version 1.0.TR-03111, 2007.
[10] Russel Housley, Tim Polk,Warwick Ford, and David Solo. Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile. RFC 3280, 2002.
[11] ISO/IEC 7816-4:2005. Identification cards . Integrated circuit cards . Part 4: Organization, security and commands for interchange, 2005.
[12] Zhiqun Chen, “Java Card Technology for Smart Cards”, ADDISON-WESLEY, 2000
[13] Sun microsystems, “Java Card 2.2.2 Virtual Machine Specification”, Oracle, 2006
[14] Sun microsystems, “Java Card 2.2.2 Java Card Runtime Environment Specification”, Oracle, 2006
[15] Sun microsystems, “Java Card 2.2.2 Application Program Interface Specification”, Oracle, 2006
[16] Sun microsystems “Java Card Applet Developer’s Guide”, 1998
[17] Jan Vossaert, Jorn Lapon, Vincent Naessens, “Developing secure Java Card applications”, 2010
[18] NIST SP-800-38D, “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC”, 2007
[19] Kim Tae Hun, Kim Young Eok, Kim Jin Cheol, ″A Study on the policy of device certification services for smartgrid″, KEPCO-KDN, 2012
[20] A Study of Remote Firmware Upgrading Schemes Hyung-Kyu Kim*, Jae-Gon Choi*, LS Industrial System*, 2011
[21] Gyo-Il Jeong, Han-Na park, Bu-Kum Jung, Jong-Su Jang, Myeong-Ae Jeong, ″A Study on SmartGrid of stability and security issues″ ETRI, 2012
[22] “Requirements Analysis of Security and Strategies for Smart Grid“ Il-kwan Yang, KEPRI, 2010
[23] “A Study on Authentication Security and Gateway Access Control about Smart Meter” Jae-Hyen Lee, Dea-Woo Park, Hoseo Graduate School of Venture, 2010
[24] Gung-Wan Nam, Hyo-Jin jo, Gwan-Tae Jo, Dong-Hoon Lee “A study on Security about Smart Meter” Korea University, 2010

◐ 저 자 소 개 ◑

양 인 석(Inseok Yang)

1998년 금오공과대학교 전자공학과 졸업(학사)
2014년 고려대학교 정보경영전문대학원 정보보호학과 졸업(석사)
2000년~2010년 삼성SDS, 스마트카드 개발팀, 책임연구원
2010년~현재 한국기계전기전자시험연구원 정보기술평가센터 선임연구원
관심분야 : 정보보안, 스마트카드, 스마트미터 등 IT 및 보안 평가 etc.
E-mail : isyang@ktc.re.kr

홍 석 희 (Seokhie Hong)

1995년 2월 고려대학교 수학과 학사
1997년 2월 고려대학교 수학과 석사
2001년 8월 고려대학교 수학과 박사
1999년 8월~2004년 2월 (주) 시큐리티 테크놀로지스 선임연구원
2003년 8월~2004년 2월 고려대학교 정보보호기술연구센터 선임연구원
2004년 4월~2005년 2월 K.U.Leuven, ESAT/SCD-COSIC 박사후연구원
2005년 3월~현재 고려대학교 정보보호대학원 부교수
관심분야 : 대칭키·공개키 암호 분석 및 설계, 컴퓨터 포렌식 etc
E-mail : shhong@korea.ac.kr