情 報 保 護 學 會 誌
第20卷 第5號, 2010. 10

스마트미터의 신뢰성 및 안전성 향상을 위한 TPM 관련 평가인증 제도 분석

이 광 우*, 원 동 호*, 김 승 주*

요 약

최근 들어, 저탄소 녹색성장에 대한 관심이 높아지면서, 전력 시스템과 IT 기술의 융합이 주목받고 있다. 이에 각국 정부에서는 스마트 그리드 사업을 추진하고 있으며, 관련 연구도 활발히 진행되고 있다. 스마트 그리드는 기존의 전력시스템과 IT 기술을 융합한 차세대 지능형 전력시스템으로, 모든 전자 기기들을 네트워크에 연결하고 실시간으로 에너지 사용량을 수집하여 사용자 및 에너지공급업체에 제공한다. 이를 통해 사용자는 에너지 소비를 줄일 수 있으며, 공급업체는 에너지 공급 효율성을 극대화할 수 있다. 이러한 서비스를 제공하기 위해서는 전력을 사용하는 각 사업장 및 가정에 스마트미터라는 장치를 설치해야만 한다. 하지만 스마트미터는 일반적으로 건물 외부에 설치되기 때문에 물리적으로 많은 공격 위협에 노출되어 있다. 따라서 플랫폼 무결성 보장, 신뢰할 수 있는 데이터 암호화, 안전한 키 저장 등을 위해 최근 스마트미터에 TPM을 도입하고자 하는 연구가 이루어지고 있다. 이에 본 논문에서는 TPM 기술 및 개발 현황을 살펴보고, TPM과 관련된 평가인증 제도를 비교·분석하고자 한다.

Ⅰ. 서 론

최근 세계적으로 저탄소 녹색성장에 대한 관심과 사회적 요구가 증가하고 있다. 이에 따라 전력 시스템과 IT 기술을 융합한 스마트 그리드 기술이 차세대 전력망 기술로 각광을 받고 있다. 각국 정부에서는 그린 IT의 일환으로 스마트 그리드 사업을 추진하고 있으며, 우리나라에서도 제주 북동부에 위치한 7천여 세대를 기반으로 제주실증단지 사업이 추진되고 있다. 정부의 계획에 따르면, 2030년에는 국가단위의 스마트 그리드 구축이 완료되는 것을 목표로 하고 있다[1].

스마트 그리드에서는 전기로 작동하는 모든 기기들이 유선 또는 무선 네트워크로 연결되며, 스마트미터가 실시간으로 에너지 사용량을 수집하여 사용자 또는 에너지공급업체에게 제공하게 된다. 따라서 수요자 중심의 양방향 서비스를 가능하며, 실시간으로 개방형 플랫폼을 통해 다양한 서비스가 지원될 수 있다. 스마트 그리드에서는 실시간 전력 수요 예측이 가능하므로, 기존 전력시스템과 달리 전력 예측량의 10% 이상을 예비전력으로 준비할 필요가 없으므로, 국가 전력 생산량을 효율적으로 관리할 수 있다는 장점을 갖는다[2].

스마트 그리드에서 스마트미터는 각 사업장 및 가정에 설치되어 자동으로 에너지를 계량하고 관리하는 장치이다. 일반적으로 스마트미터를 통해 실시간으로 수집되는 정보는 스마트미터에 저장되었다가, 사용자 또는 에너지공급업자에게 제공된다[3]. 이 때, 스마트미터에 저장되는 정보가 제3자에게 유출될 경우에는 프라이버시 침해 문제가 발생할 수 있으며, 스마트미터에 포함된 정보가 위변조될 경우에는 악성코드에 의한 서비스 거부 공격을 통해 대규모 전력 공급 중단이 발생할 수 있다. 특히 스마트미터는 건물 외부에 설치되기 때문에 접근이 용이하여 물리적으로 많은 위협에 노출될 수 있다. 따라서 최근 TPM(Trusted Platform Module)을 적용하여, 스마트미터에 대한 보안을 제공하고자 하는 연구가 이루어지고 있다.

이에 본 논문에서는 스마트미터의 신뢰성과 안전성을 향상시키기 위해, 최근 주목받고 있는 TPM 기술 및 TPM 관련 평가인증 제도를 분석해 보고자 한다.

* 성균관대학교 정보보호연구소 ({kwlee, dhwon, skim}@security.re.kr)

Ⅱ. TPM

2.1 TPM 개요

1999년 Intel, AMD, IBM, HP, Microsoft 등의 컴퓨터 관련 대기업들은 신뢰 컴퓨팅에 대한 연구를 진행하기 위하여 그룹을 조직하였다. 신뢰 컴퓨팅 기술은 컴퓨터가 처음 의도한대로 동작함을 보장하기 위한 기술로, 하드웨어 기반의 보안 칩을 모든 기기에 탑재하여 신뢰 컴퓨팅 환경을 구축한다는 개념으로 시작하였다. 이후, 2003년 신뢰 컴퓨팅에 대한 중요성이 부각되면서, 하드웨어 기반의 신뢰 컴퓨팅 및 보안 기술에 대한 산업 표준을 개발, 정의 및 활성화하는 표준화 단체인 TCG (Trust Computing Group)가 설립되었다[4].

신뢰 컴퓨팅에서 가장 기본이 되는 TPM은 물리적인 공격에 대해서도 정보 유출 차단 및 훼손 방지(tamper-proof)가 보장되어야 하기 때문에, 하드웨어 형태의 칩으로 구현된다. 현재 TPM은 Infineon, Atmel, Broadcom, Intel, Sinosun, ST마이크로일렉트로닉스, Nuvoton(구 Winbond), ITE, TOSHIBA 등에 의해 제조되고 있으며, 모바일 디바이스, 노트북 등 보안 및 신뢰성이 필요한 다양한 기기에 도입되고 있다.

2.2 TPM의 구성요소

TPM은 일반적으로 암호 프로세서, 비휘발성 저장소, 휘발성 저장소로 구성된다[5].

가. 암호 프로세서(Cryptographic processor)

- Random number generator
- RSA Key generator
- SHA-1 hash generator
- Encryption-Decryption signature engine

나. 비휘발성 저장소 (Persistent memory)

- Endorsement Key(EK) : TPM을 인증하는 키로써, TPM 고유의 유일한 키이다.
- Storage Root Key(SRK) : TPM 외부에 저장된 키들을 보호하기 위한 최상위 키이다.

다. 휘발성 저장소(Versatile memory)

- Platform Configuration Registers(PCR) : 플랫폼의 상태값을 저장하는 레지스터(160비트)이다. 플랫폼 및 소프트웨어의 무결성을 검증하는데 사용된다.
- Attestation Identity Key(AIK) : 데이터에 대한 디지털 서명키이다.
- Storage Keys : TPM 내부 또는 외부에 저장되는 키이다. 또 다른 키를 암호화하기 위해 사용될 수 있다.

2.3 TPM이 제공하는 기능

신뢰 컴퓨팅을 구축하기 위해 TPM에서 제공하는 기능은 다음과 같다[4-5].

- 난수 생성 및 암호화 키의 생성
- 암복호화, 해쉬, MAC, 전자서명/검증
- 데이터, 키, 패스워드의 안전한 저장
- 동작환경 및 알고리즘에 대한 무결성 보장
- 인증 및 식별 메커니즘, 접근제어
- 카운터

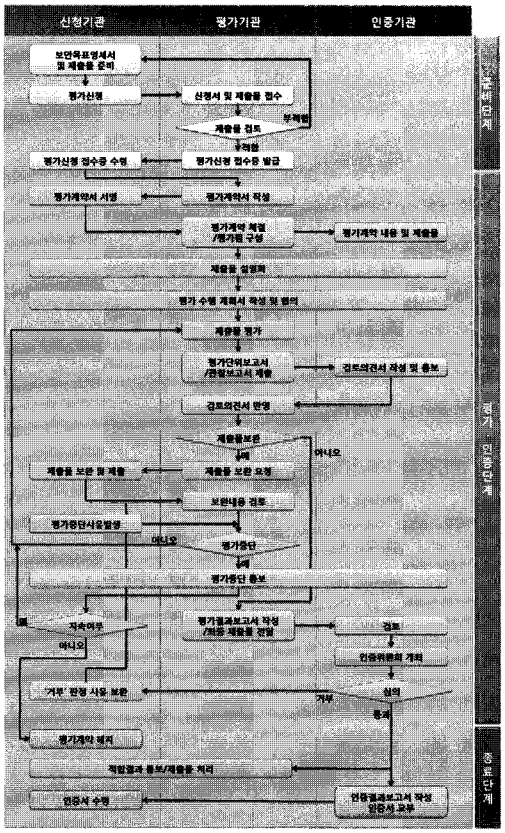
Ⅲ. TPM 관련 평가인증 제도

현재 TPM 칩에 대한 평가인증 사례는 CC가 유일하다. 하지만, 향후 다른 평가인증 제도에서도 평가인증이 발생할 수 있다. 본 절에서는 TPM과 관련성이 있는 평가인증 제도로 CC, CMVP, ISCCC, ZKA 등을 살펴보도록 한다.

3.1 CC(Common Criteria, 공통평가기준)

CC는 보안기능이 구현된 IT 제품이나 시스템의 보안성을 평가하기 위한 공통의 요구사항을 제시한 국제적인 기준(ISO/IEC 15408)이다[6-8]. CC 평가인증 제도는 CC에 기반하여 민간업체가 개발한 정보보호제품에 구현된 보안기능의 안전성과 신뢰성을 보증하여 사용자들이 안심하고 제품을 사용할 수 있도록 지원하는 제도이다.

최초 미국, 영국, 프랑스 등 선진국들은 국가 간 상이한 평가기준으로 인해 평가결과가 상호인정되지 않는 불편함을 개선하기 위해, 각국의 보안성 평가기준을 통합하여 일원화하고자 하였으며, 이를 통해 CC를 출범하게 되었다. CC는 국가별로 동일한 평가기준을 적용



〔그림 1〕 CC 평가인증 절차

함으로써, 평가시간·비용 절감, 제품 가격의 인하, 신제품 개발의 가속화 등을 가능하게 하였다. 우리나라에서는 1998년 2월부터 정보보호제품 평가인증 제도를 시행하였으며, 2002년부터 CC에 따라 정보보호 제품을 평가하고 있다. 우리나라는 2006년 5월 국제상호인정협정(CCRA, Common Criteria Recongnition Arrangement)에 따라 인증서발행국(CAP, Certificate Authorizing Participants)으로 가입함으로써, 우리나라에서 CC 평가인증서를 획득한 정보보호제품은 EAL 4 이하 평가보증등급에 한해 CCRA 회원국에서 그 평가결과를 인정받을 수 있게 되었다.

CC에서는 평가대상을 TOE(Target of Evaluation)라고 부르며, TOE에 대한 보증 수준에 따라 평가보증등급(EAL, evaluation assurance level)을 EAL1에서 EAL7까지의 7 등급으로 구분하고 있다. 평가시 평가보증등급이 높을수록 TOE에 대한 설계 검증 및 시험이 강화됨으로 보증 수준이 높아지게 된다.

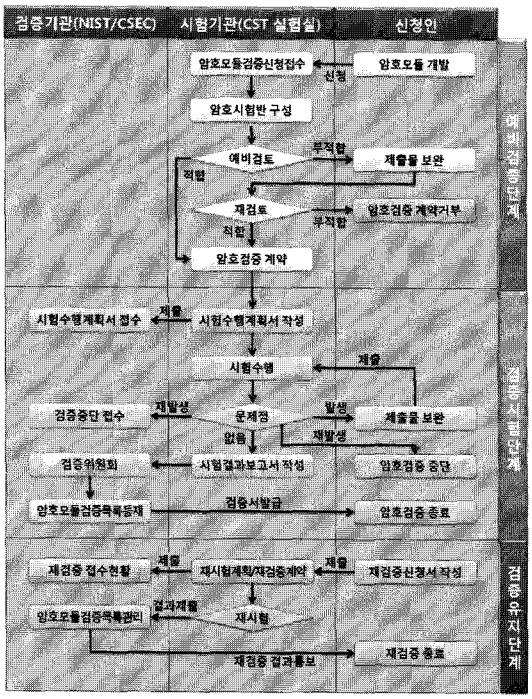
CC 평가인증 절차는 평가신청 준비단계, 평가계약단계, 평가단계, 인증단계, 인증 효력유지단계로 구분하며, [그림 1]과 같다[9].

CC에서 평가 기준이 되는 문서를 보호프로파일(PP, Protection Profile)이라고 하는데, TPM에 대한 보호프로파일은 TCG에서 2008년에 개발한 "PC Client Specific Trusted Platform Module Family 1.2; Level 2"가 있다. 이 보호프로파일의 평가보증등급은 EAL4+이며, "TCG Trusted Platform Module Main Specification, version 1.2"와 "PC client specific interface specification"에 정의되어 있는 기능을 구현한 하드웨어, 펌웨어 및 소프트웨어를 평가대상으로 하고 있다. 2010년 10월 현재 TPM 보안 칩 중에서 CC 평가를 받은 제품으로는 Infineon의 "SLB9635TT1.2 / m1566-a13 HW a13 / FW 03.17.0008.00"이 유일하다.

3.2 CMVP (Cryptographic Module Validation Program)

CMVP는 1995년 7월 미국의 NIST(National Institute of Standards and Technology)와 캐나다 CSEC (Communications Security Establishment Canada)에 의해 확립된 제도로써, 현재는 2001년 5월에 개정된 FIPS 140-2에 근간을 두고 있다[10]. FIPS 140-2는 암호모듈의 안전성 평가를 위한 보안요구사항을 4가지 평가등급에 따라 11개 영역으로 분류하고 있으며, 암호모듈의 핵심기능인 암호 알고리즘 등을 포함하여 물리적인 보안까지 광범위하게 다루고 있다. 미국의 NIST (National Institute of Standards and Technology)는 민간 기업이 개발한 암호제품을 미연방 정부기관의 안전한 사용을 위해 FIPS 표준을 제정하였으며, 현재 FIPS 140-2를 적용하고 있다. 또한 NIST는 FIPS 140-2의 원활한 평가를 위해 암호모듈의 개발자 및 평가자를 위한 문서를 제공하고 있다. 해당 문서는 현재 암호검증기준(ISO/IEC 19790)과 암호시험기준(ISO/IEC 24759)으로 표준화되어 있다. 하지만, 암호모듈은 국가마다 정책이 상이하고, 국가의 중요 기밀 정보 취급과 관련이 있으므로, CC 평가 인증과 달리 국가 간에 검증 결과가 상호인정되지 않는다는 차이점이 있다[11].

암호모듈의 실제 평가는 NIST의 NVLAP (National Voluntary Laboratory Accreditation Program)에 의해 인정된 신뢰할 수 있는 제 3의 기관인 CST (Cryptographic and Security Testing) 실험실에 의해 수행된



〔그림 2〕 CMVP 평가인증 절차

다. 현재 CST 실험실은 미국에 11개, 캐나다, 일본에 각각 2개씩, 독일, 대만, 스페인에 각각 1개씩으로 18개가 지정되어 있다. CST 실험실에서 작성된 결과보고서를 바탕으로 NIST는 평가받은 암호모듈에 대한 인증서를 발행하고, 인증된 제품은 암호모듈 검증리스트(Validation List)에 공개하고 있다[12].

CMVP에서는 암호모듈의 분석 수준을 4가지 평가등급으로 분류하고 있으며, 전체 요구사항을 11개의 영역으로 구분하여 4가지 평가등급에 따른 요구사항을 분류하여 정의하고 있다. CMVP에서는 암호모듈에 대한 시험을 위해 신청인이 제출한 문서와 구현물(소스코드 또는 회로도)를 분석하고, ISO/IEC 24759에 명세된 암호모듈 적합성 시험을 수행한다. 시험 항목에는 물리적 시험, EMI/EMC(전자파 장해 및 전자파 적합성) 시험, 부채널 공격 시험, 운영 시험, 암호 알고리즘 및 난수생성기 시험 등이 포함된다. CMVP 평가인증 절차는 예비검증단계, 검증시험단계, 검증유지단계로 구분되며, [그림 2]와 같다.

3.3 ISCCC (IT Security China Compulsory Certification)

ISCCC는 중국에서 IT 분야의 응용범위가 확대되면서 정보보호에 대한 문제점이 대두됨에 따라, 국가/공공의 정보보호를 위해 IT제품의 보안성 및 신뢰성을 평가·인증하기 위해 도입된 중국의 평가·인증 제도이다. 이 제도는 평가 과정에서 소스코드의 공개를 요구하고 있어, 제조사의 핵심기술이 유출될 수 있다는 지적을 받고 있다. 하지만, 향후 휴대폰, PC, 노트북 등으로 인증 범위가 광범위하게 확대될 수 있어 중국 수출을 목표로 하는 기업에서는 심각하게 받아들이고 있다[13]. 따라서, ISCCC는 중국 자국의 컴퓨터와 정보기술 산업을 발전시키고, 중국 기업을 보호하기 위한 보호 무역 조치로 판단되고 있다. 이러한 이유로 ISCCC는 도입 초기부터 많은 어려움을 겪어왔는데, 도입 경과는 다음과 같다.

- '07.8월: '09.5월부터 ISCCC 제도 도입계획을 WTO에 통보
- '08.3월: ISCCC 제도 시행에 대한 공고문을 발표함
- '08.11월, '09.3월 : WTO/TBT (WTO Technical Barriers to Trade)위원회에서 미/일 등과 공조하여 이의 제기. 국제상호인정체제인 CCRA에 중국의 가입을 요구함
- '09.4월: '10.5월로 1년 연기하고 적용대상을 정부조달로 축소함. 국영기업(학교 및 병원 등)은 대상에서 제외함
- '10.4월 : 일본 경산성은 중국국가인증감독위원회(CNCA, China National Candy Association)를 방문하여 소스코드 공개의 문제점을 논의하고, CCRA 가입을 권유함
- '10.5월: 한국반도체산업협회는 반도체협의회(한·중·일·대만·미국·EU의 6개 회원국 모임)를 통해 EU와 공조하여 중국 측에 우려를 전달함

ISCCC는 중국에서 기존에 실시되던 CCC(China Compulsory Certificate) 제도를 IT 시스템에 적용한 것이다. CCC 인증은 "중국강제인증"으로 통칭되는 규격으로써, 중국 내에 유통되는 모든 상품에 대해 IEC (국제전기 표준 협회) 및 중국 국가 표준에 준하여 안전인증과 품질인증을 받도록 한 제도이다[14].

CCC를 취득하기 위해서는 중국인증기관에 신청서, 기술문서와 시험제품을 제출하고 중국 내 시험기관에서

안전·품질검사를 실시하며, 이 과정을 통과하면 공장을 방문 평가 후 적합하다고 인정될 경우 인증서가 발급된다.

CCC 평가인증 절차는 신청 및 접수, 샘플형식시험, 공장심사, 심사결과 평가 및 승인, 사후검사로 구성되며, 다음과 같다[13,14].

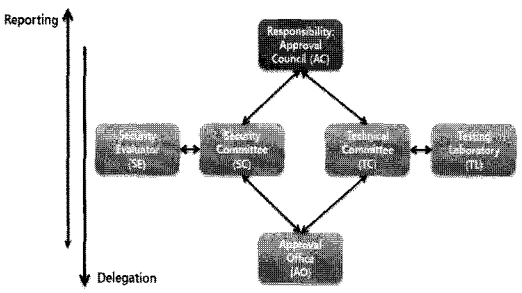
- 신청 및 접수: 신청인은 기술자료 및 샘플을 시험기관에 제출하고 인증을 신청한다.
- 샘플형식시험: 신청인은 중국 시험기관의 요구에 따라 샘플을 발송해야 하며, 각 제품별로 사전에 정의되어 있는 규격에 따라 시험이 진행된다.
- 공장심사: 공장품질보증시스템(공장품질보증능력 평가) 검사와 상품의 일관성 확인(명판, 상품구조의 일관성, 중요부품 확인)을 수행한다.
- 심사결과 평가 및 승인: 샘플테스트, 공장심사에 대한 결과 평가를 바탕으로 인증서를 발행하고, CCC 마크 사용을 승인한다.
- 사후검사: CCC에서는 공장심사, 샘플링 검사 등을 수시로 실시하여, 사후 관리를 실시한다.

CCC 제도에서 사후심사는 제조공장의 품질보증능력에 대한 재평가 및 인증제품의 일치성을 심사내용으로 인증증서를 발급 받은 날부터 7개월 후에 1차 사후심사를 실시하고, 그 이후로는 12개월마다 정기 검사를 진행한다. 하지만, 필요에 따라 심사기관이 샘플링 시험을 의뢰할 수도 있다. 제조자의 품질보증능력에 대한 재평가의 실시는 필수사항과 선택사항으로 나누어 실시하고 적어도 4년 안에 한 번씩 모든 항목에 대해 재평가를 실시한다. 재평가시 발생한 요건 불일치 항목에 대해서는 3개월 내에 보정조치를 취해야 하며, 조치가 이행되지 않았을 경우에는 인증증서를 취소하고, CCC 인증마크 사용을 중지시키며 이를 대외에 공개한다.

3.4 ZKA(Zentraler Kreditausschuss)

ZKA 인증은 독일중앙신용위원회에서 독일 시장에 대한 전자지불스킴들의 적합성 여부를 판정하기 위해 개발한 평가인증 제도이다[15]. ZKA 인증에서는 전자지불스킴에 대한 평가를 기능성 평가 시험과 보안성 평가 시험으로 나누어 실시한다.

ZKA 인증 체계의 구조는 [그림 3]와 같으며, 각 주체별 역할은 다음과 같다.



〔그림 3〕 ZKA 인증 체계의 구조

- Approval Council(AC): Payment scheme에 대한 최종인증기관이다.
- Security Committee(SC): 인증대상에 대한 보안정책 및 요구사항을 관리하는 위원회로써, 보안성 평가보고서를 검토하며, AC를 지원한다. 이때, 평가내용은 외부로 공개하지 않는다.
- Security Evaluator(SE): 인증대상에 대한 보안성 평가를 수행하는 외부기관으로, 보안성평가보고서를 작성하여, AC와 SC에 제출한다. SE 수행기관은 ZKA에 의해 선정된다.
- Technical Committee(TC): 인증대상에 대한 기능성 평가 요구사항을 결정하는 위원회로써, 인증대상, 시험대상, 시험절차 등을 제안한다. 기능시험 보고서를 검토하며, AC를 지원한다.
- Testing Laboratory(TL): 인증대상에 대한 기능성 평가를 수행하는 기관으로, 기능시험보고서를 작성하여, AC와 TC에 제출한다.
- Approval Office(AO): SC 및 TC를 지원하는 사무국이다.

ZKA 인증 절차는 신청 및 등록, 기능 및 보안성 평가, 의견 작성, 최종 판결의 4단계로 구성되며, 다음과 같다.

- 신청 및 등록 단계 : 제조사가 인증을 수행하기 위한 대상 제품 및 시스템을 등록하는 단계이다.
- 기능 및 보안성 평가 단계 : 등록된 대상에 대한 기능 시험 및 보안성 평가를 수행하는 단계이다. 평가가 완료되면 추후 인증 여부 판단을 위한 보고서를 작성한다.
- 의견 작성 단계 : 이전 단계에서 작성된 보고서를 바탕으로 인증 대상에 대한 의견을 작성하는 단계이다.
- 최종 판결 단계 : 인증 대상에 대한 최종 판단을 내리는 단계이다.

3.5 TPM 관련 평가인증 제도의 비교 · 분석

이상 앞서 살펴본 CC, CMVP, ISCCC, ZKA 제도를 비교한 결과는 다음 [표 1]과 같다. 현재 TPM에 대한 평가는 CC가 유일하나, 향하 다른 평가인증 제도에서도 평가가 고려될 수 있을 것으로 판단된다.

〔표 1〕 TPM 관련 평가제도 분석 결과 비교

구분		CC	CMVP	ISCCC	ZKA
평가대상		보안기능이 구현된 IT 제품	암호모듈	IT 제품	전자지불스킴
평가등급		존재 (EAL1-7)	존재 (Leval 1-4)	존재하지 않음	존재하지 않음
평가 주체	신청기관	보안기능이 구현된 IT 제품의 개발업체	암호모듈 개발업체	IT제품 개발업체	전자지불 관련 개발업체
	평가기관	평가기관	CST 실험실	중국 시험기관	Security Evaluator(SE) Testing Laboratory(TL)
	인증기관	각국의 인증기관 (IT보안인증사무국)	미국의 NIST, 캐나다의 CSEC	중국국가인증감독위원회	Approval Council(AC)
평가절차		평가신청준비 단계 → 평가계약 단계 → 평가 · 인증 단계 → 인증효력유지 단계	예비검증단계 → 검증시험단계 → 검증유지단계	신청및 접수 → 샘플형식시험 → 공장 심사 → 결과평가 및 승인 → 사후관리	신청 및 등록단계 → 가능 및 보안성 평가단계 → 의견작성단계 → 최종판결단계
유효기간		없음	5년	수서 정기적인 사후검사(4년)	없음
장점		CCRA 가입국들 간 평가결과를 인정	암호 모듈의 알고리즘 및 물리적 보안까지 평가	중국 시장 진출을 위한 강제인증제도로 중국 내 시장 보호	기능 시험과 보안성 평가를 별로로 시험하여, 실제 금융 시장에서의 적합성 여부를 평가
단점		암호모듈에 대한 세부적인 평가 방법이 존재하지 않아, 평가자의 시험방법에 의존함	전체 시스템에 대한 평가는 하지 않음	소스코드 제출로 제조사의 핵심 기술이 유출될 수 있음	독일 시장 진입을 위한 제도임
제출물		보안목표명세서 준비절차서 기능명세서 사용자운영설명서 형상관리문서 보안구조서 TOE 설계서 배포문서 시험서 개발보안문서 생명주기정의문서 검증명세서 개발도구문서 취약성분석서 평가대상제품	기본및상세설계서 형성관리문서 제품사용설명서 시험절차및결과서 취약성분석및대응방법기술문서 평가대상제품	중문사용설명서 서비스 매뉴얼 조립도 회로도 중요안전부품리스트 평가대상제품	-
TPM 관련 평가기준		PC Client Specific Trusted Platform Module Family 1.2; Level 2 (EAL 4+)	없음	없음	없음
TPM 관련 기평가제품		Infineon Technologies AG SLB9635TT1.2/m1566a13 (EAL 4+)	없음	없음	없음

Ⅳ. 결 론

스마트 그리드에서 스마트미터를 통해 수집되는 데이터들은 사용자와 에너지 공급업자 및 관련 업체에게 제공되어 에너지에 대한 효율적인 관리 및 다양한 서비스를 가능하게 한다. 하지만, 에너지 공급업체 및 관련 업체는 스마트미터에 접근해 전력 소비량과 관련된 데이터를 조작하거나 유출하여 프라이버시 침해 문제를 일으킬 수 있으며, 악의적인 공격자는 물리적으로 스마트미터에 접근하여 마이크로컨트롤러와 펌웨어를 조작하여 데이터 유출 및 악성코드를 감염시킬 수 있다. 만약 스마트미터에 대하여 불법적인 조작 및 공격이 가능해 진다면, 서비스 거부 공격의 원인이 되어 대규모 에너지 공급 중단이 초래될 수도 있다. 이를 방지하기 위해서는 변조 방지, 기밀성, 무결성, 가용성, 부인방지, 인증의 서비스를 제공하는 TPM을 도입하는 것이 대안이다.

TPM은 스마트미터에 적용되어 스마트미터에 저장된 데이터에 대한 임의 삽입, 변경, 삭제를 방지할 수 있으며, 스마트미터 플랫폼 자체의 무결성을 제공할 있다. 따라서 TPM에 대한 신뢰성 및 안전성 확보가 중요하다. 이에 본 논문에서는 TPM과 관련된 평가인증 제도를 비교·분석하였다.

참 고 문 헌

[1] 정영곤, 최현우, 염홍열, "스마트 그리드 보안 동향", *정보보호학회학회지* 제20권 제4호, pp66-79, 2010년 8월.

[2] 이상준, "차세대 전력 인프라를 위한 보안솔루션", 유넷시스템, 2009년 11월.

[3] 장두석, "스마트그리드 산업의 동향 및 산업화 방안", 산은경제연구소, 2010년 1월.

[4] 김영수, 박영수, 박지만, 김무섭, 김영세, 주홍일, 김명은, 김학두, 최수길, 전성익, "신뢰 컴퓨팅과 TCG 동향", 전자통신연구원, *전자통신동향 분석*, 22권 1호, 2007년 2월.

[5] 박정숙, 조태남, 한진희, 전성익, "Trusted Computing 기술 및 TCG 표준화 동향", 전자통신연구원, *전자통신동향 분석*, 23권 4호, pp.48-60 2008년 8월.

[6] ISO/IEC 15408-1, "Information technology – Security techniques – Evaluation criteria for IT security – Part 1:Introduction and general model"

[7] ISO/IEC 15408-2, "Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements"

[8] ISO/IEC 15408-3, "Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements"

[9] 국가정보원 2009. 3. 20 정보보호제품 평가·인증 수행규정

[10] NIST, "FIPS 140-2: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES", May 2001.

[11] 국내·외 암호모듈 검증정책, IT보안인증사무국

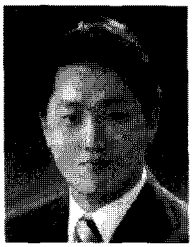
[12] NIST CMVP, http://csrc.nist.gov/groups

[13] China Information Security Certification Center, http://www.isccc.gov.cn

[14] CCCKorea, http://www.ccckorea.com

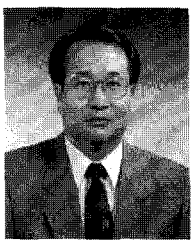
[15] ZKA Approved Scheme V1.2 "http://www.zka-online.de/"

〈著者紹介〉



이 광 우 (Kwangwoo Lee)
학생회원

2005년 성균관대학교 정보통신공학부 졸업(학사)
2007년 성균관대학교 대학원 컴퓨터공학과 졸업(공학석사)
2009년 성균관대학교 대학원 전자전기컴퓨터공학과 박사수료
관심분야 : 암호이론, 정보보호제품 보안성 평가, 전자투표, 디지털 복합기 보안



원 동 호 (Dongho Won)
종신회원

1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1992년~1994년 성균관대학교 전자계산소 소장
1995년~1997년 성균관대학교 교학처장
1997년~1998년 정보화추진위원회 자문위원 (발령 정보화추진위원회 위원장 국무총리)
1999년~2001년 성균관대학교 정보통신대학원 원장
2002년~2003년 한국정보보호학회 회장
2002년~2004년 대검찰청 컴퓨터 범죄 수사 자문위원
2002년~2004년 성균관대학교 연구처장
2002년~2003년 감사원 IT 감사 자문위원
2002년~2004년 산학연 정보보안협의회 회장
2005년~현재 정보보호인증기술연구소 소장
2005년~2008년 한국정보보호진흥원 이사
2009년~현재 성균관대학교 BK21 사업단장
관심분야 : 암호이론, 정보이론, 정보보호

김 승 주 (Seungjoo Kim)
종신회원

1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년: 한국정보보호진흥원 팀장
2004년~현재: 성균관대학교 정보통신공학부 교수
2001년~현재: 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년~현재: 교육인적자원부 유해정보차단 자문위원, 디지털 콘텐츠유통협의체 보호기술워킹그룹 그룹장
2007년~현재: 대검찰청 디지털수사 자문위원, KISA VoIP 보안기술 자문위원, 기술보증기금 외부 자문위원, 전자정부 서비스보안위원회 사이버침해사고대응 실무위원회 위원
관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET