情 報 保 護 學 會 誌
第 14 券 第 1 號, 2004. 2

HSM 제품 동향 및 안전성 분석

김 지 연*, 권 현 조*, 전 길 수*, 임 선 간*, 이 재 일*

요 약

인터넷 뱅킹, 전자상거래 등 다양한 분야에서 암호기술의 사용이 증가되면서, 고비도·고성능의 암호장비에 대한 수요도 증가하고 있다. 본 논문에서는 인증기관을 중심으로 이러한 고비도·고성능의 암호장비로 관심이 고조되고 있는 상용 HSM(Hardware Security Module) 장치의 특징 및 안전성에 대해 살펴본다. 본 논문이 국내 HSM의 올바른 선택과 사용에 유용한 자료로 활용될 수 있을 것으로 기대한다.

Ⅰ. 서 론

암호기술이 인터넷 사회 전반에 걸쳐 적용되면서 암호기술을 기반으로 하는 인터넷 서비스의 안전성을 제고하기 위해 고도의 보안기능을 갖춘, 고도의 성능을 갖춘 암호장비에 대한 수요도 증가하고 있다. HSM 장치도 이러한 암호장비중에 하나로서 인증서비스를 제공하는 인증기관을 중심으로 HSM 장치에 대한 관심이 고조되고 있다.

HSM 장치란, CA 서버의 키, SSL 서버의 키 또는 OCSP 서버의 키 등 중요한 암호키의 관리를 위한 전용 하드웨어 장비로, 키 노출의 위협에 대처할 수 있는 안전한 키 저장소를 제공한다. HSM은 서버의 운영체제와는 독립적으로 동작하여 키를 저장·관리하며, 암호연산을 독립적으로 수행한다. HSM 장비는 하드웨어 기반의 암호연산(예를 들어, 난수 생성, 키 생성, 전자서명, 키 저장 및 복구 등) 기능들을 제공하며, 비대칭형 암호연산에 사용되는 개인 키에 대한 물리적 보안을 제공한다. 이들 대부분의 상용 제품들은 FIPS 140-1의 2등급/3등급의 안전성을 검증받은 제품들이다. HSM 장치는 "Tamper-evidence/Tamper-resistance" 성질로 인한 보안성 향상 및 자체 프로세서 이용으로 인한 성능향상의 목적으로 사용하며, 일반적으로 인증기관의 키 생성기 및 키 저장소, 인증서버 보조 장치로써의 전자서명 검증기, SSL 가속기, 민감한 정보의 안전한 저장소, 데이터베이스에 저장된 데이터에 대한 무결성 검증기 및 스마트카드의 키 생성기로써 활용하고 있다.

인증기관은 신뢰성 있는 인증서비스 제공을 위해 보안취약성으로 인한 위험을 최소화하는 여러 가지 수단을 강구하고 있다. 특히, 인증서 발급시 사용하는 인증기관의 전자서명생성키(루트키) 노출은 인증기관의 신뢰성에 큰 타격을 미치게 됨으로 루트키 보호 수단으로 스마트 카드를 이용하여 왔다. 하지만 스마트카드에 대한 공격기법의 발달로 루트키의 노출 위험이 증가함에 따라 보다 안전한 키저장 매체인 HSM 장치로 대체하는 추세이다.

또한 국내의 경우 인터넷 뱅킹, 온라인 증권거래 등 인증서 활용분야가 다양해지고 인증서의 수요가 증가함에 따라, 인증서 발급 신청이 집중되고 이로 인해 인증서버 다운으로 인한 발급 지연 등 사고가 일어날 가능성이 존재할 수 있다. 실제로 온라인 증권거래시 사용할 인증서 발급 신청자가 급증하여 약 15분간 공인인증서 발급이 중단되는 사태가 발생하기도 하였다. PKI 관련 암호연산 수행시 서버의 중앙처리장치를 90% 이상 점유해야 하기 때문에 인증서 발급과정에서 생기는 인증서버의 암호연산 수행으로 인해 인증서 발급 지연 현상이 발생하게 된다. 따라서 인증기관들은 작년부터 이러한 인증서 발급신청이 집중될 경우 인증서버의 다운, 속도 저하 등의 문제를 해결하는 방안으로 자체 암호연산 수행기능을 갖춘 HSM 장치를 채택하고 있다.

* 한국정보보호진흥원({jykim, hckwon, kschun, seongan, jilee}@kisa.or.kr)

국내의 경우 증권사의 공인인증서 도입 의무화, 공인인증서를 이용한 인터넷 뱅킹 사용자 증가 등의 이유로 금융권 전반의 보안과 속도 개선에 대한 요구가 커지고 있는 실정이다. 현재 전자서명인증관리센터를 비롯한 행정자치부, 한국증권전산, 한국정보인증, 외환은행, 조흥은행, BC카드, 제일은행 등 공인인증기관과 금융권 중심으로 HSM 수요가 증가하는 추세이다. 영국 nCipher社 HSM 장치의 국내 총판인 한국전자증명원과 캐나다 Chrysalis-ITS社와 협력사 관계를 맺은 비씨큐어, 드림시큐리티, 핌스텍 등이 국내 HSM 장치 시장을 주도하고 있다. 국내에 공급된 HSM 장치는 거의 외산제품이며 국내시장의 요구에 따라 이들 HSM 장치에는 SEED 및 KCDSA를 탑재하거나 탑재를 계획하고 있다.

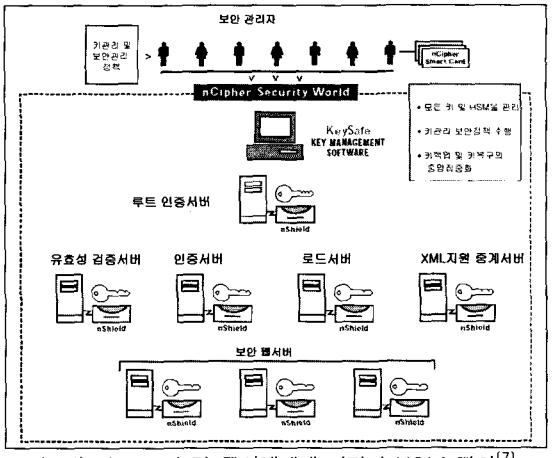
국외의 경우 영국 nCipher社와 캐나다 Chrysalisa-ITS社가 HSM 시장을 선점하고 있다. IDC에 따르면 Chrysalisa-ITS社의 HSM 제품이 전체 시장의 36%를 차지하고 있으며 연평균성장률(CAGR) 33%로 2005년에는 112백만 달러에 이를 것으로 전망하고 있다. 또한 nCipher社의 HSM 제품은 전체 시장의 38%를 차지하고 있으며 2005년에는 116백만 달러에 이를 것으로 전망하고 있다. 이 두 개 회사의 제품이 VeriSign社, Entrust社, Baltimore社 등 세계 PKI 주요 업체의 제품에 탑재되어 전 세계적으로 공급되어 있다. 국외에서는 인증기관의 키보관 장치로서 HSM 장치를 사용할 뿐만 아니라 전자지불의 주요 키 보호, SSL용 개인키 보호, 가입자/클라이언트 키 생성 등 다양한 용도로 개발된 HSM 장치를 사용하고 있어 HSM 장치의 시장 규모는 더욱 성장할 것으로 예측된다.

본 논문에서는 세계 시장 점유율이 높은 Chrysalis-ITS社와 nCipher社의 HSM 제품을 중심으로 HSM 제품 동향 및 안전성을 분석하고자 한다.

II. PKI에서의 HSM의 활용

본 절에서는 PKI에서 HSM 장비가 어떻게 활용되고 있는지를 살펴보도록 한다. PKI 각각의 구성객체에 연결된 HSM의 주요 역할은 다음과 같다.

- 인증서버 : 루트 인증서버는 인증서 발급시 인증서에 대한 전자서명을 생성하기 위한 루트키를 가지고 있어 이를 보호하기 위하여 HSM장치를 활용한다. 또한 비밀분산기법을 이용하여 루트키를 보호하고 있기 때문에 전자서명생성시 루트키를 재구성하기 위해서는 여러 관리자가 스마트카드를 제시하도록 구성함으로써 루트키 접근에 대한 권한을 분산시킨다.
- 인증서유효성 검증서버 : OCSP(Online Certificate Status Protocol)를 지원하는 실시간 검증서버는 PKI기반의 응용서비스 이용시 인증서 유효성 확인 요청이 있을 경우 해당 인증서의 현재 상태를 확인한다. 검증서버에 연결된 HSM 장치는 검증과정에 필요한 모든 키를 관리 및 보호하며, 전용 암호프로세서를 가지고 있어 SSL연산 및 전자서명 연산 속도를 가속화시킴으로써 검증시 병목현상을 제거한다.



〔그림 1〕 PKI의 각 구성객체에 연결된 HSM 장치[7]

PKI가 활성화됨에 따라 인증서비스 및 관련 통신량이 증가하고 있어 처리속도의 향상이 요구되고 있다. HSM은 PKI 보안의 핵심인 루트 키에 대한 보호기능을 제공하기도 하지만, PKI 서비스 제공시 처리속도를 가속화시키는 역할도 한다. 전자서명 수행시 서버의 도움 없이 HSM 장치의 전용 암호프로세서에서 수행하기 때문에 인증서버는 HSM 장치가 전자서명을 수행할 동안 디렉토리 또는 데이터베이스 와 같은 정보자원을 이용하여야 하는 이용자의 요청에 대해 더 많이 응답할 수 있어 인증서비스에 대한 속도를 증가시킬 수 있다.

III. HSM 제품 동향

본 절에서는 세계 시장 점유율이 높은 Chrysalis-ITS社와 nCipher社의 HSM 제품 및 Rainbow社

의 CryptoSwift HSM와 SPYRUS社의 LYNKS Privacy Card HSM 제품 동향을 살펴보도록 한다.

1. Chrysalis-ITS社의 HSM 제품

1.1 Chrysalis-ITS사 HSM 제품별 특징

Chrysalis-ITS사의 HSM 제품은 용도나 형태에 따라 크게 4가지로 분류된다.

1.1.1 Luna CA^3

Luna CA^{3}는 PC 카드형태의 PKI 관련 키 전용 하드웨어 암호토큰인 HSM 장치이다. PKI 시스템의 핵심인 키에 대한 성능 및 보호를 최대 수준으로 제공해준다. Luna CA^3 HSM은 키의 생명주기(키 생성, 저장, 사용, 파기)내내 HSM내에서만 사용하도록 유지 관리한다. 또한 관리자 및 사용자에 의한 비인가된 접근을 방지하기 위하여 Luna CA^{3}는 SAAC(Secure Access and Authentication Control)이라 하는 인증방법을 제공한다. Luna PED 인증장비를 추가함으로써 SAAC 기능을 제공할 수 있으며, 이를 통해 2-factor 인증, 안전한 경로를 이용한 인증, 역할 분리에 따른 접근통제 등이 가능해진다. Luna CA^{3}는 기존 PKI 시스템에 쉽게 통합될 수 있도록 PKCS#11, MS CAPI, Java JCA 및 Open SSL CAPI 등 다양한 암호라이브러리를 지원하고 있다.

Luna CA^{3}는 FIPS 140-1 3등급의 안전성을 검증받았으며, 현재 세계 주요 PKI 서비스 업체인 VerSign 社, Entrust社, MS社, RSA社, Baltimore社 등이 Luna CA^{3}를 사용하고 있으며, PKI 서비스를 이용하고 있는 상위 500개 회사들 중 84%가 Luna CA^{3}를 사용하고 있다.

1.1.2 Luna XPplus

Luna XPplus는 e-Business에서의 전자거래시 이용되는 전자서명 처리 성능을 높여주는 HSM 장치로, Luna CA^3 루트키 관리 시스템에 연결되어 동작한다. 전자서명 생성 외에 원격지 인증, 전자거래 조정, 전자서명 검증, OCSP 응답 등 부가기능을 수행함으로써 Luna CA^3 루트키 관리 시스템의 부하를 줄일 수 있다. Luna XPplus는 RSA 1024비트 키를 기준으로 초당 500개의 전자서명을 생성하며, 하나의 PCI controller 카드에 데이지 체인방식으로 여러 대의 Luna XPplus를 연결할 수 있어 시스템 확장이 용이하다.

1.1.3 Luna RA

Luna RA은 PC카드 형태로 안전한 키 발급 기능을 제공하는 HSM 장치이다. 전자 인증서를 기반으로 하는 기반구조에서 최종 통신 당사자가 신뢰를 갖도록 하는데 있어, 키를 안전하게 발급하는 것은 매우 중요한 일이다. Luna RA는 가입자의 인증서의 공개키에 대응되는 개인키를 안전하게 생성한다. 원격지 관리시스템 또는 스마트 카드 관리시스템에 장착된 HSM은 FIPS 140-1 3등급으로 안전성을 검증 받은 난수생성기를 이용하여 가입자의 개인키를 생성하고, 스마트 카드 관리시스템이 생성된 개인키를 담은 스마트 카드를 발급하면, 생성된 개인키는 HSM내에서 삭제한다. 또한 PKI의 구성요소는 등록시스템을 통해 키 생성 및 삭제에 대한 감사가 가능하다. 스마트 카드내에서 키쌍을 생성하는 것이 가능하지만, 많은 가입자에게 일일이 키쌍 생성이 가능한 스마트카드를 발급하는 것은 비용효과 면에서 효율적이지 않다. Luna RA를 이용하면 인증서 발급과정을 더 빠르고 안전하게 수행할 수 있어, 비용 효과면에서 효율적으로 인증시스템을 운영할 수 있다. 일단 가입자의 카드발급이 순서적으로 완료되면 HSM은 카드에 입력시켰던 개인키의 복사본을 안전하게 파기한다. 결과적으로 Luna RA는 인증서발급과정에서 없어서는 안될 중요한 구성요소이다.

1.1.4 Luna 2

Luna 2는 PCMCIA 카드 형태로 전자서명 및 암호 기능을 갖는 토큰인 HSM 장치이다. Luna 2는 하드웨어 기반의 키관리 및 저장에 대한 무결성을 요구하는 응용분야에 적합하도록 키생성, 전자서명 생성 및 검증, 암호화 기능 등을 제공한다. Luna 2는 소형 PCMCIA 카드 형태이기 때문에 휴대 가능하고 가격도 저렴하기 때문에 응용서비스를 이용하는 클라이언트에서 사용하기에 적합하다.

1.2 Luna CA^{3}의 특징

본 절에서는 Chrysalis-ITS社의 대표적인 HSM 제품인 Luna CA^{3}의 안전성 측면에서의 특징을 살펴보도록 한다. Luna CA^3 루트키 관리 시스템(root key management system)은 Luna Dock 토큰 리더기, Luna CA^3 안전한 암호토큰, PED키, Luna PED 인증 장치 등으로 구성된다.

1.2.1 FIPS 140-1 안전성 검증

NIST가 개발한 FIPS 140-1 표준은 암호모듈의

물리적 보안 및 운영 보안을 위한 기준 요구사항을 집합한 것이다. NIST는 응용환경별 보안수준에 따라 암호모듈을 다양한 환경에 적용할 수 있도록, FIPS 140-1의 보안등급을 4개의 등급으로 구성하였다. 1등급이 제일 하위등급이고, 4등급이 최상위 등급이다. HSM 내에 있는 개인키를 보호(tamper-resistance, 물리적 보안, 데이터 무결성, 접근통제 등)할 때 요구되는 물리적 보안수준을 HSM 장비가 갖추고 있음을 FIPS 140-1의 검증을 통해 확인한다.

Chrysalis-ITS Luna CA^{3}는 보안환경에서 동작하는 조건에서 FIPS 140-1 보안등급 3을 받았다. 또한 CC 평가와 FIPS 140-2 검증을 받기 위해 준비중이다.

1.2.2 하드웨어 기반의 안전한 키 생성

Chrysalis-ITS Luna CA^{3}는 개인키 뿐만 아니라 모든 키를 하드웨어 기반의 안전한 암호토큰 내에서 생성한다. 또한 난수성을 갖는 씨드(seed) 값을 생성하기 위한 난수생성기가 Luna CA내에 장착되어 있어, Chrysalis-ITS Luna CA^{3}는 키생성 절차에 대한 부가적인 보호조치를 제공하고 있다. 여기에 장착된 난수생성기는 ANSI 9.17 및 9.82의 부록 C를 따르도록 설계된 것이다.

1.2.3 하드웨어 기반의 안전한 키 저장

Chrysalis-ITS Luna CA^{3}는 FIPS 140-1 3등급의 안전도를 가진 암호 하드웨어 토큰내에 개인키를 저장하며, 개인키의 불법복제, 훼손 또는 삭제의 위협에 대처하기 위하여 개인키 관련 정보(private key material)를 하드디스크에 저장하거나 서버의 메모리에 절대로 전송하지 않는다.

1.2.4 하드웨어 기반의 안전한 키 백업

Chrysalis-ITS Luna CA^{3}는 자사의 Luna DOCK PC 카드리더기 범위 내에서 개인키 백업과정("Luna Key Cloning")을 수행한다. Luna DOCK은 PC 카드형태의 암호토큰에 2개의 슬롯을 가지고 있어 개인키 저장장비로부터 루트 키를 안전하게 백업할 수 있도록 한다. Luna DOCK는 HSM 장비 밖으로 개인키를 노출시키지 않은 채 안전한 경로를 통해 개인키를 복제할 수 있도록 해준다. 여기서 안전한 경로란 FIPS 140-1 3등급의 안전성을 가진 암호토큰과 같은 등급의 안전성을 가진 또 다른 암호토큰사이의 경로를 말한다.

1.2.5 하드웨어 기반의 안전한 전자서명 수행

Chrysalis-ITS Luna CA^{3}는 암호연산에 이용되는 개인키에 대한 무결성 보호를 보장할 수 있도록 안전한 하드웨어 토큰 내에서 모든 암호연산이 이루어지도록 한다. 또한 Chrysalis-ITS Luna CA^3 하드웨어 암호토큰은 전용 암호연산 프로세서를 이용하여 서명에 대한 성능을 증가시킨다.

1.2.6 PKI 기반의 인증서비스 관련 소프트웨어 업데이트

Chrysalis-ITS사는 Luna CA^3 암호토큰에 설치될 소프트웨어의 제조, 프로그래밍, 및 유지보수를 하는데 있어 엄격한 통제를 한다. 또한 Chrysalis-ITS사는 하드웨어에 탑재되는 알고리즘에 대한 tampering 공격을 방지할 수 있도록 "변경 불가능한 안티 퓨즈 프로세스(irreversible anti-fuse process)"를 이용하여 하드웨어 컴포넌트들을 프로그램한다. Chrysalis-ITS사는 펌웨어를 토큰에 로드하고 로드한 펌웨어에 대한 무결성 훼손여부를 검사할 경우 펌웨어 암호전용 프로세스를 이용한다. 일단 프로그램되면, 부팅시 마다 펌웨어 이미지 원본으로부터 계산된 CRC(cyclic redundancy code)를 이용하여 펌웨어의 무결성 보존 여부를 확인하다. 하드웨어 설계, 소프트웨어 개발, 컴포넌트의 어셈블리 및 선적의 모든 과정은 보안용 모니터를 통해 철저하게 감시되고 있다. 제조이후에 펌웨어를 업데이트하는 경우, 업데이트된 펌웨어의 이미지를 랜덤하게 생성한 키로 암호화한 한다. 이 키는 해당 제품 고객의 허가코드로부터 파생된 키를 이용하여 보호한다. 보호된 키 정보는 암호관련 헤더에 포함되며, Chrysalis-ITS의 마스터 개인키를 이용하여 서명한 후, 업데이트된 펌웨어 이미지 파일에 첨부된다. 헤더에 있는 서명 값에 대한 검증이 성공한 경우에만 암호화된 이미지 파일이 복호화 된다. 펌웨어를 토큰에 업데이트하는 과정은 업데이트된 이미지가 토큰에서 수행되기 이전에 완전하고 정확하게 토큰으로 옮겨졌음을 보증하는 과정이다.

1.2.7 물리적 보안

Chrysalis-ITS Luna CA^{3}는 FIPS 140-1의 3등급의 안전성을 검증 받았으며, "intrusion resistance" 및 "tamper evidence" 부분에 대해서는 FIPS 140-1의 4등급의 안전성 검증을 받은 HSM 장비이다. 이 장비는 전원공급장치를 독립적으로 갖추고 있으며 안전한 마운팅 기능(mounting capabilities)을 갖춘 것이 특징이다. 선택사항인 Luna Lock은 HSM에서

토큰을 불법적으로 제거하는 것을 방지하는 잠금 메커니즘을 제공해줌으로써 Luna DOCK 토큰 리더기의 물리적 보안을 보완해 준다.

1.2.8 호스트에 독립적으로 동작, 2-factor 인증 제공

로그인 및 인증 절차는 호스트 서버와는 독립적으로 수행된다. 이때 HSM와 호스트 서버와의 안전한 연결 경로를 통해 2-factor 인증을 수행한다. 개인키에 대한 접근통제의 훼손을 방지하기 위해서, Chrysalis-ITS 사는 호스트서버가 개인키 연산에 알맞은 접근통제 및 인증 연산을 수행하지 않도록 권고하고 있다. 호스트에서 접근통제 및 인증 기능을 수행하도록 하는 경우 공격자가 호스트 서버의 보안상의 문제를 악용하여 접근통제정보를 획득하게 할 수 있는 기회를 제공한다. 이러한 위협에 대처하기 위해서, Chrysalis-ITS사는 Luna PED를 제공한다. Luna PED는 호스트와 독립적으로 인증기능을 수행하는 장비이다. 2-factor 인증은 HSM에 대한 불법적인 접근을 방지하기 위한 필요한 가장 기본적인 요소이다. 2-factor 인증이란 3가지 인증형태(알고있는 것을 이용한 인증, 가지고 있는 것을 이용한 인증, 생체특징을 이용한 인증) 중 2가지의 인증형태를 취하는 것이다.

Chrysalis-ITS Luna CA^{3}에는 키패드 장치인 Luna PED를 포함되어 있다. Luna PED는 암호토큰과 직접적으로 통신함으로써 HSM에 대한 로그인 및 인증을 독립적으로 수행할 수 있도록 해준다. 통신경로로 Luna DOCK의 안전한 데이터 포트에 연결되어 있는 전용 케이블을 이용한다. 이로써 인증과정이 수행되는 동안에 Luna PED 및 Luna 토큰과의 안전한 통신경로를 제공한다.

1.2.9 운영직무 수행

한사람의 단독 행동, 비인가된 행동 등을 방지하기 위해 운영 직무를 분산하여 어느 한 사람에게 운영권한이 과도하게 가지 않도록 한다.

Chrysalis-ITS Luna CA^{3}는 직무를 5개로 구분하며, 이에 따른 인증도 서로 다른 PED 키를 이용하여 수행한다.

① grey PED key : Luna CA^{3}토큰 초기화를 위해 한번만 사용되는 키
② blue PED key : 토큰 설정 및 보안관리 작업을 위해 보안관리자가 사용하는 키
③ black PED key : 관리자 또는 운영요원 용 키
④ red PED key : Chrysalis-ITS Luna CA^3 토큰에서 다른 토큰으로 키를 백업하는데 사용하는 키
⑤ green PED key : M of N 비밀분산 기법을 이용한 접근통제를 수행하는데 사용하는 키

안전한 암호토큰에 저장되어 있는 개인키에 접근하기 위해서는 M명중 N명 이상의 키가 있어야 한다. 이는 운영요원 사이의 공모 위험을 감소시킬 수 있다. 적어도 N명 이하의 공모로 인한 루트 키 훼손은 방지할 수 있기 때문이다. 이는 Chrysalis-ITS Luna CA^{3}의 접근통제에 대한 선택사항이다. M과 N은 조직의 운영지침에 따라 시스템 설치 및 환경 설정 시에 미리 정해놓은 것이다. 예를 들어 루트 키에 대한 접근권한을 가진 관리자는 자신의 black PED 키를 이용하여 루트 키에 대한 연산을 수행하지만, 루트 키를 삭제 또는 복제하는 데 필요한 복제용 red PED 키와 초기화용 grey PED 키를 가지고 있지 않기 때문에 루트 키를 삭제하거나 복제할 수 없다.

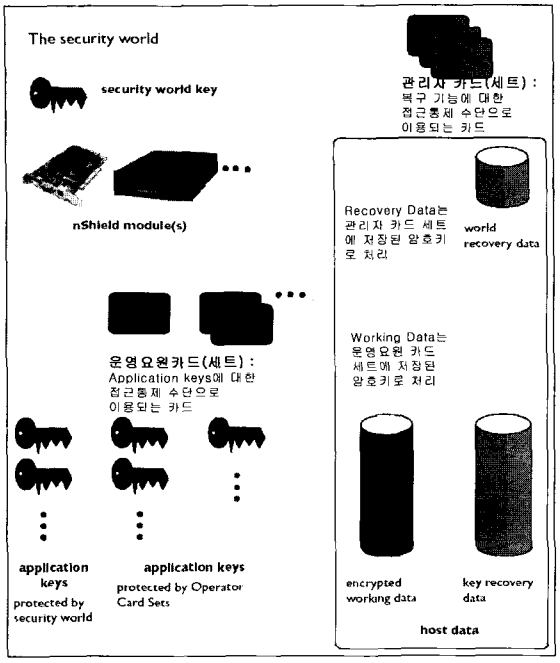
1.2.10 독립기관에 대한 감사 수행

Chrysalis-ITS 社는 고객에게 HSM 장비에 대한 무결성을 입증시키기 위해 제품 개발에 대한 외부 전문감사기관에게 감사를 의뢰한다. 최고 수준의 보안성을 제공하면서도 감사 절차를 간소화하기 위해서, Chrysalis-ITS 社의 감사업무를 위임할 가장 적합한 기관과 함께 감사에 대한 문서를 작성하고 절차를 개발한다.

2. nCipher社의 HSM 제품

2.1 nCipher사의 Security World

HSM 장치가 키를 보호하는 기능을 제공하기는 하나, 키의 생명주기동안의 통제 과정, 즉 키 관리 기능을 HSM 장치 자체만으로는 제공할 수 없다. HSM과 외부 사이를 연결해줄 수 있는 인터페이스로서의 소프트웨어가 필요하다. 또한 'HSM의 물리적 환경'과 'HSM을 연결하고 있는 컴퓨터 시스템의 논리적 환경' 및 'HSM 이용자' 사이를 연결해주는 과정을 주의 깊게 설계할 필요가 있다. nCiper사는 이러한 필요성을 충족시키기 위해 "nCipher의 Security World"라고 하는 키를 안전하게 보관하여 사용할 수 있도록 하는 기본 골격을 제시하였다.



〔그림 2〕 Security World 기본 구성요소

Security World의 특징은 다음과 같다.

- 키 생명주기의 안전한 관리 : 보안관리자가 키관리 업무를 좀더 안전하고 쉽게 수행할 수 있도록 한 단계 높은 유용성을 제공하며, 이러한 키관리 업무에는 키 생성 및 관리, 키의 백업 및 복구 업무를 포함한다.
- 다각적인 보호장치 : 물리적 보안과 논리적 보안 방법을 적절히 조화시킴으로써 더 나은 보안조치를 취할 수 있다. 물리적 보안을 위해 하드웨어 자체를 애폭시(epoxy)로 코팅하였으며 tamper-evident 성질을 가질 수 있도록 봉인하였다. 예를 들어 하드웨어에 대한 공격 발생시, 하드웨어의 내용을 클리어시킨다거나 키를 파기하도록 설계하는 것은 공격으로 인한 피해 범위를 최소화하려는 종합적인 대책의 일환이다. 하지만 이러한 물리적 보안 조치만을 취하고 논리적 보안 방법의 일환인 키 백업을 수행하지 않았다면, 물리적인 공격 발생시 파기된 키를 더 이상 복구시킬 수가 없게 된다. 이는 키를 밖으로 노출시키지는 않았을지라도 키를 잃어버린 손실과 같은 문제를 초래하게 된다. 따라서 물리적 보안뿐만 아니라 논리적 보안조치가 함께 적절히 이루어져야 한다.
- 안전한 키 저장 : 비도가 높은 암호기법 및 비밀분산 기법 등 높은 수준의 암호기술을 사용함으로써 키가 저장되어 있는 동안 매우 높은 수준의 보안강도를 제공한다. 키는 암호화되어 저장되고 있으며 HSM 영역 밖으로 나갈 때는 보호된 파일 형태("key blobs")로 내보낸다. key blobs는 키를 암호화한 상태를 해쉬하여 전자서명을 한 파일이며, 파일을 복호화하는 것은 HSM 영역 내에서만 가능하다. 예를 들어 키가 조각화되어 저장되어 있는 경우에, 보안정책 설정시에 정해진 일정 수 이상의 조각키 및 적합한 서명이 있는 신원증명서가 있어야 HSM 영역 내에서 키를 재구성할 수 있다.
- 키에 대한 접근통제 : 누가, 언제, 무엇을 하는지에 따라 상세하게 규정해 놓은 nCipher 자사의 고유 접근통제목록이 있다. 또한 주요 키에 대한 접근통제를 강화하기 위하여, 접근통제 정책에 따라 정해진 수만큼의 조각키를 접근 시 동시에 요구할 수 있도록 하였다. 이때 조각키들은 토큰내에 저장되어 있다.
- 사용하기 쉽고 사용자에게 친숙한 토큰 사용 : 관리자 및 운영요원들은 해당 직무 수행시 사용자 인증에 필요한 스마트카드 형태의 토큰을 발급 받는다.
- 비계층적 키관리 : 관리기능과 운영기능을 명확하게 분리함으로써, 지나친 접근권한을 가지는 'super-user'가 없도록 하였다.
- 모듈 키의 유일성 : nCipher社는 모듈을 초기화할 때, 하드웨어 기반의 안전한 난수 생성기를 이용하여 난수성이 좋은 키를 생성함으로써 외부에서 절대 예측할 수 없도록 하였다.
- 시스템 확장성 : 추가 모듈은 네트워크에 연결되어 다른 nShield HSM 장치들과 함께 이용될 수 있도록 하드웨어 구조를 설계하였다. 동일한 모듈 키를 이용하여 Security World내에 있는 nShield HSM 장치들의 환경 및 동작 설정이 가능하도록 함으로써, 네트워크를 통해 중앙에서 통제하면서 HSM 장치들을 이용할 수 있으며, 중앙 집중식 보안관리를 할 수도 있다.

2.2 nShield의 특징

nCipher社는 인증기관의 전자서명생성키를 안전하게 보관하고 관리할 수 있는 플랫폼으로 nShield 제품군을 판매하고 있다. nShield 제품군은 서버와의 연결을 위해 SCSI 방식과 PCI 방식을 지원한다. nShield

제품군은 일반용 HSM 제품인 nShield F2와 보안 영역 내에서 동작하는 응용프로그램도 통제함으로써 안전성을 강화시키는 SSE(Secure Execution Engine) 기술을 지원하는 일반용 nShield F3가 있다. 또한 이 두 제품에 대해 각각 속도를 향상시킨 nShield F2-UltraSign, nShield F3-UltraSign 제품으로 구성된다. 그리고 nCipher社는 HSM에 내장되어 있는 키생성 등의 키관리 기능과 사용자 사이의 인터페이스를 위해 "KeySafe"라고 하는 키관리용 GUI인 소프트웨어를 제공한다.

nShield와 KeySafe가 제공하는 특징은 다음과 같다.

- 기존 PKI와의 호환성 : 기존의 PKI에 HSM 장치를 추가함으로써 인증서 발급, 인증서 등록 및 인증서 유효성 검증 업무 등 인증서비스의 주요 기능 수행시 필요한 전자서명생성키 보호를 위한 하드웨어 기반의 안전한 환경을 제공한다.
- 키에 대한 물리적 보호 : 전자소자에 대한 물리적 공격에 대처하기 위하여 nShield 내부 전기회로를 애폭시로 포팅(potting)함으로써 tamper-resistant 기능을 제공한다.
- 안전성 검증 : nShield F2 제품군은 FIPS 140-1 및 FIPS 140-2의 보안등급 2의 안전성 검증을 받았으며, nShield F3 제품군은 FIPS 140-1 및 FIPS 140-2의 보안등급 3의 안전성 검증을 받았다.
- 안전한 키관리 프레임워크 : nCipher社의 키관리 프레임워크인 Security World는 확장성을 가지기 때문에 새로운 서비스가 개발되고 네트워크 통신량이 증가하는 대규모 그룹에서 사용할 수 있으며, 조직의 특성에 맞는 보안정책에 따른 키관리가 가능한 유연한 구조를 가진다.
- 키관리의 효율성 : 키관리용 소프트웨어인 "KeySafe"를 이용하여 PKI의 구성객체에 연결된 각각의 HSM을 중앙에서 관리할 수 있도록 함으로써 키관리 및 인증업무의 효율성을 증가시킨다.
- 스마트카드를 이용한 키에 대한 접근통제 : 스마트카드를 이용하여 보안정책에 대한 권한을 국부적으로 수행하도록 한다. 즉, 관리권한의 위임 및 할당으로 독점적 권한을 지닌 "super user"가 없게 함으로써 권한남용으로 인한 위험을 최소화한다.
- 키 관련 연산속도의 향상 : 전자서명생성속도를 향상시킨다(SSE를 지원하는 UltraSign nShield의 경우 초당 400번의 서명생성을 수행).
- 장애허용성 : nShield 고장시 연결되어 있는 다음 nShield가 동작하여 고장난 nShield의 업무를 대행하도록 설계할 수 있다.
- 원격지 관리기능 지원 : nShield는 원격지 네트워크 관리 콘솔에서 HSM에 대한 상태정보 및 시간당 처리 속도 통계치 등 정보를 검색할 수 있도록 SNMP(Simple Network Management Protocol)을 지원한다.

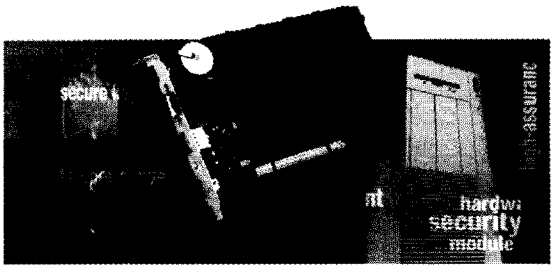
이 외에도 nCipher社는 SSL 가속기 HSM 장비로 nFast 제품과 nForce 제품을, 안전한 전자지불용 HSM 장비로 payShield 제품을 판매하고 있다.

3. 기타 HSM 제품

3.1 Rainbow社의 CryptoSwift HSM

Rainbow社는 1984년에 설립되어 인터넷 전자상거래를 위한 보안솔루션 개발업체로 CryptoSwift HSM 장치를 PKI 보안 솔루션중의 하나로 개발하여 판매하고 있다.

CryptoSwift HSM 장치는 서버 내부에 키를 안전하게 보관할 수 있도록 하는 하드웨어의 일부이다. 물리적 Tampering 공격에 대처할 수 있는 HSM 장치내에 중요정보를 저장하여 보호하고 민감한 정보에 대한 암호화 및 복호화 과정은 CryptoSwift HSM 장치 내부에서 일어난다. 만약 HSM이 Tampering 공격으로 훼손된다면 HSM 내에 있는 모든 정보들은 '0'으로 클리어된다. CryptoSwift HSM 장치는 FIPS 140-1 보안등급 3의 안전성을 검증받았으며, 웹서버에 플러그인되어 웹서버의 성능을 가속화시킨다. 또한 전자서명생성시 CryptoSwift HSM 장치내에서 전자서명 연산을 수행하기 때문에 웹서버의 증명서(Credential)을 보호하게 된다. CryptoSwift HSM 장치는 보호하여야 하는 키를 "tamper-active circuitry"로 감싸고 있기 때문에 인증서버의 루트 키나 인증서유효성검증서버(OCSP)의 전자서명생성키를 보호할 수 있다. 모든 전자서명생성 및 검증관련 암호연산은 CryptoSwiftift HSM 장치내에 수행되기 때문에 이들 서버의 성능 및 보안성을 향상시키게 된다. CryptoSwift HSM 장치는 키생성, 키저장, 키검색, 키복제 및 키이동 등의 기능을 제공하며, 백업을 위해 HSM 장치 외부로 나가는 경우에는 암호화된 형태로 유출한다. 이를 위해



〔그림 3〕 CryptoSwift HSM

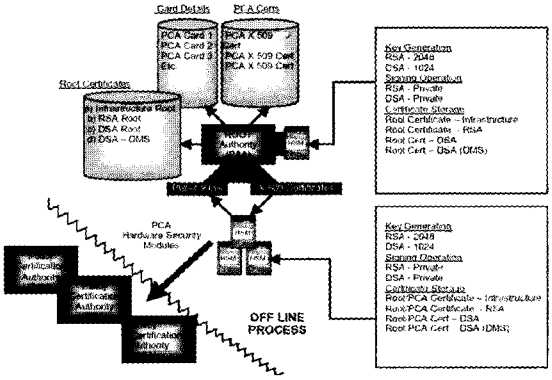
Java 기반의 키관리 소프트웨어를 제공한다. 관리자 및 운영자를 인증하기 위해서는 2-factor 인증기법을 이용하며 이때 Rainbow사의 USB 키인 iKey 인증 솔루션을 이용한다. CryptoSwift HSM 장치는 SSL 가속기 기능도 갖추고 있으며 웹서버가 초당 200개의 SSL 세션을 유지할 수 있도록 해준다.

CryptoSwift HSM 장치는 그림에서처럼 PIC 형태의 add-on 카드이며, 비인가된 접근으로부터 주요 회로를 보호하기 위해 주요 회로 부분은 밀봉되어 있고, 관리자 및 운영자와의 안전한 통신채널을 형성하기 위해 필요한 USB iKey를 장착할 수 있는 포트를 포함하고 있다.

3.2 SPYRUS社의 LYNKS Privacy Card HSM

SPYRUS사의 "LYNKS Privacy Card" 제품군은 PCMCIA 형태의 HSM 장치로 FIPS 140-1 보안등급 2의 안전성을 검증받았다. 이들 제품군은 사용자 인증, 메시지 암호화, 메시지 무결성, 메시지 인증 및 안전한 저장기능(tamper-evident 하드웨어) 등 중요한 보안기능을 갖추고 있다. SPYRUS社의 "Rosetta Executive Suite Authentication" 소프트웨어를 이용함으로써 HSM 장치는 보안전자메일, Code Signing, SSL 클라이언트 인증, VPN 등 다양한 보안서비스를 지원할 수 있다. 특히, 자사의 PKI 시스템에 HSM을 장착하여 제공함으로써 SPYRUS社 PKI 시스템은 계층적인 PKI 구조로 확장성을 가지고 있기 때문에, 몇 백 명의 사용자로 구성된 소규모 환경에서부터 10만 명의 사용자로 구성된 대규모 환경에 이르기까지 다양한 환경에 PKI 시스템을 구축할 수 있다. 다음에서는 PKI 시스템의 각 구성요소에 장착된 HSM의 역할을 간략히 서술한다.

SPYRUS社 PKI 시스템은 최상위 인증기관 또는 정책승인기관(PAA, Policy Approval Authority)을 최상위 기관으로 두고, 하위기관으로 여러 기관의 정책인증기관(PCA, Policy Certification Authority)



〔그림 4〕 최상위정책기관의 정책인증기관 생성

들을 둔다. 이들 정책인증기관은 하위 인증기관의 인증서를 발급하며 인증정책을 관리한다. 하위 인증기관은 해당 등록기관 및 가입자의 인증서를 발급한다. PKI 시스템을 구성하는 최상위인증기관(정책승인기관), 정책인증기관, 인증기관들은 자신의 전자서명키를 보호하고, 전자서명 기능 수행, 키생성 등을 위해 HSM 장치를 이용한다. 최상위인증기관은 LYNKS HSM 장치를 이용하여 자신의 루트 키를 생성하고, 생성한 루트 키를 이용하여 자신의 인증서에 자가서명을 한다. 또한 최상위인증기관은 정책인증기관을 생성하며, 아울러 정책인증기관의 HSM도 생성하여 정책인증기관에 적합하도록 HSM을 안전하게 초기화한다. 초기화 과정에서 HSM 접근을 통제하기 위한 PIN을 설정하고, 정책인증기관에서 발급하는 인증서에 전자서명을 수행하기 위한 전자서명생성키도 생성한다. 즉, 최상위정책기관은 정책인증기관의 인증서를 생성하기 위한 전자서명키 등록과정에서 정책인증기관의 HSM에서 전자서명키쌍을 생성한 후, 생성된 전자서명키쌍 중 전자서명검증키는 HSM 밖으로 나와 최상위정책기관으로 전달된다. 최상위정책기관은 전달받은 전자서명검증키에 대한 인증서를 발급하고 정책인증기관의 HSM에 인증서를 저장할 수 있도록 발급한 인증서를 전송한다. 정책인증기관의 HSM에는 정책인증기관의 인증서뿐만 아니라 최상위정책기관의 인증서도 같이 저장되어 있다. 인증기관 역시 전자서명, 키관리 및 암호연산을 수행하기 위하여 LYNKS HSM을 이용한다.

이들 제품 외에도 VISA 규격을 따르고, EFTPOS 등을 지원하는 등 nCipher社의 payShield 제품과 유사한 기능을 제공하는 HSM 장치로 금융거래에 적용할 수 있도록 ATM 네트워크 환경에 적합하게 설계한 Host Security Module HSM 장치가 있으며, 이는 Rascal社의 Zaxus PC 보안모듈 및 스마

〔표 1〕 전자서명 처리 속도 비교[33]

동작환경	전자서명 암호연산 (1024비트 RSA키)	서버	HSM을 장착한 서버
· 서버 : E4500 - CPU : E4500 - 프로세서 : 4개 - 메모리 : 1GB · HSM : nShield 300	복호화	62/초	294/초
	서명생성	54/초	265/초
	서명검증	142/초	748/초
	키생성	10/분	5/초

트카드 터미널에 장착되어 동작하기도 하며, Thales 社의 e-Security RG7000 계열에 장착되어 동작한다. 2048비트의 RSA 전자서명알고리즘을 지원하며 키관리 기능도 지원하고 Security Resource Manager라는 소프트웨어를 이용하여 HSM 자원에 대한 접근을 통제한다.

Ⅳ. HSM 제품의 특징 및 안전성 비교 분석

1. HSM 장치의 장 · 단점

앞서 살펴본 상용 HSM 장치의 특징을 고려한 HSM 장치의 장점 및 단점은 다음과 같다.

1.1 HSM 장치의 장점

- 자체 암호연산 기능을 갖춘 HSM 장치내에서 암호키를 이용한 암호연산을 직접 수행함으로써, 서버의 취약성으로 인한 키 노출 위협에 대처할 수 있다.
  ※ 서버에서 암호연산을 수행하는 경우 암호키 저장매체로부터 암호키를 서버의 메모리로 로드하는데 이 과정에서 서버의 보안 취약성으로 인해 암호키가 노출될 위험이 있음. 즉, 서버에서의 암호연산 수행을 위해 암호키를 저장매체 밖으로 유출시킬 필요성을 제거
- 키생성, 키저장, 키파기 등 키 생명주기 동안 안전한 키관리 기능 제공한다.
- 공격자가 물리적 공격을 시도하여 암호모듈에 대한 물리적 접근권을 획득할 수 없도록 "tamper resistance" 특성을 갖게 하드웨어를 설계함으로써 암호키 노출 위협에 대처한다.
- 대부분의 상용 HSM 장치는 FIPS 140-1의 2/3 보안등급의 안전성 검증을 받음으로써 암호모듈의 안전성 · 신뢰성을 보장한다.

〔표 2〕 주요 HSM 장치 가격[34]

회사(국가)	HSM 장치	가격
Chrysalis-ITS Inc.(캐나다)	Luna CA3	$ 3,995
nCipher(영국)	nShield F3(PCI)	$12,200
	nShield F3 UltaSign(PCI)	$16,000
Rainbow Tech.	CryptoSwift	$ 4,990

- HSM 장치는 프로세서를 가지고 있어 암호연산을 자체적으로 수행하므로 서버의 암호연산으로 인한 부하를 줄임으로써 암호서비스의 속도 및 성능을 향상한다.
  ※ 서버에서 암호연산을 수행하는 경우 암호연산은 비트단위의 복잡한 수식계산을 해야 하기 때문에 서버의 CPU을 90%이상 점유하게 되어 서버의 기본 동작 수행에 지연 발생

1.2 HSM 장치의 단점

- HSM 장치는 제공하는 기능 및 보안성에 따라 가격의 차이가 나지만 약 천 달러에서부터 만 달러에 이르기까지 장치 가격이 고가이므로 비용부담이 크다.
- HSM는 하드웨어 기반이기 때문에 이에 대한 업그레이드가 어려워 기능 변경에 대한 유연성 부족하다.
  ※ 만약 기존 암호알고리즘에 대한 취약성이 발견되면 HSM 장치로부터 관련 부분을 삭제하고 이에 대한 보안조치를 취한 새로운 암호 소프트웨어 모듈을 HSM 장치로 플러그 인하여야 하는데, HSM 장치는 하드웨어 기반이므로 기능 삭제 · 추가가 어려움
- HSM 제조업체에게 암호키 노출 허용의 위험이 존재한다.
  ※ 구조상 물리적 제약조건으로 인해, HSM 제조 공정과정에서 HSM내에 모듈키 또는 루트키를 설치하여야 한다. 따라서 루트키 또는 모듈키는 제조과정에서 HSM 제조업체에게 노출되게 된다. HSM 제조업체에 대한 신뢰를 상실하면 관리자는 키에 대한 외부의 접근을 막을 수 있는지의 여부를 확신할 수 없음
- 키에 대한 안전성은 HSM에 대한 안전성에 기인하기 때문에 HSM 장치가 도난 또는 훼손되는 경우 키에 대한 안전성을 유지할 수 없다.

〔표 3〕 HSM 장치의 특징 비교-1

특징 \ 제품명		Luna CA[3]	Luna XPplus	Luna RA	Luna 2	CryptoSwift	LYNKS Privacy Card
회사		Chrysalis-ITS Inc.				Rainbow Tech.	SPYRUS Inc.
용도		PKI의 주요 키 보호	전자서명 기능 지원	가입자/클라이언트 키생성	저가의 휴대용 PKI 키 보호	PKI의 주요 키 보호	PKI의 주요 키 보호
FIPS 140-1 등급		3	3	2	2	3	2
접근통제	관리자/운영자 인증방식	2factor 인증 (PED 키 + PIN)	2factor 인증 (PED 키 + PIN)	2factor 인증 (PED 키 + PIN)	2factor 인증 (PED 키 + PIN)	2factor 인증 (iKey + PIN)	PIN 인증
	역할(직무) 구분	O	O	N/A	N/A	O	O
	비밀분산	O	O	×	×	×1)	×
물리적 보안	Tamper-Evident	O	O	O	O	O	O
	Tamper-Resistant	O	O	×	×	O	×
동작환경		Luna DOCK	Luna CA3 Key management system	Luna DOCK	Luna DOCK	SSL을 지원 하는 웹서버	Win.2000 인증서버
서버와의 연결형태		PCI ※Luna DOCK이 서버에 연결	PCI ※Luna DOCK에 연결	PCMCIA	PCMCIA	PCI ※add-on card 형태로 서버에 직접 연결	PCMCIA
성능	처리속도 (전자서명*생성수/초)	25	500	-	25	200	-
	저장용량 (키쌍 수, 인증서 수)	400, 400	-	-	600, 400	-	-
알고리즘 (키길이)	공개키 및 키교환	RSA(4096), DSA(1024), DH(1024)	RSA(4096) DSA, DH	RSA(4096), DSA(1024), DH(1024)	RSA(4096), DSA(1024), DH(1024)	RSA(1024), DSA(1024)	RSA(1024), DSA(1024), DH
	대칭키	DES/3-DES, RC5 CAST (128), RC2, RC4	DES/3-DES, RC5 CAST (128), RC2, RC4	DES/3-DES, RC5 CAST (128), RC2, RC4	DES/3-DES,, RC2, RC4, RC5 CAST 128	DES/3-DES, RC4	DES/3-DES, Skipjack
	MAC	SHA-1, MD5	MD5, MD2	SHA-1, MD5	SHA-1, MD5	SHA-1, MD5	-
S/W 인터페이스 지원방식		PKCS#11, MS API, JCE/JCA, OpenSSLL	PKCS#11	PKCS#11	PKCS#11, MS API, JCE/JCA, OpenSSLL	PKCS#11, OpenSSL	PCKS#11
키관리용 S/W		× (H/W 기반 키관리)	× (H/W 기반 키관리)	× (H/W 기반 키관리)	× (H/W 기반 키관리)	O	O (Signal Identity Manager)
키복구 및 키백업 지원 여부		O (key cloning) ※ 복구기능 지원	O (key cloning) ※ 키백업만 지원	O (key cloning) ※ 키백업만 지원	×	O (key cloning)	O (Skipjack) ※ 복구기능 지원
가격		$ 3,995	-	-	$795	$4,990	-
기타		외부 감사기관이 감사수행	좌동	좌동	좌동	OCSP 서버의 키 보호 장치	미국방부의 DMS 등 연방정부에 적용

※1) Key를 두 개로 split하여 관리자와 사용자가 각각 나누어 각자의 iKey에 저장

2. HSM 제품의 특징 및 안전성 비교

HSM 전 세계 시장을 선점하고 있는 Chrysalis-ITS사의 Luna 제품군과 nCipher사의 nShield 제품 등을 중심으로 제품의 지원알고리즘, 성능, 가격, 서버와의 연결 형태 등의 특징 비교는 〔표 3,4〕와 같다.

또한, 각 상용제품에 대한 안전성 비교를 키 보관 형태, 키 저장소, 키에 대한 접근권한의 분산, 지원 키 길이, 인증방식, 물리적 보안등의 항목을 기준으로 비교하였다. 대부분의 HSM 장치들은 각 응용서비스에서 사용되는 키를 보호하기 위하여 마스터키, 모듈키, 또는 이들 키들로부터 유도된 키 등으로 암호화하여 저장하며, 키를 암호화하는 데 사용된 키를 HSM 개발업체의 특성에 따라 고유한 방법으로 보관하고 있다. Chrysalis-ITS社의 경우 각 HSM에 내장된 마스터키로 응용서비스의 키를 3-DES알고리즘을 이용하여 암호화한 후, 해당 마스터키를 Shamir의 비밀분산 기법을 적용하여 조각화하여 Green PED키에

〔표 4〕 HSM 장치의 특징 비교-2

특징 \ 제품명		nShield F2(F2) (PCI/SCSI), nShield F2 UltraSign(F2-U) (PCI/SCSI)	nShield F3(F3) (PCI/SCSI), nShield F3 UltraSign(F3-U) (PCI/SCSI)	payShield	nForce 150 (PCI/SCSI)	nForce 300	nForce 400
회사		nCipher Inc.					
용도		PKI의 주요 키 보호	PKI의 주요 키 보호	전자지불의 주요 키 보호	SSL용 개인키 보호	SSL용 개인키 보호	SSL용 개인키 보호
FIPS 140-1 등급		2	3	3	2	2	2
접근통제	관리자/운영자 인증방식	2factor 인증 (패스프레이즈 + 스마트카드)	2factor 인증 (패스프레이즈 + 스마트카드)	2factor 인증 (패스프레이즈 + 스마트카드)	2factor 인증 (패스프레이즈 + 스마트카드)	2factor 인증 (패스프레이즈 + 스마트카드)	2factor 인증 (패스프레이즈 + 스마트카드)
	역할(직무) 구분	O	O	O	O	O	O
	비밀분산	O	O	O	O	O	O
물리적 보안	Tamper-Evident	O	O	O	O	O	O
	Tamper-Resistant	O/×	O	O	×	×	×
동작환경		SEE(opt.)	SEE(opt.)	SEE	SEE Diabled	SEE Diabled	SEE Diabled
서버와의 연결형태		PCI/SCSI	PCI/SCSI	Wide SCSI	PCI/SCSI	PCI	SCSI
성능	처리속도 (전자서명*생성수/초)	F2 : 150/150, F2-U : 300/400	F3 : 150/150, F3-U : 300/400	150	150/150	300	400
	저장용량 (키쌍 수, 인증서 수)	-	-	-	-	-	-
알고리즘 (키길이)	공개키 및 키교환	RSA(4096), DSA(2048), KCDSA(2048), El-Gamal(4096), DH(4096), DES/DES3 XOR	좌동	좌동	좌동	좌동	좌동
	대칭키	DES/3-DES, CAST(128,256), AES(256), ArcFour(2048)	좌동	좌동	좌동	좌동	좌동
	MAC	SHA-1, MD5, MD2, RIPEMD160	좌동	좌동	좌동	좌동	좌동
S/W 인터페이스 지원방식		PKCS#11, MS API, JCE/JCA, OpenSSLL, nCipehr nCore API	좌동	좌동	좌동	좌동	좌동
키관리용 S/W		O (KeySafe)	O (KeySafe)	O (KeySafe)	O (KeySafe)	O (KeySafe)	O (KeySafe)
키복구 및 키백업 지원 여부		O	O	O	O	O	O
가격		F2 : $6,800/$7,500 F2-U : $10,400/-	F3 : $12,200/$13,500 F3-U : $16,000/$19,500	-	$5,700/$6,400	$9,400	$12,000
기타		S/W 및 H/W의 혼합형 방식 키관리	좌동	좌동	좌동	좌동	좌동

※ '-' : 언급된 자료가 없음

저장하여 보관한다. 한편, 마스터키로 암호화된 응용서비스의 키는 HSM 내부에 저장된다.

nCipher社의 경우 응용서비스의 키를 HSM 장치 내부에 저장하여 보관하지 않고 호스트 서버의 하드드라이브나 데이터베이스에 저장하여 보관할 수 있도록 하기 위해, HSM 장치내부에 저장한 정도의 안전성을 유지하는 "key blob"라는 nCipher社의 고유한 키 보관 형태를 개발하였다. "key blob"을 생성하기 위해 먼저, 응용서비스의 키에 대한 접근통제목록을 생성하여 키와 접근통제목록을 포함하는 키 객체를 생성한다. 또한 키 객체에 대한 MAC 값 및 전자서명 값을 계산하여 키 객체에 포함시킨다. 이때 전자서명 값은 모듈 전자서명키로 생성한 값이다. 이로써 "key blob"이 생성된다. "key blob"을 암호화하기 위해 HSM 장치의 자체 난수생성기에서 생성한 값을 3-DES 키로 사용한다. "key blob"을 암호화하기 위해 사용된 3-DES 키를 논리적 토큰이라 한다. 논리적 토큰을 보호하기 위해 모듈키로 암호화 한 후 암호화된 논리적 토큰을 Sharmir 비밀분산 기법을 적용하여 조각화한다. 모듈키, 패스프레이즈, 조각 번호, 스마트카드

〔표 5〕 주요 HSM 제품의 안전성 비교

비교 항목 \ 제품		Luna CA3/ Luna XPplus	Luna RA/ Luna 2	nShield F2 제품군	nShield F3 제품군/ payShield	CryptoSwift	LYNKS Privacy Card
키	보관 형태	3-DES 암호화	3-DES 암호화	Key blob	Key blob	3-DES 암호화	Skipjack 암호(정부용)/ 3-DES 암호(상업용)
	저장소	HSM 내부	HSM 내부	서버/DB	서버/DB	HSM 내부	HSM 내부
	키암호용 키의 저장매체	PED 키	PED 키	스마트카드	스마트카드	iKey 토큰	HSM 내부
	접근 권한 분산	○	○	○	○	○	×
	비밀분산 적용 여부	○	○	○	○	×[1]	×
	비밀분산 대상정보	마스터 키	마스터 키	암호화된 논리적 토큰	암호화된 논리적 토큰	해당없음	해당없음
	사용자 패스워드 생성주체	사용자	사용자	사용자[2]	사용자[2]	보안관리자	보안관리자
	최대 지원 키 길이	RSA : 4096 DSA : 1024 D-H : 1024	RSA : 4096 DSA : 1024 D-H : 1024	RSA : 4096 DSA : 2048 D-H : 4096 KCDSA : 2048	RSA : 4096 DSA : 2048 D-H : 4096 KCDSA : 2048	RSA : 1024 DSA : 1024	RSA : 1024 DSA : 1024
사용자 인증	관리자 2factor인증	○	○	○	○	○	×
	일반 사용자 2factor인증	○	×	○	○	○	×
물리적 특성	Tamper-evident	○	○	○	○	○	○
	Tamper-resistant	○	×	×	○	○	×

1) 비밀분산 기법을 적용한 키 조각화는 아니지만, 키를 두 개의 조각으로 분리하여 보안관리자와 일반사용자의 iKey 토큰에 각각 저장하여 관리

2) 키를 저장하고 있는 스마트카드에 대한 사용자의 접근통제를 위해 패스프레이즈를 사용하여 패스프레이즈에 대한 길이 제한은 없으나, 초기화에 기본값으로 패스프레이즈가 설정되어 있으나 언제든지 사용자가 "KeySafe" 키관리용 S/W를 이용하여 패스프레이즈를 변경할 수 있음

ID 등의 정보를 결합하여 "share key"를 생성한 후 "share key"로 조각화된 논리적 토큰을 다시 암호화하여 해당 스마트카드에 기록한다.

Rainbow社의 경우 개인키, 비밀키 및 기타 중요 보안정보들은 HSM에서 보안영역으로 설정된 RAM에 평문형태로 저장되며, 플래쉬에 저장되기도 한다. 플래쉬에 저장되는 경우 마스터키인 3-DES3KEY 키로 암호화한다. 마스터키는 초기화 과정에서 보안관리자가 생성한 랜덤한 키로 BBRAM에 저장된다. 또한 RSA 개인키를 암호모듈로 안전하게 로드하거나 암호모듈 외부로 안전하게 내보내기 위해서 Key-Wrapping-Key(3DES3KEY)로 암호화한다. Key-Wrapping-Key는 보안관리자가 "Write Key Split" 명령어를 수행시켜 키 분할 작업을 시작하면 키가 두 개의 조각으로 분할되어 한 개의 조각은 보안관리자의 iKey에 기록되며 보안관리자가 로그아웃한 후 사용자가 로그인하여 마찬가지로 "Write Key Split" 명령어를 수행시키면 나머지 다른 한 개의 조각은 사용자의 iKey에 기록된다. 두 개의 iKey 토큰에 저장된 키 조각들은 "CODE"라고 레이블된다. 이로써 물리적으로 분리된 서로 다른 장치에 키 조각들이 각각 저장된다.

SPYRUS社의 경우 정부용은 Skipjack 알고리즘을, 상업용은 3-DES 알고리즘을 사용한다. 보호하고자 하는 키 또는 중요 정보를 Skipjack MEK로 암호화하고 MEK는 Skipjack TEK로 다시 암호화한다. 상업용인 경우 3-DES로 암호화하고 3-DES키를 보호하기 위해 또 다른 3-DES키로 암호화한다.

〔표 5〕에서는 4개사 HSM 제품을 키에 대한 보관형태, 키를 보호하기 위해 사용된 키의 저장매체, 사용자 패스워드 생성주체, 비밀분산 적용 여부 등 여러 가지 안전성 측면에서 비교하였다. 특히 사용자 패스워드 생성주체에 대해 생성주체가 보안관리자인 경우, 사용

자의 프라이버시를 보장할 수 없게 된다. 또한 사용자 인증 및 물리적 특성 항목에 대해서도 비교하였다.

V. 결 론

고도의 보안기능을 갖춘 암호장비에 대한 수요가 증가하면서, HSM 장치도 이러한 암호장비 중에 하나로서 인증서비스를 제공하는 인증기관을 중심으로 그 관심이 고조되고 있다.

기존 HSM 장치는 하드웨어 기반이므로 암호기술 변화에 따른 기능 추가시 HSM 장치의 업데이트가 용이하지 않아 HSM 장치 자체를 교체하여야 하는데 이러한 단점을 해결하기 위해 기능 추가에 따른 유연성을 갖도록 하드웨어와 소프트웨어의 혼합방식을 기반으로 하는 HSM 장치 개발이 필요하다. 또한 암호기술의 사용 증가에 따라 관리하여야 하는 암호키의 종류 및 수량이 증가하는 추세이며, 분산환경 기반의 기업 보안솔루션에 암호기술을 적용하는 등 암호기술의 사용환경도 다양해지고 있어 키 보관 메커니즘 및 키관리 소프트웨어에 대한 확장성이 요구된다. 하드웨어 특성으로 인해 기존 HSM 장치는 보관 및 관리할 수 있는 키의 수가 제한적이므로, 향후 이러한 문제점을 개선할 수 있도록 확장성을 갖는 HSM 장치 개발이 필요하다. 그리고 암호기술의 사용환경이 다양해짐에 따라 이에 적합한 새로운 알고리즘 및 프로토콜이 개발되고 있어 이들에 독립적인키관리 기능을 지원하는 HSM 장치 개발이 필요하며 분산환경을 고려한 원격지 키관리 기능을 지원하는 HSM 장치 개발이 필요하다. 현재 대부분의 상용 HSM 제품들은 키백업 기능을 선택사항으로 제공하고 있으며 키복구 기능은 거의 지원하지 않고 있으나, 암호키 분실 및 손실 등과 같은 역기능을 최소화하기 위해 키복구 기능이 HSM 제품에 탑재되어야 할 것으로 사료된다.

국내의 경우 HSM 제품 개발은 거의 이루어지고 있지 않으나, HSM 장치의 수요가 증가하고 있어 향후 암호모듈 개발경험을 가진 업체를 중심으로 국내 자체 HSM 개발이 기대된다.

본 논문에서는 현재 가장 많이 사용되고 있는 상용 HSM 장치의 특징 및 기능을 살펴보고, HSM 장치의 안전성에 대한 사항도 간략히 살펴보았다. 또한 앞서 살펴본 여러 가지 상용 HSM 장치의 특징 및 기능을 고려하여 장·단점을 분석하였다. 본 논문이 국내 HSM의 올바른 선택과 사용에 유용한 자료로 활용될 수 있을 것으로 기대한다.

참고문헌

[1] 한국정보보호진흥원, "건전한 암호이용 활성화 방안 마련을 위한 보고서", 2002.12

[2] David Cross, "Deploying Certificate Services *on Windows 2000 and Windows.NET Server* with the Chrysalis-ITS Luna CA3 Hardware Security Module", 2002.3

[3] Chrysalis-its Inc., "Beyond FIPS 140-1 : Essential Best Practices for Hardware Security Modules", 2001

[4] David Cross, "Windows2000 Server and PKI : Using the nCipher Hardware Security Module", http://www.ncipher.com/resource, 2001.4

[5] nCipher Inc., "nCipher Security World White Paper", 2001.4

[6] nCipher Inc., "strengthen and manage the security of your public key infrastructure with nCipher", 2001

[7] nCipher Inc., "nShield Hardware Security Module", http://www.ncipehr.com/nshield/, 2002

[8] nCipher Inc., "KeySafe 1.0", http://www.nipher.com/

[9] nCipher Inc., "Secure Execution Engine White Paper", http://www.ncipehr.com/, 2002

[10] nCipher Inc., "nShield User Guide Solaris", 2002.8

[11] nCipehr Inc., "payShield, Hardware Security Module For E-Payment", 2002.9

[12] nCipehr Inc., "Securing 3-D Secure", 2002.9

[13] nCipehr Inc., "nFast800", 2002.

[14] nCipehr Inc., "nForce", 2002.

[15] Rainbow Tech., "PKI-Secure Key Storage", 2002.9

[16] Rainbow Tech., "Deploying HSMs into an OpenSSL Based PKI Environment", 2002.5

[17] SPYRUS, Inc., "SPYRUS PKI Release 6.0 Technical White Paper", 2002.8

[18] Rascal Com., "Host Security Module",

2002.7
[19] Chrysalis-ITS, Inc., "Luna Token Security Policies(CR-1356)", 2002.4
[20] Chrysalis-ITS, Inc., "Luna XPplus and Luna XL/XLR and XL/XLR Premium Security Policies(CR-1357)", 2002.4
[21] Chrysalis-ITS, Inc., "Certificate Authority Root Key Protection : Recommended Practices", Deloitte & Touche, 1999.7
[22] nCipher Inc., "Cryptographic security and key management systems - the nFast /KM solution", 1998.1
[23] nCipher Inc., "The nShield module security policy : nShield F2 PCI, nShield F2 PCI Ultrasign v1.1.31", 2002.7
[24] nCipher Inc., "The nShield module security policy : nShield F2 SCSI, nShield F2 SCSI Ultrasign v1.1.31", 2002.7
[25] nCipher Inc., "The nShield module security policy : nShield F2 PCI, nShield F2 PCI Ultrasign v1.2.27", 2003.2
[26] nCipher Inc., "The nShield module security policy : nShield F2 SCSI, nShield F2 SCSI Ultrasign v1.2.27", 2003.2
[27] nCipher Inc., "The nShield and payShield modules security policy : nShield F3 SCSI, nShield F3 SCSI Ultrasign and payShield v1.1.33", 2002.9
[28] nCipher Inc., "The nShield and payShield modules security policy : nShield F3 SCSI, nShield F3 SCSI Ultrasign and payShield v1.2.27", 2003.2
[29] nCipher Inc., "The nShield module security policy : nShield F3 PCI, nShield F3 PCI Ultrasign v1.1.31", 2002.7
[30] nCipher Inc., "The nShield module security policy : nShield F3 PCI, nShield F3 PCI Ultrasign v1.2.27", 2003.2
[31] Rainbow Technologies, Inc., "CryptoSwift HSM Cryptographic Accelerator", 2001.7
[32] SPYRUS, "LYNKS Privacy Card Security Policy, vA3", 1999.11
[33] nCipher Inc., "Using nCipher Hardware to Secure Your Identrus Infrastructure"
[34] Network Computing, "Network Computing's Interactive Buyer's Guide", http://ibg.networkcomputing/com/ibg/ProductInfo, 2002
[35] 권현조, 김지연, 전길수, "암호키 노출 방지기능을 갖는 HSM 제품 동향 및 안전성 분석 TM", 암호기술-2003-005, 한국정보보호진흥원, 2003. 6

〈著 者 紹 介〉

김 지 연 (Jeeyeon Kim)
종신회원

1995년 2월 : 성균관대학교 정보공학과 졸업
1997년 2월 : 성균관대학교 대학원 정보공학과 공학석사
1996년 12월~현재 : 한국정보보호진흥원(KISA) 선임연구원
〈관심분야〉 정보보호, 암호프로토콜, 키관리

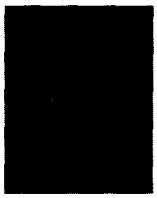
권 현 조 (Kwon Hyunjo)
정회원

1997년 2월 : 성균관대학교 정보공학과 졸업
2000년 8월 : 성균관대학교 정보통신대학원 공학석사
1997년 1월~1997년 7월 : (주) 나라계전 기술연구소 연구원
1997년 7월~현재 : 한국정보보호진흥원(KISA) 연구원
〈관심분야〉 키관리, 암호프로토콜, 스마트카드, 정보보호시스템 평가체계, 정보보호 기술 표준화

전 길 수(Kilsoo Chun)
종신회원

1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 대학원 수학과 이학석사
1998년 2월 : 서강대학교 대학원 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구

소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국정보보호진흥원(KISA) 선임연구원
〈관심분야〉 암호학, 정보보호



임 선 간 (Seongan Lim)
종신회원

1985년 : 동국대학교 수학과 학사
1987년 : 서울대학교 수학과 석사
1995년 : Purdue 대학교 수학과 박사
1999년~2002년 : 한국정보보호진흥원 선임연구원
2003년~현재 : 한국정보보호진흥원 암호인증기술팀장
〈관심분야〉 : 암호프로토콜, 정보보호 등

이 재 일 (Jae-il Lee)
종신회원

1986년 2월 : 서울대학교 계산통계학과 학사
1988년 2월 : 서울대학교 계산통계학과 석사
1991년 1월 ~ 1996년 6월 : 한국 IBM
1996년 7월 ~현재 : 한국정보보호진흥원 전자거래보호단장
〈관심분야〉 : 전자상거래 보안, 유·무선 PKI 등