S/MIME 표준적합성 시험 동향

라은주 | 한국정보보호진흥원 산업지원단 기술표준팀
TTA 암호기술연구반 참관자
정태인 | 한국정보보호진흥원 산업지원단 기술표준팀
TTA 정보보호관리연구반 간사
오남호 | 한국정보보호진흥원 산업지원단 기술표준팀
TTA 암호기술연구반 참관자
신종회 | 한국정보보호진흥원 산업지원단 기술표준팀
TTA 정보보호기술위원회 간사

1. 개요

현재 보안전자우편에 대한 중요성이 크게 대두됨에 따라, 많은 S/MIME 제품들이 출시되고 있다. 그러나 이러한 제품들이 보안전자우편 표준인 IETF의 S/MIME RFC를 준수하여 구현하였다고 하더라도 구현상의 문제나 표준문서에 대한 상이한 해석으로 인하여 제품들간의 상호운용성이 보장되지 않고 있다. 상호운용성을 높이기 위해서는 각각의 제품들이 표준을 준수하여 구현되어야 하지만, 현재 출시된 제품들은 표준문서의 일부만을 수용하고 있다. 이러한 문제점을 해결하고자 RSA에서는 S/MIME 상호운용성 시험을 수행한 바 있으며, NIST에서도 S/MIME 상호운용성 시험도구를 개발중에 있다. 국내에서는 한국정보보호진흥원이 S/MIME 표준적합성 시험에 대한 연구를 2002년도부터 진행하여 현재 모의시험을 수행중에 있다.

이에 본 고에서는 RSA와 NIST의 시험현황에 대하여 간략하게 살펴보고, 한국정보보호진흥원이 시행중인 S/MIME 표준적합성 시험에 대하여 소개하고자 한다.

2. S/MIME 상호운용성 시험현황

2.1 NIST(National Institute of Standards and Technology)

NIST는 미국 국립 표준 기술원으로서 표준을 개발하고 표준을 사용하는 산업체를 지원하기 위한 활성화 프로그램을 운영하고 있다. 특히, 최근에 활발하게 이용되고 있는 전자우편의 안전한 전송을 위하여

S/MIME 제품에 대한 보안성 및 상호운용성 시험에 대한 연구를 진행하고 있는데, IETF 표준에 기초하여 보안성 및 상호운용성에 대한 S/MIME 버전 3 클라이언트 프로파일을 2002년 11월에 개발한 바 있다. 이 프로파일은 보안전자우편제품에서의 보안성 및 상호운용성을 높이기 위하여, S/MIME RFC의 필수 요구사항을 포함하고 있으나 알고리즘상의 복잡성으로 인하여 Diffie-Hellman 키 합의(Key Agreement) 암호화 알고리즘은 제외시키고 있다.

NIST는 프로파일 이외에도 인터넷 기반의 자동화된 S/MIME 시험도구를 개발중에 있는데, 자동화된 시험도구는 S/MIME 버전 3 클라이언트 프로파일 및 S/MIME 관련 RFC에 대한 표준적합성 시험 및 상호운용성 시험에 크게 기여할 것으로 기대된다. 자동화된 시험도구에는 S/MIME 버전 3 참조구현물(Reference Implementation)이 포함되는데, 참조구현물은 메일 송수신자 역할을 수행하며 NIST의 S/MIME 버전 3 클라이언트 프로파일에 적합하게 구현될 예정이다. 이러한 시험 도구는 S/MIME 버전 3 구현제품만을 검증하는 것이 아니라 NIST의 S/MIME 버전 3 클라이언트 프로파일도 검증한다. 이 시험도구는 2003년 3/4분기에 사용 가능하도록 예정되어 있다.

2.2 RSA

1997년 설립된 RSA Data Security사는 S/MIME 버전2를 주도적으로 개발한 이후, S/MIME Interoperability Center를 운영하여 S/MIME 버전 2를 지원하는 제품에 대한 상호운용성 시험을 수행하였다. RSA사는 Worldtalk사의 WorldSecure 클라이언트를 참조 구현물로 사용하여 시험을 수행하였으나, S/MIME 표준화가 IETF로 이전되면서 2001년부터는 S/MIME 상호운용성 시험을 운영하지 않고 있다. 2001년까지 총33개의 제품들이 상호운용성 시험을 통과하였으며, 시험에 통과한 제품들에 한하여 [그림 1]과 같은 마크를 부여하였다.

[그림 1] RSA 인증 마크

RSA S/MIME 상호운용성 센터에서 수행한 S/MIME 버전 2 상호운용성 시험절차와 내용은 다음과 같으며, 대부분의 시험은 온라인으로 이루어졌다.

1. 신청인은 온라인 상호운용성 시험에 앞서, 먼저 자체시험을 수행한다. 자체시험은 Worldtalk사의 WorldSecure Client를 다운로드 받아서 상호연동 시험을 수행한다.
2. 신청인은 S/MIME 상호운용성 시험 신청서를 작성하여 RSA사에 제출한다.
3. 신청인은 512비트 RSA 키쌍을 생성하고, 공개키에 대해 베리사인(VeriSign) 클래스 1 디지털 인증서를 발급받는다.
4. 신청인은 메일 제목에 "S/MIME Interop Test: 〈업체명〉's Certificate"라고 기입하고, 서명된 전자우편 메시지를 smime-test@smime.org에 보낸다.
5. 신청인은 위의 메시지에 대한 응답으로 다음과 같은 형태의 두 개의 메시지를 받게 된다.
   - RSA 512, RC2 40, SHA-1을 사용하여 전자서명된 후 암호화된 메시지

○ RSA 512, Triple-DES, SHA-1을 사용하여 전자서명된 후 암호화된 메시지
각각의 메시지는 PKCS #7 signedData 객체로 전자서명된 후, 다시 PKCS #7 envelopedData 객체로 암호화되어 생성된다.

6. 신청인은 5에서 받은 메시지를 복호화한 다음, 복호화된 내용을 포함하여 다음과 같은 형태의 메시지를 생성하여 smime-test@smime.org로 전송한다. 이때 제목에는 "S/MIME Interop Test: 〈업체명〉's RC2 40"와 "S/MIME Interop Test: 〈업체명〉's 3DES"라 기입한다.
○ RSA 512, RC2 40, SHA-1을 사용하여 전자서명된 후 암호화된 메시지
○ RSA 512, Triple-DES, SHA-1을 사용하여 전자서명된 후 암호화된 메시지
각각의 메시지는 PKCS #7 signedData 객체로 전자서명된 후, 다시 PKCS #7 envelopedData 객체로 암호화되어 생성된다.
7. 상호운용성 센터쪽에서 6의 메시지를 복호화해서 5에서 보냈던 것과 동일한 메시지를 복구할 수 있으면 시험에 합격한 것으로 판정하고 그 결과를 신청인에게 통보하며, 시험 결과를 RSA S/MIME 상호운용성 센터 홈페이지에 게시한다.

3. S/MIME 표준적합성 시험현황

보안전자우편 표준인 S/MIME에 대한 표준적합성 시험은 국외에서는 시행된바 없고, 국내에서는 한국정보보호진흥원이 2002년부터 연구를 진행하여 현재 국내 S/MIME 제품을 대상으로 모의시험을 수행중이다. S/MIME 표준적합성 시험은 자동화된 시험 시스템과 제품간의 시험 메시지 송수신을 통하여 이루어진다. 본 절에서는 한국정보보호진흥원에서 수행중인 S/MIME 표준적합성 시험에 대하여 살펴보고자 한다.

3.1 시험항목 및 범위

S/MIME 표준적합성 시험은 S/MIME의 기본이 되는 S/MIME 메시지 규격, 암호화 메시지(Cryptographic Message Syntax) 규격, 인증서 운영규격을 위주로 시험 하였으며, 보안 서비스 확장 등의 부가적인 기능은 본 시험에서 제외하였다. 이에 따라 시험항목 및 시험범위는 [표 1]의 6개의 표준문서만으로 한정하였다.

시험은 [표 1]의 RFC에 근거하여 S/MIME 버전 2와 S/MIME 버전 3으로 분류하였으며, 각 버전별로 전자서명 데이터(Signed Data), 암호화 데이터(Enveloped Data), 전자서명 및 암호화된 데이터(Signed And Enveloped Data)에 대한 시험을 각각

[표 1] S/MIME 표준적합성시험 대상 표준문서

문서번호	내용	문서종류
RFC 2311	S/MIME Version 2 Message specification	Informational
RFC 2312	S/MIME Version 2 Certificate Handling	Informational
RFC 2315	PKCS#7 : Cryptographic Message Syntax Version 1.5	Informational
RFC 2630	Cryptographic Message Syntax	Standards
RFC 2632	S/MIME Version 3 Certificate Handling	Standards
RFC 2633	S/MIME Version 3 Message Specification	Standards

진행하였다. 각각의 시험 데이터 개수는 [표 2]와 같다.

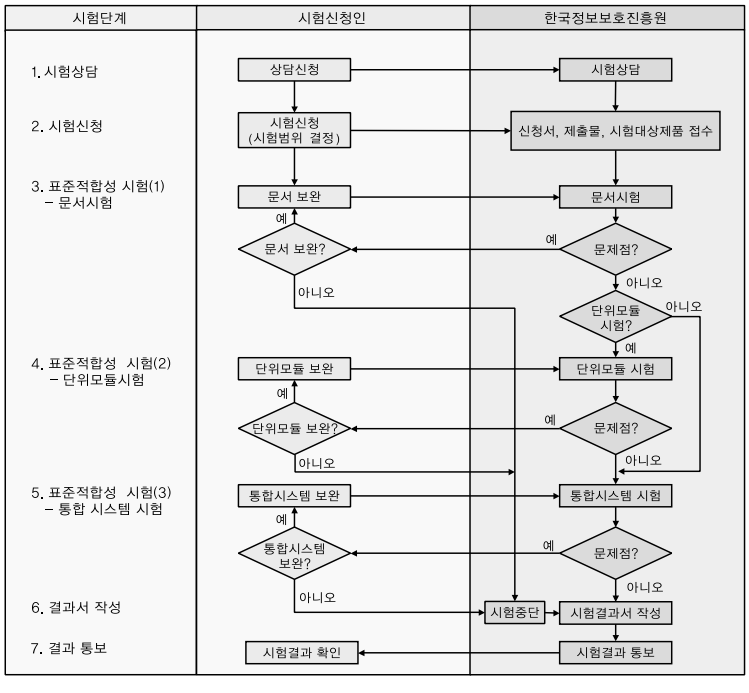
[표 2] 시험 데이터 개수

시험범위	전체항목 수
V2의 전자서명	81
V2의 암호화	32
V2의 전자서명 및 암호화	30
V3의 전자서명	91
V3의 암호화	38
V3의 전자서명 및 암호화	114
합계	386

3.2 시험절차

본 시험에서는 [그림 2]에서 보는 바와 같이 시험 상담에서부터 시험 결과 확인까지 총 7단계의 시험 절차를 갖는다.

시험은 크게 문서시험, 단위 모듈시험, 통합 시스템 시험으로 분류된다. 문서시험에서는 제품 매뉴얼, 제품의 기능 명세서, 제품의 기본 설계서에 대하여 시험을 수행하며, 단위 모듈 시험에서는 필요시 제품에 탑재되어 있는 모듈별로 시험을 수행한다. 그러나 현재 단위 모듈 시험은 수행되지 않고 있다. 통합 시스템 시험에서는 실제 제품에 대한 표준적합성 시험이 수행된다. 이러한 세가지 시험 수행중에 제품에 문제점이 발견되면 보완을 요청할 수 있으며, 보완된 제품에 대해서는 재시험을 수행하고, 보완되지 않은 제품에 대해서는 시험을 중단하게 된다.



[그림 2] S/MIME 표준적합성 시험 절차

3.3 시험 시스템

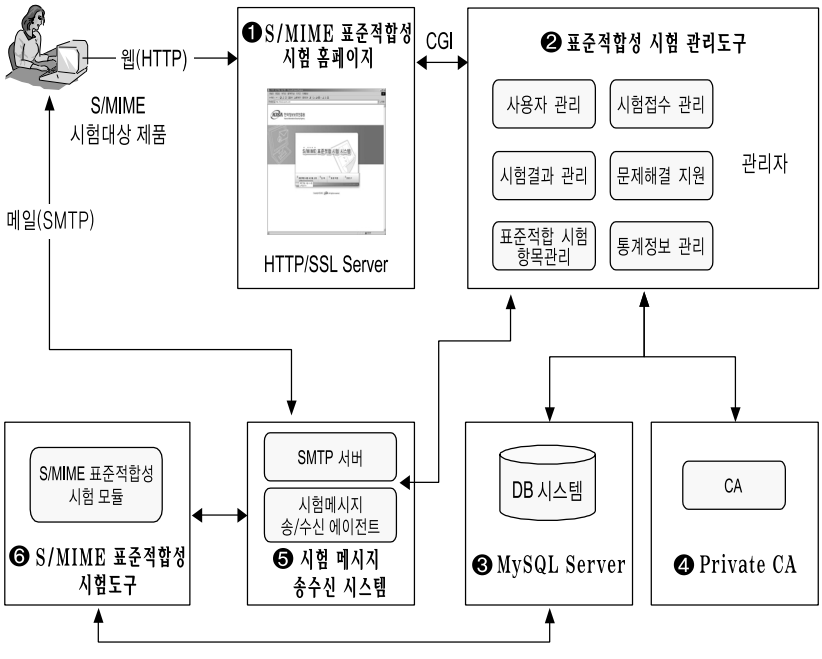
S/MIME 표준적합성 시험 시스템은 [그림 3]에서 보는 바와 같이 6개의 서브시스템으로 구성되어 있으며, 각 서브시스템은 다음과 같은 기능을 제공한다.

1) S/MIME 표준적합성 시험 홈페이지

- ㅇ 시험대상 제품에 대한 S/MIME 표준적합성 시험 접수 및 정보 제공을 목적으로 한 웹 기반 인터페이스를 제공한다.
- ㅇ 표준적합성 시험 홈페이지는 SSL(Secure Socket Layer)이 지원되는 웹 서버로 구축됨으로써 시험접수시 디지털 ID(개인키+X.509 공개키 인증서)를 발급받은 사용자만이 인증을 통해 시험결과 정보를 제공받을 수 있다.

2) 표준적합성 시험 관리 도구

- ㅇ 시험 접수 : 시험 대상 제품은 시험 홈페이지를 통해 접수를 하고, 시험관리 시스템은 접수 정보를 바탕으로 이메일 주소와 디지털 ID를 생성하여 발급한다. 이 정보는 시험 메시지 전송에 사용된다.
- ㅇ 시험도구와의 연계 : 이메일 주소와 디지털 ID를 발급 받은 시험 대상 제품만이 시험 도구에 시험 메시지를 전송할 수 있다.
  - 시험 신청인(사용자)은 이메일 주소를 시험 메시지를 송신하기 위해 사용하고, 시험시스템은 이메일 주소를 신청인이 송신한 시험 메시지를 수신하기 위해 사용한다.
- ㅇ 사용자 관리 : 시험 관리 시스템은 발급된 디지털 ID를 통해 인증된 사용자에게만 정보를 제공한다.



[그림 3] S/MIME 표준적합성 시험 시스템 구성도

○ 관리자 인터페이스 제공 : 시험 관리 도구는 SSL의 클라이언트인증을 통해 인증된 관리자만이 사용할 수 있는 인터페이스를 제공한다.
○ 시험 결과 관리 : 시험 도구에서 시험한 결과는 시험 관리 도구내의 DB에 저장되고, 시험 관리 도구는 이를 관리한다.
○ 문제 해결 지원 : 시험 항목과 시험 에러의 상세한 내용을 비교함으로써 시험 과정에서 발견된 오류 항목에 대한 해결책을 제공한다.
○ 통계정보 관리 : 시험 도구에서 시험된 모든 시험 대상 제품에 대한 정보를 저장하고, 이를 통계 수치로 관리자 및 인증된 사용자에게 제공한다.
○ 표준적합성 시험항목 관리 : 시험 도구에서 사용되는 모든 시험 항목은 관리자의 설정에 따라 추가/삭제/수정될 수 있는 인터페이스를 제공한다.

3) 데이터베이스 시스템

○ MySQL 데이터베이스를 활용하여 C++ API 및 ODBC를 이용해 표준적합성 시험 관리 도구와 연동한다.

4) Private CA 시스템

○ 시스템 안전성을 위해 X.509 공개키 인증서를 기반으로 사용자 인증, 무결성, 기밀성 등을 제공하기 위해 사용자 각각에게 디지털 ID를 발급한다.

5) S/MIME 시험메시지 송수신 시스템

○ 송수신 시스템 제어 : 시험 대상 제품은 접수 과정에서 발급 받은 E-mail 주소와 디지털 ID를 이용해서 송수신 시스템에 접근할 수 있다.
○ S/MIME 시험 메시지를 송수신한다.
– 메일(SMTP)을 통한 시험 메시지 송수신
○ 접수시 부여받은 메일 주소와 디지털 ID를 통해 전자서명된 시험 메시지를 송신함으로써 인증된 사용자만이 메일을 송수신할 수 있도록 한다.
– 웹(HTTP)을 통한 시험 메시지 송수신
○ 접수시 부여받은 디지털 ID를 이용해 홈페이지에 연결시 SSL 클라이언트 인증을 받음으로써 웹(HTTP)을 통한 송수신이 가능하도록 한다.

6) S/MIME 표준적합성 시험 도구

○ S/MIME v2, v3 시험메시지에 대한 표준적합성 여부를 판정한다.
○ MIME 및 S/MIME 버전 2, 버전 3의 메시지 규격 시험 모듈을 이용하여 메시지 규격을 시험한다.
○ S/MIME 버전 2, 버전 3의 CMS (Cryptographic Message Syntax) 규격 시험 모듈을 이용하여 CMS 규격을 시험한다.
○ S/MIME 버전 2, 버전 3의 인증서 운영 규격 시험 모듈을 이용하여 인증서 관련 사항을 시험한다.

4. 결론

국내 일부 S/MIME 제품들의 표준적합성 모의시험을 수행한 결과, 제품들이 대체적으로 표준을 만족하고는 있지만, 표준을 일정 수준이상 정확하게 구현한 제품은 그리 많지 않았다. 이러한 관점에서 한국정보보호진흥원의 표준적합성 시험은 제품개발 업체 스스로 제품의 문제점을 파악할 수 있는 계기가 되었으며, 이를 통해 보다 질 좋은 제품 개발, 제품들간의 상호운

용성 향상 등에 도움을 줄 것으로 기대된다.

따라서, 사용자에게 편리하고 안전한 전자우편제품을 제공하기 위하여 보다 많은 업체들이 표준적합성 시험에 참여하여 자사제품의 수준을 확인하는 계기가 되기를 기대한다.