전자우편보안

신동명 • TTA 정보보호기술위원회 시스템 및 네트워크보안연구반 위원
한국정보보호진흥원 기술단/기술표준팀 연구원
라은주 • 한국정보보호진흥원 기술단/기술표준팀 연구원
박희운 • TTA 정보보호기술위원회 암호기술연구반 위원
한국정보보호진흥원 기술단/기술표준팀 선임연구원

1. 서론

현재 다수의 정보보호업체에서 보안기능을 갖춘 전자우편 제품을 개발하여 판매 중에 있으나, 제품 개발 업체별로 기술규격이 서로 달라 향후 보안 전자우편 사용자간에 상호 연동문제가 발생할 수 있다. 특히, 국내에서 사용되는 보안 전자우편 제품들은 암호화를 처리하는 방식이 크게 클라이언트기반과 서버기반으로 나누어져 개발 및 출시되고 있으며, 이들간의 호환성에 문제가 발생할 수 있다.

현재 IETF(Internet Engineering Task Force)의 전자우편 보안 표준은 PGP(Pretty Good Privacy)/MIME와 S/MINE(Secure Multipurpose Internet Mail Extension) 두 종류이다. PGP/MIME과 S/MIME은 전자우편 내용과 첨부파일을 함께 보호하도록 설계되어 있으나 두 프로토콜간에 호환성이 없어 수신자나 발신자가 이 가운데 하나를 선택하여 같은 프로토콜로 통일해서 전자우편을 교환해야 한다.

IETF의 S/MIME 표준화활동 및 표준화 전망에 대해서는 "TTA IT Standard Weekly(www.tta.or.kr/weekly)"에서 이광수 교수의 "S/MIME의 표준화" 글을 참고하기 바란다. 본 고에서는 인터넷보안기술포럼(ISTF: Internet Security Technology Forum)의 국내 전자우편 보안 표준화에 대한 내용을 중심으로 서술하고자 한다.

2. 국내 전자우편 보안 표준화

국내 전자우편 보안 표준화는 정보보호 전문가, 전자우편 보안제품 개발업체, 그리고 학계, 그리고 정보통신부 정보이용보호과와 인터넷보안기술포럼 네트워크 분과의 관심업체와 KISIA를 통해 국내 정보보호업체의 참여 희망업체를 중심으로 작업반을 구성하여, 공동으로 표준화 작업이 추진되었다. 기존의 국내 전자우편 제품에서 채택하여 사용하고 있는 규격을 분석하고, 국제표준 규격을 조사분석하여, 전자우편 보안 국내규격으로 적합한 규격을 선정하였고, 선정된 S/MIME v3 규격을 기반으로 표준(안)이 작성되었다.

전자우편 보안 표준화 추진전략으로 다음의 3가지를 설정하였다.

– 국내 · 외 보안 전자우편 제품과 국제표준 규격

을 분석하여 이를 기반으로 보안 전자우편에 대한 국내표준(안)을 제안함으로써, 국내외적인 상호호환성을 보장

- 전자서명법에 의한 국내 공개키 기반구조 기술표준 및 기준을 반영함으로써, 국내 인증서비스와의 상호호환성을 보장
- 전자우편보안 표준(안) 작성을 위해 인터넷보안기술포럼의 네트워크 분과에 참여한 업체를 통해 작업수행

[표 1]에서 ISTF 국내 전자우편 보안 표준 목록과 참조 표준인 IETF의 S/MIME v3 표준 목록을 대응하여 나타내었다. 국내 전자우편 보안 표준은 IETF S/MIME v3의 RFC 문서 규격을 기반으로 표준화의 항목을 결정하고 국내 암호알고리즘을 이용한 규격을 추가로 제시하고 있다.

이 규격은 암호메시지 구문을 기술하며 임의의 메시지를 디지털 서명, 다이제스트, 인증, 암호화하는데 사용한다. 이 구문은 다중 암호화, 즉 하나의 암호화 봉인에 다른 암호화가 중첩되는 것을 허용한다. 암호 메시지 구문 값은 BER-부호화를 사용한 ASN.1을 사용하여 생성된다.

이 규격은 6가지의 콘텐츠 타입 data, signed-data, enveloped-data, digested-data, encrypted-data, authenticated-data를 정의한다. 그러나 이들 중 Data, SignedData, EnvelopedData 콘텐츠 타입만이 현재 S/MIME 메시지 명세서 규격에서 사용되고 있다.

(그림 1)에서와 같이 SEED를 이용한 키싸기 절차에서는 콘텐츠 암호화키 관련 옥텟크기가 SEED의 특성상 16의 배수가 되어야 하는 점과 SEED 고정 IV(초기화 벡터)값이 0x9e3779b97f4a7c15f39cc0605cedc834인 점을 제외하면 3중-DES 키싸기 절차와 동일하다. SEED 고정 IV값은 (SQRT(5) - 1)/2 의 소수 부분을 사용하고 동일한 콘텐츠-암호화 키가 다른 키-암호화 키로 싸여질 때는 새로운 난수 IV를 사용해야 한다. 키풀기 절차는 키싸기 절차의 역순이다.

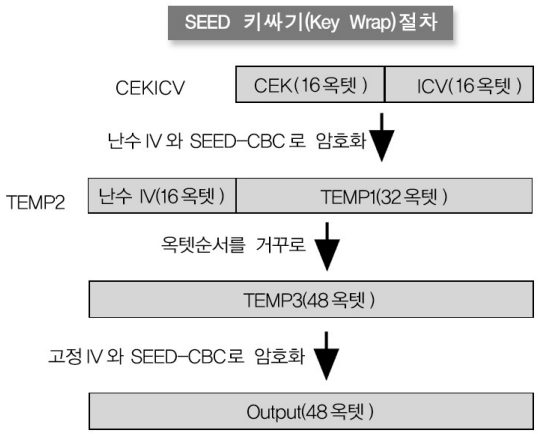
[표 1] ISTF 전자우편 보안 표준 목록

ISTF 표준	내용	참조 표준
ISTF-006	암호 메시지 규격	RFC2630
ISTF-007	Diffie-Hellman 키합의 방식	RFC2631
ISTF-008	S/MIME v3 인증서 운영 규격	RFC2632
ISTF-009	S/MIME 메시지 명세서	RFC2633
ISTF-010	안전한 전자우편을 위한 보안 서비스 확장	RFC2634
ISTF-011	CMS에서 CAST-128 암호화 알고리즘의 사용	RFC2984

3. 국내 전자우편 보안 표준 규격

본 절에서는 IETF 참조 표준과의 차이점을 중심으로 국내 전자우편 보안 표준을 간략히 소개한다. 국내 암호알고리즘 SEED, HAS160, KCDSA의 적용수준과 범위를 기술하고 SEED를 이용한 키싸기(Key Wrap), 키풀기(Key Unwrap)에 대해 소개한다.

3.1 암호메시지 규격(ISTF-006)



(그림 1) SEED 키싸기 절차

암호메시지 규격에서 다이제스트 알고리즘은 SHA-1이 필수사항(MUST)이고, HAS160은 선택(MAY)사항이다. 전자서명 알고리즘에서도 DSA는 필수사항(MUST)이고 KCDSA는 선택사항(MAY)이다. 암호메시지 규격에서 사용하는 암호알고리즘 목록[표 2]와 국내 암호알고리즘에 대한 OID는 다음과 같다.

3.2 Diffie-Hellman 키합의 방식(ISTF-007)

이 규격은 ANSI X9 F1 작업그룹이 개발한 ANSI X9.42에 기초하고 있는 Diffie-Hellman의 변형을 사용한다. Diffie-Hellman은 공유된 비밀에 합의하기 위하여 두 당사자가 이용하는 키 합의 알고리즘이다. 생성된 키는 대칭형 암호화를 위한 키로 사용된다. Diffie-Hellman 변형은 수신자가 인증서를 갖고 있는 것을 요구하나 발신자는 고정된 수명이 짧은 키 쌍을 가질 수 있다.

3.3 S/MIME v3 인증서 운영규격(ISTF-008)

S/IME v3 인증서 규격은 안전한 MIME 메시지를 보내고 받는 방법을 제공한다. 보안 서비스 제공을 위해 공개키를 이용하기 전에, S/MIME 에이전트는 공개키가 유효한지를 검사해야 한다. S/MIME 에이전트는 인터넷 X.509 공개키 인증서와 CRL 프로파

```
id-npki-app-CMSSEEDwrap OBJECT IDENTIFIER ::= { iso(1) member-body(2)
      korea(410) kisa(200004) npki-app(7) 1(smime) 1(alg) 1 }
seedCBC OBJECT IDENTIFIER ::= { iso(1) member-body(2) korea(410)
      kisa(200004) npki-alg(1) 4 }
has160 OBJECT IDENTIFIER ::= { iso(1) member-body(2) korea(410)
      kisa(200004) npki-alg(1) 2 }
kcdsa OBJECT IDENTIFIER ::= { iso(1) member-body(2) korea(410)
      kisa(200004) npki-alg(1) 1 }
```

[표 2] 암호메시지 규격에 사용되는 암호 알고리즘

알고리즘 구현수준	MUST	SHOULD	MAY	비고
다이제스트	SHA-1	MD5	HAS160	
전자서명	DSA	없음	RSA KCDSA	
키관리(키합의)	X9.42 Ephemeral Static DH	없음	없음	
키관리(키전달)	RSA(SEED 콘텐츠 암호화키 전달 포함)	없음	없음	
키싸기(대칭키)	3중DES-3중DES SEED-SEED	RC2-RC2	없음	대칭키 보안 솔루션
콘텐츠 암호화	3중DES-CBC SEED-CBC	RC2-CBC	없음	
메시지 인증코드	HMAC with SHA-1	없음	없음	

일에서 기술된 인증서를 이용해야 하며 추가적으로 이 표준에서 문서화된 인증서 처리 요구사항들을 만족해야 한다. [표 3, 4, 5, 6]에 S/MIME에서 사용하는 인증서 운영규격을 필수항목과 권고항목으로 구분하여 나타내었다.

[표 3] S/MIME v3 인증서 운영규격(1/4)

암호화 메시지 규격	필수항목	권고항목
인증서 폐지	– RFC2459 CRL 규격 – RFC2459 CRL 기반 인증서 폐지여부 검증기능 – 수신된 SMIME 메시지에서 CRL 메시지를 인식기능 – 다중CA 인증기관 인증서 처리기능	수신한 SMIME 메시지에서 CRL을 추출한 후 저장할 수 있는 기능
인증서 선택	SMIME 메시지를 수신한 클라이언트는 반드시 PKIX v1, v3 인증서를 지원해야 함.	사용자 인증서에 인터넷 전자우편 주소 포함
인증서 집합	• 수신 클라이언트는 인증서 체인으로 구성된 인증서 집합 처리(경로 검증부분) • 수신 클라이언트는 DN 기반 체인 지원	• 송신 클라이언트는 자신의 인증서+인증기관 인증서 전송(하나 이상의 인증서 체인) • 수신 클라이언트는 인증서 체인을 처리

[표 4] S/MIME v3 인증서 운영규격(2/4)

대상	필수항목	권고항목
인터넷 메일을 위한 DN 사용	• 수신 클라이언트는 subjectAltName 필드 전자우편 주소를 인식 • 수신 클라이언트는 PKCS#9 emailAddress 속성 내 DN 필드 전자우편 주소를 인식 • 수신 클라이언트는 송신된 메일 주소와 인증서 메일 일치여부 검증 • 사용자나 인증서 발급자의 이름은 S/MIME 인증서 내 포함되어야 함	• 전자우편 주소는 subjectAltName 확장 내 있어야 함 • 송신 클라이언트는 FROM/SENDER 헤더 주소와 서명자 인증서 메일주소가 동일하게 생성되어야 함.
인증서 폐지 목록	• 수신 클라이언트 X.509 v2 CRL 기반 인증서 폐지여부 검증 • 수신 클라이언트 RFC2459 인증서 상태검증 메커니즘을 통해 검증 • 수신 클라이언트는 수신한 S/MIME 메시지 내 CRL 인식	• 인증서 폐지목록 획득 메커니즘 지원 • CRL 저장 메커니즘 지원 • CRL 유효성 검증 메커니즘 지원

[표 5] S/MIME v3 인증서 운영규격(3/4)

대상	필수항목	권고항목
인증서 처리	• 송/수신 클라이언트는 인증서 저장/보호 메커니즘 지원(주소록처럼) • 사용자의 인증서에 메일주소 포함여부	
인증서 체인 검증	인증서, CRL, 체인 검증은 RFC2459 규격을 준용	• 인증서, CRL, 체인 검증은 자동적으로 이루어지도록 해야 함.

대상	필수항목	권고항목
		• 수신한 인증서, CRL, 인증서 경로 검증을 위한 데이터는 캐쉬되며 저장되어야 함.
인증서, CRL 서명 알고리즘	• 수신 클라이언트 : id-dsa-with-sha 지원	• Md2withrsa, md5withrsa, sha-1withrsa 지원

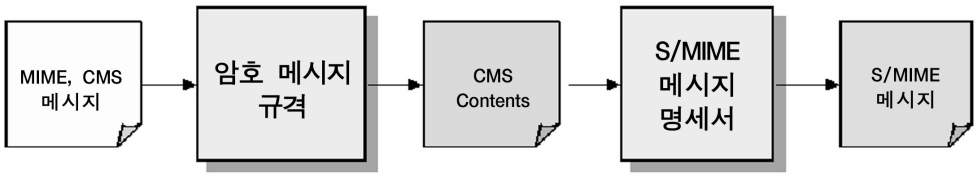
[표 6] S/MIME v3 인증서 운영규격(4/4)

인증서 처리	필수항목	권고항목
인증서 확장	• 사용자 인증서 확장 필드 기본제한필드, 키 사용확장필드, authorityKeyID, subjectKeyID, subjectAltName 지원	• 송/수신 클라이언트는 인증기관, 최상위 인증기관 인증서에 대한 인증서 확장필드 처리 • Critical, Non-Critical 여부 명확
인증서 확장필드	• 키 사용 확장필드가 사용된다면 Critical로 포함되어야 함. • 주체 선택적 이름 확장에서 전자우편 주소표현은 GeneralName 타입 RFC822로 부호화	• CA 인증서 확장필드는 기본 제한 포함, 사용자 인증서 확장필드에는 포함하지 말아야 함. • 키 사용 확장필드가 Diffie Hellman 키 교환 인증서 사용여부 체크

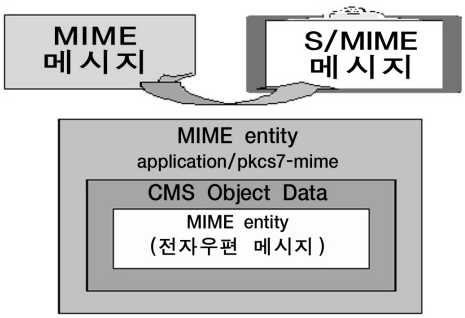
3.4 S/MIME 메시지 명세서(ISTF-009)

S/MIME 메시지 명세서는 MIME 데이터를 안전하게 송수신하는 방법을 제공한다. S/MIME은 기존의 우편서비스 사용자 에이전트(MUA, Mail User Agent)가 송신하는 메시지에 암호서비스를 부가하고 수신받은 메시지의 암호서비스를 해석하는데 사용된다. 그러나, S/MIME의 용도는 전자우편에만 한정되지 않고 HTTP와 같은 MIME 데이터를 전달하는 전송 메커니즘에도 사용된다. 따라서, S/MIME은 MIME의 객체 기반적인 특징을 이용하여 여러 가지 전송 시스템내의 메시지 교환에 사용될 수 있다. 더욱이, S/MIME은 인터넷상에서 전송된 팩시밀리 메시지의 암호화와 같이 사람이 불필요한 암호학적 보안 서비스를 사용하는 자동화된 메시지 전달 에이전트에도 사용될 수 있다.

S/MIME 메시지 명세서는 (그림 2, 3)에서와 같이 암호메시지 규격에 따라 생성된 콘텐츠를 전달하는데 이용하는 application/pkcs7-mime의 MIME 형태를 정의한다.



(그림 2) S/MIME 메시지 생성절차와 표준 규격



(그림 3) application/pkcs7-mime 객체구성

3.5 안전한 전자우편을 위한 보안 서비스 확장(ISTF-010)

이 규격은 S/MIME에 4가지의 선택적인 보안 서비스 확장방법을 기술한다. 이들 서비스는 다음과 같다.

- ○ 서명된 receipt(signed receipts)
- ○ 보안 레이블(security labels)
- ○ 보안 메일링 리스트(secure mailing lists)
- ○ 서명 인증서(signing certificates)

이들 서비스는 서명된 인증서의 반환을 통한 메시지 전달 확인, 사용자 접근권한 비교를 통한 메시지 접근통제, 다수의 수신자에게 봉인 메시지의 배포, 인증서 대치 공격을 막기 위한 서명 인증서에 대해 기술하고 있으며, 상업 및 금융 관련 등의 업무환경에 유용한 기능을 제공한다.

이 규격에 기술된 서비스들은 S/MIME v3의 확장으로 일부분은 S/MIME v2에도 적용될 수 있다. 이 규격에 기술된 확장방법에 관계없이 S/MIME v3의 사용자는 S/MIME v2의 사용자로부터 전자우편을 받을 수 있다.

3.6 CMS에서 CAST-128 암호화 알고리즘의 사용(ISTF-011)

이 규격은 대칭키 암호화를 위한 추가 알고리즘 명세로써, CAST-128(RFC2144)을 암호메시지 규격에 포함시킬 수 있도록 관련 OID와 처리단계가 제공된다.

현재 S/MIME v3 명세에서 내용 암호화와 키 암호화를 위한 의무구현 대칭알고리즘은 삼중-DES(3DES)이다. 3DES의 안전성이 일반적으로 높지만 몇몇 환경에서는 3DES가 너무 느린 수행속도를 제공하기 때문에 이와 같은 문제를 해결하기 위해, S/MIME은 내용과 키의 대칭키 암호화를 위해 사용될 수 있는 임의의 개수의 추가적인 알고리즘을 허용한다.

CAST-128 암호 알고리즘[RFC2144]은 비교적 높은 수행속도와 가변길이 키 길이(40 비트에서 128 비트까지)를 제공하며 로열티없이 상업적인 또는 비상업적인 사용에 대해 자유롭게 사용할 수 있다.

4. 결론

국내 전자우편 보안 표준 규격은 2002년 2월에 인터넷보안기술포럼(ISTF) 표준이 되었고 2002년 2월에 TTA 표준(안)으로 상정하여 심의중이다.

국내표준(안) 규격이 S/MIME v3을 기준으로 제정되었고 현재 국내의 많은 전자우편 보안 개발업체들이 S/MIME v2를 기준으로 개발하였으나, 곧 v3로 이행할 것으로 보인다. 대표적인 마이크로소프트 아웃룩 2000의 경우에도 S/MIME v3을 지원하고 있다. S/MIME v3에 기초한 국내 전자우편 보안 표준을 활용하여 국내 전자우편 보안 제품간의 상호연동성을 높이고, 국내 공인인증서의 활성화를 통해 글로벌한 보안 전자우편 사용의 활성화 및 시장확대, 국내제품의 활발한 해외진출을 꾀할 수 있을 것으로 예상된다. 또한 한국정보보호진흥원에서는 국

내 전자우편 보안 표준 규격에 따라 적합하게 개발되었는지 검증할 수 있는 표준 적합시험 방법론 및 도구 개발과 상호운용성 시험 테스트베드 구축을 위한 방법론 개발 등 표준 기술의 보급 및 활성화를 위한 연구가 진행되고 있다.

참고문헌

1. 한국정보보호진흥원, "전자우편 보안 표준화 연구", 2001. 11.
2. 신동명, "전자우편 보안 국내표준 소개", IT FORUM KOREA 2002 기술발표 세션 8-1, 2002. 4.
3. http://www.istf.or.kr/ : 인터넷보안기술포럼
4. ISTF-006 : 암호 메시지 규격, 2002. 2.
5. ISTF-007 : Diffie-Hellman 키합의 방식, 2002. 2.
6. ISTF-008 : S/MIME v3 인증서 운영규격, 2002. 2.
7. ISTF-009 : S/MIME 메시지 명세서, 2002. 2.
8. ISTF-010 : 안전한 전자우편을 위한 보안 서비스 확장, 2002. 2.
9. ISTF-011 : CMS에서 CAST-128 암호화 알고리즘의 사용, 2002. 2.
10. http://www.ietf.org/html.charters/smime-charter.html : IETF S/MIME 작업그룹
11. http://www.tta.or.kr/weekly/weekly_contents.jsp?id=67 : TTA IT Standard Weekly
12. 한국정보보호진흥원, "보안 웹 메일 솔루션 개발 현황", 정보보호뉴스 8월호, 2001. 8.

정통부, 매체별 HDTV방송 호환성 연구 10월까지 진행

지상파, 유선, 위성 HDTV 방송의 호환성 및 전송방안에 관한 정책 연구과제가 정보통신부 방송위성과 주도로 오는 10월까지 이뤄진다. 정보통신부는 5월 말부터 가전 3사와 셋톱박스 개발업체, 한국디지털위성방송(스카이라이프), 케이블방송협회 등 10여 개 기업 및 기관이 참여하는 매체별 HDTV 방송의 전송 및 호환 방안 연구과제를 진행한다고 5월 17일 밝혔다. 6개월간 진행될 이 과제에서는 △지상파 HDTV 방송의 케이블 및 위성방송을 통한 재전송시 기술적 · 제도적인 문제점 분석 및 해결방안 연구 △매체별 HDTV 전송 및 호환 관련 기술개발 및 상용화 현황조사 및 분석 △HDTV 디코더의 매체간 통합가능성 등이 집중 연구된다. 이같은 움직임은 지상파, 유선, 위성 방송의 매체별 HDTV 전송 관련 표준 및 기술방식이 상이해 발생하는 매체간 HDTV 방송의 전송 및 호환 문제를 해결할 필요가 있다는 지적에 따른 것이다. 정통부 관계자는 "이번 연구과제를 통해 지상파 HDTV 재전송을 위한 최적의 방안을 제시하고 HDTV 전송시 방송매체간 위상을 정립, 디지털방송의 조기정착에 기여할 것으로 기대하고 있다"고 말했다.