情 報 保 護 學 會 誌
第 14 券 第 2 號, 2004. 4

X.509 인증서내 식별번호를 이용한 본인확인기술 표준화 동향

박 종 욱*, 김 승 주**, 이 재 일*, 이 홍 섭***

요 약

식별번호를 이용한 본인확인기술(SIM : Subject Identification Method) 표준(안)은 국내 보안분야로는 처음으로 IETF PKIX 워킹그룹에서 논의되고 있는 순수 국내 보안기술로 연내 IETF 공식표준문서(RFC)로 채택될 가능성이 높다. 동 기술은 PKI 기반의 전자서명인증서비스에서 동일한 이름을 갖는 개인 사용자나 유사한 법인명을 갖는 법인사업자가 겪을 수 있는 본인확인의 오류를 원천적으로 방지하여 인증서 소유자의 신원을 유일하게 확인할 수 있는 방안을 제공한다. 본 고에서는 관련 국외 동향을 고려하여 SIM 표준(안)의 보안요구사항, 프로토콜, 표준화 주요 쟁점 및 진행 상황을 고찰하고자 한다.

Ⅰ. 서 론

일반적으로 인증기관은 신원확인용 X.509 인증서를 발급하는 시점에, 인증서 소유자 명칭을 포함하는 개인식별정보를 인증서 소유자(subject) 필드나 소유자 대체명칭(subjectAltName) 필드에 가입자별로 유일하게 할당하여야 한다. 그러나, 현실세계에서는 동일한 이름을 갖는 개인이나 유사한 명의의 법인이 존재하므로 전자거래기관이 인증서를 이용하여 소유자의 본인여부를 확인하는 경우, 인증서만으로는 접근통제(access control), 부인방지(non-repudiation), 감사기록(audit records) 등의 서비스에서 소유자에 대한 신원확인을 정확하게 수행하기 어렵다. 이러한 오류상황은 동일한 가입자가 여러 인증기관으로부터 서로 다른 소유자명을 갖는 여러 인증서를 발급 받거나, 소유자의 조직내 잦은 부서 이동, 이메일 주소 변경, 시스템의 IP나 DNS 명칭 변경 등과 같이 개인식별정보로 이용될 수 있는 정보가 쉽게 변경되지만 실시간으로 인증서에 반영되기 어려운 경우에도 발생한다. 상기 결과의 원인은 일차적으로 소유자의 명칭을 인증서에 나타내는 방법으로 고유이름(Distinguished Name, DN), IP주소, DNS, E-mail 주소 등 표현형식이 다양하지만 정작 실세계의 소유자 명칭을 실시간으로 정확히 나타낼 수 있는 완전한 해결책이 없다는 데에 있다. 또한, 다양한 표현형식사이의 관계 및 연결성을 판단할 수 있는 효율적인 방법이 없기 때문이다. 더구나 익명성을 보장하고 있는 사이버세계에서는 가입자의 명칭을 손쉽게 변경할 수 있으므로 향후 가입자 신원확인시 어려움이 증대되리라는 예상을 손쉽게 할 수 있다. 무엇보다도 이러한 상황은 인증기관 및 전자거래서비스기관의 명확한 인증정책 수립, 관련 표준규격의 프로파일화, 구현비용 투자라는 문제점을 발생시켜 궁극적으로 인증서비스의 신뢰성과 활성화를 저해할 수 있는 요소로 작용할 수 있다. 이에 대한 보완책으로 인증서 소유자의 식별정보가 변경되더라도 변하지 않는 식별정보를 인증서에 포함시키는 항구식별자(PI: Permanent Identifier) 개념이 IETF의 공개키기반구조 워킹그룹(PKIX, Public Key Infrastructure on X.509)에서 제안되었다. 그러나 보호되어야 하는 민감한 개인정보가 PI로 이용될 경우, 불특정 다수에게 개인정보가 공개될 수 있으므로 PI는 개인 프라이버시 보호를 위한

* 한국정보보호진흥원 전자거래보호단 ({khopri, jilee}@kisa.or.kr)
** 성균관대학교 정보통신공학부 (skim@ece.skku.ac.kr)
*** 인터넷보안기술포럼(ISTF) 의장 (hslee@kisa.or.kr)

효과적인 메커니즘이 될 수 없다. 본 고에서는 암호학적으로 보호된 개인정보를 인증서에 포함시켜 PI의 취약점을 보완하고 소유자를 정확히 영구 식별할 수 있는 PEPSI (Privacy-Enhanced Permanent Subject Identifier) 개념을 제시하는 SIM표준(안)을 소개하고자 한다. 동 기술은 이미 국내 공인인증서비스에 적용되고 있어 국내 인증서 사용자들은 인터넷상에서 인증서를 이용한 본인 확인시 사용되는 자신의 주민등록번호 또는 법인등록번호를 노출하지 않고 안전하게 관련 식별정보를 관리할 수 있게 되어 신뢰성있고 편리한 인증서비스를 제공받고 있다. 아울러 상기 SIM 표준(안)은 2002년 11월 미국 애틀란타에서 개최된 제 55차 IETF회의에서 국내 처음으로 PKIX 워킹그룹의 드래프트 문서로 채택되었다. 특히 2003년 11월의 제58차 회의에 이어 올해 3월 서울에서 열린 제 59차 IETF 회의에서는 첫 번째 논의 안건으로 채택될 만큼 비중 있는 표준화 항목으로 활발한 논의가 진행 중에 있으며 연내 IETF RFC 채택이 무난할 것으로 기대된다. 본 고에서는 먼저 인증서를 이용한 본인확인 기술에 대한 관련 국외 동향을 살펴보고, SIM표준(안)의 보안요구사항, 프로토콜, 표준화 진행 상황 및 주요 표준화 쟁점을 소개하고자 한다.

II. 관련 동향

1. 인증서 소유자명 표시 방법[1,2,3,4,5]

전술한 바와 같이 인증서 소유자명은 인증서 기본 필드의 소유자명(Subject) 필드의 DN이나 소유자대체명칭(SubjectAltName) 확장필드의 General Name 형태로 표현된다. 인증서 소유자명 필드에 나타나는 DN은 X.501, X.520, RFC2256에 정의되

〔표 1〕 DN 속성 정의

속성명	OID[1]	속성 약칭[2]	최대 길이[3]	ASN.1 스트링 타입
commonName	{id-at 3}	CN	64	DirectoryString[4]
surName	{id-at 4}	SN	64	DirectoryString
serialNumber	{id-at 5}	SERIALNUMBER	64	PrintableString
countryName	{id-at 6}	C	2	PrintableString(SIZE(2))
localityName	{id-at 7}	L	128	DirectoryString
stateOrProvinceName	{id-at 8}	S	128	DirectoryString
streetAddress	{id-at 9}	ST	128	DirectoryString
organizationName	{id-at 10}	O	64	DirectoryString
organizationalUnitName	{id-at 11}	OU	64	DirectoryString
title	{id-at 12}	T	64	DirectoryString
businessCategory	{id-at 15}	-	128	DirectoryString
givenName	{id-at 42}	GN	64	DirectoryString
initials	{id-at 43}	I/INITIALS	64	DirectoryString
generationQualifier	{id-at 44}	-	64	DirectoryString
uniqueIdentifier	{id-at 45}	-	64	BIT STRING
dnQualifier	{id-at 46}	-	64	PrintableString
pseudonym	{id-at 65}	PSEUDO	64	DirectoryString
domainComponent	0.9.2342.19200300.100.1.25	DC	64	IA5String
emailAddress	1.2.840.113549.1.9.1	MAIL	128	IA5String
rfc822MailBox	0.9.2342.19200300.100.1.3	MAIL	128	IA5String

1) Object Identifier, 오브젝트 식별자
2) 속성 약칭은 대소문자를 구분하지 않음
3) DN의 최대길이는 256 바이트로 권고함
4) DirectoryString으로 표현되는 DN 속성값은 RFC3280을 준용하여 2003년 12월 31일 이후에는 해당 속성값을 UTF8 스트링(UTF8String)으로 표현함
※ id-at OBJECT IDENTIFIER::= {joint-iso-itu(2) ds(5) attribute(4)}

어 있다. DN은 하나 이상의 RDN(Relative DN)이 순서를 가지고 구성되어야 한다. DN으로 사용되는 Name의 ASN.1 형식은 그림 1과 같으며 각각의 RDN은 표 1에서 정의되는 속성을 준용해야 한다. DN의 문자열 표현시 각각의 RDN은 ','로 구분된다. 하나의 RDN은 속성타입과 속성값으로 표현되며 '속성타입 = 속성값'과 같이 '='로 연결되는데, 만일 다중값(multi-valued) RDN을 사용하는 경우에는 "OU=Sales+CN=J"와 같이 각각의 속성타입과 속성값이 '+'로 결합되어야 함에 주의해야 한다. 속성타입은 표 1에서 정의된 속성약칭을 사용하며 속성약칭이 정의되지 않은 속성타입은 속성명 자체를 사용해야 한다. DN의 문자열 표현시 RDN 속성값은 RFC 2253을 준용하여 UTF8 스트링으로 표현해야 한다. "CN=John, Smith"와 같이 DN 값에 특수문자(,)를 포함하는 경우에는 "CN=John\, Smith"처럼 '\'를 특수문자 앞에 명시하여 이스케이프(escape) 처리해야 한다.

한편, 인증서 소유자의 추가적인 명칭을 나타내기 위해서는 인증서 소유자대체명칭 확장필드의 GeneralName 필드를 사용한다. GeneralName은 DN을 비롯하여 E-mail주소, DNS, IP주소, URI주소, OtherName 등 총 9개의 서로 다른 명칭 형식을 포함할 수 있는 확장성 있는 구조이다. GeneralName의 ASN.1 정의는 그림 2와 같다.

2. 국외 인증서내 신원확인 기술동향

국외의 경우 본인확인을 위해 인증서내 포함되는 신원확인정보를 크게 개인정보로 취급하여 암호학적 처리를 하거나 그렇지 않은 경우로 구분된다. 또한 신원확인정보를 넣는 방법은 크게 (1) 인증서 소유자 대체명칭 확장필드 활용 (2) 새로운 인증서 사설확장필드 정의 (3) 인증서 소유자명 필드내 DN 확장으로 표현하는 세 가지 방법으로 나뉠 수 있다.

1.1 IETF의 항구 식별자(Permanent Identifier)[6]

PI는 2000년 5월 IETF PKIX 워킹그룹에 첫 제안된 이후 2001년 10월 드래프트 문서의 심의허용기간이 자동 만료되어 더 이상 표준화가 진행되지 않았으나 워킹그룹 멤버들의 요청으로 2002년 2월 다시 표준화 작업을 재개하였다. PI는 공개키 소유자에 대한 유일한 이름을 부여하기 위한 영구 식별자로 서로 다른 개인식별정보에 대한 하나의 특정 명명규칙은 정의하지 않는다. 그 대신 PI를 생성하는 신뢰된 기관이 전 세계에 걸쳐 고루 분포한다는 점과 매우 많은 식별번호 형식의 다양성을 고려하고 있다. 즉, PI는 특정 PI형식의 값 생성 및 검증절차에 대한 관리기관을 지칭하는 오브젝트 식별자(OID)인 IdentifierType과 PI 관리기관이 부여하는 형식의 값을 담고 있는 IdentifierValue의 2개의 세부필드로 구성된 확장성 있는 구조이다. PI는 인증서 소유자 대체명칭 확장필드의 OtherName 형식에 포함된다.

```
PermanentIdentifier ::= SEQUENCE {
  identifierValue    UTF8String,
  identifierType     OBJECT IDENTIFIER
                     OPTIONAL
}
```

```
Name ::= CHOICE { RDNSequence }

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {
      type    AttributeType,
      value   AttributeValue }

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType

DirectoryString ::= CHOICE {
      teletexString          TeletexString (SIZE (1..MAX)),
      printableString        PrintableString (SIZE (1..MAX)),
      universalString        UniversalString (SIZE (1..MAX)),
      utf8String             UTF8String (SIZE (1..MAX)),
      bmpString              BMPString (SIZE (1..MAX)) }
```

〔그림 1〕 X.501 타입 Name의 ASN.1 정의

```
GeneralName ::= CHOICE {
      otherName                 [0]   OtherName,
      rfc822Name                [1]   IA5String,
      dNSName                   [2]   IA5String,
      x400Address               [3]   ORAddress,
      directoryName             [4]   Name,
      ediPartyName              [5]   EDIPartyName,
      uniformResourceIdentifier [6]   IA5String,
      iPAddress                 [7]   OCTET STRING,
      registeredID              [8]   OBJECT IDENTIFIER }
OtherName ::= SEQUENCE {
      type-id       OBJECT IDENTIFIER,
      value  [0]    EXPLICIT ANY DEFINED BY type-id }
EDIPartyName ::= SEQUENCE {
      nameAssigner [0]    DirectoryString    OPTIONAL,
      partyName    [1]    DirectoryString }
```

〔그림 2〕 GeneralName ASN.1 정의

그러나, PI는 identifierValue로 삽입될 수 있는 개인식별정보에 대한 암호학적 처리를 고려하고 있지 있다. 부연하면 UTF8String으로 표현되는 identifierValue는 암호학적 처리가 된 정보를 나타내기에 적절한 OCTET STRING이 아니므로 개인식별정보를 나타내기에는 부적절한 데이터 형식이다. 또한 개인식별정보 자체를 그대로 identifierValue의 값으로 사용할 경우, 개인 프라이버시 침해의 우려가 높게 된다. 마지막으로 클라이언트의 부담측면에서 보면 PI는 OID로 구성된 identifierType만을 보고는 특정 PI 부여기관의 PI생성절차 및 검증방법을 직관적으로 알 수 없으므로 해당 값을 처리하기 위해서는 특정PI 부여기관에 대한 추가적인 정보획득이 요구되므로 PI 메커니즘은 클라이언트에게 상당한 처리부담을 줄 수 있는 단점이 있다.

1.2 호주의 ABN-DSC[7]

호주 연방은 1999년 12월, 국가 PKI 프로젝트(GateKeeper)와 호환성을 유지하면서 대국민 전자정부 서비스에서 사용되는 11자리 또는 12자리의 호주 법인식별번호를 포함하는 법인용 본인확인 인증서(ABN-DSC, Australia Business Number - Digital Signature Certificate)를 발급하고 있다. ABN-DSC는 GateKeeper에서 지정한 beTRUSTed, Telstra, eSign Australia의 3개 인증기관만이 발급할 수 있는데 본 인증서는 B2G 또는 B2B 거래에만 적용되며 C2C 거래에는 적용이 배제되고 있다. 현재 호주 국세청(ATO) 및 금융권 분야에서 적용되고 있으며 향후 지역정부 및 지방자치단체 분야까지 확장시킬 예정으로 있다.

ABN-DSC는 호주 NOIE가 주도적으로 호주 표준협회(Standard Australia)와 협조하여 인증서 소유자대체명칭 확장필드와 같은 기존의 표준 확장필드를 활용하는 대신 SubjectABN이라는 새로운 사설 인증서 확장필드를 정의하고 있다. 그러나 국제 표준인 X.509 인증서와 호환성을 유지하기 위해 사설 확장필드의 critical 여부를 non-critical로 설정하여 본 확장필드를 제대로 인식하지 못하는 클라이언트의 경우에도 에러 처리에 문제가 없도록 하고 있다. SubjectABN 사설확장필드는 {iso(1) iso-member-body(2) australia(36) noie(001) gatekeeper(333) abn(1)}값을 갖는 id-pe-au-noie-subjectABN 오브젝트식별자와 법인식별번호를 평문형태의 IA5String형식으로 그대로 저장하고 있는

```
841 30   15:         SEQUENCE {
843 06    3:           OBJECT IDENTIFIER keyUsage (2 5 29 15)
848 01    1:           BOOLEAN TRUE
851 04    5:           OCTET STRING, encapsulates {
853 03    3:               BIT STRING 0 unused bits
                             '000000000000000001'B (bit 0)
                           }
                         }
858 30   23:         SEQUENCE {
860 06    6:           OBJECT IDENTIFIER '1 2 36 1 333 1'
868 04   13:           OCTET STRING, encapsulates {
870 16   11:             IA5String '12345678912'
                           }
                         }
                       }
                     }
883 30   11:   SEQUENCE {
885 06    7:     OBJECT IDENTIFIER dsaWithSha1 (1 2 840 10040 4 3)
894 05    0:     NULL
                 }
896 03   47:   BIT STRING 0 unused bits, encapsulates {
899 30   44:       SEQUENCE {
901 02   20:         INTEGER
                       27 63 23 22 E6 FF 65 79 6E 79 DB 02 A5 32 3E F7
```

〔그림 3〕 ABN-DSC의 SubjectABN 확장필드

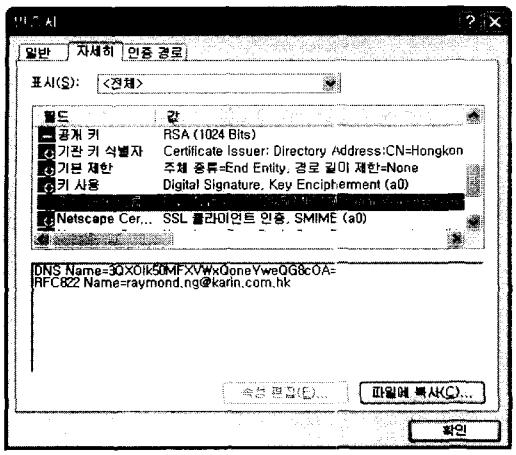
ABNInfo로 구성되어 진다. 그림 3은 ABN를 포함한 인증서의 SubjectABN 사설확장필드를 디코딩한 예를 보여준다.

1.3 홍콩의 HKID[8]

홍콩의 e-post는 국내의 주민등록번호와 유사한 9자리로 이루어진 개인식별정보인 HKID(HongKong Identity Card No.)의 해쉬값을 인증서의 소유자 대체명칭 확장필드에 삽입함으로써 가입자의 본인확인과 X.509 표준 인증서와의 호환성을 위한 기술적 토대를 동시에 마련해 놓고 있다. 그러나 호주의 ABN-DSC와 달리 HKID를 소유한 개인용 인증서를 대상으로 하며 법인용 또는 서버용 인증서는 제외하고 있다. HKID는 먼저 SHA-1 알고리즘으로 해쉬된 후 가입자의 RSA 전자서명키로 전자서명된다. 여기에 SHA-1 해쉬 알고리즘을 한번 더 적용하여 나온 결과값인 cert_hkid_hash가 그림 4와 같이 소유자 대체명칭 확장필드의 DNSname 필드에 저장된다.

$$cert\_hkid\_hash = SHA\text{-}1(RSA_{privatekey}, SHA\text{-}1(hkid\_number))$$

구체적으로 cert_hkid_hash의 생성방법은 가입자의 키 생성위치 및 주체에 따라 다소 다르다. 만일 가입자 소프트웨어에서 가입자의 키가 생성되는 경우 가입자는 cert_hkid_hash 생성을 위한 임시값인 $RSA_{privatekey}$, SHA-1 (hkid_number)값을 안전한 채널을 통해 인증기관에 보낸다. 그러면 인증기관을 다시 이를 해쉬하여 완전한 cert_hkid_hash를 구한 후 인증서에 삽입하게 된다. 그러나 인증기관이 가입

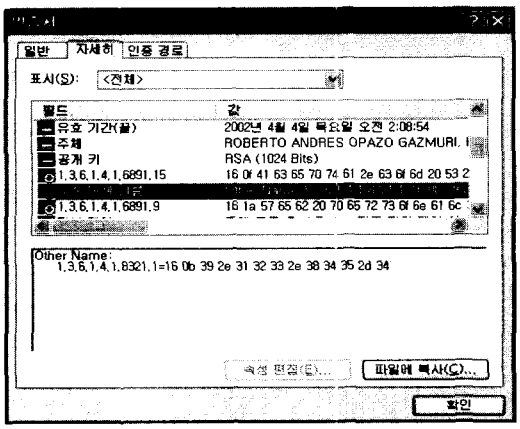


〔그림 4〕 홍콩의 HKID가 포함된 인증서

자의 전자서명키를 대리생성하는 경우에는 가입자의 개입없이 인증기관이 완전한 cert_hkid _hash값을 생성할 수 있다. 그러나 이 인증서를 이용하여 인증서 소유자에 대한 본인확인을 수행하는 신뢰당사자는 검증시 인증서내에 포함된 cert_hkid_hash값을 안전한 채널을 통해 미리 획득하거나 인증기관의 도움이 필요하다. 또한 공개키 연산을 통한 전자서명 검증이 필요하므로 무선PKI, 스마트카드 등 저전력 및 제한된 리소스 자원을 갖는 환경에 그대로 적용하기 어렵다. 또한 개인식별정보를 DNS서버의 주소를 나타내는 목적으로 정의된 DNSname 필드에 삽입한 점은 엄밀한 의미에서 표준과 부합한다고 말하기 어렵다.

1.4 칠레의 RUN[9]

칠레 정부 또한 자국의 개인식별번호로 이용되는



〔그림 5〕 칠레의 RUN이 포함된 인증서

RUN (Rol Unico Nacional)를 인증서에 포함시켜 전자거래시 본인확인을 위한 용도로 사용하고 있다. RUN은 소유자 대체명칭 확장필드내 General Name의 OtherName 필드에 포함되어 인증서 표준과 호환성을 유지한다. 그러나 호주의 ABN-DSC와 마찬가지로 RUN 정보를 있는 그대로 표시하므로 오용될 경우 개인정보침해의 우려가 높다. 그림 5는 RUN 정보를 포함하고 있는 인증서를 나타내는데 여기서 1.3.6.1.4.1.8321.1은 RUN 정보임을 나타내는 오브젝트 식별자이며 RUN 정보자체는 ASN.1 인코딩 태그값 16을 갖는 시퀀스 구조로 이루어진다.

1.5 스웨덴의 Personal Number[10]

스웨덴은 전자주민카드에 포함되는 인증서 프로파일을 정의하고 있는 자국의 SS 61 43 31표준을 통해 본인확인을 위한 방법을 정의하고 있다. 즉, 개인식별번호인 Person Number를 DN의 serial Number 속성에 할당하여 DN의 유일성을 보장하는 방법을 사용하고 있다. 그림 6은 C=SE,surname=Ericsson,given Name=Maria,serialNumber=196212173148를 ASN.1 인코딩한 예를 나타내고 있다. 이 경우 serialNumber의 속성값은 Printable String으로 표현된다. 그러나 이러한 방법 역시 다른 국외 사례와 마찬가지로 개인식별번호가 인증서 소유자명 필드에 그대로 드러나는 문제점이 있다.

```
                        -- Subject Name:
30 47                   -- SEQUENCE OF (RelDistName)
  31 0B                 -- SET OF (AttValueAssertion)
    30 09               -- SEQUENCE
      06 03             -- OBJECT IDENTIFIER
        55 04 06        -- Country
      13 02             -- PRINTABLE STRING
        53 45           -- "SE"
  31 11                 -- SET OF (AttValueAssertion)
    30 0F               -- SEQUENCE
      06 03             -- OBJECT IDENTIFIER
        55 04 04        -- Surname
      13 08             -- PRINTABLE STRING: "Ericsson"
        45 72 69 63 73 73 6F 6E --
  31 0E                 -- SET OF (AttValueAssertion)
    30 0C               -- SEQUENCE
      06 03             -- OBJECT IDENTIFIER
        55 04 2A        -- Given name
      13 05             -- PRINTABLE STRING
        4D 61 72 69 61  -- "Maria"
  31 15                 -- SET OF (AttValueAssertion)
    30 13               -- SEQUENCE
      06 03             -- OBJECT IDENTIFIER
        55 04 05        -- Serial Number
      13 0C             -- printable string
        31 39 36 32 31 32 31 37 33 31 34 38 --
                        -- "196212173148"
```

〔그림 6〕 스웨덴 인증서의 소유자명 DN

표 2에서는 전술한 IETF 및 각 국의 본인확인 기술동향을 요약 비교하였다.

〔표 2〕 각 국의 본인확인 기술 동향 비교

	식별정보	개인 여부	인증서내 위치	표준 호환성
PI	OID에 따라 다양	×	소유자대체명칭 확장필드	-
호주	ABN	×	사설확장필드	O
홍콩	HKID	O	소유자대체명칭 확장필드	△
칠레	RUN	×	소유자대체명칭 확장필드	O
스웨덴	Person Number	×	소유자 명칭 필드(DN)	O

Ⅲ. 식별번호를 이용한 본인확인기술 표준[11,12]

1. 개요

SIM 표준(안)은 인증서내 소유자 명칭 또는 소유자대체명칭이 서로 다른 다양한 형식으로 표현되거나 불가피하게 자주 변하더라도 가입자를 영구 식별할 수 있는 PEPSI 개념을 제안하여 전자거래시 발생할 수 있는 본인확인 오류 문제의 대한 효과적인 해결책이다. PEPSI는 개인의 주민등록번호 또는 법인의 사업자등록번호와 같은 식별번호를 가입자만이 알 수 있는 비밀정보인 패스워드와 등록기관이 생성한 비트열 난수를 함께 두 번 해쉬한 결과로 가입자를 영구적으로 구별할 수 있도록 한다. 더욱이 SIM표준(안)은 국외 관련 기술과 달리 단지 PEPSI를 소유하고 있다는 사실만을 증명할 수 있게 함으로써 사용자 프라이버시를 보장할 수도 있다. 예를 들어 운전면허번호를 PEPSI로 사용하는 경우, 소유자는 운전면허번호를 숨기고 운전면허가 있다는 사실만을 증명할 수 있어 개인정보 보호의 중요성이 날로 증대되어 가는 현 시점에서 현실적인 대안을 제시한다. 특히 현재 많은 응용 서비스들이 주민등록번호와 같은 가입자 식별정보로 구축된 데이터베이스를 기반으로 제공되고 있는 점을 감안할 때 주민등록번호를 가공된 형태로 인증서에 포함하는 것은 기존에 제공되는 서비스와의 연계를 수월하게 하는 장점이 있다. 또한 PEPSI는 인증서의 소유자 대체명칭 확장필드의 OtherName에 포함됨으로 관련 세계 표준인 ITU-T X.509나 IETF PKIX 표준과 호환성을 유지한다.

2. 보안 요구사항

먼저 PEPSI의 생성·검증절차에 참여하는 구성요소는 다음과 같다.

- Alice : 자신의 식별번호를 포함한 인증서 소유자
- Bob : 가입자의 식별번호에 대한 정확성을 검증하여 가입자 본인확인을 수행하는 전자거래기관과 같은 신뢰당사자
- Eve : 거짓 식별번호와 획득한 Alice의 인증서로 자신의 신분을 위장하는 공격자
- RA : 가입자에 대한 오프라인 신원확인과 인증서 발급단계에서 가입자의 식별번호를 접수받는 등록기관
- CA : 가입자의 식별번호를 삽입한 인증서를 발급하는 인증기관

SIM 표준(안)은 Alice가 선택하는 패스워드를 이용하여 다음에 가정하는 보안요구사항을 만족하는 PEPSI를 설계한다.

① Alice는 Bob에게 인증서에 포함된 자신의 식별번호가 정확한지를 증명할 수 있어야 한다.

② Alice가 보안성이 약한 패스워드를 사용한다 할지라도 Eve가 Alice의 인증서로부터 그녀의 식별번호를 유추해 내기 위해서는 상당한 계산량이 요구되어져야 한다. 만일 Alice가 암호학적으로 안전한 패스워드를 사용한다면 매우 큰 계산량이 요구되어진다.

③ 만일 Eve가 Alice의 PEPSI를 생성하는데 사용된 식별번호를 찾아낸다 할지라도 다른 사용자의 PEPSI로부터 해당 사용자의 식별번호를 찾아내는데 아무런 도움이 되지 말아야 한다.

④ Alice가 올바른 PEPSI를 생성하는 거짓 식별번호나 패스워드를 사전 계산할 수 없도록 해야 한다. 이는 PEPSI 생성에 사용되는 입력값의 생성이 전적으로 Alice에게 맡겨져서는 안됨을 의미한다.

⑤ 선택사항으로 CA가 Alice의 식별번호나 패스워드를 알 수 없어야 한다. CA가 모든 사용자의 식별번호나 패스워드를 직접 관리하는 중앙 집중적인 PKI구조는 CA에 대한 집중공격이 일어날 수 있는 가능성이 높으므로 때로 민감한 가입자의 등록정보는 RA가 관리하도록 분산시키는 구조가 적절하다.

추가적으로 관련 표준 및 PKI-aware 상용 제품과의 호환성을 위해 다음 2가지의 요구사항을 만족해야 한다.

⑥ Alice의 PEPSI 정보는 인증서의 소유자 대체명칭확장필드에 포함되어야 한다. 이 때 소유자 대체명칭확장필드의 critical 여부는 non-critical로 설정되어야 한다.
⑦ PEPSI는 MS의 인터넷 익스플로러, 아웃룩 익스프레스 및 넷스케이프의 웹브라우저 등 PKI 지원 프로그램에서 동작하는데 문제가 없음을 보장해야 한다.

3. PEPSI 생성 절차

3.1 기호 및 약어

SIM 표준(안) 전반에 걸쳐 사용되는 암호학적 기호 및 약어에 대한 설명은 다음과 같다.

- P : 인증서 소유자가 인증서 발급신청시 선택한 패스워드
- R : 등록기관(RA)이 생성한 160 비트 난수열
- SII : Sensitive Identification Information, 우리나라의 주민등록번호나 미국의 사회보장제도번호(Social Security Number)와 같은 개인식별번호
- SIItype : SII를 구별하기 위한 오브젝트 식별자(OID)
- H() : 암호학적으로 안전한(Cryptographically Secure) 해쉬함수
- PEPSI : P, R, SIItype, SII의 연접된 값을 연속적으로 두 번 해쉬한 값
- E() : CA 공개키 인증서에 포함되어 있는 공개키 암호 알고리즘으로 PEPSI를 암호화
- EPEPSI : 암호화된 PEPSI (Encrypted PEPSI)
- D() : E()에 사용된 공개키 암호 알고리즘으로 EPEPSI를 복호화

3.2 PEPSI 생성 절차 요약

3.1에서 전술한 보안요구사항을 만족하기 위해서 PEPSI=H(H(P‖R‖SIItype‖SII))와 같이 정의하며 생성 및 검증 절차는 다음과 같이 요약된다.

① Alice는 자신이 선택한 패스워드 P, 식별번호타입 식별자 SIItype, SIItype에 해당하는 SII를 RA에게 안전하게 전송한다.
② RA는 Alice가 보낸 SII의 정확성을 검증한다.
③ RA는 160비트 난수열 R을 생성한다.
④ RA는 Alice의 PEPSI=H(H(P‖R‖SIItype‖SII))를 생성한 후 이를 SIM = R‖PEPSI의 형태로 변환한다.
⑤ RA는 SIM를 CA에게 전송한다.
⑥ 선택사항으로 CA가 Alice의 SII를 알고자 하는 경우 RA는 EPEPSI = E(SII‖SIM)를 CA에게 보낸다.
⑦ 선택사항으로 CA는 D(EPEPSI)를 하여 SII, SIM를 구한 후, SII의 정확성을 검증한다.
⑧ CA는 SIM를 Alice 인증서의 소유자대체명칭확장필드의 OtherName형식으로 넣은 인증서를 발급한다.

4. PEPSI 검증 절차

PEPSI를 이용하여 강력한 사용자 접근통제 및 부인방지 서비스를 수행하는 신뢰당사자 Bob은 Alice의 요구사항과 자신의 서비스환경을 고려하여 Alice에 대해 3종류의 서로 다른 본인확인절차를 수행할 수 있다.

예 1. Bob이 Alice의 SII를 모르는 경우
예 2. Bob이 Alice의 SII를 아는 경우
예 3. Alice가 자신의 SII를 Bob에게 노출시키고 싶지 않은 경우

그림 7은 예 2의 본인확인 절차로 Alice가 PEPSI를 포함한 인증서와 P를 Bob에게 제시하는 상황이다. 이 때 Bob은 Alice의 인증서로부터 SIM를 추출하고 이를 이용하여 PEPSI'에 필요한 R을

단계	Alice	암호채널	Bob
1	P 정보전송	→	
2	인증서 전송	→	
3			인증서에서 SIM 추출 SIM에서 R과 PEPSI 추출
4			PEPSI' 계산
5			PEPSI와 PEPSI' 동일 여부 확인

〔그림 7〕 Bob이 Alice의 SII를 알고 있는 경우의 확인절차

얻는다. 이제 Bob은 PEPSI'를 새로 생성한 후 인증서에서 추출한 PEPSI와 비교하여 인증서 소유자가 Alice 본인인지를 확인할 수 있게 된다. 이와는 달리 Bob측에 Alice의 SII가 사전에 등록되어 있지 않은 경우나 Alice가 Bob으로부터 자신의 SII을 보호하고자 하는 경우의 본인확인 절차는 그림 7의 단계 1,3,4에서 처리하는 정보의 차이만 있을 뿐 전체적으로는 비슷한 과정으로 구성된다. 즉 Bob이 Alice의 SII를 모르는 경우인 예 1의 단계1에서는 P뿐만 아니라 SII, SIItype을 함께 보내야 한다. 단계 3에서는 예 1과는 달리 PEPSI'를 생성하는데 단계 1의 SII, SIItype 정보와 함께 인증서의 R이 함께 입력된다. 단계 4는 예 1의 단계 3과 같다. 한편 Alice가 자신의 SII를 Bob에게 노출시키지 않고 본인확인절차를 거치고자 하는 예 3의 경우는 단계 1에서 Alice가 H(P‖R‖SIItype‖SII)를 Bob에게 전달한다. 단계 3에서는 단계 1의 중간 해쉬값에 한 번 더 해쉬함수를 적용하여 PEPSI'를 생성하게 되고 이를 단계 4에서 PEPSI와 비교함으로써 Alice에 대한 본인확인 과정을 수행하게 된다. 참고로 본인확인 과정에 상관없이 그림 7의 단계 1,2에서 전송되는 데이터의 순서는 관계가 없으며 각각의 예에서 전달되는 P, SII, SIItype, H(P‖R‖SIItype‖SII) 정보는 항상 Eve에게 유출되지 않도록 안전한 암호채널을 통해 전달되어야 한다. 특히 PEPSI 구성의 핵심인 P에 대한 보호는 매우 중요하다.

5. 안전성 분석

PEPSI는 Alice가 패스워드 P를 안전하게 사용함으로 전수공격(brute-force attack)에 강한 성질을 지닌다. 비록 Eve가 길이가 짧은 SII에 대해 성별, 나이, 년도 등 부분적인 정보를 가지고 SII를 추측할 수 있을지라도 P를 획득하지 못하면 자신이 추측한 SII가 정확한지 확인할 방법이 없다. 또한 PEPSI는 적어도 충돌회피의 성질을 갖는 암호학적으로 안전한 SHA-1 알고리즘의 사용을 전제하고 있어 Eve가 동일한 해쉬값이 나올 수 있는 다른 P, SII, SIItype를 찾기가 어렵다. 즉, 생일문제에 기반을 둔 암호공격의 경우 $2^{n/2}$번의 반복작업을 요구하게 되므로 PEPSI는 암호학적으로 안전(cryptographically secure)하다고 할 수 있다. 비록 P가 신뢰당사자에게 네트워크를 통해 전달되는 경우가 있으나 이럴 경우 SSL/TLS와 같은 암호채널을 통해 전달되므로 P에 대한 유출 위험이 없다. 참고로 P의 노출에 따른 위험을 사전에 막기 위해 주기적으로 P을 갱신함으로써 안전성을 더욱 높일 수 있다. 또한 PEPSI 구조는 PEPSI 생성에 필요한 입력값 중 R의 생성을 Alice가 아닌 RA가 하므로 Alice가 동일한 PEPSI값을 생성해 내는 거짓 P, SII 등 입력값을 사전 계산할 수 없도록 한다.

Ⅳ. SIM 표준화 동향

SIM 표준(안)은 제55차 IETF회의에서 처음으로 제안·발표되었다. 그리고 제55차 IETF 정기회의 이후 지금까지 IETF 보안분야(Security Area) 의장인 러스 허슬리(Russ Housley)와 PKIX 워킹그룹 의장인 팀 포크(Tim Polk)가 근무하고 있는 미국 국립표준연구소(NIST)에서의 전문가 그룹 등 여러 국외 PKI전문가와의 긴밀한 협조체계를 통해 공동 합의된 기술적 개선사항들을 반영해 오고 있다. 주요 기술적 개선 사항은 주민등록번호와 같은 개인정보의 노출방지를 위해 보다 안전한 해쉬 알고리즘 정의 추가 및 공격자 또는 인증서 소유자 자신으로부터의 추측공격(guessing attack)과 전수공격(brute-force attack)으로부터 안전한 PEPSI 형식 보완 등 암호학적 개선사항들을 포함한다. 또한 국내 주민등록번호뿐만 아니라 각 국마다 다양한 개인식별번호체계를 수용하기 위해 SIItype과 SII를 수용하도록 PEPSI 구조체의 확장이 병행되었다. 특히 2003년 11월에 개최된 제58차 IETF회의에서는 SIM 표준(안)이 PKIX 워킹그룹의 첫 번째 현안으로 채택되어 한국정보보호진흥원(KISA)과 NIST의 공동발표로 약 25분간 논의되었다. 여기서는 1차 개정(안)에 대한 전반적인 문서작업 현황 및 여러 가지 기술적 이슈사항이 소개되었다. 첫 번째로 인증서내 PEPSI 구조체의 저장위치로 의미상 '소유자 대체명칭 확장필드'가 적합하다는 의견과 PKI 도메인간 상호연동성을 고려하여 사설확장필드가 적절하다는 의견이 교환되었으며, 두 번째 이슈로 비트열 난수 R의 생성주체와 관련하여 클라이언트와 등록기관 모두 생성해야 한다는 견해와 등록기관 단독으로 생성해도 문제가 없다는 의견이 제시되었다. 다음 세 번째 사항으로는 R의 기밀필요여부에 대해서도 논의되었는데 전술한 2,3번째 이슈사항의 발단은 PEPSI 구조체에 대해 근본적으로 서로 다른 암호학적 견해가 존재하는 데에서 기인하였다. 즉, PEPSI 구조체의 모든 정보가 전적으로 인증서 소유자에 의해

선택되어지는 정보일지라도 충돌회피의 성질을 갖는 암호학적으로 안전한 해쉬함수를 이용한다면 굳이 사전계산공격을 고려하지 않아도 무방하다는 의견과 그렇지 않다는 의견이 공존하였다. 최종적으로 IETF 회의 셋째날(11/12)에 KISA는 러스 허슬리와 팀 포크와 가진 별도 회의를 통해 상기 이슈사항들을 한번에 해결할 수 있도록 PEPSI=H(X‖ H(P‖R‖ SIItype‖SII))의 구조체를 도출해 냈으며 이에 근거하여 올해 3월 서울에서 열린 제 59차 IETF 서울회의에서 2차 개정안이 발표되었다. IETF 서울회의 및 PKIX 메일링리스트에서 제기된 의견을 반영한 SIM 3차 개정안은 2004년 상반기내 PKIX 워킹그룹내 라스트콜(Last Call)을 목표로 하고 있어 SIM 표준(안)이 향후 국내 PKI 분야로는 처음으로 IETF RFC 문서로 채택되는데 큰 문제가 없을 것으로 판단된다. 이와 같은 일련의 주요 표준화 진행상황을 정리하면 표 3과 같다.

V. 결 론

본 논문에서는 국내 순수 보안기술로 KISA, 인터넷보안기술포럼(ISTF), 공인인증기관, (주)비씨큐어간의 논의 과정을 거쳐 개발되어 IETF에서 표준화 논의중인 SIM 표준(안)에 대해 고찰하였다. SIM 표준(안)은 X.509 인증서의 소유자 대체명칭 확장필드에 PEPSI를 포함하여 인증서 소유자에 대한 정확한 본인확인을 강력한 사용자 인증 메커니즘을 제시한다. 또한 보호되어야 할 개인식별정보를 노출시키지 않으면서 사용자 프라이버시를 보장할 수도 있다. SIM 표준(안)이 향후 IETF 공식표준으로 제정될 경우, 사실상의 국제 업계표준으로 통용돼 이미 KISA에서 개발한 기술규격에 따라 시스템을 구축하고 있는 국내 공인인증기관과 보안업체는 개발비등을 크게 절감하게 되는 효과를 거둘 수 있을 것이다. 아울러 국내 기술의 우수성을 국제적으로 인정받음으로써 국내 인증서

〔표 3〕 SIM 표준(안)의 IETF 표준화 동향

[illegible]	[illegible]	비고
'02. 11	· SIM 초안 기고 및 IETF PKIX 워킹그룹 발표 · Russ Hosely와 Tim Polk 등 국외전문가와 협력체계 구축	제55차 IETF회의
'03. 03	· SIM 1차 개정안 표준화 진행상황 및 기술적 이슈사항 발표 - VID(구 PEPSI)의 ASN.1 구문 수정 - ID, VID(구 PEPSI) 용어를 SII, PII(구 PEPSI)로 대체 - PII의 검증예제 부연설명 보강	제56차 IETF회의
'03. 04 ~ '03. 08	· 국외 전문가와 E-mail를 통한 SIM 1차 개정안 검토 - PII 용어를 PEPSI로 재정의 - PEPSI = H(H(SII‖R)) 구조체의 안전성 논의 - 암호학적으로 안전한 해쉬함수의 정의 합의 - 인증서 소유자 및 공격자로부터의 추측공격 및 사전계산공격 가능성에 대한 대안 논의	
'03. 11	· SIM 1차 개정안 기고 및 발표 - 인증서내 PEPSI 식별자 저장위치 논의 - PEPSI = H (X ‖ H (P‖R‖SIItype‖SII))로 잠정 합의 ※ X값은 아예 사용하지 않거나 만일 사용되어야 한다면 암호학적 안전성을 고려하여 추가변수를 정의해야 하며, 사용여부를 추후 결정하기로 합의	제58차 IETF회의
'04. 03	· SIM 2차 개정안 기고 및 발표 - SIM 구조체 확정 SIM = R‖PEPSI, PEPSI = H(H(P‖R‖SIItype‖SII)) - 소유자 대체명칭 확장필드에 PEPSI 저장	제59차 IETF회의
'04. 05	· SIM 3차 개정안 기고 - EPEPSI내 SIItype 포함 - CA 공개키 알고리즘에 대한 추가사항 반영(DH 알고리즘 등)	
'04. 06	· SIM 표준(안) PKIX 워킹그룹내 라스트콜(Last Call) 예정	

비스 분야의 국제 경쟁력이 크게 강화될 것으로 예상된다.

참 고 문 헌

[1] ITU-T Recommendation X.501 (1997 E) : Information Technology-Open Systems Interconnection-The Directory : Models, June 1997

[2] ITU-T Recommendation X.520 : Information Technology-Open Systems Interconnection-The Directory: Selected Attribute Types,, June 1997

[3] M. Wahl, IETF RFC 2256, "A Summary of the X.500(96) User Schema for use with LDAPv3", December 1997

[4] ITU-T Recommendation X.509 (1997 E) : Information Technology - Open Systems Interconnection-The Directory: Authentication Framework, June 1997

[5] R. Housley, W. Ford, W. Polk, and D. Solo, IETF RFC 3280, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", April 2002

[6] D. Pinkas, T. Gindin, ietf-draft-pkix-pi-09.txt, "Internet X.509 Public Key Infrastructure Permanent Identifier", January 2004

[7] Australian Government, "ABN-DSC Broad Specification", http://www.noie.gov.au/ projects/confidence/Improving/abn-dsc.htm, 2003

[8] Hongkong Post, "e-Cert Certification Practice Statement", 2001

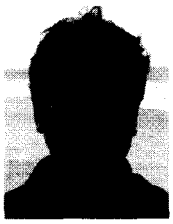
[9] Acepta.com, http://www.acepta.com

[10] SEIS, "Identification Cards Electronic ID Certificate", http://www.seis.se/seis/doc/dok/SS614331.rtf,

[11] Jongwook Park, Jaeho Yoon, Seungjoo Kim, Sangjoon Park, Jaeil Lee, Hongsub Lee, Polk, Tim, draft-ietf-pkix-sim- 03.txt "Internet X.509 Public Key Infrastructure Sujbect Identification Method", February, 2004

[12] KISA, "식별번호를 이용한 본인확인 기술규격", http://www.rootca.or.kr, 2002년 9월

〈著 者 紹 介〉

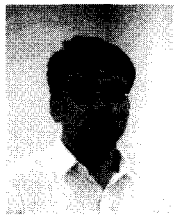


박 종 욱 (Jongwook Park)
학생회원

1998년 2월 : 아주대학교 정보 및 컴퓨터공학부 졸업
2004년 2월 : 고려대학교 정보보호대학원 공학석사
2004년 3월~현재 : 고려대학교 정보보호대학원 박사과정
1998년 3월~2000년 5월 : 삼성SDS
2000년 5월~현재 : 한국정보보호진흥원(KISA) 선임연구원
〈관심분야〉 정보보호, 유·무선PKI, 유비쿼터스 보안

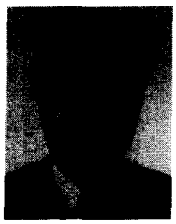
김 승 주 (Seungjoo Kim)
종신회원

1994년 2월 : 성균관대학교 정보공학과 공학사
1996년 2월 : 성균관대학교 대학원 정보공학과 공학석사(암호학 전공)
1999년 2월 : 성균관대학교 대학원 정보공학과 공학박사(암호학 전공)
1998년 12월~2004년 2월 : 한국정보보호진흥원(KISA) 평가1팀장
2004년 3월~현재 : 성균관대학교 정보통신공학부 조교수
〈관심분야〉 암호학, 정보보호



이 재 일 (Jaeil Lee)
종신회원

1986년 2월 : 서울대학교 계산통계학과 학사
1988년 2월 : 서울대학교 계산통계학과 석사
1991년 1월~1996년 6월 : 한국IBM
1996년 7월~현재 : 한국정보보호진흥원(KISA) 전자거래보호단장
〈관심분야〉 정보보호, 유·무선PKI, 유비쿼터스 보안



이 홍 섭 (Hongsub Lee)
종신회원

1979년 2월 : 한양대학교 전자공학과 학사
1985년 2월 : 한양대학교 전자공학과 석사
1998년 8월 : 대전대학교 컴퓨터공학과 박사
1980년~1996년 : 한국전자통신연구원 실장
1996년~현재 : 한국정보보호진흥원 기반시설보호단장, 한국정보보호학회 상임부회장, 인터넷보안기술포럼(ISTF) 의장, 홈네트워크시큐리티포럼 의장, 네트워크시큐리티포럼 의장, 정보통신국가표준심의회 위원
〈관심분야〉 시스템 및 네트워크 정보보호, 정보보호기술 표준화