情報保護學會論文誌
第16卷 第5號, 2006. 10

X.509 인증서에 포함된 프라이버시 보호기능을 가진 개인 식별 방법

이 재 일,[1†] 박 종 욱,[2] 김 승 주,[3] 송 주 석[4]
[1]한국정보보호진흥원, [2]고려대학교, [3]성균관대학교, [4]연세대학교

Privacy-Enhanced Subject Identification method Embedded in X.509 Certificate

Jaeil Lee,[1†] Jongwook Park,[2] Seungjoo Kim,[3] JooSeok Song[4]
[1]Korea Information Security Agency, [2]Korea University,
[3]SungKyunKwan University, [4]Yonsei University

요 약

CA는 소유자와 공개키를 연계시키기 위해 X.509 공개키 인증서를 발급한다. 소유자는 인증서의 "subject" 필드나 "subjectAltName" 확장필드에 있는 하나 이상의 소유자 명에 의해 특정되어진다. 그러나 실세계에서는 동일하거나 유사한 이름을 갖는 개인들이 존재한다. 이런 모호성은 같은 소유자에게 발급되는 모든 인증서 내에 여러 CA간에 유일성을 보장해주는 "항구식별자"를 포함시킴으로써 해결될 수 있다. 그러나 많은 경우에 있어서 개인의 유일한 식별자는 민감한 개인정보이기 때문에 소유자 필드에 단순 포함시켜서는 안 된다. 누출될 경우 오용될 수 있기 때문이다. 본 논문에서는 X.509 인증서의 표준 확장필드에 포함되는 PEPSI를 통하여 사용자 식별자의 기밀성을 제공함으로써 보다 안전하고 정확한 사용자 인증방안을 제시한다.

ABSTRACT

A Certification Authority issues X.509 public key certificates to bind a public key to a subject. The subject is specified through one or more subject names in the "subject" or "subjectAltName" fields of a certificate. In reality, however, there are individuals that have the same or similar names. This ambiguity can be resolved by including a "permanent identifier" in all certificates issued to the same subject, which is unique across multiple CAs. But, a person's unique identifier is regarded as a sensitive personal data. Such an identifier cannot simply be included as part of the subject field, since its disclosure may lead to misuse. We present a new method for secure and accurate user authentication through the PEPSI included in the standard certificate extension of a X.509 certificate. The PEPSI can be served not only for user authentication but also for the user anonymity without divulging personal information.

Keywords : *PKI, X.509, Certificate, Authentication, Privacy*

Ⅰ. 서 론

일반적으로 인증기관은 X.509 인증서 소유자의 명칭을 포함하는 식별정보를 인증서 소유자(subject)필드나 소유자대체명칭(subjectAltName) 필

접수일: 2006년 6월 12일; 채택일: 2006년 9월 25일
† 주저자, jilee@kisa.or.kr

드에 가입자별로 유일하게 할당해야 한다[1, 2]. 그러나 실제 응용에서는 동일한 이름을 갖는 소유자가 존재하고 식별정보의 잦은 변경이 인증서에 실시간으로 반영되지 않으므로 인증서 정보만으로는 접근통제(access control), 부인방지(non-repudiation) 서비스 등에서 소유자에 대한 정확한 신원확인을 보장하기 어렵다. 이에 대한 보완책으로, 다수의 인증기관사이에서도 인증서 소유자에 대한 유일성을 보장하는 항구식별자(PI: Permanent Identifier) 개념이 제안되었다[3]. PI는 동일 소유자에게 발급된 모든 인증서 내에 포함된다. 그러나 보호되어야 하는 민감한 식별정보가 PI로 이용될 경우, 불특정 다수에게 식별정보가 공개될 수 있으므로 PI는 개인 프라이버시 보호를 위한 효과적인 메커니즘이 될 수 없다.

따라서 이러한 종류의 프라이버시에 민감한 식별자는 평문 형태로 인증서 내에 포함되어서는 안 된다. 그러나 이러한 식별자는 실제로는 비밀 형태로 존재하지 않을 수도 있다. 특정 거래에서는 사람들이 자신의 식별자를 노출하여야만 하는 경우도 있다. 예를 들어, 은행에서 은행계좌를 개설하거나, 대출 등을 받기 위해서는 자신의 주민번호나 운전면허번호 등을 보여 주어야만 한다. 신원확인을 위한 수단으로서 실제 증명서를 제시하여야만 하는 것이다.

온라인 환경에서 이러한 응용을 지원하기 위해서는, 신뢰 당사자(relying party)가 특정 인증서의 소유자가 이와 같은 개인식별자를 갖고 있는 실 소유자인지를 증명할 수 있어야 한다. 이상적으로는 응용에 사용되는 전자적 증명서 (예를 들어, X.509 공개키 인증서)를 통해 이러한 증명이 가능해야 하지만, 인증서 내에 포함된 소유자 항목은 이에 필요한 충분한 정보를 제공하지 않는다.

본 논문에서는 암호학적으로 보호된 식별정보를 인증서에 포함시켜 PI의 취약점을 보완하고 소유자를 정확히 식별할 수 있는 Privacy-Enhanced Permanent Subject Identifier (PEPSI)를 제시한다. PEPSI는 인증서 소유자가 지정한 사람만이 정확하고 안전하게 사용자 인증을 할 수 있도록 한다. 또한 필요한 경우 단지 PEPSI를 소유하고 있다는 사실만을 증명할 수 있게 함으로써 사용자 식별자의 기밀성을 보장할 수도 있다. 예를 들어 운전면허번호를 PEPSI로 사용하는 경우, 소유자는 운전면허번호를 숨기고 운전면허가 있다는 사실만을 증명할 수 있다.

본 논문은 다음과 같이 구성되어진다. 2장에서는 본 논문에서 사용되는 기호 및 보안요구사항에 대해 정의한다. 3장에서는 민감한 개인 식별자를 인터넷 상에서 안전하게 사용할 수 있는 PEPSI 메커니즘을 제안한다. 그리고 4장에서는 PEPSI의 안전성에 대해 분석한다. 마지막으로 5장에서 결론을 맺는다.

II. 요구사항 정의

2.1 기호

다음과 같은 암호학적 기호들을 정의한다.

H( ) 암호학적으로 안전한 해쉬 알고리즘.
SHA-1[FIPS 180-1] 또는 더 안전한 해쉬 함수가 요구된다.

SII 민감한 식별 정보
(예, 주민번호, 신용카드번호 등)

SIItype SII의 유형을 식별하는 객체 식별자 (Object Identifier)

R 사용자에 의해 생성된 난수

PEPSI 프라이버시 보호기능을 갖는 소유자 식별정보
입력 값 R, SIItype, SII와 H()의 두 번 반복 적용을 통해 계산된 값.

E( ) PEPSI 값을 암호화 하기위한 암호 알고리즘.

EPEPSI 암호화된 PEPSI.

D( ) EPEPSI를 복호화 하기 위한 복호화 알고리즘.

2.2 보안요구사항

PEPSI가 작용되어질 환경에 대해 다음과 같이 가정한다.

- Alice : 주민번호 등 민감한 개인식별자 SIIa를 보유하고 있는 인증서 소유자,
- Bob : Alice의 SIIa에 대한 제출을 요구하는

신뢰 당사자
- Eve : Alice의 인증서를 획득한 공격자
- A RA : Alice가 자신의 SIIa를 최초 한 번 공개해야만 하는 등록기관
- A CA : Alice의 인증서를 발급하는 인증기관

Alice가 선택한 패스워드를 사용하여 다음과 같은 성질을 갖는 PEPSI를 설계한다.

요구사항 1. Alice는 Bob에게 자신의 SII, SIIa의 소유 사실을 증명할 수 있다.

요구사항 2. Eve가 Alice의 인증서로부터 SIIa를 알아내기 위해서는 막대한 양의 작업 시간을 요구한다.

요구사항 3. 설령, Eve가 SIIa를 알아냈다 하더라도, 다른 PEPSI로부터 관련된 다른 SII를 알아내는 것은 똑같은 정도의 계산 어려움을 갖는다. 즉, 다시 말해 다른 인증서에 포함된 PEPSI에 대한 공격을 용이하게 하는 어떠한 사전 계산도 존재하지 않는다. 그리고 그녀가 성공한 공격으로부터 다른 공격을 도울 수 있는 어떠한 정보도 얻을 수 없다.

요구사항 4. CA는 RA에 의해 보내어진 SII를 증명할 필요가 있는 경우를 제외하고는 Alice의 SIIa에 대해 알수 없다.

요구사항 5. CA는 PEPSI를 X.509 인증서 확장필드 "subjectAltName"에 포함된 하나의 부가 이름으로서 처리가 가능하며, 별도의 처리를 필요로 하지 않는다.

요구사항 6. Alice는 인증서 내에 포함될 PEPSI 값을 구성하기 위해서는 반드시 정당한 SIIa와 R 값을 사용해야만 한다. 즉, 자신을 위장하기위한 방법으로, PEPSI 값을 구성할 수 있는 또 다른 SII (SIIx)와 난수 R을 찾아낼 수 없다.

2.3 PEPSI의 구성 및 사용

PEPSI의 정의는 다음과 같다.

PEPSI = H(H(R || SIItype || SII))

다음은 PEPSI의 구성 및 사용 방법에 대해 정의한다.

1) Alice는 난수 R을 생성하고, R, SIItype 과 SII를 RA에 전달한다(안전한 전송 채널을 가정).
2) RA는 SIItype과 SII를 검증한다, 즉, SII 값이 소유자와 맞게 연관되어 있고 SIItype이 올바른지 확인한다.
3) RA는 PEPSI을 생성한다. 이때 PEPSI는 H(H(R || SIItype || SII))와 같다.
4) RA는 Alice에게 PEPSI을 안전한 방법 (out-of-band means)으로 전달하고 CA에게도 전송한다.
5) Alice는 CA에 인증서발급요청을 하고, CA는 인증서 SubjectAltName 확장필드의 General-Name 구조에 otherName의 형태로 PEPSI를 포함시켜 인증서를 발행한다.
6) Alice는 인증서와 R, SIItype, SII를 Bob에게 보낸다, 이 때 인증서를 제외한 나머지 값들은 기밀성을 유지하기 위해 안전한 전송채널을 통해 보내져야 한다.
7) Bob은 보내진 값들을 이용 PEPSI′ = H(H(R || SIItype || SII)) 을 계산하고, SII를 검증하기 위해 Alice 인증서 내에 포함된 PEPSI 값과 PEPSI′ 값이 같은지 비교한다.

만일 Bob이 Alice의 SII 값을 미리 알고 있어 이를 요구하지 않을 경우 단계 7)은 다음과 같이 수정된다.

7) Alice는 인증서와 R을 Bob에게 보낸다, 이 때 R은 기밀성을 유지하기 위해 안전한 전송채널을 통해 보내져야 한다.
8) Bob은 PEPSI′ = H(H(R || SIItype || SII)) 을 계산하고, SII를 검증하기 위해 Alice 인증서 내에 포함된 PEPSI 값과 PEPSI′ 값이 같은지 비교한다.

만일 Alice가 Bob에게 자신의 식별자를 드러내지 않고, RA에 의해 검증된 식별자의 소유자임을 증명하고자 할 경우의 단계 7) 과 8) 은 다음과 같다.

7) Alice는 SII 노출 없이 중간 계산 값 H(R || SIItype || SII)와 인증서만을 Bob에게 보낸다.
8) Bob은 인증서 내에 있는 PEPSI 값과 중간 계산 값을 해쉬한 결과를 비교한다. 이를 통해

Alice가 R과 SII를 알고 있음을 인증한다.

Eve가 Alice의 SII를 찾기 위해서는 H(R || SIItype || SII)에 대해 전수조사를 해야만 한다. 이 것은 R의 크기(3장에서 언급) 때문에 상당히 어려운 문제(fairy hard problem)가 된다.

만일 Eve가 Alice의 R과 SII를 찾거나 R과 SII 값들에 대한 광범위한 사전을 구축한다 하더라도, 다른 SII 값을 찾는 데는 도움이 되지 않는다. 왜냐하면 각각의 PEPSI에는 새로운 R이 사용되기 때문이다.

III. PEPSI 메커니즘

3.1 SII와 SIItype 정의

사용자는 특정한 SII가 자신에게 할당되었다는 증거를 제시한다. SIItype은 SII 값의 영역 및 형식을 정의하는 Object Identifier (OID)를 말한다.

3.2 난수 R의 생성

사용자는 난수 R을 생성한다. 각각의 PEPSI마다 새로운 R이 할당되어져야만 한다. 난수 R은 사용자만이 알 수 있는 비밀정보로 해쉬 함수의 결과 값과 같은 길이를 갖는 비트열 난수이다. 만일 SHA-1이 사용되었다면 난수의 길이는 160비트가 된다. 난수 R은 SII와 연접되어 PEPSI의 전체적인 비도 증가를 위해 사용되는 동시에 암호 채널을 통해 신뢰당사자에게 전달되어 PEPSI를 검증할 때 중요한 역할을 하는 파라미터이다.

난수 R은 사용자의 개인키 관리레벨과 동등한 수준에서 관리되어야 하며 사용자의 PSE(Personal Security Environments)에 따라 서로 다른 난수 관리 메커니즘이 적용될 수 있음에 주의해야 한다. 만일 사용자의 인증서 관련 저장매체가 로컬디스크나 계산능력이 없는 스마트카드를 사용하는 경우 난수 R은 그림 1과 같이 개인키와 함께 PKCS#8을 준용하여 저장해야 한다[6]. 반면 계산능력이 있는 PKCS#11 호환 암호토큰을 저장매체로 사용하는 경우에는 R의 저장을 위해 표 1과 같은 데이터 오브젝트(DATA OBJECT)를 정의해야 한다[8]. 이러한 경우 난수 R 대신 개인키의 해쉬값인 H(sk)를 사용하여 PEPSI=H(H(H(sk) || SIItype || SII))의 형태로 구성할 수 있다. 이럴 경우 앞에서 제시된 R값을 별도 관리해야 하는 부담을 덜 수 있으며 사용자가 이미 소유하고 있는 개인키를 다른 형태로 활용할 수 있다는 장점이 있다.

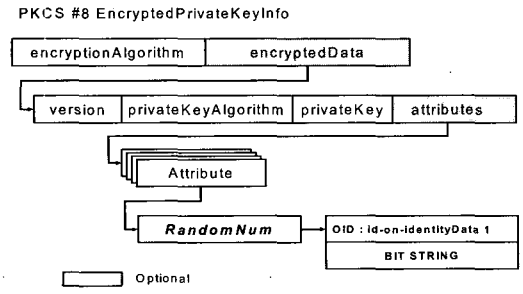

그림 1. 난수 R을 포함하는 PKCS#8 구조

표 1. 난수 R을 저장하는 PKCS#11 데이터 오브젝트 속성

Attribute name	Attribute type	Value
CKA_CLASS	CK_OBJECT_CLASS	CKO_DATA
CKA_TOKEN	CK_BBOOL	FALSE(default)
CKA_PRIVATE	CK_BBOOL	TRUE
CKA_MODIFIABLE	CK_BBOOL	TRUE
CKA_LABEL	Local string	"Random value"
CKA_APPLICATION	Local string	-
CKA_VALUE	Byte array	R

3.3 PEPSI의 생성

인증서 subjectAltName 확장필드 내에 있는 PEPSI는 인증서 내에 복수개의 subjectAltName이 나타난다 해도 객체를 식별하여 준다. RA는 다음 알고리즘을 가지고 지정된 입력 값을 이용 PEPSI 값을 계산해야만 한다.

PEPSI = H(H(R || SIItype || SII))

SII는 사용자 등록 시 RA에 제출된다. 사용자로부터 RA로 R과 SII를 전송할 경우에는 누출이나 변경에 대비하여 안전한 전송채널을 사용하여야만 한다.

여기서 항상 보호되어야 할 개인식별정보인 SII는 일반적으로 성별, 생년월일 등과 같이 쉽게 추정할 수 있는 정보로 구성되는 성격을 지니고 있다. 더구나 대부분의 SII의 길이가 10자리 내외이고 ASCII

문자 중 알파벳이나 숫자만이 사용되므로 SII 자체적으로는 노출가능성에 대한 암호학적 안전성을 제공할 수 없다. PEPSI의 계산처리속도 증가를 위해 대칭키 알고리즘 대신 암호학적 해쉬함수를 적용하며 해쉬함수는 충돌회피(collision-free)성질을 갖는 SHA-1 알고리즘의 사용을 전제로 한다. 연이은 해쉬함수의 적용은 서론에서 언급한 바와 같이 사용자가 SII를 소유하고 있다는 사실만을 알리고 싶어 하는 경우, 즉 사용자 식별자의 기밀성을 요구하는 환경 또한 수용 가능하게 한다.

3.4 인증서 요청

난수 R과 공개키쌍을 생성한 가입자는 인증서 요청을 위해 CRMF 또는 PKCS#10을 이용할 수 있으며 PEPSI 정보 또한 이것을 이용하여 CA에게 전달된다[4,5,7]. 이 때 CA는 PEPSI 정보만으로는 사용자의 PEPSI 진위를 파악할 수 없으므로 사용자는 CA에게 PEPSI 생성에 중요한 데이터인 R을 함께 전송해야 한다. 본 논문에서 R값은 사용자를 식별할 수 있는 결정적인 값이며 기밀성을 요하므로 PEPSI와 R을 함께 CA의 공개키로 암호화한 EPEPSI=E(PEPSI‖R) 형태를 그림 2와 같이 인증서요청형식에 포함시켜 인증기관에게 전송해야 한다.

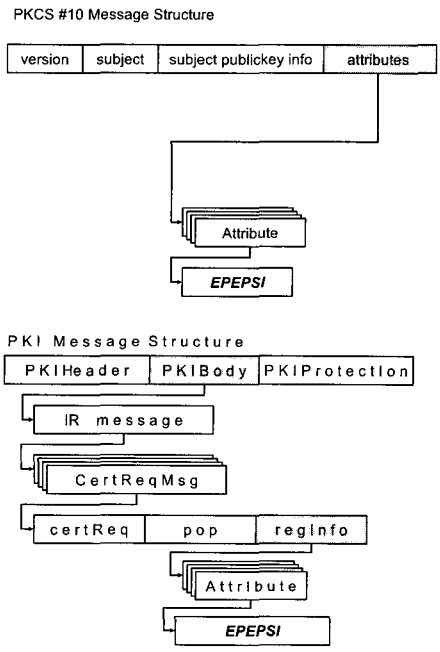

그림 2 EPEPSI를 포함하는 인증서요청형식

3.5 인증서 검증 및 발급

인증서 발급을 위해 CA는 인증서요청형식에서 추출한 EPEPSI에 대해 다음의 검증과정을 수행한다. 즉,

PEPSI, R = D(EPEPSI)
PEPSI′ = H(H(R‖SIItype‖SII))
PEPSI ≟ PEPSI′

CA는 자신의 개인키로 EPEPSI를 복호화하여 PEPSI와 R을 획득한다. 그런 다음, CA는 새로운 PEPSI′을 생성하여 복호화된 PEPSI와 동일여부를 확인하게 된다. 이 때 CA는 사용자의 개인식별정보를 가입자 신원확인 과정을 통해 미리 소유하고 있어야 한다는 점에 유의해야 한다. PEPSI 검증이 성공되면 CA는 X.509 인증서의 확장필드 중 소유자대체명칭(subjectAltName)에 그림 3에서 기술하는 ASN.1 형식으로 PEPSI를 생성하여, 인증서를 발급하게 된다. 여기서 주목할 점은 IdentityData의 realName필드가 소유자의 실명을 표현할 수 있고 userInfo 필드가 다양한 개인식별정보를 저장할 수 있는 확장영역으로 정의되어 있어 PEPSI는 IETF의 PI구조를 수용할 수 있다는 것이다.

```
-- IdentityData
    IdentityData ::= SEQUENCE {
      realName  UTF8String (SIZE (1..100)),
      userInfo  SET SIZE (1..MAX) OF AttributeTypeAndValue
          OPTIONAL -- PEPSI 속성 추가
  }
```

```
-- PEPSI
     ProtectedIDInfo ::= SEQUENCE {
        hashAlg              AlgorithmIdentifier,
        protectedIDInfo  [0]  OCTET STRING -- PEPSI
     }

     HashContent ::= SEQUENCE {
        identifier       PrintableString, -- SII
        randomNum        BIT STRING
     }
```

그림 3. PEPSI의 ASN.1 구조 정의

3.6 신뢰당사자의 PEPSI 검증

PEPSI를 이용하여 강력한 사용자 접근통제 및 부인방지 서비스를 수행하는 신뢰당사자는 다음과 같

은 사용자의 요구사항과 자신의 서비스 환경을 고려하여 별개의 검증절차를 수행할 수 있다.

(i) 신뢰당사자가 사용자의 SII를 모르는 경우
(ii) 신뢰당사자가 이미 사용자의 SII를 알고 있는 경우
(iii) SII를 신뢰당사자로부터 보호하고자 하는 경우.

(ii)의 경우 사용자는 PEPSI을 포함한 자신의 인증서와 난수 R을 신뢰당사자에게 전달해야 한다. 이때 신뢰당사자는 별도의 방법을 통해 획득한 SII와 사용자로부터 전달받은 난수 R을 이용하여 PEPSI'를 새로 생성할 수 있다. 이를 사용자 인증서에서 추출한 PEPSI와 비교하여 사용자 인증을 수행하게 된다.

마찬가지로 (i)처럼 신뢰당사자가 사용자의 SII를 별도로 획득하지 못한 경우나 (iii)과 같이 사용자가 신뢰당사자로부터 자신의 SII와 R이 노출되는 것을 꺼려하는 경우의 검증절차는 신뢰당사자에게 전달되는 정보의 차이만 있을 뿐 전체적으로는 대동소이한 과정으로 구성된다. 즉 (i)에서 사용자는 SII과 R을 함께 보내야 하며 (iii)의 경우 사용자는 PEPSI의 중간값 형태인 H(R || SIItype || SII)만을 신뢰당사자에게 보내 자신의 사용자 식별자에 대한 기밀성을 보장받을 수 있다. 반면 신뢰당사자는 (i)의 경우 전달받은 SII와 R로 PEPSI'을 만들 수 있으며 (iii)에서는 H(R || SIItype || SII)를 한차례 더 해쉬함으로써 PEPSI'를 생성할 수 있다. 결국 모든 경우에 있어 신뢰당사자는 인증서에 있는 PEPSI와 자신이 생성한 PEPSI'과의 동일여부를 확인할 수 있게 된다.

Ⅳ. 분석

본 장에서는 '2.2 보안요구사항'에서 제시했던 6가지 요구사항을 만족하는지 여부를 분석하도록 한다. 하지만, 요구사항들 중에서 요구사항 5는 보안요구사항이 아닌 기존 시스템의 활용가능성에 대해 명시하는 요구사항이므로 분석하는 항목에서 제외하도록 한다.

4.1 요구사항 1

제안한 PEPSI는 '3.6 신뢰당사자의 PEPSI 검증'에 의해 요구사항 1을 만족한다.

4.2 요구사항 2

Eve가 Alice의 인증서에 있는 PEPSI를 통해서 SIIa를 알아낼 수 있다고 한다면, Eve는 해쉬함수 H의 역상 공격이 가능한 공격자임을 의미한다. 그러므로 해쉬함수의 일방향성에 의해서 PEPSI로부터 SIIa를 알아내는 방법은 해쉬함수 H의 역상 공격을 수행하는 만큼의 막대한 양의 작업 시간이 필요하게 된다.

4.3 요구사항 3

Eve가 Alice의 SIIa를 우연한 경로를 통해 습득한 경우라 할지라도 해쉬함수 H의 일방향성에 의해 Alice의 R을 찾아내기도 쉽지 않을 뿐 아니라 다른 사용자의 PEPSI'으로부터 해당 사용자의 SII'를 찾아내는 방법에도 전혀 도움이 되지 않는다.

4.4 요구사항 4

CA를 요구사항 2의 Eve와 동일하게 생각한다면, 제안한 PEPSI이 요구사항 2을 만족함을 보이는 과정과 동일한 과정으로 제안한 PEPSI가 요구사항 4를 만족함을 보일 수 있다.

4.5 요구사항 6

Eve가 Alice로 위장할 수 있다면, Eve가 Alice의 PEPSI = H(H(R' || SIItype || SII'))을 만족하는 R', SII'를 찾아낼 수 있어야 한다. 이것은 Eve가 해쉬함수의 충돌쌍 공격이 가능한 공격자임을 의미한다. 그러므로 해쉬함수의 충돌회피성에 의해서 Eve는 Alice로 위장할 수 없어 제안한 PEPSI가 요구사항 6을 만족함을 보일 수 있다.

Ⅴ. 결 론

최근 IETF는 인증서 소유자의 중복성 문제를 해결하기 위해 PI라는 식별방법을 제안하였다. 그러나 PI는 식별정보에 대한 보호방법을 제시하고 있지 않아 주민번호나 운전면허 등과 같은 민감한 개인정보가 식별자로서 사용될 경우, 오용 및 도용의 문제를 야기 시킬 수 있다. 본 논문에서는 X.509 인증서의 확장필드에 PEPSI를 포함하는 방법을 제시함으로써

보호되어야 할 개인식별정보를 노출시키지 않으면서도 안전하게 신뢰 당사자에게 전달 할 수 있도록 하였다. 기존의 방식에서는 인증서를 이용 사용자를 인증할 수는 있었지만, 사용자를 유일하게 식별할 수는 없었다. 따라서 사용자를 유일하게 식별하기 위해서는 주민번호 등 개인식별번호를 추가로 제출하여야만 하였으나, 이를 안전한 방법으로 인증서에 포함시킴으로써 개인식별번호의 빈번한 제출이 없이도 사용자를 유일하게 식별하는 것이 가능해 졌다. 개인식별정보를 인증서 내에 포함시킴으로써 요즘 사회적으로 큰 문제가 되고 있는 주민번호의 도용과 같은 문제도 원천적으로 해결이 가능해졌다. 뿐만 아니라 사용자가 자신의 개인식별정보를 신뢰당사자에게 노출하지 않고도 자신을 인증시킬 수 있는 방법을 제시함으로써, 자신의 개인식별정보에 대한 기밀성을 보장할 수 있는 안전한 사용자 인증 메커니즘을 제시하였다.

참 고 문 헌

[1] ITU-T Recommendation X.509, Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, 2000.

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

[3] D. Pinkas, T. Gindin, RFC4043, Internet X.509 Public Key Infrastructure Permanent Identifier, March, 2005.

[4] IETF RFC 2510, Internet X.509 Public Key Infrastructure: Certificate Management Protocols, 1999.

[5] M. Myers, C. Adams, D. Solo and D. Kemp, IETF RFC 2511, Internet X.509 Certificate Request Message Format, 1999.

[6] RSA Laboratories PKCS#8, Private Key Information Syntax Standard, 1993.

[7] RSA Laboratories PKCS#10 v1.7, Certification Request Syntax Standard, 2000.

[8] RSA Laboratories PKCS#11 v2.11 , Cryptographic Token Interface Standard Revision 1, 2001.

[9] J. W. Park, J. I. Lee, H. S. Lee, S. J. Park, Polk, Tim, draft-ietf-pkix-sim-08.txt, "Internet X.509 Public Key Infrastructure Subject Identification Method (SIM), " July 2006

〈著者紹介〉

이 재 일 (Jaeil Lee) 정회원

1986년 2월: 서울대학교 계산통계학과 졸업
1988년 2월: 서울대학교 계산통계학과 석사
2006년 8월: 연세대학교 컴퓨터과학과 박사
1996년 6월: 한국IBM 소프트웨어연구소
1996년 7월~현재: 한국정보보호진흥원 IT기반보호단장
〈관심분야〉 PKI, 네트워크 보안, 프라이버시 보호기술

박 종 욱 (Jongwook Park) 정회원

1998년 2월 : 아주대학교 정보 및 컴퓨터공학부 졸업
2004년 2월 : 고려대학교 정보보호대학원 석사
1998년 2월~2000년 5월 : 삼성 SDS
2000년 5월~2004년 5월 : 한국정보보호진흥원
2004년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 PKI, Ubiquitous 보안, 무선 인터넷 보안

김 승 주 (Seungjoo Kim) 종신회원

1994년 2월 - 1999년 2월: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년 12월~2004년 2월: 한국정보보호진흥원 팀장
2004년 3월~현재: 성균관대학교 정보통신공학부 교수
2001년 1월~현재: 한국정보보호학회 논문지 및 학회지 편집위원
2002년 4월~현재: TTA IT 국제표준화 전문가
〈관심분야〉 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 평가, PET

송 주 석 (JooSeok Song) 종신회원

1976년 2월: 서울대학교 전기공학과 졸업
1979년 2월: 한국과학기술원 전기 및 전자공학과 석사
1988년 Univ. of California at Berkeley, 컴퓨터과학 박사
1988년~1989년: Assistant Professor in Naval Postgraduate School
1989년~현재: 연세대학교 컴퓨터과학과 정교수
2006년~현재: 한국정보보호학회장
〈관심분야〉 Information Security, Cryptography, Protocol Engineering