情 報 保 護 學 會 誌
第 12 券 第 5 號, 2002. 10

IETF PKIX 작업반(Working Group)의 공개키 기반구조 표준화 동향

이 승 우*, 곽 진*, 정 찬 주**, 원 동 호***

요 약

최근 인터넷을 통한 전자상거래와 금융서비스가 널리 확산됨에 따라 인터넷 상에서 전송되는 정보의 안전과 신뢰성 확보에 필요한 정보보호 기술의 표준화 요구가 높아지고 있다. 이러한 인터넷 정보보호 기술의 표준화는 인터넷의 통일성과 표준을 유지하기 위해 설립된 IETF에 의해 수행되고 있으며, 공개키 기반구조(Public Key Infrastructure)에 관한 기술은 PKIX(Public Key Infrastructure X.509) 작업반에서 그 표준화를 담당하고 있다. 본 고에서는 IETF PKIX 작업반의 공개키 기반구조 관련 표준을 조사하였으며 최근의 표준화 활동을 분석한다.

Ⅰ. 서 론

최근 인터넷을 이용한 전자상거래가 급속히 증가하면서 개방된 네트워크인 인터넷에서의 정보보호를 위한 보안 관련 기술의 연구가 활발히 진행되고 있으며, 이에 대한 표준화 요구 역시 높아지고 있다. 이러한 정보보호 기술의 표준화를 위해 ISO/IEC JTC SC27, ITU-T, IETF(Internet Engineering Task Force)[1]와 같은 국제적 기구에서 표준화 작업을 진행하고 있으며, 이 중 IETF는 인터넷 상에서의 통일성과 표준을 유지하기 위해 설립된 국제 단체로서 정보보호 기술을 포함한 다양한 분야의 표준화를 진행하고 있다.

전자상거래와 같은 응용 분야에서 요구되는 다양한 정보보호 기술 중 상대방의 신분을 확인하고 전송하는 메시지에 대한 무결성 보장과 부인 방지 서비스를 제공하여 개방된 네트워크 환경에서 통신하는 당사자들에게 신뢰를 제공하는 기반 기술로 공개키 암호 방식[2]과 전자서명 기술이 널리 사용되고 있다. 이러한 공개키 암호 방식과 전자서명 기술에서는 각 사용자의 공개키에 대한 정당성을 검증할 수 있는 메커니즘이 필요하며, 이에 대한 해결 방안이 바로 공개키 기반구조[3]라 할 수 있다. IETF에서는 공개키 기반구조에 관련된 표준을 PKIX 작업반이 담당하고 있다.[4]

국내에서도 인터넷을 이용하는 전자상거래 등의 다양한 서비스가 급증하고 있으며, 이에 따른 정보보호 기술 표준화의 요구가 증가하고 있다. 이에 따라 관련 기관에서 정보보호 기술의 표준화가 진행되고 있으며, 이러한 표준화 과정에서 국제 표준을 준용하는 국내 표준을 제정하기 위한 국제 표준화 동향의 분석은 필수적이라 할 수 있다.

본 고에서는 공개키 기반구조의 표준화 동향을 분석하기 위해 IETF PKIX 작업반의 표준을 조사하고 최근의 표준화 활동을 분석한다.

본 고의 구성은 다음과 같다. Ⅱ장에서는 IETF의 표준화 과정과 PKIX 작업반에 대하여 소개하고, Ⅲ장에서는 PKIX 작업반의 표준화 현황을 살펴 본다. Ⅳ장에서는 IETF에서 PKIX 작업반의 최신 동향을 살펴보며, Ⅴ장에서 결론을 맺는다.

Ⅱ. IETF PKIX 작업반(Working Group)

1. IETF 개요

IETF는 네트워크 설계자, 운영자, 인터넷 구조

* 성균관대학교 정보통신공학부 정보통신보호연구실 ({swlee, jkwak}@dosan.skku.ac.kr)
** 한국정보보호진흥원(KISA) (cjchung@kisa.or.kr)
*** 성균관대학교 정보통신공학부 교수 (dhwon@dosan.skku.ac.kr)

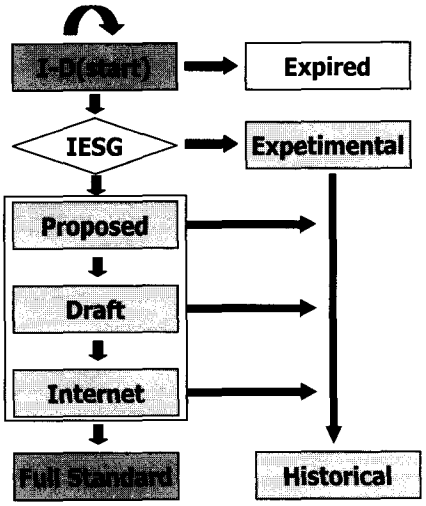
의 효율적인 운영과 관련된 연구 개발자들로 구성된 개방된 국제 단체로, 인터넷의 운영과 기술에 대한 문제점을 해결하기 위해 인터넷상의 프로토콜과 구조에 관한 표준 개발하고 있다.[5]

IETF의 실질적인 기술적 활동은 응용(Applications), 인터넷(Internet), 보안(Security) 등의 8개의 영역(Area)의 작업반 활동을 통해 이루어진다. 이중 보안 영역은 인터넷 정보보호 관련 사항을 연구하는 영역으로 인증기술의 표준을 개발하는 CAT(Common Authentication Technology), S/MIME 메일 보안 기술 표준을 개발하는 SMIME, 공개키 기반구조의 기술 표준을 개발하는 PKIX 등의 총 19개의 작업반이 소속되어 있으며, 이러한 IETF 작업반의 연구 결과는 IETF 문서들로 나타나게 된다.

IETF 문서는 크게 임시 문서인 I-D(In- ternet-Draft)와 RFC(Request For Com- ments)로 구분되며, RFC는 다시 표준 문서인 Proposed Standard, Draft Standard, Internet Standard와 비 표준 문서인 Historical, Informational, Experimental RFC로 구분할 수 있다.

I-D는 IETF에 의해 발표되며 이에 대한 다양한 의견이 메일링 리스트를 통해 제시된다. I-D는 6개월의 유효기간을 가지며 언제나 수정된 새로운 문서로 대체될 수 있다. 이렇게 대체된 문서는 다시 6개월의 유효기간을 갖게 된다. 이러한 I-D는 최종 Internet Standard으로 제정되기 위한 표준 트랙(Standards Track)에 오르기 위해 해당 영역 의장(chair)의 요청에 의해 IESG[6]에 제출되며, IESG의 승인을 얻게 되면 I-D는 RFC 일련번호를 부여 받아 Proposed Standard, Draft Standard, Internet Standard의 3단계로 나뉘어진 표준 트랙의 첫 번째 단계인 Proposed Standard로 지정된다. 이후 서로 다른 코드 기반의 상호 운용되는 독립적인 구현 명세가 개발되고 성공적 운영 경험이 존재하며, 해당 표준이 기반하고 있는 다른 표준들이 Draft Standatd 단계 이상인 경우 Draft Standard 단계로 승격 된다. 마지막으로 상당기간의 성공적인 운영 경험을 획득한 표준은 Internet Standard 단계가 되어 RFC 일련번호를 유지한체 별도의 표준 번호를 부여받게 된다.

표준 트랙의 문서가 다른 표준 문서로 대체되는 경우 Historical RFC의 지위를 갖게되며, 표준으로서의 의미를 상실하게 된다. Informational RFC는 표준 개발을 위한 일반적인 정보를 제공하기 위해 작성된다. Experimental RFC는 연구·개발 과정에서 만들어진 문서로 표준화 과정에 도움이 되리라 여겨지는 연구 결과를 나타낸다.[7]



[그림 1] IETF 표준화 문서 진행 과정

2. PKIX 작업반

PKIX 작업반은 인터넷에서 X.509 기반의 공개키 기반구조를 지원하기 위해 요구되는 인터넷 표준 개발을 목적으로 1995년 가을에 설립되었으며, ITU-T 공개키 기반구조 표준[8]을 기반으로 인터넷에 적합한 X.509 기반의 공개키 기반구조에 대한 새로운 표준을 개발하고 있다.

PKIX 작업반은 X.509 버전 3 인증서(certificate)와 X.509 버전 2 인증서 폐지 목록(Certificate Revocation List)의 명세(profile)를 제공하는 "인터넷 X.509 공개키 기반구조 인증서 및 인증서 폐지 목록 프로파일"[9, 10]을 개발하였으며, "인터넷 속성 인증서(Attribute Certificates) 프로파일"[11], 인증서와 인증서 폐지 목록의 저장을 위한 "인터넷 X.509 공개키 기반구조 LDAP v2 스키마"[12], "인터넷 X.509 공개키 기반구조 적격 인증서(Qualified Certificates) 프로파일"[13], "인터넷 X.509 공개키 기반구조 인증서 정책 및 인증 준칙 프레임워크"[14]와 같은 본래의 설립 목적을 위한 표준 트랙 문서를 개발하였다.

또한 PKIX 작업반은 ITU-T에서 기술하지 않고 있는 확장된 범위의 표준으로 "인터넷 X.509 공개

키 기반구조 인증서 관리 프로토콜(CMP)"[15], "인터넷 X.509 공개키 기반구조 온라인 인증서 상태 프로토콜(OCSP)"[16], "인터넷 X.509 인증서 요청 메시지 형식(CRMF)"[17], "인터넷 X.509 공개키 기반구조 타임 스템프 프로토콜(TSP)"[18], "CMS를 이용한 인증서 관리 메시지"[19], 공개키 기반구조의 운영에 관한 전송을 위한 "인터넷 X.509 공개키 기반구조 운용 프로토콜 : FTP와 HTTP"[20] 등이 새로 개발되었다. 그리고 PKIX 문서들 간의 관계를 제공하는 "roadmap"이 Infor- mation RFC로 제공된다.

현재 PKIX 작업반에서는 기존 표준 트랙에 존재하는 표준들을 Proposed Standard에서 Draft Standard로 진행시키기 위한 작업이 진행되고 있으며, LDAP과 같이 다른 영역의 프로토콜과 관련된 표준의 개정 작업이 진행되고 있다. 또한 위임 경로 발견/위임 경로 검증(DPD/DPV)과 관련된 문서의 개발 작업과 인증서에 대한 정보를 사용자가 직관적으로 이해하도록 표현하는 로고 유형(logotype) 개발, 프록시(proxy) 인증서 확장과 이의 처리방법의 개발, 공개키 기반구조 손상 회복에 대한 문서의 개발 등이 새로운 작업 사항으로 진행되고 있다.

Ⅲ. PKIX 작업반의 표준화 동향

IETF pkix 작업반의 문서는 다음과 같이 서로 다른 5개의 영역으로 나누어 볼 수 있다.[21]

- 인증서 및 인증서 폐지 목록 프로파일
- 운영 프로토콜(Operation Protocol)
- 관리 프로토콜(Management Protocol)
- 인증서 정책과 인증 준칙
- 타임 스템핑과 데이터 인증 서비스

첫 번째 영역은 인터넷을 위한 X.509 버전 3 인증서와 X.509 버전 2 인증서 폐지 목록 표준의 프로파일을 포함하며, 두 번째 영역에서는 인증서와 인증서 상태와 같은 정보를 얻는 운영 프로토콜을 포함한다. 세 번째 영역은 공개키 기반구조 운영을 위해 요구되는 정보들을 교환하는 각 객체들 간의 운영 프로토콜을 포함하며, 네 번째 영역은 인증서 정책과 인증 준칙에 관한 정보를 제공하고, 마지막 다섯 번째 영역에서는 타임 스템프(Time Stamp) 프로토콜과 부인 방지와 같은 서비스에 사용될 수 있는 데이터 인증 서비스에 대해 다룬다.

1. 프로파일(Profiles)

ITU-T X.509 버전 3 공개키 인증서는 기본 필드(field)와 많은 선택적인 확장(extension)으로 구성된 매우 복잡한 데이터 구조를 갖고 있다. X.509 버전 3 공개키 인증서에 기반한 인터넷 공개키 기반구조를 구축하기 위해 PKIX 작업반은 인터넷에 적합한 X.509 버전 3 공개키 인증서 프로파일을 개발했다.

X.509 버전 3 공개키 인증서 프로파일은 공개키 인증서 필드들의 내용과 반드시 지원되어야 하는 확장 필드들과 지원 가능해야 하는 확장 필드들, 그리고 때로는 지원하면 안되는 확장 필드에 대해 세부적으로 기술하고 있다. "인터넷 X.509 공개키 기반구조 인증서 및 인증서 폐지 목록 프로파일[RFC 2459]"은 인터넷 공개키 기반구조를 위한 X.509 버전 3 공개키 인증서의 프로파일을 제공하며 많은 확장 필드에서의 값들에 대한 범위를 제시하고 있으며, 또한 X.509 버전 2 인증서 폐지 목록 프로파일을 제공한다.

최근 [RFC 2459]를 개정한 [RFC 3280]이 발표 되었다. 이 [RFC 3280]에서는 그동안 문제로 지적되었던 인증서 검증 알고리즘을 더욱 자세히 기술하였으며, 인증서 폐지 목록을 사용하여 인증서의 상태를 결정하기 위한 알고리즘이 추가 되었다. 또한 delta-CRL을 이용하는 모델이 제공되었으며, subject info access, inhibit any-policy, freshest CRL의 4개의 확장 필드가 새롭게 추가되었다.

공개키 기반구조에서 특정 암호학적 알고리즘을 위한 Object Identifier(OID)를 정의하기 위해 공개키 인증서와 인증서 폐지 목록을 위한 부가적인 기술서가 필요하다. PKIX 작업반에서는 특정 알고리즘의 적합한 구현에 대한 가이드를 제공하는 두 문서 [RFC 2528]과 [RFC 3279]를 제작하였다.

현재 많은 국가에서 전자서명을 승인하고 통제하기 위해 법률 구조를 개정하는 과정에 있다. 이에 적격 인증서(Qualified Certificates)라고 불리는 공개키 인증서의 기본적인 요구사항이 요구된다. 이러한 요구의 결과로서 인증된 주체의 명백한 신원을 표현하기 위한 공통된 구조에 대한 표준화 토대를 제공하는 명확한 공개키 인증서 프로파일의 제정 필

요성이 제기되었다. 1998년 12월, PKIX 작업반은 이에 대한 결과로 공개키 인증서의 더욱 자세한 프로파일인 적격 인증서[RFC 3039]를 채택했다.

[표 1] 인증서 및 인증서 폐지 목록 프로파일 관련 표준

문서명	표준 상태
Internet X.509 Public Key Infrastructure Certificate and CRL Profile [RFC 2459]	Historical
Internet X.509 Public Key Infrastructure Certificate and CRL Profile [RFC 3280]	Proposed
Internet X.509 Public Key Infrastructure Qualified Certificates [RFC 3039]	Proposed
An Internet Attribute Certificate Profile for Authorization [RFC 3281]	Proposed
Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates[RFC 2528]	Informational
Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile [RFC 3279]	Proposed
Internet X.509 Public Key Infrastructure Permanent Identifier	I-D
Supplemental Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile	I-D
Internet X.509 Public Key Infrastructure Proxy Certificate Profile [Proxy]	I-D
Internet X.509 Public Key Infrastructure Logotypes in X.509 Certificate [Logo]	I-D
X.509 Extensions for IP Addresses and AS Identifiers	I-D
Warranty Certificate Extension	I-D

X.509 버전 3 공개키 인증서와 마찬가지로 속성 인증서(Attribute Certificate) 또한 매우 복잡한 데이터 구조를 갖고 있다. 이러한 속성 인증서에 기반한 인터넷 권한관리 기반구조(Privilege Management Infrastructure)를 구축하기 위해 PKIX 작업반은 속성 인증서 프로파일을 개발하였다.

속성 인증서 프로파일은 속성 인증서의 내용과 확장 필드, 응용 가능한 속성(attribute)들에 대한 설명이며, [RFC 3281]는 인터넷 X.509 버전2 속성 인증서의 프로파일을 제공한다.

■ Internet X.509 Public Key Infrastructure Certificate and CRL Profile [RFC 2459]

이 문서는 인터넷을 위한 X.509 버전3 공개키 인증서와 버전 2 인증서 폐지 목록의 형식과 의미를 기술한다. 또한 인증 경로를 처리하기 위한 절차 역시 기술된다. 이 프로파일은 1988년에 발표된 ASN.1으로 기술되며, 기본적인 인증 경로 검증과정을 포함한다. 이 문서는 [RFC 3280]으로 대체되어 Historical RFC의 상태를 갖는다.

■ Internet X.509 Public Key Infrastructure Certificate and CRL Profile [RFC3280]

이 문서는 [RFC 2459]의 개정본이다. 이 개정에서 ITU-T X.509 인증 경로 검증 결과와 [RFC 2459]의 인증 경로 검증 결과가 서로 다르게 나왔던 문제점을 해결하기 위해 인증 경로 검증 알고리즘이 강화되었으며, CRL의 검증 알고리즘이 추가되었다. 또한 새로운 인증서와 CRL의 확장 필드들이 추가되었다. 기존 [RFC 2459]에서 다루었던 공개키와 전자서명 알고리즘의 식별자(Identifier)와 인코딩은 [RFC 3279]로 분리되었다.

■ Internet X.509 Public Key Infrastructure Qualified Certificates [RFC 3039]

이 문서는 [RFC 2459]에 근거한 인터넷에서 사용되는 적격 인증서라 불리는 특정 형태의 공개키 인증서에 대한 프로파일을 제공한다. 적격 인증서는 관할 법률 안에서 특정 자격의 지위를 갖는 인증서를 나타내기 위해 사용되며, 자연인에게만 발행된다.

이 문서의 목적은 국가별 또는 지역별 법적 요구사항으로부터 독립된 일반적인 구문을 정의하는 것으로, 인증서 공개키의 사용목적에 오직 부인 방지만을 나타낸다. 하지만 미 적격 인증서 프로파일 자체는 인증서에 대한 어떠한 법적 요구사항도 정의하지 않는다.

■ **An Internet Attribute Certificate Profile for Authorizations [RFC 3281]**

이 문서는 다양한 인터넷 프로토콜에서 요구되는 권한 인증 서비스를 제공하기 위한 X.509 버전 2 속성 인증서의 요구사항을 정의하며, 속성 인증서 형식을 기술한다.

기본적인 권한 인증(basic authorizations)의 지원과 대리인(proxy)을 통해 수행될 수 있는 서비스들의 지원에 관한 프로파일이 정의되어 있다.

■ **Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates [RFC 2528]**

이 문서는 키 교환 알고리즘(KEA)를 사용하는 공개키 기반구조의 사용자를 위한 가이드와 식별자를 제공한다. 이 문서는 KEA 키들을 담고 있는 X.509 버전 3 공개키 인증서의 subjectPublicKeyInfo 필드와 keyUsage extension의 구문과 의미를 설명한다. KEA를 제공하려는 사람은 이 문서의 프로파일을 따라야 한다.

■ **Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile [RFC 3279]**

이 문서는 인증서와 인증서 폐지 목록에서 사용되는 암호학적 알고리즘, 키(key), 키 관련 파라메터(parameter)와 전자서명의 표현을 위한 알고리즘 식별자, 그리고 인코딩 형식을 지정한다. 본 문서의 내용은 [RFC 2459]의 7장과 대응된다.

■ **Internet X.509 Public Key Infrastructure Permanent Identifier [PI]**

이 문서는 공개키 기반구조에서 각 개체의 공개키 인증서의 subjectAltName 확장 필드에 포함되는 Permanent Identifier(PI)라는 새로운 이름(name) 형식을 정의한다. 인터넷 상의 각 개체에게 할당되는 PI는 인증기관(Certificate Authority)에 의해 발행된 모든 인증서들에서 유일하다. 이러한 PI는 인증기관의 이름 또는 가입사항이 변경되더라도 동일인에 관련된 인증서를 지정할 수 있도록 사용할 수 있는 선택적인 방법이다. PI는 접근 제어(Access Control)와 부인 방지(Non-repudation)에 있어 매우 중요하다.

■ **Supplemental Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile**

이 문서는 새로운 암호학적 알고리즘의 표현을 위한 인코딩 형식과 알고리즘 식별자를 지정함으로써 [RFC 3279]의 부족한 면을 채우며, SHA-256과 같은 큰 해쉬 함수를 사용한 전자서명 뿐 아니라 lattice 기반의 공개키 알고리즘을 포함한다.

■ **Internet X.509 Public Key Infrastructure Proxy Certificate Profile [Proxy]**

이 문서는 [RFC 2459]의 개정판인 [RFC 3280]에서 정의된 X.509 공개키 기반구조 인증서에 기반하는 인터넷 사용을 위한 대리 인증서(Proxy Certificate)의 프로파일을 구성한다.

대리 인증서는 공개키 기반구조에 기반한 인증 시스템에서 제한된 대역(impersonation) 지원을 목적으로 하는 일반적인 X.509 Public Key End Entity certificate, 또는 다른 대리 인증서로부터 서명 또는 유도된 인증서를 설명하는데 이용된다.

■ **Internet X.509 Public Key Infrastructure Logotypes in X.509 Certificate [Logo]**

이 문서는 공개키 인증서와 속성 인증서에서 공인 인증서 마크와 같은 로고유형을 정의하여 사용자에게 직관적인 인증서의 정보를 제공하는 인증서 확장 필드를 기술한다.

■ **X.509 Extensions for IP Addresses and AS Identifiers**

이 문서는 두 사적(private) X.509 버전 3 인증서 확장 필드를 정의한다. 첫 번째는 IP 주소 리스트를 인증서 주체에 연결하는 것이고, 두 번째는 자율 시스템(Autonomous System)의 식별자를 인증서 주체에 연결하는 것이다. 이러한 인증서 확장 필드는 인증서 주체의 권한 허가(authorization)에 사용된다.

■ **Warranty Certificate Extension**

이 문서는 인증기관에 의해 제공된 보증(warranty)을 명확히 기술하기 위한 인증서 확장 필드를

설명한다.

보증 인증서 확장은 X.509 공개키 인증서와 관련된 보증 정책(warranty policy)을 나타내게 된다. 종종 인증기관은 인증서의 적용 범위를 보증하기 위해 특정 보험 정책을 제시하게 되며, 인증서 보증은 인증기관의 합법적인 책임을 보장하기 위해 보증 타입과 금액 등의 확장 범위를 제공하게 된다.

2. 운영 프로토콜(Operation Protocol)

운영 프로토콜은 인증서를 사용하는 시스템들 간의 인증서와 인증서 폐지 목록(또는 인증서 상태 정보)을 전송하는데 요구된다. 이러한 정보의 전송은 인증서와 인증서 폐지 목록을 전송하는 DNS, LDAP, HTTP, FTP, X.500 등에 기반한 배포 과정을 포함하는 다양한 수단이 요구된다.

〔표 2〕 운영 프로토콜(Operation Protocol) 관련 문서

문서명	표준 상태
Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2 〔RFC 2559〕	Proposed
X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP 〔RFC 2560〕	Proposed
Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP 〔RFC 2585〕	Proposed
Internet X.509 Public Key Infrastructure LDAPv2 Schema 〔RFC 2587〕	Proposed
Diffie-Hellman Proof-of-Possession Algorithms 〔RFC 2875〕	Proposed
Internet X.509 Public Key Infrastructure LDAP Schema and Syntaxes for PKIs and PMIs	I-D
Simple Certificate Validation Protocol (SCVP)	I-D
Delegated Path Validation and Delegated Path Discovery Protocol Requirements	I-D
Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv3	I-D

■ Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2 〔RFC 2559〕

이 문서는 저장소(repository)로부터 인증서와 인증서 폐지 목록을 발행 또는 검색하는 공개키 기반구조 요소 프로토콜로 LDAPv2의 사용에 관해 기술한다. 이 문서에 기술된 메커니즘은 〔RFC 1777〕에 정의된 LDAPv2에 기초하고 있으며 공개키 기반구조에서 사용하기 위한 프로토콜의 프로파일을 정의하고 〔RFC 1778〕의 인증서와 인증서 폐지 목록에 대한 인코딩을 갱신한다.

■ X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP 〔RFC 2560〕

이 문서는 인증서 폐지 목록을 사용하지 않고 인증서의 현재 상태를 결정하는데 유용한 프로토콜을 기술한다. 인증서 기반 시스템의 가장 큰 문제점은 인증서 사용자가 인증서 검증 과정에서 현재 인증서 폐지 목록을 검색해야하는 것이다. 인증서 폐지 목록의 크기를 감안하면 이것은 인증서를 사용하는 시스템에 있어 심각한 문제가 될 수 있다.

또한 인증서 폐지 목록을 사용하는 방식의 경우 적시성 또는 현재성(timeliness) 문제를 야기할 수 있다. 만약 인증서 폐지 목록이 중간 발표 없이 일주일의 주기로 발행된다면, 인증서는 실제로 폐지된 상태로 일주일간 사용될 수 있고 이로 인해 인증서의 정당하지 않은 사용이 일어날 수 있다. OCSP는 이러한 문제를 다루고 있다.

OCSP는 relying party가 하나 또는 여러 인증서를 인증된 OCSP responder에게 제시하고 responder는 그 인증서에 대한 "revoked", "notRevoked", "unknown" 등의 인증서의 상태를 되돌려주는 메커니즘을 제공한다. 이러한 메커니즘은 인증서 폐지 상태를 전송하는데 필요한 통신 대역폭을 매우 효과적으로 줄일 수 있다. 이로서 relying party는 인증서의 상태를 체크하기 위해 수많은 인증서 폐지 목록을 검색 할 필요가 없게 된다.

이러한 OCSP를 사용함으로서 인증서 폐지 상태 공표의 적시성을 향상시키며, 폐지된 인증서를 사용하게 되는 가능성이 줄어들게 된다.

이 문서에서는 인증서의 상태를 검사하는 클라이언트와 인증서 상태를 제공하는 서버간에 교환되는 데이터의 형식을 정의한다.

■ **Internet X.509 Public Key Infrastructure Operational Protocols : FTP and HTTP [RFC 2585]**

이 문서는 공개키 기반구조 저장소로부터 인증서와 인증서 폐지 목록을 얻는 FTP(File Transfer Protocol)프로토콜과 HTTP(Hyper-text Transfer Protocol)프로토콜을 사용하기 위한 규약을 기술한다.

■ **Internet X.509 Public Key Infrastructure LDAPv2 Schema [RFC 2587]**

이 문서는 공개키 인증서와 인증서 폐지 목록의 검색을 위한 LDAPv2를 지원하는데 필요한 최소한의 스킴을 정의하고 공개키 기반구조를 위한 기능들을 설명한다. 공개키 기반구조의 저장소로 작동하는 LDAP 서버는 이 문서에서 정의된 객체 클래스들을 지원해야 한다.

■ **Diffie-Hellman Proof-of-Possession Algorithms [RFC 2875]**

이 문서는 Diffie-Hellman 키 쌍으로부터 무결성 검사값을 생성하기 위한 두 방법을 기술한다. 첫 번째 알고리즘에서는 특정 수신자와 확인자를 위해 확인자의 공개키로 무결성 검사값을 생성하며, 두 번째 알고리즘에서는 임의의 확인자를 위해 무결성 검사값을 생성한다. 이러한 메커니즘은 인증서 요청 과정에서 요구되며, 일반적인 목적의 서명이 아니라 개인키 소유 증명(Proof-of-Possession)을 지원하기 위해 설계되었다.

■ **Internet X.509 Public Key Infrastructure LDAP Schema and Syntaxes for PKIs and PMIs**

이 문서는 [RFC 2587]에서의 공개키 기반구조와 권한관리 기반 구조를 지원하도록 요구되는 LDAP 스킴을 기술한다. 또한 인증서 및 인증서 폐지 목록의 저장을 위한 스킴을 기술하며, LDAP 디렉토리 서버에서 속성 인증서와 속성 인증서 폐지 목록의 적절한 매칭을 기술한다. 이 Internet-Draft는 [RFC 2587]의 내용을 폐지하는 것이 아니라 이를 보충하는 것이다.

■ **Simple Certificate Validation Protocol [SCVP]**

SCVP(Simple Certificate Validation Protocol)는 인증서 처리의 부담을 기존의 클라이언트에서 서버에게 부가하는 프로토콜로 서버는 인증서가 유효한지 또는 인증 경로가 신뢰 지점에 도달하는지 등의 인증서에 관련된 다양한 중요 정보를 제공할 수 있다.

■ **Delegated Path Validation and Delegated Path Discovery Protocol Requirements [DPV&DPD- REQ]**

이 문서는 대리 인증서 경로 검증(DPV: Delegated Path Validation)과 대리 인증서 경로 발견(DPD: Delegated Path Discovery) 서비스의 요청·응답(request·response) 쌍을 위한 요구사항을 기술한다. 첫 번째로 DPV는 DPV 서버에게 인증 경로 검증 과정을 전부 위임하기 위해 사용될 수 있다. 두 번째로 DPD는 DPD 서버에게 인증서 상태 정보를 포함한 인증 경로 발견을 위임하는데 사용할 수 있다.

■ **Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv3**

이 문서는 X.509 인증서와 인증서 폐지 목록에 기반한 공개키 기반구조를 지원하기 위해 요구되는 LDAPv3에 대해 기술한다.

LDAPv2는 다른 문자 집합을 지원하지 못하며 제한된 인증 스킴을 정의하는 등의 특정 환경에서 자신의 유용한 기능이 제한되는 많은 결함을 가지고 있기 때문에 IETF는 이의 표준화를 중단하였으며, 이를 LDAPv3로 대체하였다. 이 문서는 X.509에 기반한 공개키 기반구조를 지원하는 서버를 위해 필요한 LDAPv3의 특성들을 기술한다.

3. 관리 프로토콜(Management Protocol)

관리 프로토콜(Management protocols)은 공개키 기반구조의 사용자와 관리 개체(Management entities)들 사이의 온라인(on-line) 상호작용을 지원하는 프로토콜이다. 예를 들면 관리 프로토콜은 인증기관과 클라이언트 시스템 또는 두 인증기관 사

이에서의 상호 인증에 사용될 수 있다. 관리 프로토콜은 사용자 또는 클라이언트 시스템의 등록 정보를 전송하기 위해 또는 인증서의 취소를 요청하는데 사용될 수 있다.

관리 프로토콜은 둘로 나눌수 있다. 첫 번째는 전송되는 메시지의 형식이고, 두 번째는 메시지의 전송을 관리 운용하는 실제 프로토콜이다. PKIX 작업반은 요구되는 메시지 포맷을 기술한 [RFC 2511]과 인증서 관리 메시지 형식(CMMF: certificate management message format)의 두 문서와, 메시지를 서로 교환하기 위한 프로토콜로 [RFC 2510]과 [RFC 2797]의 두 문서를 개발했다. 하지만 CMMF 드레프트에 정의된 메시지 포맷은 두 [RFC 2510]과 [RFC 2797]에 삽입되었기 때문에 CMMF 드레프트는 PKIX 작업반의 문서에서 탈락되었다.

[표 3] 관리 프로토콜(Management Protocol) 관련 문서

문서명	표준 상태
Internet X.509 Public Key Infrastructure Certificate Management Protocols [RFC 2510]	Proposed
Internet X.509 Certificate Request Message Format [RFC 2511]	Proposed
Certificate Management Messages over CMS [RFC 2797]	Proposed
Certificate Management Protocols [2510bis]	I-D
Certificate Request Message Format [2511bis]	I-D
Certificate Management Messages over CMS [2797bis]	I-D
Transport Protocols for CMP [CMPT]	I-D
CMC Transport	I-D
Attribute Certificate Request Message Format [ACRMF]	I-D
Attribute Certificate Management Messages over CMS [ACMC]	I-D

■ *Internet X.509 Public Key Infrastructure Certificate Management Protocols [RFC 2510]*

이 문서는 공개키 기반구조 요소들 중에서 [RFC 2511]에서 기술된 메시지 전송을 위해 개발된 새로운 프로토콜을 기술한다. 일반적으로 [RFC 2510]은 [RFC 2511]과 공동으로 사용되며, 완전한 공개키 기반구조 관리 서비스를 지원하기 위해 S/MIME, HTTP 등의 전송 서비스와 함께 사용될 것이다.

■ Internet X.509 Certificate Request Message Format [RFC 2511]

[RFC 2511]은 relying party가 인증기관에 새로 인증서를 요청하는 경우나 등록기관(Registration Authority)에게 인증서를 요청하기 위해 도움을 받을 때 권장되는 형식을 기술한다. 요청 메시지 형식은 많은 다른 메시지 형식들이 완성되기 이전에 요구되었기 때문에 분리된 문서로 만들어졌다.

이 문서는 오직 메시지의 형식만을 기술하고 있으며, 메시지를 전송하기 위한 프로토콜의 설계 명세는 [RFC 2511]의 범위 밖이다.

■ Certificate Management Messages over CMS [RFC 2797]

이 문서는 공개키 기반구조상의 클라이언트와 서버가 전송 정보의 안전을 위해 S/MIME작업반의 암호학적 메시지 구문(CMS)를 사용할 때 공개키 기반구조 메시지를 교환하는 방법을 정의한다. [RFC 2797]은 다른 여러 인증서 관리 메시지들처럼 인증서 요청 메시지 형식[RFC2511]에서 기술된 인증서 요청 메시지 body를 제공한다.

이 설계 명세의 첫 번째 목적은 공개키 기반구조 관리 프로토콜로서 새로운 프로토콜을 개발하지 않고 이미 개발된 프로토콜(S/MIME CMS)을 사용하기 위함이며, 두 번째 목적은 인증서 요청을 위한 산업계 실용 표준인 PKCS#10 메시지를 IETF 표준으로 만들기 위함이다.

■ Certificate Management Protocols [2510bis]

이 문서는 [RFC 2510]의 개정판이며, 상호운용 테스트의 결과를 반영하고 있다. 개정된 문서에서는 새로운 드레프트 문서인 [CMPT]로 [RFC 2510]의 전송 프로토콜을 분리하였으며, 현재 상호 운용 테스트 결과의 문서화를 준비하고 있다.

■ Certificate Request Message Format [2511bis]

이 문서는 [RFC 2511]의 개정판이며, 상호 연

동 테스트의 결과를 반영하고 있다.

현재 상호 운용 테스트 결과의 문서화를 준비하고 있다.

■ Certificate Management Messages over CMS [2797bis]

이 문서는 [RFC 2797]의 개정판이다.

■ Transport Protocols for CMP [CMPT]

이 문서는 [RFC 2510] 인증서 관리 프로토콜이 다양한 전송 프로토콜 상에서 어떻게 이용되는지를 기술한다. [RFC 2510] 5장에 기술된 다양한 프로토콜상에서의 직접적인 DER 인코딩 인증서 관리 메시지의 전송 과정이 기술되었다.

이 문서의 목적은 상호 운용에서의 충돌을 피하기 위해 프로토콜을 강화시키는 것이며, 후에 전송관련 부분을 다른 프레프트로 분리하고자 한다.

■ CMC Transport [TPCMC]

이 문서는 [RFC 2797] 메시지를 전송하는데 사용되는 다양한 전송 메커니즘을 정의한다. 이러한 전송 메커니즘들로 HTTP, file, mail, TCP 등이 기술되어 있다.

■ Attribute Certificate Request Message Format [ACRMF]

인증서 요청 메시지 형식[RFC 2511]은 인증기관 또는 지역 등록기관(Local Registration Authority)으로부터 X.509 공개키 인증서를 요구하는 형식을 명시한다.

이 문서는 [RFC 2511]에 기반하며 속성기관(Attribute Authorities) 또는 속성 등록기관(Attribute Registration Authority)으로부터 X.509 속성 인증서를 요구하는 형식을 명시한다.

■ Attribute Certificate Management Messages over CMS [ACMC]

이 문서는 속성 인증서를 관리하기 위한 [2797bis]의 수정사항들을 기술한다.

이 문서는 독립적으로 사용되지 않고 반드시 [2797bis]와 함께 사용되야하며, [ACRMF]와 함께 사용된다.

4. 정책(Policy)

앞서 기술한 인증서 프로파일과 운영 및 관리 프로토콜은 실제 안전한 공개키 기반구조의 개발과 구현 문제에 관한 부분을 나타낸다. 공개키 기반구조에서는 인증서 정책(Certificate Policy)과 인증 업무 준칙(Certification Practice Statement)의 개발 역시 필요하다. 인증서 정책과 인증 업무 준칙은 인증서 발급과 사용에 있어 물리적, 인적 보안사항, 주체 신원확인 사항, 인증서 폐지 정책등의 다양한 항목들을 나타내야 한다. [RFC 2527]은 인증 업무 준칙의 프레임워크를 제공한다.

[표 4] 정책(Policy) 관련 문서

문서명	표준 상태
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC 2527]	Informational
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	I-D

■ Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC 2527]

앞선 설명에서처럼 인증서 프로파일, 운영 프로토콜, 관리 프로토콜에 대한 기술과 구현은 공개키 기반구조 구축의 단지 한 부분이다. 인증서 보안 정책과 인증 업부 준칙의 개발과 적용 역시 모두 다 중요하다.

이 문서의 목적은 인증서 정책(CP)과 인증 업무 준칙(CPS)들 사이의 명확한 관계를 설립하고, 인증서 정책 또는 인증 업무 준칙의 작성자들을 위한 프레임워크를 제공하는 것이다. 특히, 프레임워크는 인증서 정책 또는 인증 업무 준칙을 공표하는 경우 고려해야 할 요소들을 명시한다. 이 문서에서는 특정 인증서 정책 또는 인증 업무 준칙을 정의하지는 않는다.

■ Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [2527bis]

이 명세는 [RFC 2527]의 개정판이며, 위에서기

술한대로 이 문서의 목적은 인증서 정책과 인증 업무 준칙 사이의 관계를 명확히 하는 것과 인증서 정책과 인증 업무 준칙의 작성자들을 돕는 프레임워크를 제공하는 것이다. 이 문서 안에서 기술한 프레임워크는 기본적으로 [RFC 2527]에서 기술된 프레임워크의 포함집합(superset)이다.

5. 타임 스템핑과 테이타 검증 서비스

1998년 후반, PKIX 작업반은 본래의 작업반 작업영역에는 없었지만, 작업반에서 원하는 보안 서비스들을 제공하는데 사용될 수 있는 기반구조 서비스를 개발하기 시작했다.

이러한 서비스의 첫 번째는 [RFC 3161]에서 기술된 타임 스템핑(Time Stamping)이다. 이 서비스는 신뢰된 제삼자(TTP; Trusted Third Party)인 타임 스템프 기관(TSA; Time Stamp Authority)이 주어진 메시지가 타임 스템핑된 시간 이전에 존재했다는 증거를 제공하기 위해 메시지에 서명하는 서비스다. 타임 스템핑은 사용자가 업무 또는 거래가 나중에 비밀키의 손상으로 위조되었다는 주장을 할 수 없도록하는 부인방지를 위한 지원수단을 제공한다.

[RFC 3161]의 있는 몇몇 구성요소들은 저작권을 소유한 특허에 관련되어 있어 [RFC 3161]를 구현하는데 관심이 있는 사람은 누구나 이 지적 소유권 문제를 알고 있어야 한다.

두 번째는 데이터 검증 및 인증 서버(DVCS)의 정의다. DVCS는 제시된 특정 데이터의 정확성을 검증하는 TTP다. 이 또한 실뢰할 수 있는 서버의 위임을 허락하며, 검증의 체인을 허락한다.

TSA의 경우 인증을 얻기 위해 전송된 메시지를 검증하지 않고 단지 현재 시간에 대한 증거만을 서명을 통해 첨부 할 뿐 주어진 메시지의 정확함이나 정당성에 대한 어떠한 증거도 제공하지 않는다. 이에 대조적으로 DVCS는 데이터의 소유 또는 전자서명의 검증을 인증하며, 이때 DVCS는 요청의 전자서명에 대한 정확성을 검증하며, 전자서명의 신뢰지점에서부터의 전체 인증 경로를 검사한다.

DVCS는 부인방지 서비스를 두가지 방법으로 제공한다. 첫번째로 DVCS는 서명 또는 공개키 인증서가 특정 시점에서 유효했다는 증거로 데이터 검증 인증서(DVC; Data Valid- ation Certificate)를 제공한다. DVC는 해당 공개키 인증서가 폐기되었거나 폐지 정보가 인증서 폐지 목록에서 더이상 사용가능하지 않더라도 사용될 수 있다. 두 번째는 전자서명이나 공개키 인증서의 인증을 위한 서명된 응답의 데이터 검증 인증서의 생성은 요청된 전자서명 또는 공개키 인증서의 검증에 대한 충분한 노력이 요청자에 의해 수행되어진 증거를 제공한다.

[표 5] 타임 스템프와 데이터 인증 서비스 관련 문서

문서명	표준 상태
Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols [RFC 3029]	Experi-mental
Internet X.509 Public Key Infrastructure Time Stamp Protocols [RFC 3161]	Proposed
Delegated Signature Validation Protocol Requirements (DSV-REQ)	I-D
Internet X.509 Public Key Infrastructure Time-Stamp Protocol [3161bis]	I-D
Policy Requirements for Time-Stamping Authorities	I-D

위임 서명 검증 서버(Delegated Signature Validation Server)의 개념은 위임 인증 경로 검증 서버(Delegated Path Validation Server)의 유사한 개념으로 소개되었다. 위임 서명 검증 서비스들은 relying party가 특정시간의 인증 경로를 포함한 전자서명된 객체의 정당성을 확인한다.

■ Internet X.509 Public Key Infrastructure Time Stamp Protocols [RFC 3161]

이 문서는 타임 스템프 서비스(Time Stamp Service)를 위한 명세사항을 정의한다. 이 문서는 신뢰할 수 있는 타임 서비스를 유지하는 TTP인 TSA를 정의한다. TSA는 타임 스템프 요청을 받게되면 특정 시간 이전에 요청이 있었다는 것을 인증할 수 있는 토큰을 생성하기 위해 요청에 현재 시간을 첨부하고 이를 서명한다. 이는 업무 또는 거래의 소급시 정당한 사용자를 보호함으로서 부인방지를 제공한다. 이러한 서비스를 제공함으로서 업무

또는 거래를 소급해 정당성을 문제삼을 수 없도록 한다.

TSA는 어떠한 데이터 분석(data parsing) 서비스도 제공하지 않는다는 점에 주의해야 한다. 이것은 TSA가 서명의 정당함은 검증하지 않는다는 것이다.

■ **Internet X.509 Public Key Infrastructure Data Certification Server Protocols [RFC 3029]**

이 문서는 메시지 또는 서명의 존재와 정확함 모두를 확인하는데 사용되는 데이터 검증 및 인증 서비스(DVCS; Data Validation and Certification Service)를 정의한다.

DVCS는 전자서명된 문서의 정확성, 공개키 인증서의 유효성, 데이터의 소유나 존재 사실을 증명하며 데이터 검증 서비스를 제공하는 TTP이다. 이러한 검증의 결과로 DVC를 생성하게 되고, 이 DVC는 데이터 소유 주장의 정확성, 공개키 인증서의 유효성이나 폐지 상태, 전자서명된 문서의 유효성과 정확성 등에 관한 증거를 제공하기 위해 사용될 수 있다.

DVC의 존재는 전자서명된 문서나 공개키 인증서가 DVC에 표시된 시점에서 유효했음에 대한 증거를 제공함으로써 부인 방지 서비스를 지원한다.

■ **Delegated Signature Validation Protocol Requirements [DSV-REQ]**

이 문서는 디지털 서명의 검증을 위임 서명 검증 서버에게 전적으로 위임하기 위한 요구사항을 기술한다. 검증은 서명 정책(Signature Policy)이라 불리는 규칙 집합을 사용하여 수행된다.

이 문서는 두 요청/응답의 쌍을 위한 정의된 서명 정책의 세목을 얻기 위해 서명 검증 서버가 서명 정책을 나타낼 수 있게 하거나 서명 정책의 참조(reference)를 주기 위한 요구사항을 정의한다.

■ **Internet X.509 Public Key Infrastructure Time-Stamp Protocol [3161bis]**

이 문서는 [RFC 3161]의 개정판이다.

■ **Policy Requirements for Time-Stamp Authorities**

이 문서는 타임 스템핑 서비스의 운영에서 가입자들이 신뢰할 수 있는 TSA의 운영과 관리 업무의 정책 요구사항을 정의한다.

이 문서의 내용은 기술적으로 ETSI TS 102 023 V1.1.1과 동등하다.

〈그림 2〉는 지금까지 소개한 표준 문서들의 관계를 나타낸 것이다.

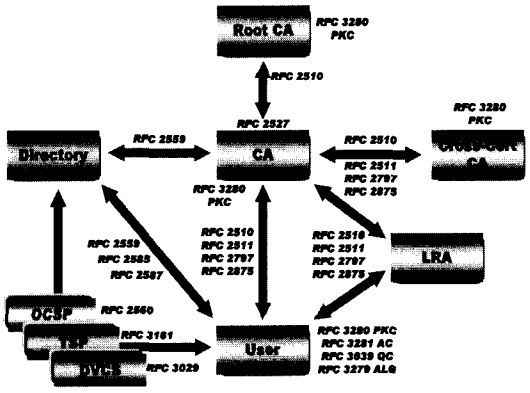
Ⅳ. 최근 동향

1. 52차 솔트레이크 IETF 미팅

본 절에서는 지난 2001년 12월에 있었던 52차 솔트레이크 IETF 미팅[22]에서의 PKIX 작업반의 회의 내용을 정리한다.

먼저 PKIX 작업반의 문서들의 상태를 살펴보면 [RFC 2459]를 대체하기 위한 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile(draft-ietf-pkix-ipki-new- part1-11.txt)"과 "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile (draft-ietf-pkix-ipki-pkalgs-05.txt)"이 IESG에 의해 승인되 RFC 작성자 큐(queue)에 올랐다.

또 "Internet X.509 Public Key Infrastructure: Roadmap"과 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [2527bis]" 두 문서는 수정되어 Informational RFC로서 재발행을 준비하고 있다.



[그림 2] IETF 표준의 상호 관계

[RFC 2510], [RFC 2511], [RFC 2560] 세

RFC는 Draft Standard 상태로 진행되기 위해 준비중이다. 이중 [RFC 2510]과 [RFC 2511]은 상호 연동 가능성 시험을 완료했으나 문서화되기 위한 결과가 요구되고 있으며, [RFC 2560]은 상호 연동 가능성 시험을 완료하였고, 그 결과의 문서화 역시 완료되었다. [RFC 2797]은 이러한 과정을 뒤따르게 된다.

상호 연동 가능성 시험(Interoperability Testing)에서는 [RFC 2459]의 개정을 위한 "draft-ietf-pkix-ipki-new-part1-11.txt"에서 상호 운영을 위해 MUST가 아닌 ALL 옵션이 주어져야 한다는 점이 언급되었다.

구현 경험(Implementation Experience)에서는 자바기반의 인증 경로 검증 API의 사용이 개발자의 부담을 줄일 수 있다는 점이 논의 되었으며 Sun사에 의한 구현이 소개되었다.

속성 인증서 프로파일은 RFC 작성자 큐에서 개정될 [RFC 2459]의 발행을 기다리고 있으며 아직까지 속성 인증서 프로파일의 구현에 대한 언급은 없다.

[DPV&DPD-REQ]는 많은 토의를 거쳐 I-D로 발행되었으며, DSV를 다른 문서로 분리 하였다. 분리된 검증(Validation)과 발견(Discovery) 정책은 서버에서 각각의 고유 기능으로서 사용되기 위해 적용되었다. 각 정책의 관리는 분리되었으며, 각각 분리된 프로토콜로 처리될 수 있다. 이러한 구조는 간단한 요청과 응답을 가능하게한다. 이러한 정책은 제한된 환경의 클라이언트에서 사용하는 DPV/DPD의 동기와 일치한다.

DPV/DPD에서 두 OCSP와 인증서 폐지 목록(CRL)의 고유한 적응 지연시간을 위한 경계 기간(cautionary period) 파라메터의 사용에 주의해야한다는 점이 언급되었다.

[SCVP]는 DPV/DPD문서의 요구사항에 부합하도록 SCVP를 교정하는 작업을 수행중이다. 미팅 기간의 토의에서는 관리 프로토콜과 요청·응답 프로토콜을 다루기 위한 문서의 분리를 논의했으며, 확장(Extension)의 사용과 그 중요도(criticality)는 여전히 문제로 남았다. 또한 요청에서 처리되지 않은 인증서를 어떻게 문의할 것인지가 명확히 해결되지 않았다. LDAP의 계속적인 사용이 논의되었으며, 속성인증서의 지원은 연기되었다. 또 클라이언트와 서버간에 어떻게 메시지를 인증할 수 있는가와 DPV와 마찬가지로 DPD를 지원하기 위해 SCVP가 확장되어야 하는가에 대한 토의가 이루어졌다.

[Proxy]에 관한 작업은 문서내에서 계속되고 있으며, 이의 구현은 Globus 프로젝트의 한 부분으로 2002년에 개발될 것이다.

[DSV-REQ]는 DPV/DPD 요구사항과 비슷한 DSV를 위한 요구사항들의 집합을 나타낸다. 미팅에서는 DSV가 리스트에 올라야하는 적합한 새로운 작업 사항인지의 토론이 있었고, 이를 DPV/DPD와 분리하자는 합의는 지켜졌다.

Supplemental Algorithms and Identifiers (draft-ietf-pkix-pkalgs-supp-00.txt)는 확장된 DSA와 SHA, 그리고 NTRU 알고리즘에 대한 향상된 ASN.1(Abstract Syntax Notation 1)을 포함하는 공개키 기반구조에 사용되는 인증서와 인증서 폐지 목록과 프로토콜에서 사용될 수 있는 부가적인 알고리즘을 기술한다.

LDAPv3에 관한 문서에 대해서는 IETF 응용영역의 ldapbis 작업반에서 LDAPv2가 historical 문서로 변경되기 때문에 LDAPv2 문서의 참조를 대체하기 위해 LDAPv2의 내용을 LDAPv3문서에 추가할 것인가에 대한 토의가 이루어졌다.

LDAP 스킴과 메칭 규칙에 관한 문서인 Internet X.509 Public Key Infrastructure LDAP Schema and Syntaxes for PKIs and PMIs (draft-ietf-pkix-ldap-schema-02.txt)는 공개키 기반구조를 위한 스킴이 추가되었으며, 구문의 변화와 속성인증서를 위한 규칙 요소가 포함되었다.

타임 스템프 서비스를 위한 정책 요구사항에 관해 ETSI 문서를 Informational RFC로서 발행하는 문제에 대해 토의가 있었으며, 그 결과 PKIX 작업반의 문서 목록에 올려지는 것이 결정되었다. 또한 [RFC 3161]를 Draft Standard로 진행하기 위한 상호 연동 가능성 시험 결과에 대한 발표가 있었다.

마지막으로 PKIX 작업반 영역 밖의 작업 사항으로 한국 정보보호 진흥원에서 제안한 무선 환경에서의 인증서 요청에 관한 Wireless Internet X.509 Public Key Infrastructure Certificate Request Message Format and Protocol(WCRMFP)에 대한 발표가 있었다.

2. 53차 미네아폴리스 IETF 미팅

제 53차 IETF 미팅은 2002년 3월 17일부터 22일까지 미국의 미네아폴리스에서 개최된다. PKIX

작업반에서는 DPD/DPV의 요구사항과 프로토콜에 대해 [DPV&DPD-REQ]와 [SCVP]에 대한 발표와 OCSP의 개정에 관한 발표가 예정되 있다. 또 새로운 문서인 [ACRMF]와 [ACMC], Out-of-Band Certificate and Key Identifier Protocol [OCKID]의 발표와 타임 스템프 기관에 대한 정책 요구사항에 관한 문서에 대한 발표가 예정되어있다.

마지막으로 현재 진행중인 작업사항에 관한 TSP의 상호 연동 가능성 시험 결과와 영구 식별자(permanent identifiers), 대리 인증서, 로고유형(logotypes)에 관한 발표가 예정되 있다.

V. 결 론

본 고에서는 IETF의 표준화 과정과 PKIX 작업그룹의 목적 및 연구 내용을 소개하였고 PKIX 작업그룹의 표준화 진행사항을 살펴보았다.

IETF는 인터넷에 대한 통일성과 표준 제정을 위한 국제 표준화 단체로 각 분야별로 표준화 활동을 수행하고 있으며, 보안 영역에서 PKIX 작업 그룹은 인터넷에서의 X.509 공개키 기반구조에 대한 표준화를 진행하고 있다.

현재 국내에서도 한국정보보호진흥원을 중심으로 인터넷보안기술포럼, 한국정보통신기술협회, 정보보호기술위원회 등에서 공개키 기반구조에 대한 표준화가 활발히 진행되고 있다. 이러한 표준화 활동에 있어 국제 표준과 상호호환성을 유지하는 국내 표준을 제정하기 위해 IETF 등의 국제 표준화 단체의 표준화 동향을 분석하는 과정은 필수적이라 할 수 있다. 이에 지속적인 국제 표준화 동향의 분석과 표준화 활동에의 참여가 요구된다.

참고문헌

[1] http://www.ietf.org

[2] W.Diffie and M.Hellman. "New Directions In Cryptography", IEEE Trans on Information Theory, vol.IT-22, pp.644- 654. Nov, 1976

[3] H. Johner, S Fujiwara, A. Sm Yeung, A. Stephanou, J. whitmore. "Deploying a Public Key Infrastructure". IBM. Feb, 2000

[4] http://www.ietf.org/html.charters/pkix-charter.html

[5] http://www.ietf.org/overview.html

[6] http://www.ietf.org/iesg.html

[7] RFC 2026, "The Internet Standards Process", Sep, 1998

[8] ISO/IEC 9594-8. "Information techno logy Open System Interconnection The Directory : Authentication Frame work", X.509, June, 1997

[9] R.Housley, W.Ford, W.Polk, D. Solo. RFC 2459 "Intranet X.509 Public Key Infrastructure Certificate and CRL Profile", Jan, 1999

[10] R. Housley, W.Ford, W.Polk, D. Solo. RFC 3280 "Intranet X.509 Public Key Infrastructure Certificate and CRL Profile", Apr, 2002

[11] S. Farrell, R. Housley, RFC 3281 "An Internet Attribute Certificate Profile for Authorization", Apr, 2002

[12] S. Boeyen, T. Howes, P. Richard, RFC 2587, "Internet X.509 Public Key Infrastructure LDAPv2 Schema", Jun, 1999

[13] S. Santesson, W. Polk, P. Barzin, M. Nystrom, RFC 3039, "Internet X.509 Public Key Infrastructure Qualified Certificates Profile", Jan, 2001

[14] S. Chokhani, W. Ford, RFC 2527, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", Mar, 1999

[15] C. Adams, S. Farrell, RFC 2510, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", Mar, 1999

[16] M.Myers, R.Ankney, A.Malpani, S. Galperin, C.Adams. RFC 2560 "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP". IETF Standard. June,1999

[17] M. Myers, C. Adams, D. Solo, D. Kemp, RFC 2511, "Internet X.509

Certificate Request Message Format", Mar, 1999
[18] C. Adams, P. Cain, D. Pinkas, R. Zuccherato, RFC 3161, "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)", Aug, 2001
[19] M. Myers, X. Liu, J. Schaad, J. Weinstein, RFC 2797, "Certificate Management Messages over CMS", Apr, 2000
[20] R. Housley, P. Hoffman, RFC 2585, "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP", May, 1999
[21] A. Arsenault, S. Turner, draft-ietf-pkix-roadmap-08.txt, "Internet X.509 Public Key Infrastructure: Roadmap", May, 2002
[22] http://www.ietf.org/proceedings/02mar/index.html

〈著者紹介〉

이 승 우 (SeungWoo Lee)
학생회원
본호의 "무선 PKI 환경에서 사용 가능한 사용자 보안 모듈의 개발 동향과 향후 전망" 저자 소개 참조

곽 진 (Jin Kwak)
학생회원
본호의 "무선 PKI 환경에서 사용 가능한 사용자 보안 모듈의 개발 동향과 향후 전망" 저자 소개 참조

정 찬 주 (ChanJoo Chung)
일반회원
1999년 2월 : 강남대학교 전자계산학과 공학사
2001년 2월 : 성균관대학교 전기전자 및 컴퓨터공학부 석사
2000년 12월 ~ 현재 : 한국정보보호진흥원 평가인증사업단 전자서명인증관리센터 연구원

원 동 호 (DongHo Won)
종신회원
본호의 "무선 PKI 환경에서 사용 가능한 사용자 보안 모듈의 개발 동향과 향후 전망" 저자 소개 참조