情 報 保 護 學 會 誌
第 14 券 第 2 號, 2004. 4

IETF 공개키 기반구조 및 PKI-기반 응용 표준화 동향

염 흥 열*

요 약

지금까지 IETF에서 공개키 기반구조에 대한 표준화 작업은 PKIX 작업반[5]에서 주로 수행되었지만, 최근 들어 4개의 새로운 작업반이 만들어졌다. 새로 생성된 작업반은 IPSEC을 위한 공개키 기반구조 표준을 개발하는 PKI4IPSEC(PKI for IPSEC) 작업반[36], 장기간 서명 데이터의 존재와 디지털 서명된 데이터의 타당성과 존재성을 증명하기 위한 표준을 개발하고 있는 LTANS(Long-Term Archive and Notary Service) 작업반[32], 공개키/개인키와 인증서 등으로 구성되는 크리덴셜(Credential)을 획득하기 위한 등록 과정에 대한 모델을 표준화하기 위한 ENROLL(Credential and Provisioning) 작업반[41], 그리고 안전하게 크리덴셜을 한 장치에서 다른 장치로 안전하게 전달하기 위한 표준을 개발하는 SACRED(Securely available Credentials) 작업반[28] 등이다. 본 논문에서는 IETF 보안영역에서 수행되고 있는 공개키 기반구조에 바탕을 둔 여러 작업반에서 최근 수행중인 표준화 동향을 분석한다.

Ⅰ. 서 론

공개키 기반구조는 모든 공개키 암호알고리즘을 이용하는 정보보호 시스템의 바탕 기술이다.[1-4] 공개키 기반구조에 바탕을 둔 다양한 서비스가 전자정부와 e-비지니스 분야에서 급격히 활성화되고 있다. 공개키 기반구조의 활용은 제품간 상호 연동성을 보장하기 위한 표준의 개발을 요구한다. 지금까지 IETF에서 공개키 기반구조 표준 작업은 PKIX 작업반에서 주로 수행되었지만, 최근 들어 4개의 새로운 작업반이 만들어졌다. 새로 생성된 작업반은 IPSEC을 위한 공개키 기반구조 표준을 개발하는 PKI4IPSEC(PKI in IPSEC) 작업반, 장기간 서명 데이터의 존재와 디지털 서명된 데이터의 타당성과 존재성을 증명하기 위한 표준을 개발하고 있는 LTANS(Long-Term Archive and Notary Service) 작업반, 공개키/개인키와 인증서 등으로 구성되는 크리덴셜(Credential)을 획득하기 위한 등록 과정에 대한 모델을 표준화하기 위한 ENROLL(Credential and Provisioning) 작업반, 그리고 안전하게 크리덴셜을 한 장치에서 다른 장치로 옮기기 위하여 요구되는 표준을 개발하는 SACRED(Securely available Credentials) 작업반 등이다. 본 고에서는 IETF 보안영역에서 수행되고 있는 공개키 기반구조에 바탕을 둔 여러 작업반에서 최근 수행중인 표준화 동향을 분석한다.

본 고의 2장에서는 PKIX, SACRED, LTANS, PKI4IPSEC, ENROLL 작업반의 표준화 개요와 현재 개발이 완료된 표준, 개발이 진행중인 표준, 그리고 향후 표준화가 수행될 사항을 중심으로 분석했다. 3장에서는 결론을 맺는다.

Ⅱ. IETF 공개키 기반구조 및 응용 표준화 동향

2.1 PKIX 작업반 표준화 동향

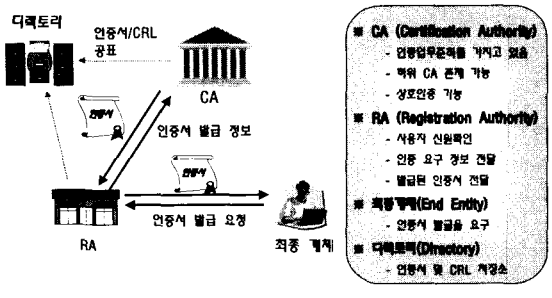
가. 개요

정보시스템에서 정보보호 기술을 적용하기 위해서는 공개키 암호 알고리듬의 적용이 요구되고 있다. 공개키 암호 알고리듬을 사용하는 정보 시스템이 안전성과 신뢰성을 보장 받기 위해서는 주체 공개키에 대한 무결성(Integrity)과 인증성(Authenticity)이 보장

† 본 논문은 충남대학교 IIRTRC 지원에 의하여 수행되었습니다.
* 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

되어야 한다. 무결성은 사용자의 공개키가 중간의 다른 개체에 의하여 변경되지 않았음을 증명하는 것이고, 인증성은 사용자의 공개키가 소유자라고 주장하는 주체에 진정 속해 있음을 제삼의 기관(예를 들어, 인증기관)이 보장하는 것이다. 인증서는 사용자 공개키, 사용자의 이름, 그리고 인증기관의 이름 등의 정보를 인증기관의 개인 서명키로 서명한 데이터 구조이다. 공개키 기반구조(PKI:Public-Key Infrastructure)는 기본적으로 암호 시스템 및 서명 시스템에서 요구되는 사용자 공개키에 대한 무결성과 인증성을 보장하기 위하여 인증기관에 의하여 발행되는 인증서에 바탕을 두고 있다. 공개키 기반구조는 사용자에게 인증서를 발행하고, 발행된 인증서를 이를 사용하는 신뢰 당사자들에게 분배하며, 개인키의 누설과 이름의 변경 등의 사유로 이미 발행되었던 인증서를 취소하고, 취소된 인증서를 인증서 취소목록 형태로 공표하며, 인증서와 인증서 취소목록을 디렉토리를 통하여 공개하고, 발행된 인증서의 상태와 인증 경로의 적합성을 온라인으로 검증하며, 인증기관 사이의 신뢰를 확장을 위한 상호 인증서(다시 말해, 인증기관 인증서)를 발행하는 등의 업무를 수행하기 위한 정보시스템의 기반 기술이라고 정의할 수 있다.

PKI을 이루고 있는 주요 구성요소들은 그림 1과 같이 인증기관, 등록기관, 최종개체, 그리고 디렉토리 등이다. 인증기관(CA : Certification Authority)은 최종 개체에게 인증서를 발행하며, 등록 기관(RA: Registration Authority)은 인증기관이 일부 위임한 업무인 사용자에 대한 신원 확인 업무를 수행하고, 최종 개체 (EE : End Entity)는 인증서 발행을 요청하고 발행 받는 개체이다. 또한 디렉토리(또는 레포지토리) 시스템은 발행된 인증서와 취소된 인증서에 대한 인증서 취소목록을 저장하기 위한 시스템이다. 현재 공개키 기반구조의 기술은 마이크로소프트사의 익스플로러, SSL/TLS, IPSec 등의 다양한 분야에



〔그림 1〕 PKI 구성 요소

적용되어 이용되고 있고, 앞으로도 그 활용의 영역을 확대할 예정이다.[1,2]

나. 표준화가 완료된 문서

현재 RFC로 표준화된 PKI 문서의 내용은 표 1과 같이 인증서 및 인증서 취소목록, 인증서 관리, 온라인 인증서 상태 프로토콜, 인증서 정책, 인증서 운영, 타임스탬프, 데이터 검증, 대리인증경로 발견 및 대리인증경로검증, 로고타입 인증서 확장자, 적격인증서 등의 문서를 포함하고 있다.[6-27]

인증서 및 CRL 규격은 IETF RFC 2459로 표준화되었으며, 2002년 4월 RFC 3280으로 다시 개정되었다. 이는 기본 필드와 다양한 확장 필드를 정의하고 있고, 인증서 규격으로 X.509 버전 3 인증서 규격을, 인증서 취소목록 규격으로 X.509 버전 2 인증서 취소목록 규격을 사용하고 있다. 또한 인증서와 인증서 취소목록에 대한 검증 알고리듬을 제시하고 있다.

RFC 2510으로 표준화된 인증서 관리 프로토콜은 사용자와 인증 기관사이에 인증서의 발행을 요구하거나 인증기관 사이에 상호 인증을 요구하기 위한 과정과, 이를 위한 데이터 요소를 정의하고 있다.

RFC 2527로 표준화된 인증서 정책은 특정의 공개키 인증서가 적당한 가격의 전자 거래에 활용될 수 있는지를 판단할 수 있게 하는 규칙들의 집합이다. 인증서 정책과 관련된 인증업무준칙은 인증기관이 공개키 인증서를 발급할 때 사용되는 세부적인 업무준칙을 포함하고 있다. 인증서 정책은 물리적 및 개인 보안, 주체 신분확인 요구사항, 그리고 인증서 취소 정책 등의 규칙을 포함한다.

RFC 2560으로 표준화된 온라인 인증서 상태 프로토콜(OCSP : Online Certificate Status Protocol)은 특정 인증서의 취소 상태를 온라인으로 시기적절하게 제공하기 위한 절차이다. 인증서 상태 프로토콜은 OCSP 서버와 OCSP 클라이언트간에 수행된다. OCSP 클라이언트는 특정 인증서의 유효성과 취소 상태를 서버에 문의하고, 서버는 인증서 유효성과 취소 상태를 전달한다. 클라이언트는 서버로부터 인증서가 유효하고 취소되지 않았다는 정보를 수신한 후에 문의한 인증서를 사용해야 한다.

RFC 3161로 표준화된 타임 스탬프 서비스는 제삼의 기관인 서버가 특정 메시지가 특정 시간 이전에 존재했음을 증명하기 위하여 사용된다. 타임 스탬프 서비스는 기본적으로 전자적인 데이터에 대한 존재 사실만을 증명하는 서비스라고 할 수 있다. 타임 스탬프

〔표 1〕 IETF RFC 문서

구 분	문 서 명	표준트랙	발표일시
RFC 2459/3280	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	표준	1999.1./ 2002.4.
RFC 2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols	표준	1999.3.
RFC 2511	Internet X.509 Certificate Request Message Format	표준	1999.3.
RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	정보	1999.3.
RFC 2528	Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates	정보	1999.3.
RFC 2559	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2	표준	1999.4.
RFC 2560	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP	표준	1999.6.
RFC 2585	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP	표준	1999.5.
RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	표준	1999.6.
RFC 2797	Certificate Management Messages over CMP	표준	2000.4.
RFC 2875	Diffie-Hellman Proof-of-possession algorithm	표준	2000.7.
RFC 3029	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols	실험	2001.2.
RFC 3039	Internet X.509 Public Key Infrastructure Qualified Certificates Profile	표준	2001.1.
RFC 3161	Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP)	표준	2001.8.
RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile	표준	2002.4.
RFC 3281	An Internet Attribute Certificate Profile for Authorization	표준	2002.4.
RFC 3379	Delegated Path Validation and Delegated Path Discovery Requirements	정보	2002.9.
RFC 3628	Policy Requirements for Time-Stamping Authorities (TSAs)	정보	2003.11
RFC 3647/2527 대체	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	정보	2003.11
RFC 3709	Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates	표준	2004.2.
RFC 3739/ RFC 3039 대체	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile	표준	2004.3.

기관은 모두가 믿는 제삼의 기관이며, 특정 데이터에 대한 타임 스템프 토큰을 생성하다. 클라이언트는 메시지 자체를 서버로 보내는 것이 아니라 메시지에 대한 해쉬 값만을 서버로 전송한다.

RFC 3029로 표준화된 데이터 검증 및 인증 서비스는 타임 스템프 서비스를 확장한 인증 응용 서비스이다. 클라이언트는 데이터 자체나 데이터의 해쉬값, 데이터에 대한 서명문, 서명문 검증을 위한 인증경로 등을 서버로 전달한다. 모든 클라이언트가 믿는 서버는 타임스템프 서비스와 마찬가지로 특정 데이터가 소

지 사실을 증명하거나, 특정 데이터 자체가 존재했음을 확인하거나, 특정 데이터에 대한 서명문이 유효하거나, 서명문 검증을 위한 인증경로가 유효함을 검증한다.

RFC 2585와 2559로 표준화되고 있는 운영 프로토콜은 인증서를 사용하는 시스템으로 인증서나 CRL을 전달하기 위한 방법을 기술하고 있다. 전달 방법에는 LDAP, HTTP, FTP, X.500 프로토콜에 기반을 둔 다양한 수단들이 이용될 수 있다.

RFC 3279로 표준화된 인증서와 인증서 취소목록을 위한 알고리듬과 확인자는 디지털 서명과 공개키를 위한 ASN.1 부호화 형태와 알고리듬 식별자를 규정하고 있다. 이 문서는 RFC 3280 인증서와 인증서 취소목록을 지원한다. 이 문서는 인증서와 CRL에 포함되어 있는 signatureAlgorithm, signatureValue, signature, 그리고 subjectPublicKeyInfo 필드를 정의한다. 이 규격에서는 디지털 서명과 함께 이용되는 해쉬 알고리듬을 정의하고 있다. 본 규격에서 다루는 서명 알고리듬은 RSA, DSA, 그리고 ECDSA 서명 알고리듬이다. 인증서의 subject PublicKeyInfo 필드를 위한 부호화 형태를 포함하고 있다. 이의 대상은 RSA, DSA, DH, KEA 등이다.

RFC 3281는 X.509 속성 인증서에 대한 프로파일을 정의하고 있다. 속성 인증서는 다양한 응용과 환경에서 사용될 것이다. 이 문서의 목적은 일반적인 응용을 위한 공통 기반을 설정하기 위한 것이다. 이 프로파일은 전자메일, IPSEC, WWW 보안 응용을 지원하는 속성 인증서를 중점적으로 다루었다. 속성 인증서와 공개키 인증서와의 차이점은 공개키 인증서는 여권에 비유될 수 있고, 속성 인증서는 여권 내의 비자에 대응될 수 있다. 공개키 인증서는 수명이 길고, 속성 인증서는 수명이 짧으며, 속성 인증서에는 공개키가 존재하지 않는다는 것이다. 이는 속성 인증서를 접근 제어를 하기 위한 인가 정보만을 포함하고 있다는 것을 의미한다. 일반적으로 인가 정보를 넣는 방법은 공개키 인증서에 넣거나 별도의 속성 인증서에 넣는 방법이 존재하나, 인가 정보를 공개키 인증서에 넣으면 속성의 주기가 일반적으로 공개키 인증서의 주기보다 짧게 되어 자주 공개키 인증서를 갱신해야 하는 단점이 존재하게 된다. 따라서 별도의 인가 인증서를 발행하는 방법을 정의하고 있다. 속성 인증서는 접근 통제, 데이터 발신지 인증, 부인방지 등을 포함하는 다양한 보안 서비스에 이용될 수 있다. 공개키 인증서는 신분정보에 대한 정보를 접근 제어 판별 기능에 제공한다. 그러나, 많은 환경에서 신분정보가 접근 제어를 위하여 사용되는 기준이 아니고, 차라리 접근자의 역할이나 그룹 회원 권한이 접근 제어를 위한 기준이 된다. 그러한 접근 제어 기법은 역할 기반 접근 제어 기법이라고 불리워진다. 속성 인증서를 기반으로 접근 제어 판단을 결정할때, 접근 제어 기능은 적절한 속성 인증서 소지자가 접근을 요청했다는 것을 검증할 필요가 있다. 한 가지 방법은 속성 인증서 내에 공개키 인

〔표 2〕 IETF PKIX 주요 드래프트 문서

표준화 분야	주 요 내 용	문서상태
SCVP	최근 채택된 DPD/DPV 요구사항 문서를 만족하는 SCVP 프로토콜을 변경하였음. 이 표준은 WG last call 상태에 있고, 2004년 3월 말에 AD(Srea Director)에게 전달될 예정임.	열네번째 드래프트 (2003.10)
WLAN 인증서 확장필드	IEEE 802.1X에서는 WLAN에서의 인증을 위한 EAP-TLS의 사용을 고려하고 있음. 사용자가 다른 WLAN을 액세스할 때 이 응용을 지원하기 위한 인증서의 확장필드가 필요함. 이 문서는 현재 WG last call을 마치고 AD에게 넘겨져 있는 상태임.	여섯 번째 드래프트 (2004.3.)
속성 인증서 정책 확장필드	속성 인증서 관련 두 개의 확장필드가 정의되고 있음. 이 문서 역시 WG last call를 마치고, AD에게 넘겨져 있는 상태임.	여섯 번째 드래프트 (2003.12.)
항구적인 식별자	하나의 개체에 대한 항구적으로 사용될 식별자를 할당하고, 여러 인증서 들에서 하나의 공통 식별자 PI을 이용하여 위한 확장필드가 정의되고 있음. 이 문서 역시 WG last call를 마치고, AD에게 넘겨져 있는 상태임.	열 번째 드래프트 (2004.1.)
보증 인증서 확장 필드	보증 인증서 확장 필드는 보증 정도를 인증서 확장자를 통하여 전달하는 확장자며, WG last call 이 완료되어 현재 IESG 과정을 수행하고 있고, 곧 RFC 문서로 발표될 예정임.	다섯 번째 문서 (2004.4.)

증서를 연결시키고, 공개키 인증서 내의 개인키를 이용하여 접근 요구에 대한 인증을 수행한다. 속성 인증서를 분배하는 방법은 디렉토리를 이용하여 분배하는 방식과 프로토콜의 일부로 해당 주체가 전달하는 방법이 있다. 본 문서는 속성 인증서에 대한 프로파일을 정의하고, 각 필드들의 신택스와 프로파일을 정의하고 있다.

RFC 3379는 DPD/DPV(Delegated Path Discovery/Delegated Path Validation) 요구사항은 온라인 인증서 검증 프로토콜들이 가져야할 기본적인 요구사항을 포함하고 있다. 이 문서는 여러 온라인 인증서 검증 프로토콜로 제안되고 있는 SCVP, OCSPv2, 그리고 CVP(Certificate Validation Protocol)을 위한 가이드라인 문서로 이용되었다.

RFC 3628은 타임스탬프 서비스를 위한 인증기관이 갖어야할 요구사항을 기술한 문서이며, ETSI의 표준안을 IETF 정보 RFC로 다시 표준화한 문서이다. 이 문서는 타임스탬프 서비스의 일반적인 개념과 목적 등을 기술하고, 타임스탬프 정책을 위한 식별자를 기술했으며, 각 주체가 가져야 할 의무와 책임을 기술하고, 키생성, 개인키 보호, 공개키 분배, 리키, 키 수명관리 등의 타임스탬프 기관이 지켜야 할 키관리에 대한 요구사항, 타임스탬프 토큰은 안전하게 발행되어야 하고 적절한 시간을 포함해야 한다는 타임스탬프 토큰에 대한 요구사항, 그리고 보안 관리, 관리 요원 보안, 물리적 보호, 환경적 보안, 운영 관리, 시스템 접근 관리, 신뢰 시스템 설치 및 유지보수 등의 관리 및 운영에 대한 요구사항을 기술하고 있다.

RFC 3647은 RFC 2527을 대체한 문서이며, 인증서 정책과 인증 업무 준칙에 관한 문서이다.

RFC 3709는 로고타입 인증서 확장자에 대한 표준으로, 로고타입(Logo-type) 인증서 확장필드는 여러 개의 인증서 들 중에서 특정 응용에 적합한 하나의 인증서를 선택해야 하는 경우에 적용할 수 있는 인증서 확장필드이다. 인증서를 효율적으로 선택하기 위하여 인증서에 대한 이미지 정보와 오디오 정보를 인증서 확장필드 형태로 신뢰당사자에게 제공함으로써 사람 개입을 통한 기존의 인증서에 대한 신뢰성을 향상하고 검증 기능을 보조하기 위한 확장필드이다.

RFC 3739는 적격 인증서(Qualified Certificate)에 대한 프로파일이며, 이 인증서는 유럽 전자서명법에서 사용되는 적격 인증서에 대한 프로파일을 제시하고 있다. 적격 인증서는 생체 정보와 사용자에 대한 정보가 좀더 자세하여 고가의 전자서명에 대한 부인 방지 서비스에 활용 가능한 프로파일이다.

다. 표준화가 진행되고 있는 문서

현재 표준화가 진행되고 있는 표준화 동향은 표 2와 같이 SCVP(Simple Certificate Validation Protocol), 항구적인 식별자, WLAN(Wireless LAN) 확장필드, 그리고 보증 인증서 확장필드 등을 포함하고 있다[5].

SCVP 프로토콜은 DPD/DPV 요구사항을 만족하는 온라인 인증서 검증 프로토콜이다[43]. SCVP는 인증서 상태를 문의하거나 인증 경로에 대한 유효성을 문의하기 위한 프로토콜이다. 이는 SCVP 서버와 클라이언트 간에 수행되며, 서버는 클라이언트로 인증서의 유효성과 취소 상태, 그리고 서명문 검증을 위한 인증서 체인의 유효성에 대한 결과를 전달한다.

보증(warranty) 인증서 확장필드는 인증서의 사용으로 인하여 신뢰 당사자가 입을 피해를 보상하기 위한 보증의 정도를 인증서의 확장필드를 통하여 신뢰 당사자에게 전달하고자 하는 인증서 확장필드이다. 이 인증서 확장필드는 화폐의 단위와 지불액의 가치를 나타내는 부분으로 나누어 질 수 있다.

무선근거리통신망에 사용자를 인증 하기 위한 인증서의 도입이 IEEE 802.1x에서 추진되고 있다. 따라서 이러한 환경에서 자동화된 인증서 선택 기능을 제공하기 위한 확장필드이다. 이 확장필드는 특정의 무선근거리통신망의 이름을 포함하는 하는 SSID(Service Set Identifier)를 포함하고 있다.

항구적인 식별자(PI)는 인증서의 확장필드 필드이며, 여러 인증서에 분산되어 있는 주체를 하나의 항구적인 식별자를 이용하여 동일한 주체로 확인하고자 하는 경우 활용될 수 있다. 이는 인증서에 특정 할당 기관에 의하여 할당된 주체에 대한 항구적인 식별자를 포함한다.

라. 향후 표준화 방향

향후 표준화 될 문서는 대리 경로 발견과 대리 경로 검증 기능을 갖는 SCVP(Simple Certificate Validation Protocol), 인증서 경로 검증, NIST SHA-224 규격, NIST ECC 규격, 한국에서 제안한 SIM(Subject Identification Method), 인증서와 CRL을 조회하기 위한 LDAP v3 규격, 그리고 POP 방법에 대한 표준인 RFC 2511bis 표준 등이다. 이중 SCVP는 거의 WG last call을 마친 상태이고, 인증서 경로 검증은 거의 WG last call을 마

치고 2004년 3월에 AD에게 넘겨질 예정이다. 또한 SHA-224 규격은 SHA의 출력 길이를 224비트로 확장한 문서로 2003년 3월부터 2주간의 WG last call 이 완성되면, 2004년 4월 AD에게 표준 트랙 문서를 위하여 넘겨질 예정이다. 또한 ECC 알고리즘 프로파일은 역시 2004년 4월에 2주간의 WG last call을 완성하고, 2004년 4월 표준 트랙 문서를 위하여 AD에게 넘겨질 예정이다. SIM 문서는 현재 거의 모든 comment를 수정했고, 2004년 4월에 WG last call를 완성할 예정이다. 이외에는 LDAP 규격과 OCSPv2에 대한 문서도 표준화 될 예정이다. LDAP 규격은 거의 기술적으로 완성된 상태에 있다. 또한 한가지 주목해야 할 문서는 인증서 발행 과정에서 개인키 소지 증명을 다루고 있는 POP(Proof of Possession) 방법을 위한 문서로, 6가지의 POP 방식을 제안하고 있다. 이는 CMP에서 유용하게 활용될 수 있는 프로토콜이다.

2.2 SACRED 작업반 표준화 동향

가. 개요

PKI에서 사용되는 크리덴셜은 대표적으로 공개키/개인키, 인증서와 인증서 체인, 그리고 신뢰 루트 인증기관 정보로 구성된다. 이 크리덴셜은 주로 응용 한정 메모리의 일부분으로 데스크 탑이나 랩탑 컴퓨터에 저장되어 있다. 현재 응용에서 크리덴셜의 엑스포트(export)와 임포트(import)는 매우 일정치 않고, 최종 사용자가 PKI 크리덴셜을 생성하고 관리하기 위한 메카니즘에 너무 깊이 관여하고 있다. 일반적으로 응용에 한정되어 메모리에 저장되어 있다는 것은 여러 다양한 디바이스에 다양하게 활용될 수 없음을 의미하게 되어 크리덴셜의 이동을 어렵게 한다. 일반적으로 스마트 카드나 스마트 토큰을 사용하는 경우 이동성이 허용되나, 많은 다바이스에서 하드웨어 인터페이스를 기능을 갖추고 있지 않기 때문에 문제가 된다.

따라서 이를 해결하기 위한 문제로 하나는 표준화된 크리덴셜 전달 표준을 만들고, 각 디바이스에서 이를 지원하게 하면 가능해진다. 물론 이경우는 소프트웨어에 기반을 둔 크리덴셜을 의미한다. 현재까지 고려되고 있는 크리덴셜 이동성(Mobility)을 지원하기 위한 방법은 크리덴셜 서버를 두고 디바이스가 크리덴셜 서버로 크리덴셜을 업로드하고, 필요시마다 사용자 인증 과정을 완료한후 안전한 채널을 통하여 크리덴셜을 다운받는 방법인 크리덴셜 서버 방식과, 하나의 디바이스에서 다른 하나는 디바이스로 직접적으로 크리덴셜을 전달하는 직접 전달 방법이 제안되고 있다. 하나의 공통의 프로토콜을 개발할 수 도 있을지 확실치 않으나 현재는 두개의 프로토콜이 필요할 것으로 확인되고 있으며, 하나는 크리덴셜 서버와 디바이스간에 상호동작을 위하여 필요한 프로토콜이며, 다른 하나는 크리덴셜을 직접 전달하기 위한 디바이스간의 프로토콜이다.

이 프로토콜에서 요구되는 보안 기능은 크리덴셜을 업로드하거나 다운로드할 때 이용되어야 하는 사용자 인증 서비스와, 업로드와 다운로드시에 중간에 필요한 크리덴셜 정보를 도청하는 공격을 막기 위한 기밀성과 메시지 무결성, 메시지 인증성 등의 서비스가 요구된다. 또한 크리덴셜 서버는 다양한 형태의 디바이스에게 서비스를 제공하해야하는 가용성 문제가 해결해야 할 주요 문제로 대두되고 있다.

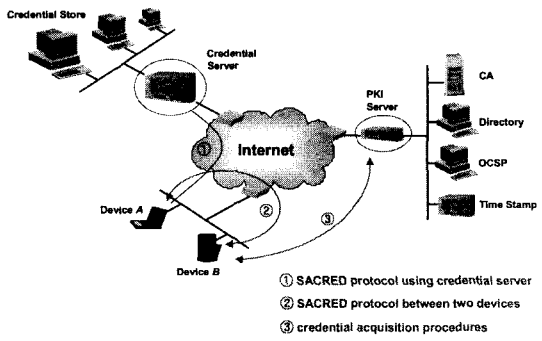
현재 IETF 보안 영역에서 크리덴셜 이동성에 관한 표준을 제정하고 있는 작업반은 SACRED(Securely Available Credentials) 작업반이며, 이 작업반의 주요 임무는 크리덴셜 이동성을 보장하기 위한 임의의 프로토콜에 대한 세부 요구사항을 확인하고 기술하는 정보문서와 개발된 프로토콜에 대한 세부 기술적인 사항을 다루는 표준-트랙 문서를 표준화하는 것이다. 현재 개발된 문서는 표와 같이 하나의 RFC 문서와 2개의 ID(Internet Draft) 문서이다.

나. 표준화가 완료된 문서

지금까지 표준화가 완료된 문서는 표 3과 같다. RFC 3157[29]은 크리덴셜 이동성을 위한 요구사항을 확인하고, 프레임워크 문서와 프로토콜 문서의 기반 문서의 역할을 수행하고 있다. PKI에 의존하는 많은 유형의 디바이스들이 존재하게 되었고, 대표적인 디바이스는 데스크탑 컴퓨터, 랩탑 컴퓨터, PDA, 무선 전화기, 그리고 페이저 등이다. 무선 전자상거래를 이용하는 사용자는 데스크 탑에서 사용하는 서명용 개인

〔표 3〕 IETF SACRED RFC 문서

구 분	문 서 명	표준트랙	발표일시
RFC 3157	Securely Available Credentials - Requirements	정보	2001.8.



〔그림 2〕 SACRED 프로토콜의 종류

키를 무선 전화기에서도 사용하기를 원할 것이다. 즉, 데스크 탑에서 사용하는 서명용 개인키를 이용하여 서명된 메일을 보냄과 동시에 이 개인키를 이용하여 무선 전화기에서도 서명된 메일을 보내길 원할 것이다. 서로 다른 크리덴셜 저장 장치는 다른 보안 특성과 서로 다른 처리 능력을 갖는다. 따라서, SACRED 프로토콜은 이들 서로 다른 디바이스간, 서로 다른 저장 매체, 서로 다른 위치간에 안전한 크리덴셜의 이동성을 제공해야 한다. 이 문서는 프레임워크에 대한 요구사항을 기술했고, 안전한 크리덴셜 전달을 위하여 요구되는 일반적인 요구사항과 두개의 솔류션 등급에 대한 개별 요구사항을 기술하고 있다. 기본적으로 크리덴샬을 전달하기 위한 방법은 크리덴셜 서버를 두고 이를 통하여 크리덴셜을 업로드라고 다운로드하는 방법과 또 다른 방법은 두개의 디바이스간에 바로 크리덴셜 정보를 전달하는 직접 방법이 제안되어 있다. 기본적으로 프레임워크를 위한 요구사항은 프레임워크는 두가지 전달 방법 모두를 지원해야 하고, 크리덴셜 서버 방법과 직접 방법은 가능한 한 동일한 기술을 사용하는 것이 좋다는 것이다. 크리덴샬의 형태는 프로토콜에 opaque 이어야 한다는 것이다. 이는 프로토콜은 크리덴셜의 형태나 유형에 종속적이어서는 않됨을 의미한다. 프로토콜과 관련된 요구사항은 SACRED 프로토콜이 보호를 제공해야할 취약성을 확인하였다. 또한 크리덴셜이 디바이스로에서 서버로 또는 서버에서 디비이스로 전달되거나, 디바이스간에 바로 전달되어야 한다는 요구사항과 프로토콜의 어느 노드에서도 평문으로 존재하지 않아야 한다는 요구사항 등을 규정한 일반 요구사항과, 크리덴샬은 사용자 인증후에 다운로드되거나 업로드 되어야 한다는 크리덴셜 서버 기반 프로토콜에 대한 요구사항, 수신자가 자신이 수신한 메시지가 주장된 송신 디바이스로부터 왔다는 것을 인증하는 것이 좋다는 등의 직접 전달 프로토콜에 대한 요구사항 등을 포함하고 있다.

〔표 4〕 IETF SACRED 드래프트 문서

문서제목	주 요 내 용	문서상태
SAC 크리덴셜 서버 프레임워크	이 문서는 안전한 크리덴셜 전달을 위한 프레임워크를 기술하고 있다. 네트워크 구조, 프로토콜의 종류 등을 확인하고 기술하고 있다. 이 문서는 WG last call 이 완료되었다.	여덟번째 드래프트 (2003.11)
SAC 프로토콜	이 문서는 안전한 크리덴셜을 전달받기 위한 프로토콜을 기술하고 있다. 이 문서는 WG last call 이 완료되었다.	열 번째 드래프트 (2003.11)

다. 표준화가 진행중인 문서

현재 표준화는 크리덴셜 서버를 이용하는 프레임워크와 관련 프로토콜을 집중적으로 수행하고 있다. 이러한 두 가지 ID(Internet Draft)는 다음 표 4와 같다.[30-31]

SAC 크리덴셜 서버 프레임워크에 관한 문서는 크리덴셜의 안전한 교환을 위한 일반적인 프레임워크를 제안하고, 하나 이상의 SACRED 프로토콜을 개발하기 위한 가이드라인을 제공한다. 본 문서는 두가지 서로 다른 네트워크 구조를 설명하고, 크리덴셜 업로드 절차, 크리덴셜 다운로드 절차, 크리덴셜 삭제 절차, 크리덴셜 관리 절차를 기술하고 있다. 또한 세션 채널에 대한 보안 요구사항으로 서버 인증, 사용자 인증, 세션키 협상, 하나 이상의 크리덴셜이 협상된 세션키로 보호되어야 한다는 요구사항을 제시하고, 강한 패스워드 인증 방식(Secure Password Authentication Protocol)과 TLS(Transport Layer Protocol) 라는 두가지 기존 프로토콜을 이용할 것을 제시하였다. 또한 TCP, HTTP, BEEP 등의 트랜스포트 프로토콜을 이용한다.

SAC 프로토콜에 관한 문서는 사용자에 한정되는 구성 설정 없이 크리덴셜 서버로부터 자국에 설치된 신뢰성있는 소프트웨어를 갖고 있는 워크스테이션을 이용하여 암호학적 크리덴셜을 얻기 위한 프로토콜을 기술하고 있다. 이 문서는 XML로 표현되어 있다. 이 문서는 클라이언트가 계정 정보 생성에 필요한 정보를 얻기 위한 정보 요구, 계정 생성, 계정 제거를 위한 계정삭제, 계정 변경 등의 계정 관리 동작, 크리덴셜 업로드, 크리덴셜 다운로드, 크리덴셜 제거 등의 실시

간 동작, 세션 보안, 하나의 계정에 대한 다중 크리덴셜 처리, 크리덴셜 형식 등을 기술하고 있다.

라. 향후 표준화 방향

현재 준비되어 있는 크리덴셜 서버를 위한 프레임워크와 관련 프로토콜에 대한 표준화가 진행될 것이며, 직접 전달 방법을 위한 프레임워크와 프로토콜에 대한 표준화도 수행될 것으로 예측된다. 직접 전달을 위한 문서는 아직 WG 홈페이지에 나타나 있지 않고 있다.

2.3 LTANS 작업반 표준화 동향

가. 개요

여러 가지 응용에서 장기간에 걸쳐서 디지털 데이터와 증거를 보존할 필요성이 대두되고 있다. 특히 데이터가 중요하고 오래 기간이 경과되고 나서 사용될 필요가 있다면, 이는 아주 안전한 방법으로 영구적으로 보관될 필요가 있다. 만약 데이터가 법원에서 증거자료로 활용되어야 한다면, 과거의 특점 시점에서 데이터가 존재했고 이 데이터의 무결성이 유지되었다는 것을 검증할 필요가 있다. 장기간 무결성 서비스는 데이터를 장기간 보존하고 데이터의 가용성을 제공할뿐만 아니라 데이터의 존재성과 부인방지를 보존하는 활동을 주기적으로 수행한다.

현재 IETF 보안 영역에서 표준화된 LTANS 관련 표준은 두가지 종류가 있다. 하나는 RFC 3161로 표준화된 시점확인(Time Stamp Protocol) 서비스이고 다른 하나는 RFC 3029로 표준화된 DVCS (Dats Validation and Certification Server) 서비스이다. 시점확인 서비스와 DVCS 서비스는 특정 데이터가 특정 시점에서 존재했다는 것을 확인하는 서비스이고, DVCS 서비스는 데이터의 내용이 특점 시점에서 존재했다는 것을 증명하는 것이다. 물론 이 두 가지 방식은 법원에 제출하여 법률적 증거로 활용될 수 있다. 그러나 이 방식에는 디지털 서명문이 시간이 경과함에 따라 안정성이 약화되어서 제삼자가 위조가 가능해지고, 다양한 암호 공격의 개발로 인하여 특정의 암호시스템이 깨지게 되어서 서명문의 위조가 가능해지며, 공개키 인증서의 유효기간이 경과하여 결국 검증이 어렵게 돼는 문제가 있다. 따라서 장기간으로 제공되는 부인방지 서비스는 매우 중요하다. 이러한 문제를 해결하는 메카니즘에 대한 표준은 서명자 공개키 인증서의 유효기간 경과와 시점확인 기관의 공개키 인증서에 대한 유효기간의 경과 등과 같은 일상적인 사건을 다룰 필요가 있다. 이를 위한 표준을 개발하고자 하는 작업반이 장기간 아카이브 및 공증 서비스 (LTANS : Long-Term Archive and Notary Services) 작업반이다.

〔표 5〕 IETF LTANS 인터넷 드래프트 문서

문서제목	주 요 내 용	문서상태
장기간 아카이브 서비스를 위한 요구사항	장기간 아카이브 서비스를 위한 기술적 요구사항을 기술하고 있다. 이 문서는 2004년 1월부터 리스트에서 논의가 시작되어 현재 다음 버전의 문서가 준비중에 있다.	첫 번째 드래프트 (2004.2)
증거 기록 신택스 (Evidence Record Syntax)	이 문서는 2004년 2월에 공표되어, 아직 리스트에서 논의되고 있지 않다.	첫 번째 드래프트 (2003.11)

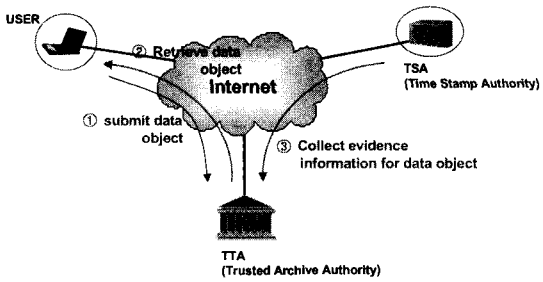
LATNS 작업반의 목표는 아카이브 및 공증 서비스를 위한 요구사항, 데이터 구조, 그리고 프로토콜을 정의한다. 이를 위하여 작업반은 장기간 아카이브 서비스를 위한 요구사항을 확인하고, 장기간 부인방지 서비스를 제공하기 위한 아카이브 서비스를 개발하며, 이를 위한 공통의 데이터 구조와 형태를 정의하고, 이후에 공증 서비스에 대하여 상기의 과정을 반복할 계획을 가지고 있다.

나. 표준화가 완료된 문서

현재까지 RFC로 표준화가 완료된 문서는 없다.

다. 표준화가 진행되고 있는 문서

현재 표준화되고 있는 문서는 표 5와 같다.[33-35] 장기간 아카이브 서비스를 위한 요구사항에 관한 문서는 장기간 아카이브 시스템을 위한 기술적 요구사항을 규정하고 있다. 요구사항 분석은 두 부분으로 나뉘어지는데, 첫 번째 부분은 응용 시나리오를 제시하고, 두 번째 부분에서는 서비스의 기능, 데이터의 구조, 그리고 장기간 아카이브 시스템과 상호동작하기 위한 프로토콜 요구사항을 다루고 있다. 저장 매체 관점, 개별 법률적 요구사항, 계정과 관련되는 의문점, 그리고 과금시스템 등에 대한 운영 요구사항은 이 문서에서 다루지 않는다. 이 문서에서는 장기간 데이터의 유용성과 무결성 요구사항, 법원에 대한 데이터의 존재와 무결성에 대한 제시, 서명된 데이터에 대한 증거 보존 등의 장기간 아카이브에 대한 일반 요구사항, 장기간 아카이브 시스템은 데이터 객체를 오래기간동안



〔그림 3〕 장기간 아카이브 시스템 구성도

저장해야 한다는 등의 장기간 아카이브 서비스의 요구사항, 그림 3과 같이 신뢰된 아카이브 기관인 TAA (Trusted Archive Authority)에게 데이터 객체를 제출하고 TAA로부터 저장된 데이터를 조회하는 사용자, 사용자로부터 아카이브 데이터를 수신하여 이를 장기간 유지하는 신뢰된 아카이브 기관(TAA), 데이터 객체에 대한 부인방지 증거 데이터를 제공하는 시점확인 기관 등으로 구성되는 장기간 아카이브 시스템의 실제적인 예와 구조를 제시하였다. 또한 보존을 위한 데이터 객체나 데이터 객체 그룹을 수신해야 하고 서명된 데이터에 대한 유효성을 검증하기 위한 검증 데이터를 수집하고 유지해야 한다는 등의 장기간 아카이브 서비스의 기본 기능 및 품질에 대한 요구사항, 아카이브 데이터 구조는 아카이브 데이터 객체와 아카이브 데이터에 대한 검증 기록을 포함해야 한다는 등의 데이터 구조 요구사항, 그리고 프로토콜은 아카이브 데이터 객체를 제출하고 조회하며 삭제하는 등의 상호 동작을 포함해야 한다는 프로토콜에 대한 요구사항 등을 포함하고 있다.

증거 기록 신택스에 관한 문서는 기간이 결정되어 있지 않은 장기간에 걸쳐서 디지털 서명된 데이터에 대한 존재성과 무결성을 제공하기 위하여 디지털 서명된 데이터의 존재성에 대한 장기간 부인방지를 위하여 설계된 증거 메시지에 대한 신택스와 처리 과정을 규정한다. 증거 기록 신택스는 기본적으로 하나의 단일 데이터 객체나 데이터 객체의 그룹을 지칭하는 아카이브 타임스템프이다. 아카이브 타임스템프는 타임스템프의 결합인 해쉬 트리로부터 유도된다. 타임스템프는 해쉬 트리의 루트 타임스탬프를 위하여 요구된다. 해쉬 값과 타임스템프 값들의 집합이 아카이브 타임스템프를 생성한다. 초기 아카이브 타임스템프는 파일 또는 여러개의 파일들로 구성되는 데이터 객체 등의 데이터 객체로부터 생성된다. EvidenceRecord는 기본적으로 버전을 나타내는 version, 데이터 객체를 해쉬하는데 사용되는 모든해쉬 알고리즘을 나타내는 digest Algorithm, achiveTimeStampSequence를 검증하는데 이용되는 인증서, CRL 등의 crypto-Infos, 데이터 객체를 암호화하기 위하여 사용되는 encryption, 그리고 아카이브될 데이터 객체를 보관하는 archiveTimeStampSequence 등으로 구성된다. 이의 생성과정은 아카이브될 데이터 객체를 모으고, 이를 기본으로 초기 아카이브 타임스템프를 만들며, 타임스템프 갱신 과정이나 해쉬 트리 갱신과정을 통하여 아카이브 타임스템프를 갱신하는 과정으로 구성된다. 아카이브 타임스템프는 기본적으로 특정 시점에 데이터의 존재를 검증하기 위한 타임스템프와 해쉬 값들의 목록이다. 이 해쉬값의 목록은 순서를 갖는 해쉬 트리에 의하여 생성될 수 있다. 이 문서에서는 아카이브 타임스템프 체인, 아카이브 타임스템프 계열, 그리고 암호를 위한 신택스를 정의하고 있다.

라. 향후 표준화 방향

LTANS 작업반은 58차 IETF 회의에서부터 표준화 작업을 시작하였고, 현재까지 작업반에서 나온

〔표 6〕 IETF PKI4IPSEC 인터넷 드래프트 문서

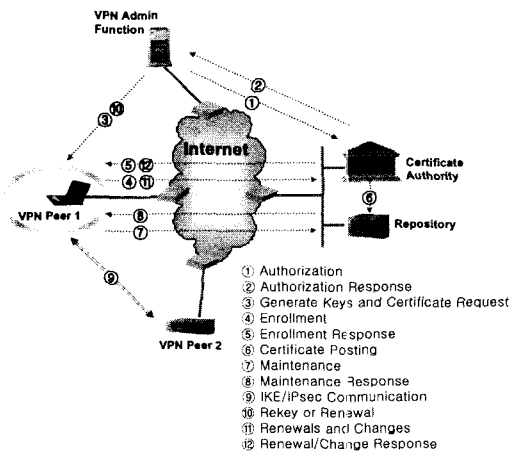
문서제목	주 요 내 용	문서상태
인증서 관리 프로파일을 위한 요구사항	이 문서는 VPN IPSEC 시스템과 PKI 시스템과의 상호 동작을 통한 인증서 관리를 위한 요구사항을 기술하고 있다. 이 문서는 2004년 1월에 발표되었고, WG 문서가 아니라 개인 문서의 지위를 갖고 있다.	첫 번째 문서 (2004.1.)
IKE/ISAKMP을 위한 PKI 프로파일	이 문서는 ISAKMP를 위한 PKI 프로파일과 PKIX 인증서 및 CRL 프로파일을 다루고 있다. 이 문서는 곧 IETF PKI4IPSEC 작업반 홈페이지에 나타날 것이다.	다섯 번째 문서 (2004.2.)
IKE 버전 1을 위한 인증서 사용 프로파일	이 문서는 IKEv1을 위한 PKI 프로파일을 기술하고 있으며, 아직 많은 논의가 필요한 문서이다.	첫 번째 문서 (2003.12)

RFC는 없으나, 3개의 드래프트 문서가 마련되었고, 이는 요구사항, 데이터 구조, 그리고 프로토콜에 대한 문서이다. 요구사항 문서는 금년 2월 공개되었으며, 데이터 구조는 금년 2월 공개되었고, 프로토콜은 아직 웹상에 나타나고 있지 않고 있다. 따라서, 먼저 요구사항 문서가 정보 표준화 될것이고, 이후 이 요구사항을 만족하는 데이터 구조와 프로토콜에 대한 문서가 표준화될 것으로 예측된다.

2.4 PKI4IPSEC 작업반 표준화 동향

가. 개요

IPSEC 프로토콜은 지난 5년전에 표준화되었고, 이중 IKE나 ISAKMP 프로토콜은 PKIX X.509 인증서를 사용자나 개체 인증을 위하여 사용할 것을 규정하고 있다. 그러나 인증서를 사용하고 있는 IPSEC 시스템은 많지 않다. 이에 대한 주요 이유는 IPSEC 표준에서 어떻게 인증서를 사용할 것인지에 대한 구체적인 기술이 많이 부족하고, IPSEC 시스템이 인증서를 얻고, PKI 시스템과 인증서 관리 동작을 수행하기 위한 간단하고 규모 가변이며 분명히 기술되어 있는 문서가 없음에 기인하고 있다. 따라서 PKI4IPSEC 작업반에서는 3가지 주제에 대한 표준화 작업을 수행할 예정이다. 첫 번째 주제는 IKEv1과 IKEv2 측면에서 X. 509 인증서를 어떻게 처리할 것인지에 대한 분명한 문서를 표준화 할것이다. 이 문서에서는 인증서의 어떤 필드가 어떤 값을 가져야 하는지와 인증서의 특정 값들이 어떻게 처리되어야 하는지를 다루는 인증서 프로파일을 다룰 것이다. 두 번째 주제는 PKI 등록(enrollment)과 IPSEC 시스템과 VPN 시스템 간의 인증서 관리 동작 등의 프로파일에 대한 요구사항을 확인하고 기술하는 정보문서를 표준화하는 것이다. 세 번째 주제는 요구사항 문서를 만족하는 CMC (CMS을 통한 인증서 관리 메시지) 프로토콜에 대한 세부 규격을 정의하는 것이다. 이 작업반의 IPSEC 시스템 대상은 게이트웨이간 접근과 최종 사용자의 원격 접근 등을 포함하는 기업 규모의VPN 이용에 대한 표준을 중점적으로 수행할 예정이다. 현재까지 발표된 문서는 IPSEC 인증서 관리를 위한 요구사항 문서, IKE/ISAKMP를 위한 PKI 프로파일, 그리고 IKE 버전 1을 위한 인증서 프로파일 문서가 발표되었다.



〔그림 4〕 PKI4IPSEC을 위한 주요 동작

나. 표준화가 완료된 문서

현재까지 RFC로 표준화되어 있는 문서는 없다.

다. 표준화가 진행되고 있는 문서

현재 표준화 중인 문서는 표 6과 같다.[37-40] 인증서 관리프로파일을 위한 요구사항에 관한 문서는 IKE와 PKI 시스템을 이용하여 공개키 인증서의 상호동작을 처리하기 위한 인증서 관리 프로토콜을 위한 요구사항을 확인하고 기술하고 있다. 이 문서의 적용 대상은 기업 차원의 VPN 시스템이다. 이 문서는 표준 트랙 문서로 표준화될 것이다. 이 문서는 IPSEC VPN과 PKI 시스템간에 수행되어져야 할 처리과정을 분명히 하였다. 이 문서는 IPSEC 시스템과 PKI시스템간의 상호 연동성을 달성 가능케 할 것이다. 이를 위한 과정은 인증서 발행을 위한 사전 인가(pre-authorization) 과정, 인증서 요구 및 조회를 포함하는 등록(enrollment) 과정, 인증서 갱신, 변경, 검증, 취소, 그리고 저장소 탐색 등의 관리 과정으로 구성된다. 이러한 문서의 결과로 얻을 수 있는 결과는 인증서 발행을 원하는 개인이나 개인들의 집합을 인가할 수 있고, VPN peer에 신분정보를 제공하며, 원격 접근 및 게이웨이간 접근을 위한 VPN peer 접근 제어 정책을 설정할 수 있고, 인증서의 자동적인 갱신, 그리고 취소 정보의 시기 적절한 제공 등을 얻을 수 있다. 또한 이러한 규격을 이용하면, 상호 동작이 가능한 VPN 제품과 PKI 제품을 생산할 수 있다. PKI 시스템과 VPN 시스템간의 전체적인 구조는 그림 4와 같다. PKI 시스템은 인증서를 발행하고, 사용자를 인가하기 위하여 필요한 기능을 제공하며, 인증서 취소 정보를 제공한다. VPN 관리자 기능은 보안 정책을 정의하고, 일괄된 보안 정책 하에서 사용자를 대신하여 PKI 시스템과 상호 동작을 하는 기능이며, VPN peer는

인증서와 연관된 개인키를 생성하고 PKI 시스템과 상호동작하는 게이트웨이나 원격 사용자 시스템을 지칭한다. VPN 시스템과 PKI 시스템과의 상호 동작은 ID 와 인증서의 내용을 VPN 관리 기능이 PKI 시스템에게 전달하는 인가 요구 과정, 인가 요구과정에서 전달된 결과(ID와 일회용 패스워드)를 PKI 시스템이 VPN 관리시스템에게 전달하는 인가 응답 과정, VPN 관리기능이 VPN peer에게 키생성과 인증서를 요구하는 과정, VPN peer가 PKI 시스템에게 인증서 갱신을 요구하는 등록 요구 과정, 등록 요구에 응하여 PKI 시스템이 VPN peer에게 전달하는 등록 응답 과정, 인증기관이 레포지토리로 인증서를 공표하는 과정, VPN과 PKI 시스템간의 인증서 관리(유효성 검증, 인증서 취소목록 요구, 인증서 갱신) 과정, 관리 요구에 응하여 PKI 시스템이 관리 응답 과정, VPN peer 간의 IKE/IPSEC 통신 과정, VPN 관리 기능이 VPN peer에게 인증서 갱신과 리키를 요구하는 과정, VPN peer가 인증서 갱신 및 리키 요구에 응하여 PKI 시스템에게 인증서 갱신 및 리키를 요구하는 과정, PKI 시스템이 VPN peer에게 전달하는 인증서 갱신 및 리키 응답 과정 등으로 구성된다. 세부 요구사항은 하나의 프로토콜을 사용하도록 권고하는 요구사항 등의 일반적인 요구사항, 인가 과정에서 요구되는 하나 이상의 인가, 하나의 채널에 여러다중 처리 등에 대한 인가와 관련된 요구사항, 키 생성 위치(IPSEC peer, VPN 관리자)와 인증서 요구 구성 위치등에 대한 요구사항, 온라인 프로토콜의 이용과 하나의 연결상에서 요구와 응답이이루어져야 한다는 등의 등록 과정에 대한 요구사항, 신분 확인, 경로 검증, 키용도, 확장키 사용, 취소 확인을 위한 동작 등의 PKI 상호동작을 위한 인증서 프로파일에 대한 요구사항, 인증서 갱신 및 변화에 대한 요구사항, 레포지토리에서 인증서를 찾는 방법에 대한 요구사항, 인증서 취소 방법에 대한 요구사항 등을 다루고 있다. 이 문서는 추가로 개발될 프로토콜과 규격을 위한 기반 문서로 활용될 수 있다.

IKE/ISAKMP을 위한 IPSEC 보안 PKI 프로파일에 관한 문서는 IPSEC 환경에서 PKI 사용을 위한 ISAKMP에 대한 프로파일을 제공한다. 또한 공개키 인증서와 키잉 자료의 존재를 가정하고 있는 IKE 등과 같은 프로토콜에도 적용될 수 있다. 이 문서는 신분확인(identification) 페이로드, 인증서 요구 페이로드, 인증서 페이로드, 인증서 프로파일, CRL 프로파일을 다루고 있다. 기본적으로 이 문서가 나오게 된 배경은 ISAKMP에서 공개키 인증서의 사용을 전제하고 있지만, 수많은 규정되지 않은 항목으로 인하여 IPSEC peer 간에 상호 동작에 큰 저해가 되고 있다. 따라서 이 문서는 IPSEC ISAKMP을 위한 PKI 관련 표준을 개발함에 목적이 있다. ISAKMP에서 이용되는 PKI 관련 페이로드는 크게 주장하고자 하는 신분정보를 나타내는 ID 페이로드, 상대 peer에게 인증서를 요구하는 인증서 요구 페이로드, 상대 peer로부터 인증서 요구를 수신한 peer 가 인증서를 전달하기 위한 인증서 페이로드 등이 있다. 이 문서는 이러한 페이로드에 대한 규격을 분명하게 기술하고 있다. 또한 인증서와 CRL 관련 프로파일을 정의하고 있으며, 인증서는 버전, 주체이름, 인증서 확장자(인증기관 키 확인자, 주체 키 확인자, 키 용도, 개인키 사용 기간, 인증서 정책, 주체 대체 이름, 인증기관 대체 이름, 주체 디렉토리 속성, 기본 제한자, 이름 제한자, 정책 제한자, 확장 키 용도, CRL 분배점, 금지 any 정책, 최신 CRL, 인증기관 정보접근자, 주체 정보 접근자) 등에 대한 프로파일을 정의하고 있고, 다양한 CRL에 대한 프로파일을 정의하고 있다.

IKE 버전 1을 위한 인증서 사용 프로파일에 관한 문서의 내용은 다음과 같다. IPSEC에서 보안 연계를 설정하는 가장 일반적인 방법은 IKE 프로토콜을 이용하는 것이다. IKE 프로토콜은 인증서를 이용하여 사용자 인증을 수행하고 있다. 이 문서의 주목적은 IPSEC IKE에서 인증서 형태와 공개키 정보 교환 방법에 대한 선택을 줄여 주기 위함이다. 이 문서는 사용 가능한 인증서로 PKIX 인증서를 사용해야 하고, 디지털 서명용의 키확장자, 1024비트 이상의 sha-1 WithRSAEncrytion 서명 알고리듬을 사용할 것을 권고하고 있다. 또한 이 문서는 IKEv1 에 대한 인증서 처리 방법을 제시하고 있다. IKEv1을 위한 메인 모드를 다루며, 두 VPN peer는 RSA 서명 알고리즘으로 인증을 수행해야 하며, 두개의 VPN peer는 CERTREQ와 CERT 페이로드를 전송할 수 있어야 하며, VPN 시스템은 인증서 취소 정보를 접근할 수 있어야 하며, 전체 경로 검등을 수행할 수 있어야 한다고 기술하고 있다.

라. 향후 표준화 방향

현재 RFC로 표준화된 문서는 없으므로, 향후에는 IPSEC 인증서 관리 프로파일을 위한 요구사항 문서가 정보 RFC 문서로 먼저 표준화될 것이고, ISAKMP에 적용될 수 있는 PKI 프로파일과 IKEv1

과 IKEv2 와 관련된 X.509 인증서 프로파일을 표준화 할 것이다.

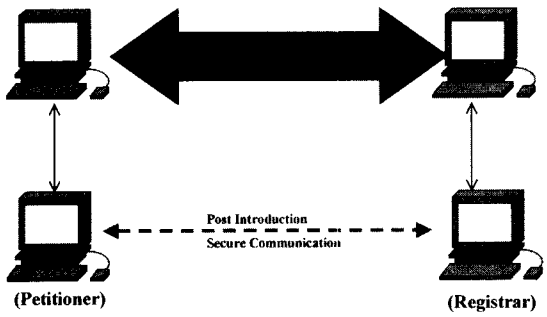
2.5 ENROLL 작업반 표준화 동향

가. 개요

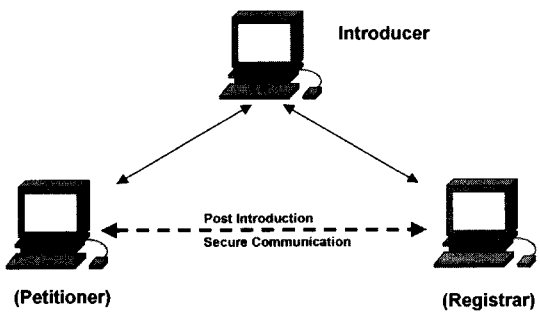
PKI 시스템이 일반화 되고 있지만, 등록 과정에 대한 사용자의 부담이 PKI 활성화에 커다란 장애로 작용하고 있다. 등록(Enroll) 과정을 통하여 사용자는 크리덴셜을 획득한다. 크리덴셜(Credential)은 사용자의 개인키/공개키, 인증서, 인증서 체인 등의 사용자 관련 암호 정보로 구성된다[41-42]. 서비스 고객이 서비스를 접근할 때 사용할 수 있는 크리덴셜을 서비스 제공자에 접근하여 얻을 수 있다. 등록 과정은 일반적으로 오프라인으로 수행되는 사전 소개(Pre-introduction) 과정과 온라인으로 수행되는 사후 소개(Post Introduction) 과정으로 구성되며, 사전 소개 과정은 주로 오프라인으로 실행되어 왔으며, 사후 소개를 위한 비밀을 공유한다. 사전 소개 과정은 고객과 서비스 제공자가 최초로 접근하는 과정이라고 할 수 있다. 고객과 서비스 제공자와의 초기 접촉은 서로 신분을 확인하는 과정을 포함하고 있다. 지금까지 대표적인 등록(Enroll) 프로토콜은 PKIX 인증서 관리 프로토콜, PKCS #7 인증서 요구 등이 있으며, 이들 프로토콜은 실제적으로 고객이 크리덴셜을 획득할 때 반드시 채널외 밴드(Out-of-band)를 통하여 크리덴셜의 일부를 제공받도록 구성되어 있다. 이러한 과정을 사전소개(pre-introduction) 단계라고 하며, 이 사전 단계는 지금까지는 오프라인 방법으로 수행되었다. 대표적인 오프라인 방식은 전화, e-메일, 플러피 디스크, 스마트카드이며, 이 사전 소개 단계에서 획득된 정보는 추후 사후 소개를 위한 정보로 이용된다. 사전 단계에서 교환되는 정보는 크게 3가지로 구분된다. 하나는 인증받고자 하는 주체와 인증하는 주체 사이에 공유되는 비밀키이고, 다른 하나는 인증하는 주체의 공개키이고, 다른 하나는 공개키의 핑거프린트인 인증서이다. 이러한 사전 소개 단계에서 공유된 정보는 사후 단계인 실제적인 크리덴셜을 청구인이 등록인으로 얻고자 할 때 이용된다.

서비스 고객이 서비스제공자에 등록 할 때, 인증을 위하여 3가지 정보가 제공되어야 한다. 하나는 서비스 제공자에 의하여 제어되는 이름 공간내의 신분확인 정보이고, 두 번째는 사후 소개단계에서 신분 확신을 위하여 이용되는 키잉정보(Keying Information)이며, 서비스 고객이 접근할 수 있는 서비스를 기술하는 허가 등에 관한 정보이다.

이 개념은 그림 5와 같은 기존의 사전 소개 단계를 그림 6과 같은 소개기관(Introducer)을 두고 사전 소개 단계를 수행함으로써, 서비스 고객과 서비스 제공자간에 크리덴셜을 획득하기 위한 사후 소개 과정을 안전하게 실행하는데 그 목적이 있다. 여기서 청원자(petitioner)는 보안 영역에 가입하고자 하는 디바이스(클라이언트)이고, 등록인(registrar)은 보안 영역의 인증 및 인가 구조이며 서버라고 불리운다. ENROLL 작업반은 오프라인으로 실행되는 사전 소개 과정을 온라인으로 변경하기 위하여 소개자(Introducer)를 두고 사전 소개 과정을 수행하기 위한 표준을 개발하기 위한 작업반이다. 이러한 표준이 이용 가능한 시나리오는 무선 프린트를 사서, 집으로 가져와서, 무선 프린터를 홈 네트워크에 등록하고자 할때, 무선 프린터를 사용자가 설정하고, 소개자와 통신하여 사전 소개 과정을 수행하고, 사전 소개 과정을 통하여 세가지 정보(신분확인자, 키잉 재료, 그리고 인가 정보) 등을 이용하여 사후 과정을 통하여 크리덴셜을 획득하는 과정을 수행할 때 적용될 수 있다.



〔그림 5〕 기존의 초기 소개 과정



〔그림 6〕 소개자를 이용한 초기 소개 과정

이 작업반에서는 등록 과정을 위한 모델을 정의하고, 등록 과정을 수행하는 방법에 대한 프레임워크를 만들고, 3가지 키잉 방법에 대한 프레임워크 사용에 대한 프로파일을 표준화하는 문서를 생성한다.

나. 표준화가 완료된 문서

이 작업반은 2003년 7월에 BOF 로 시작하여 아직 RFC 로 표준화된 문서가 없다.

다. 표준화가 진행되고 있는 문서

아직 웹 사이트에 어떤 인터넷 드래프트도 나타나고 있지않다. 이 작업반은 표준화의 초기 단계에 있다고 볼 수 있다. 따라서 많은 작업이 이루어지지 않고 있다.

라. 향후 표준화 방향

향후 이 작업반에서는 작업장 현장에 따라서 등록 과정을 위한 모델을 정의하고, 등록 과정을 위한 프레임워크를 생성하며, 세가지 키잉 방법에 따른 프로파일을 개발할 것이다.

Ⅲ. 결 론

IETF 보안 영역중의 PKIX 작업반은 X.509 기반 PKI를 지원하기 위한 표준을 개발하고 있고, SACRED 작업반에서는 안정한 크리덴셜의 전달을 위한 표준을 개발하고 있으며, ENROLL 작업반은 크리덴셜을 얻기 위한 사전 소개 과정에 대한 표준을 개발하고 있고, LTANS 작업반은 장기간 부인방지 서비스에 대한 표준을 개발하고 있으며, PKI4IPSEC 작업반은 IKE나 ISAKMP에서 이용되는 PKI 기술에 대한 표준을 개발하고 있다. 지금까지 하나의 작업반(PKIX)에서 수행되던 PKI 에 대한 표준 개발이 4개의 새로운 작업반(ENROLL, SACRED, PKI4IPSEC, LTANS)이 신설되어 PKI 응용 관련 표준을 개발할 예정이다. 이들 4개의 작업반은 PKIX 작업반과 긴밀히 협조하여 관련 표준을 개발하고 있다.

본 고에서는 IETF 보안 영역의 5개의 PKI 관련 작업반에서 수행되고 있는 지금까지의 표준화 동향, 현재 표준화가 진행되고 있는 항목, 그리고 앞으로 표준화가 진행될 분야를 중심으로 기술하였다. 본 연구의 결과는 정책당국의 경우 국내 표준화 정책개발시에, 국내 산업체의 경우 정보보호 제품 개발시에 가이드라인으로 활용될 수 있을 것이다.

참 고 문 헌

[1] 염흥열, "PKI 표준화 동향과 PKI 영영간 상호연동 방법", 한국정보보호학회지, 제12권 4호, 2002.8.

[2] 이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영, "전자상거래 보안기술", 생능출판사, 1999

[3] 염흥열외, "선진국의 정보보호기술 개발사업 동향분석 및 국내 대응방향 연구", 정보통신진흥원, 2002.2.

[4] 염흥열외, "유·무선 PKI 운용환경 분석 및 연동방안 제시에 관한 연구", 한국전자통신연구원, 2001.12.

[5] IETF-pkix, http://www.ietf.org/html.charters/pkix-charter.html

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

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

[8] RFC 2511, "Internet X.509 Certificate Request Message Format", M. Myers, C. Adams, D. Solo, D Kemp, March 1999

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

[10] RFC 2528, "Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates", R. Housley, W. Polk, March 1999

[11] RFC 2559, "Internet X.509 Public key Infrastructure Operational Protocols - LDAPv2", S. Boeyen, T. Howes, P. Richard, April 1999

[12] RFC 2585, "Internet X.509 Public Key Infrastructure Operational Protocols : FTP and HTTP", R. Housley, P. Hoff-

man, May 1999
[13] RFC 2587, "Internet X.509 Public Key Infrastructure LDAPv2 Schema", S. Boeyen, T.Howes, P.Richard, June 1999
[14] RFC 2560, "X.509 Internet Public Key Infrastructure Online Certifiate Status Protocol -OCSP", M. Myers, R. Ankney, A. Malpani, S. Galperin, C.Adams, June 1999
[15] RFC 2797, "Certificate Management Me ssages over CMS", M. Myers, X. Liu, J. Schaad, J. Weinstein, April 2000
[16] RFC 2895, "Diffie-Hellman Proof-of-Pos session Algorithms", H. Prafullchandra, J. Schaad. July 2000
[17] RFC 3039, "Internet X.509 Public Key Infrastructure Qualified Certificates Profile", S. Santeson. W. Polk, P. Barzin, M. Nystrom, January 2001
[18] RFC 3029, "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols", C. Adams, P. Sylvester, M. Zolotarev. R. Zuccherato. February 2001
[19] RFC 3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", C. Adams, P. Cain, D. Pinkas, R. Zuccherato, August 2001
[20] RFC 3279, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certifiate Revocation List (CRL) Profile. W. Polk, R. Housley, L. Bassham, April 2002
[21] RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, R. Housley, W. Polk, W. Ford, D. Solo, April 2002
[22] RFC 3281, "An Internet Attribute Certificae Profile for Authorization", S. Farrell, R. Housley, April 2002
[23] RFC 3379, "Delegated Path Validation and Delegated Path Discovery Protocol Requirements", D. Pinkas, R. Housley, September 2002
[24] RFC 3628, "Policy Requirements for Time-Stamping Authorities (TSAs)", D. Pinkas, N. Ross, November 2003
[25] RFC 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, November 2003
[26] RFC 3709, "Internet X.509 Public Key Infrastructure : Logotypes in X.509 Certificates", S. Santesson, R. Housley, T. Freeman, February 2004
[27] RFC 3739, "Internet X.509 Public Key Infrastructure : Qualified Certificates Profile", S. Santesson, M. Nystrom, T. Polk, March 2004
[28] IETF-sacred, http://www.ietf.org/html.charters/sacred-charter.html
[29] RFC 3157, "Secure Available Credentials - Requirements ", A. Arsenault Diversinet, S. Farrell, August 2001
[30] IETF-sacred-framework-Internet Draft, "Securely Available Credentials - Credential Server Framework", D. Gustafson future Foundation, M. Just, November 2003
[31] IETF-sacred-protocol-Internet Draft, "Securely Available Credentials protocol ", Stephen Farrell, November 2003
[32] IETF-ltans,http://www.ietf.org/html.charters/ltans-charter.html
[33] IETF-ltans-reqs-Internet Draft, "Long-term Archive Service Requirements", Carl Wallace, Ralf Brandner, February 2004.
[34] IETF-ltans-ers-Internet Draft, "Evidence Record Syntax", R. Brandner, February 2004
[35] IETF-ltans-LTANS-reqs Draft, http://ltans.edelweb.fr. P.Sylvester, Jerman Blazic, March, 2004
[36] IETF-pki4ipsec, http://www.ietf.org/

html. charters/pki4ipsec-charter.html
[37] IETF-pki4ipsec-profile-reqs Draft, "Requirements for an IPSec Certificate Management Profile", Chris Bonatti, Sean Turner, Gregory Lebovitz, January, 2004
[38] IETF-pki-profile Draft, "The Internet IP Security PKI Profile of IKE/ISAKMP and PKIX", Brian Korver, Eric Rescorla, February, 2004
[39] IETF-pki4ipsec-profile Draft, "Profile for Certificate Use in IKE version 1", Paul Hoffman, December, 2003
[40] IETF-pki4ipsec, http://honor.icsalabs.com/mailman/listinfo/pki4ipsec, "Proposed PKI4IPSEC Certificate Management Requirements Document", Chris Bonatti, March, 2004
[41] IETF-enroll, http://www.ietf.org/ietf/03nov/enroll.txt, November, 2003
[42] IETF-enroll, http://www.ietf.org/html.charters/enroll-charter.html
[43] IETF-pkix-scvp-Draft, "Simple Certificate Validation Protocol (SCVP)", A. MAlpani, R. Housley, T. Freeman, October, 2003

〈著 者 紹 介〉

염 흥 열 (Heung-Youl Youm) 종신회원

1981년 2월 : 한양대학교 전자공학과 학사
1983년 2월 : 한양대학교 전자공학과 석사
1990년 2월 : 한양대학교 전자공학과 박사
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~현재 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사
2003년 9월~현재 : ITU-T SG17/Q10 Associate Rapporteur
〈관심분야〉 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안