CROSSCERT™ CPS

CROSSCERT 인증 업무 준칙

CrossCert 공용 인증 서비스(PCS) 지원
클래스1-3 DIGITAL ID℠/인증서

버전 1.2

발행일: 1999년 11월
발효일: 1999년 11월

우편 번호 137-725 서울시 서초구 서초동 1674-4 하림 빌딩 9층 한국전자인증(주)

Ref. 009

CROSSCERT 인증 업무 준칙

경고: CROSSCERT의 공용 인증 서비스 사용은 대한민국 형법의 적용을 받습니다.

CROSSCERT는 CROSSCERT 공용 인증 서비스에 직접적 영향을 미치는 범죄를 저지르는 자를 찾아내어 고발에 조력할 권리가 있습니다.

주요 CPS 권리 및 의무 개요

자세한 내용은 본 CPS의 본문을 참조하십시오. 이 내용은 개요입니다. 기타 중요한 사항은 CPS에 수록되어 있습니다.

1. 인증 업무 준칙(용어 정의 *참조*)은 인증(용어 정의 *참조*) 신청[§ 4], 신청서의 타당성 검사[§ 5], 인증서 발행[§ 6], 승인[§ 7], 사용[§ 8], 일시 중지 및 취소[§ 9] 등 CrossCert 공용 인증 서비스(용어 정의 *참조*)의 규정과 사용에 관한 기준입니다.

2. 사용자는 (i) 인증서를 신청하기에 앞서 공용 키 기술의 사용에 대한 적절한 훈련을 받았으며, (ii) CrossCert[§ 1.6]로부터 디지털 사인, 인증서, PKI, PCS에 대한 설명서, 훈련, 교육을 받을 수 있음을 인지합니다.

3. CrossCert는 각각 다른 클래스의 인증서[§ 2.2]를 제공합니다. 사용자는 어떤 클래스의 인증서가 사용자 측에 적합한지를 결정해야 합니다.

4. 사용자는 인증 신청서[§ 4.2]를 제출하기 전에 신뢰할 만한(용어 정의 *참조*) 방법[§ 4.1.1]으로 키 쌍[§ 2.3.3, 4.1]을 생성하고 개인 키 보안[§ 4.1]이 손상(용어 정의 *참조*)되지 않도록 해야 합니다. 사용자의 해당 소프트웨어 시스템에 이러한 기능이 있어야 합니다.

5. 사용자는 다른 사람에게 인증서를 전달하거나 다른 사람의 인증서 사용을 유도하기 전에 인증서를 승인[§ 7.1]해야 합니다. 사용자는 인증서(용어 정의 *참조*)를 승인함으로써 특정한 중요 진술[§ 7.2]을 합니다.

6. 디지털 서명이나 인증서의 신뢰에 대한 결정 책임은 전적으로 디지털 서명 및 인증서의 수취인에게 있습니다. CrossCert는 사용자가 인증서를 신뢰하기 전에 CrossCert 저장소(용어 정의 *참조*)를 점검하여 해당 인증서(용어 정의 *참조*)가 취소(용어 정의 *참조*) 또는 일시 중지(용어 정의 *참조*)되지 않은 유효한(용어 정의 *참조*) 것임을 확정(용어 정의 *참조*)한 다음, 디지털 서명(용어 정의 *참조*)이 인증 기간 중에 인증서(용어 정의 *참조*) 목록의 공용 키(용어 정의 *참조*)에 대응하는 개인 키(용어 정의 *참조*)로 작성되었으며 디지털 서명(용어 정의 *참조*) 관련 메시지(용어 정의 *참조*)가 변경되지 않았다는 것을 확인[§ 8.1]하는 것을 권장합니다.

7. 사용자는 개인 키(용어 정의 *참조*)가 손상(용어 정의 *참조*)되는 상황이 발생하면 즉시 해당 발행 기관(용어 정의 *참조*)에 통지[§ 12.10]해야 합니다.

8. 인증 업무 준칙(용어 정의 *참조*)에는 CrossCert와 발행 기관이 제공한 다양한 보증이 수록되어 있으며[§ 11.2] 여기에는 CrossCert의 환불 제도도 포함되어 있습니다[§ 11.1]. 그 이외에는 CrossCert와 발행 기관은 보증을 부인하고 신뢰성을 제한합니다[§ 11.3, 11.4, 11.5, 4.3].

9. 인증 업무 준칙(*용어 정의 참조*)에는 이 외에도 다양한 기타 규정[§ 12]이 수록되어 있으며 해당 수출 규칙의 준수[§ 12.2] 및 그 위반의 금지[§ 12.14]를 규정하고 있습니다.

자세한 내용은 CrossCert 웹 사이트(https://www.crosscert.com)*을 방문하거나 고객 서비스 센터*(customer-service@crosscert.com)*로 문의하십시오.*

감사의 말씀

CrossCert 인증 업무 준칙의 기준이 되는 VeriSign 인증 업무 준칙의 개발과 검토에 있어 제안이나 편집 비평, 기타 도움을 주신 다음 분들께 감사 드립니다.

법률

Dr. Mads Bryde Andersen 교수	University of Copenhagen, Denmark
Harold S. Burman	U.S. State Department
Robert Daniels	U.S. Social Security Administration
Jos Dumortier 교수	University of Leuven, Belgium
Deborah Fuerer	United States Fidelity and Guaranty Company
Eugene E. Hines	American Society of Notaries
Janette M. Hoover	Tomlinson Zisko Morosoli & Maser LLP
Toshio Kosone	Kosone & Associates, Japan
Charles R. Merrill	McCarter & English
Ray Nimmer	Weil, Gotshal & Manges
Arthur F. Purcell, B.E., J.D.	U.S. Patent and Trademark Office
Ira Rubenstein	Microsoft Corporation
John D. Ryan	America Online, Inc.
Ruven Schwartz	West Publishing Company
John F. Simanski Jr.	United States Fidelity and Guaranty Company
Michiru Takahashi	Showa Law Office, Japan
Timothy Tomlinson	Tomlinson Zisko Morosoli & Maser LLP
Shinya Watanabe	Showa Law Office, Japan

엔지니어링 및 기술

Frank Chen	Netscape Communications Corporation
Allan Cooper	Microsoft Corporation
Steve Crocker	CyberCash, Inc.
Steve Duss	RSA Data Security, Inc.
Taher Elgamal, Ph.D.	Netscape Communications Corporation
James M. Galvin, Ph.D.	CommerceNet
Peter Landrock, Ph.D.	Cryptomathic, Denmark
Ron Rivest, Ph.D.	Massachusetts Institute of Technology
Jeff Schiller	Massachusetts Institute of Technology
Allan Shiffman	Terisa Systems
David I. Solo	BBN, Inc.

관리 및 컨설팅

Dwight Arthur	National Securities Clearing Corporation
Kaye Caldwell	Software Industry Coalition
Bruce Crabtree	Conanicut Communications
F. Jo Goodson	Goldman, Sachs & Co.

버전 1.2 - -1999년 11월 발행

Mark Greene, Ph.D.	IBM Corporation
F. Lynn McNulty	RSA Data Security, Inc.
Michel Peereman	Belgian Federation of Chambers of Commerce
Guy Richard	La Poste, France

감사 및 비즈니스 관리

Eric T. Ashdown	KPMG Peat Marwick
Cris R. Castro, CISP	Ernst & Young(구 KPMG Peat Marwick)
Kevin M. Coleman	KPMG Peat Marwick
Steven A. Dougherty	KPMG Peat Marwick
Martin Ferris	U.S. Department of the Treasury
Dwight Olsen	Data Securities International
Gary W. Riske	KPMG Peat Marwick
Horton Sorkin 교수, Ph.D.	Howard University
Stephen Spaulding	KPMG Peat Marwick
Geoffrey W. Turner	Ernst & Young(구 KPMG Peat Marwick)

이 외에도 해당 분야의 발전에 지대한 공헌을 하고 있는 American Bar Association의 Electronic Commerce and Information Technology Division, Section of Science and Technology와 Digital Signature Guidelines, 그리고 Information Security Committee에서 기꺼이 도와 주셨습니다.

마지막으로, MasterCard/Visa의 전자 상거래 기술 표준인 Secure Electronic Transaction(SET) 프로토콜은 보안 프로토콜 설계 원칙(예: 계층 구조) 자원으로서 본 CPS에서 채택하게 될 프로토콜입니다.

의견 및 제안 사항

사용자들의 입장에서 바라는 CPS 개정에 대한 편집 의견 및 제안 사항을 보내주시기 바랍니다. 보내실 주소는 다음과 같습니다. practices@crosscert.com 또는 우편 번호 137-725, 서울시 서초구 서초동 하림 빌딩 9층 한국전자인증(주)

목 차

1. 서 문

이 단원에서는 Crosscert의 인증 업무 준칙(CPS)과 본 인증 업무 준칙의 구조 및 기본 규칙에 대해 설명합니다. CPS에서 사용되는 머리글자 및 약어 목록은 이 단원의 마지막에 수록되어 있습니다.

1.1 개요

CrossCert 인증 업무 준칙은 VeriSign의 인증 업무 준칙(*https://www.verisign.com/cps* 참조)에 기반을 둔 것으로, CrossCert의 공용 인증 서비스는 CrossCert의 공용 인증 서비스(PCS) 한국전자인증㈜(이하 "CrossCert"라 함)와 CrossCert의 발행 기관(IA) 그리고 CrossCert 이외의 IA가 담당하는 인증서 기반의 공용 키 구조(PKI) 유지 및 인증서의 발행과 관리 업무를 말합니다. CPS는 IA의 구축과 개시, 저장소 운영부터 가입자 등록에 이르는 전체 인증 프로세스를 열거하며 통제합니다. PCS는 인증서의 발행, 관리, 사용, 일시 중지, 취소 및 갱신 서비스를 제공하며,CPS는 이러한 PCS의 범위 내에서 인증서를 작성, 사용, 발효하는 모든 당사자들을 합법적으로 통합하고 통지하기 위해 고안된 것입니다. 그림 1에 나타난 것처럼 CPS는 PCS 관리에 있어 중심적인 역할을 합니다.

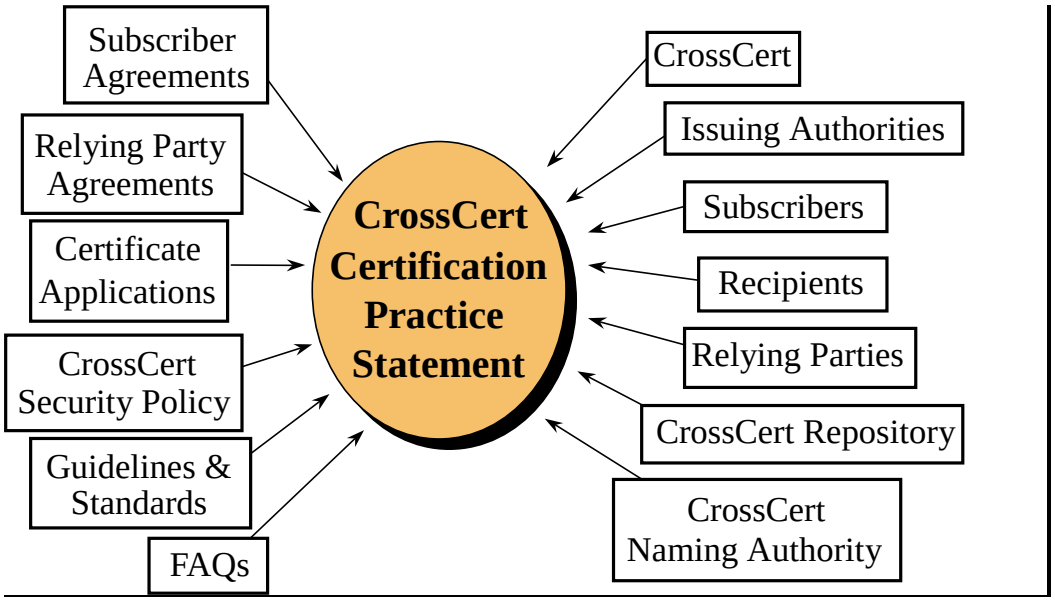

그림 1 – CROSSCERT CPS의 중심 역할

CPS는 **CROSSCERT**에서 제공하는 일부 서비스에만 적용되며,기타 **CROSSCERT** 서비스에는 일련의 IA 또는 IA 구조의 호출이 필요 없을 수도 있습니다. PCS는 시장의 수요에 따라 다른 구조도 적용할 수 있도록 발전될 것입니다. 본 CPS는 새로운 서비스를 반영하고 PCS 하부 구조를 전반적으로 향상시킬 수 있도록 주기적으로 갱신됩니다. CPS – 12.12.2를 참조하십시오.

버전 1.2 – – 1999년 11월 발행

1.2 CPS의 구조

CPS는 인증 프로세스를 "생성에서 소멸" 까지의 주기로 설명하며 IA 구축을 시작으로 IA 운영, 등록, 인증서 사용, 인증서 중지, 인증서의 취소 및 종료와 같은 전반적인 IA 운영을 포괄합니다. 이런 접근 방식이 갖는 장점은 사건을 순차적으로 표현할 수 있으며 민간 분야 및 공공 분야의 주요 업무 준칙 구조와 호환할 수 있다는 것입니다.

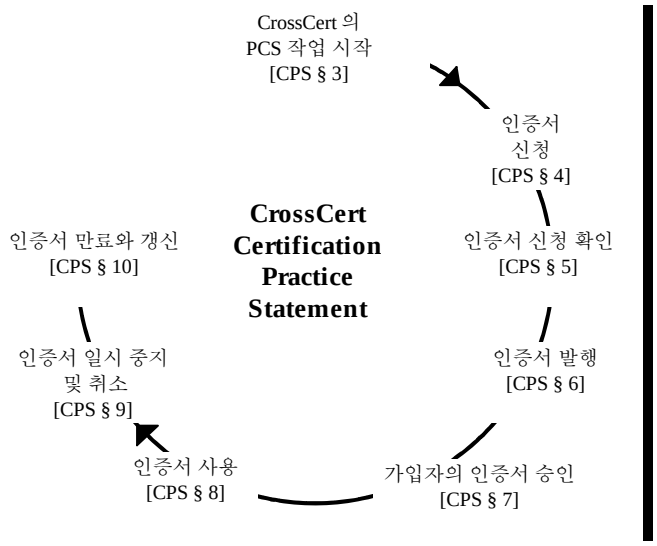

그림 2 - CPS의 주기 구조

1.3 CPS의 인용

다른 문서에서 본 인증 업무 준칙을 언급할 때는 "**CROSSCERT** CPS"나 "**CROSSCERT** 인증 업무 준칙"으로 표기해야 합니다. 내부적으로는 "CPS"나 "CPS § _"로, 부록은 "부록 § 13._"으로 표시합니다. CPS는 주기적으로 갱신됩니다. CPS의 버전은 "CPS" 다음에 버전 숫자로 표시합니다 (*예:* "버전 1.2" 또는 "CPS 1.2").

1.4 밑줄친 텍스트

CPS 온라인 버전에서 밑줄친 텍스트는 해당 용어(부록 13.1 – 용어 정의 *참조*)가 이 CPS에서 처음으로 사용되었음을 나타냅니다. WWW 기반의 CPS 버전에서는 CPS 내의 교차 참조를 비롯한 용어 정의 및 기타 관련 문서의 빠른 참조에 하이퍼텍스트 링크(HTML)가 사용됩니다.

1.5 발행

CPS의 발행 형식은 다음과 같습니다.

(i) CrossCert 저장소(https://www.crosscert.com)와 ftp://ftp.crosscert.com/repository/CPS에서 보거나 다운받을 수 있는 파일 형식

(ii) CPS-requests@crosscert.com에서 전자 우편을 통해 발행되는 전자 문서

(iii) 우편 번호 137-725 서울시 서초구 서초동 1674-4 하림 빌딩 9층 한국전자인증(주)에서 받아볼 수 있는 문서 형식

• 참조된 각 CrossCert의 인터넷 URL은 Secure Sockets Layer(SSL) 보안 프로토콜을 사용하여 HTTP를 호출함으로써 "보안 모드"로 레코드를 검색할 수 있도록 고안된 것입니다 (SSL 지원 브라우저를 사용하는 경우).*https://*를 *http://*로 변경하면 "비보안 모드"에서도 이러한 레코드를 사용할 수 있습니다. CrossCert 저장소에 들어 있는 웹 기반 문서의 공식 버전에 액세스할 때는 반드시 보안 모드를 사용해야 합니다.

• 웹 기반 CPS 버전의 무결성을 보장할 수 있도록 S/MIME으로 디지털 서명한 복사본을 CrossCert 저장소에서 다운로드 받을 수 있습니다.

• 이 CPS에서 언급된 일부 URL은 실제 메시지가 아닌 해당 디렉토리를 나타냅니다. 이렇게 함으로써 메시지를 다양한 형식으로 유지하여 독자의 편의를 도모할 수 있습니다. 전자우편으로 customer-service@crosscert.com에 요청할 경우 이 CPS의 CrossCert URL이 참조하는 대부분의 정보를 파일 또는 문서 형식으로 받아 보실 수 있습니다.

1.6 고객 서비스 지원, 교육 및 훈련

이 CPS는 독자가 일반적으로 디지털 서명, PKI, CrossCert PCS에 익숙하다고 가정합니다. 따라서 익숙하지 않다면 인증서를 적용하기 전에 공용 키 사용에 필요한 교육을 받는 것이 좋습니다. 교육 및 훈련 정보는 CrossCert 웹 페이지(https://www.crosscert.com 및 https://digitalid.crosscert.com)에서 확인할 수 있습니다. 자세한 내용은 CrossCert 고객 서비스 담당자(customer-service@crosscert.com)에게 문의하십시오.

모든 PCS 신청자 및 가입자는 (i) 인증서를 신청하기 전에 공용 키 사용법에 대한 적절한 훈련을 받도록 권고받았으며, (ii) CrossCert로부터 디지털 서명, 인증서, PKI, PCS에 대한 설명서, 훈련, 교육을 받을 수 있음을 인지합니다.

1.7 머리글자 및 약어 일람표

CA	인증 기관(certification authority)
CK	공통 키
CPS	CrossCert 인증 업무 준칙(Certification Practice Statement)
CRL	인증 취소 목록(certificate revocation list)
CSR	인증서 서명 요청(certificate signing request)
DAM	ISO 표준 수정 초안(draft amendment)
FIPS	연방 정보 처리 표준(Federal Information Processing Standard)
FTP	파일 전송 프로토콜(File Transfer Protocol)
GMT	그리니치 표준 시간(Greenwich Mean Time)
HTTP	하이퍼텍스트 전송 프로토콜(Hypertext Transfer Protocol)
HTTPS	SSL을 사용한 하이퍼텍스트 전송 프로토콜(Hypertext Transfer Protocol with SSL)
IA	발행 기관(issuing authority)
LRA	지역 등록 기관(local registration authority)
LRAA	지역 등록 기관 관리자(local registration authority administrator)
NSI	미확인 가입자 정보(nonverified subscriber information)
PCA	VeriSign 주요 공식 인증 기관(public primary certification authority)
PCS	CrossCert 공용 인증 서버스(public certification services)
PIN	개인 식별 번호(personal identification number)
PKCS	공용 키 암호화 표준(Public Key Cryptography Standards)
PKI	공용 키 하부 구조(public key infrastructure)
RDN	상대적 식별명(Relative Distinguished Name)
RSA	암호화 시스템(cryptographic system(용어 정의 참조))
SET	보안 전자 거래(Secure Electronic Transaction)
S/MIME	보안 다목적 인터넷 메일 확장(Secure Multipurpose Internet Mail Extensions)
SSL	보안 소켓 레이어(Secure Sockets Layer)
URL	웹 주소(uniform resource locator)
VR	VeriSign 루트
CSP	CrossCert 보안 절차(CrossCert Security Procedures)
WWW 또는 Web	월드 와이드 웹(World Wide Web)
X.509	인증서 및 해당 인증 프레임워크에 대한 ITU-T 표준

표 1 – 머리글자 및 약어 일람표

2. CROSSCERT 인증 하부 구조

이 단원에서는 CrossCert 공용 인증 서비스뿐 아니라 인증 클래스, 인증서 확장, 타임 스탬프 기능 및 CrossCert 저장소의 기초가 되는 구조에 대해 설명합니다.

2.1 인증 하부 구조

CrossCert의 공용 인증 서비스(PCS)는 안전한 전자 상거래와 기타 일반적인 보안 서비스를 지원하여 전자 서명과 기타 네트워크 보안 서비스에 대한 사용자의 기술적, 사업적, 개인적 요구에 부응하도록 설계되었습니다. 이를 위해 CrossCert가 권한을 부여한 발행 기관(IA – 정의 *참조*)은 신임된 제3자로서 업무 준칙에 따라 인증서를 발행하고 관리하며 효력을 정지하거나 취소하는 작업을 수행합니다.

CrossCert PCS의 관리 기능은 통신 및 정보 보안에 대한 다양한 요구를 가진 광범위하게 분포되어 있는 매우 큰 사용자 커뮤니티에 적용할 수 있도록 설계되었습니다. CrossCert 서비스가 충분히 일관된 것임을 사용자가 확인할 수 있도록, CrossCert PCS의 무결성 보호에 사용되는 관리 업무에 대한 일반 준칙이 CPS에 수록되어 있습니다. 이와 같은 CrossCert PCS는 광범위한 지역에 분포된 큰 커뮤니티에 적용되어 사용자의 서비스 신뢰도를 높이는 기능을 합니다. *PCS 시스템 구현에 대한 다양한 논리적 실체는 CPS § 2.5에 설명되어 있습니다.*

이 CPS에 의한 CrossCert나 IA의 인증서 발행은 CrossCert와 기타 CrossCert IA 또는 CrossCert가 인증하는 IA에 의해 발행된 인증서와 기능적으로 동일하며 상호 사용이 가능합니다. CrossCert는 이 CPS에 설명된 서비스를 제공하는 데 있어 CrossCert와 Verisign Trust Network 마크를 사용할 수 있도록 허가합니다.

2.1.1 인증서 발행 및 관리 개요

IA는 권한을 부여받은 제3자로서 공용 키와 명명된 실체("명명" 정의 *참조*) 간의 관계를 확인하는 기능을 합니다. 이러한 확인은 IA가 전자 서명을 첨부하여 발행하는 인증서에 명시적으로 표시됩니다(CPS § 2.5 *참조*).이 인증 프로세스의 상위 수준 관리에는 등록, 명명, 적절한 인증서의 신청, 발행, 취소, 효력 정지, 감사 등이 포함됩니다. 명명은 주로 CrossCert나 기타 당사자가 수행합니다. 등록자 명명에는 인증 효력이 발생되어 유효하게 사용되는 시점을 결정하는, 인증서 관리에 사용되는 프로세스와는 다른 별도의 등록 프로세스가 포함됩니다.

CrossCert는 현재 세 가지 수준의 공용 인증 서비스를 제공하고 있습니다. 각 인증 수준이나 클래스별로 각기 다른 기능과 보안 기능을 제공합니다. 인증 신청자는 자신의 필요에 따라 이 세 수준 중 알맞은 서비스 품질을 선택합니다. 즉, 신청자가 원하는 인증 클래스를 지정해야 합니다. 원하는 인증 클래스에 따라 인증 신청자는 전자 우편 및 서면으로 IA에 신청하거나 지역 등록 기관(LRA)을 직접 방문하여 신청합니다. IA에서 발행하는 각 인증서는 특정 PCS 신임 수준을 갖습니다. 지정된 신임 수준에 대해 인증서를 발행하는 IA는 여러 곳이며, 이러한 IA의 종류는 각 커뮤니티에 맞는 부가 가치 서비스 및 수행 업무에 따라 달라집니다.

인증서를 신청하면 인증서가 인증 신청자에게 발행되거나 인증서 내용 초안이 인증 신청자에게 전송됩니다. 인증 신청자는 인증서나 초안을 검토하여 사용 목적에 적절한지 확인한 다음 만족

스러우면 인증 등록 프로세스에 따라 인증을 승인합니다. 새 등록자는 이 CPS에 나오는 의무 사항을 준수할 것에 동의합니다.

인증서 관리에는 인증 취소와 효력 정지 프로세스를 통한 인증 무효화 및 해당 개인 키 철회가 포함됩니다. 그 외에도 IA 서비스에는 특정 용도에 따른 인증서 목록의 표시, 배포, 발행, 저장 및 검색이 포함됩니다.

2.1.2 보안 서비스

CrossCert의 공용 인증 서비스는 통신 및 정보 자산을 보호하기 위한 다양한 보안 메커니즘을 지원합니다. 그러나 인증서만으로 그러한 메커니즘이 완성되는 것은 아닙니다. CrossCert PCS는 기타 통신 당사자들이 사용할 보안 서비스 프레임워크를 제공하는 것입니다. 이 프레임워크는 전자 서명과 그 서명의 검증을 통해 공개 데이터 네트워크 상에서 이루어지는 통신 및 컴퓨터 기반 상거래를 보호하고, 보안 서비스가 원래 의도한 대로 기능하는 지를 확인하는 수단을 제공합니다.

인증서 기반 보안 서비스는 사용자 정의 환경에서 보안을 위협하는 문제를 해결하는 데 사용됩니다. 사용자는 예상 위험 수준에 맞는 보안 메커니즘, 보안 기술, 보안 서비스 계약 및 PCS를 선택하여 자신의 통신 환경을 보호합니다.

CrossCert PCS는 현재 모든 인증서 관련 용도에 RSA 공용 키 시스템을 사용하고 있습니다. 그러나 대체 시스템을 요구하는 시장 수요에 따라 CrossCert에서는 이외의 전자 서명 표준을 지원하는 데 전념할 것입니다.

2.1.3 PCS 도메인 관리

CrossCert PCS 관리는 CrossCert 이외의 당사자도 특정 PCS 작업을 수행할 수 있는 방법으로 이루어 집니다. 서비스가 기능적인 면과 물리적인 면으로 분산되어 제공됨에도 불구하고 서비스 품질은 일정하게 유지됩니다. 도메인 관리의 기본 원칙은 철저한 권한 위임에 있으며,CrossCert는 이를 위해 특정 업무에 대한 감사 가능한 분산된 IA 계약에 의존합니다.

각 IA는 규정된 방법에 따라 특정 PCS를 수행하기 위한 상위 IA의 승인을 받습니다. 그러한 책임을 다른 측에 위임하지 않는 경우 각 IA는 LRA의 역할을 수행합니다. 이러한 기능 중 일부는 IA 생성과 관련된 것인 반면, 나머지 기능들은 상위 IA가 승인을 하고 난 다음 하위 IA가 수행하는 승인된 절차의 실행과 관련된 것들입니다. 상위 IA는 PCS의 일관성 강화를 위해 특정 임무를 다른 측에 위임합니다. CrossCert의 관리 정책은 독립적인 당사자들이 CrossCert PCS의 일관성을 유지하는 방법으로 인증서 발행 및 관리 절차를 실행하도록 합니다.

2.2 인증 클래스

CrossCert PCS는 현재 세가지 인증 클래스를 지원하고 있으며, 각 클래스는 지정된 신임 수준을 제공합니다. 다음 세부 절에서는 각 인증 클래스에 대해 설명합니다. 표 2(신임에 영향을 주는 인증 속성)에 자세한 정보가 나와 있습니다.

각 인증 클래스에 대한 설명(아래 표 2의 설명 포함)은 사용자가 구현하였거나 구현 중인 응용 프로그램 및 통신 시스템을 반영합니다. 이것은 CROSSCERT나 IA가 모든 용도에 대해 그러한 응용 프로그램이나 통신 시스템을 보증하거나 권장한다는 것을 의미하는 것이 아니므로 이를 절

대적으로 신뢰해서는 안됩니다. 사용자는 어떠한 목적으로든 각 인증 클래스의 적합성을 개인적으로 평가하고 결정해야 합니다.

2.2.1 클래스 1 인증서

설명: 클래스 1 인증서는 개인에게만 발행됩니다. 클래스 1 인증서는 사용자 이름(또는 별칭)과 전자 우편 주소가 CrossCert 저장소에 저장되어 있는 명백한 주체 이름을 구성한다는 것을 확인합니다. 클래스 1 인증서는 등록자에게 전자 우편으로 전송되어 등록자의 사용 가능한 인증서 세트에 추가됩니다. 일반적으로 이 인증서는 주로 웹 브라우징과 개인 전자 우편에 사용되어 이러한 환경의 보안을 개선합니다. 또한 다음 통신 작업 수행자가 동일한 사용자라는 것을 확인함으로써 통신 절차의 연속성을 구축하는 데도 사용됩니다. 클래스 1 인증서는 신청자가 선택적으로 인증 신청서에 지정된 "등록 필드 정보"(국가, 우편 번호, 나이, 성별)를 등록 과정에서 입력하여 전송함으로써 제 3의 서비스 제공자가 등록자의 인증서를 통해 그러한 정보를 사용할 수 있게 하여 제 3의 서비스 제공자(웹 사이트 호스트)가 특별한 혜택을 제공할 수 있게 합니다.

보증 수준: 클래스 1 인증서는 등록자의 확실성의 보증을 돕지 않습니다. 대신, CrossCert 저장소에 있는 주체 이름이 모호하지 않은지 간단히 검사하고 전자 우편 주소에 대한 제한적인 검증을 실시합니다. 클래스 1 인증서에 포함된 등록자의 공통 이름(및 전송된 등록 필드 정보)은 미확인 등록자 정보(NSI)로 간주됩니다. 이 인증서는 모든 CROSSCERT 인증서 중 최저 수준의 보증을 제공합니다. 신원 확인이 필요한 사업용으로 설계된 것이 아니므로 그러한 용도로 이 인증서를 신뢰해서는 안됩니다.

2.2.2 클래스 2 인증서

설명:클래스 2 인증서는 현재 개인에게만 발행되고 있습니다. 클래스 2 인증서는 등록자가 제공하는 신청 정보가 널리 인정받은 소비자 데이터베이스의 정보와 상충하지 않는지 확인합니다. 일반적으로 클래스 2 인증서는 조직 내 전자 우편과 조직 간 전자 우편, "위험도가 낮은" 소규모 거래, 개인 전자 우편, 암호 교체, 소프트웨어 유효성 확인, 온라인 가입 서비스 등에 주로 사용됩니다. CrossCert는 또한 소프트웨어 유효성 확인이나 개체 서명과 같은 다른 기능을 지원하기 위해 특화된 클래스 2 인증서를 제공합니다. 클래스 2 인증서는 인증 신청자가 등록 과정에서 선택적으로 인증 신청서에 지정된 등록 필드 정보를 입력하여 전송함으로써 제 3의 서비스 제공자가 등록자의 인증서를 통해 그러한 정보를 사용할 수 있게 되는 경우, 이 제 3의 서비스 제공자(예: 웹 사이트 호스트)가 특별한 혜택을 제공할 수 있게 합니다.

클래스 2 등록자 계약서가 온라인으로 CrossCert 클래스 2 지역 등록 기관(LRA)에 전송되면 관련 인증 신청자 등록 데이터는 제3자 데이터베이스와의 비교를 통해 확인됩니다. LRA는 그러한 확인 결과를 기반으로 신청을 승인하거나 거부합니다(CPS § 5 – 인증 신청서 유효성 확인 *참조*).신청이 승인되면 IA는 CrossCert 조직이 아닌 LRA에 발행된 인증서를 제외한 모든 인증 신청서의 우편 주소를 확인합니다(CPS § 5.1.4 *참조*).

보증 수준: 클래스 2 인증서는 인증 신청서에 입력된 신청자의 이름, 주소 및 기타 개인 정보를 널리 참고되는 데이터베이스와 비교하는 자동화된 온라인 프로세스를 바탕으로 등록자의 신원을 합리적으로 보증하지만 절대적이지는 않습니다. 확인은 제 3의 데이터베이스를 신청서의 정보와 비교하는 CrossCert의 고유 기준을 기반으로 합니다.

CROSSCERT의 클래스 2 온라인 신원 확인 프로세스는 인증 신청자의 신원을 확인하는 자동적 방법이기는 하지만 신청자가 지역 등록 기관이나 공증인 등의 신임 당사자 앞에 직접 출석할 필요는 없습니다. 결국, 클래스 2 인증서의 취득과 사용, 신뢰 여부를 결정하기 위해서는 상대적인 장점과 제한 사항을 고려하고 그에 따라 인증서를 사용해야 합니다. 이 온라인 인증 프로세스에 대한 자세한 정보는 CROSSCERT 저장소(https://www.crosscert.com)에서 찾아볼 수 있습니다.

등록 시 클래스 2 인증서에 포함된 등록 필드 정보는 NSI로 간주됩니다.

2.2.3 클래스 3 인증서

설명: 클래스 3 인증서는 개인 및 조직에 발행됩니다.

• **개인** – 클래스 3 인증서는 등록자와 클래스 3 LRA 또는 공증인과 같은 대리인의 실제 출석을 통해 개별 등록자의 신원을 정확하게 확인하여 보증합니다. 기타 클래스 3 개인 인증서로는 "클래스 3 LRAA 인증서"가 있습니다. 이 인증서는 인증된 LRAA 용으로만 발행되며 CrossCert 조직이 아닌 LRA에 소속된 승인된 LRA 관리자(LRAA)에게만 발행됩니다. LRAA는 (인증된 레코드를 통해) 해당 LRA로부터 권한을 위임받아야 LRAA 인증서를 승인할 수 있습니다. 클래스 3 LRAA 인증서에 포함된 공용 키와 쌍을 이루는 개인 키는 하드웨어 기반 암호화 모듈의 요구 사항과 같은 해당 요구 사항에 따라 신뢰할 수 있는 방법으로 작성되어 저장되어야 합니다.

• **조직** – 클래스 3 인증서는 정부 기관이나 기업과 같은 다양한 공조직과 사조직의 존재 및 이름에 대한 보증을 제공할 수 있습니다. 조직에 대한 클래스 3 인증 신청서의 유효성 확인에는 해당 클래스 3 IA가 신청자나 제 3의 기업 데이터베이스 및 조직에 대한 별도의 콜백("오프라인" 통신)으로 얻는 인증서 레코드 검토가 포함됩니다. CrossCert 고객들은 주로 전자 뱅킹, 전자 데이터 교환(EDI), 회원제 온라인 서비스와 같은 전자 상거래 응용 프로그램에 클래스 3 인증서를 사용합니다. 이 외에도 CrossCert는 소프트웨어 유효성 확인을 지원하기 위한 특화된 클래스 3 상업용 소프트웨어 발표자 인증서를 제공합니다. CrossCert는 또한 서버에 강력한 암호화 세션을 제공하는 Global Sever 인증서를 제공합니다 (https://www.crosscert.com/repository/export_faq의 Global Sever 인증서 FAQ *참조*).

보증 수준: 클래스 3 인증 프로세스는 다양한 절차를 통해 개별 등록자의 신원을 확인합니다. 이러한 타당성 검사 절차를 통해 클래스 2 인증보다 더 확실하게 신청자의 신원을 보증합니다. 클래스 3 인증서의 실질적인 사용과 신뢰도는 법률로 승인된 기존의 주요 인증 프로세스인 공증의 적용을 통해 한층 강화됩니다. 사업자용 클래스 3 인증서는 지정 요건에 따라 사업체와 "오프라인"으로 통신하고 제3자를 통해 사업자 정보를 확인하여 보증의 신뢰도를 높입니다.

2.2.4 테스트 인증서

테스트 인증서는 CrossCert에서 인증한 테스트 용도로만 발행합니다. 테스트 인증서는 PCS와 상관없이 CrossCert Test CA CPS의 적용을 받는 CrossCert Test CA에서 발행하며 https://www.crosscert.com/repository/test_ca_cps.html*을 참조하십시오*. 승인받은 사람만 테스트 인증서를 사용할 수 있습니다. ***참고:*** **테스트 인증서에 들어 있는 정보는 NSI로 간주됩니다.**

2.3 인증서 클래스 속성

표 2는 각 인증 클래스의 속성을 나타낸 것입니다. 각 제목 아래에 세부 내용이 설명되어 있습니다.

	신원 확인 요약	IA 개인 키 보호	인증 신청자와 등록자 개인 키 보호	사용자가 구현하거나 계획하는 응용 프로그램 사용자
클래스 1	이름과 전자 우편 주소 자동 검색	PCA:신뢰할 수 있는 하드웨어; CA: 신뢰할 수 있는 소프트웨어 또는 신뢰할 수 있는 하드웨어	암호화 소프트웨어(PIN 보호 설정) 권장 사항. 필수는 아님	웹 브라우징 & 전자 우편 사용
클래스 2	클래스 1과 동일한 확인 작업 외 등록 정보 및 주소 자동 확인	PCA & CA: 신뢰할 수 있는 하드웨어	암호화 소프트웨어(PIN 보호 설정) 필수	개인 및 회사 내, 회사 간 전자 우편, 온라인 가입, 암호 교체, 소프트웨어 유효성 확인
클래스 3	클래스 1과 동일한 확인 작업 외 직접 출석, ID 문서 및 개인에 대한 클래스 2 자동 ID 확인, 조직에 대한 사업 레코드(또는 파일링) 확인	PCA & CA: 신뢰할 수 있는 하드웨어	암호화 소프트웨어(PIN 보호 설정) 필수; 하드웨어 토큰 권장. 필수는 아님	전자 뱅킹, 기업 데이터베이스 액세스, 개인 뱅킹, 회원제 온라인 서비스, 내용 무결성 서비스, 전자 상거래 서버, 소프트웨어 유효성 확인; LRAA 인증서; 특정 서버의 강력한 암호화

표 2 – 신임에 영향을 주는 인증서 속성

각 인증 클래스는 다음과 같은 속성의 수준에 따라 특성이 구분됩니다. 속성에는 신원 확인(예: 직접 출석 또는 조사를 통한 확인), IA 개인 키 보호(및 용도에 맞는 보증), 인증 신청자와 등록자의 개인 키 보호 및 작동 제어 등이 있습니다. 인증서 및 CrossCert 지원 제품과 서비스에는 이 외에도 여러 가지 속성이 있지만 표 2에 표시된 속성이 상대적 신임에 영향을 미치는 몇 가지 면을 구별하는 기본이 됩니다. 다음은 각 속성에 대한 설명입니다.

2.3.1 가입자 신원 확인

인증서 신청 처리 과정에서 IA가 신청자의 신원을 확인하고 신청자가 제공한 정보를 확인하기 위해 수행하는 여러 가지 작업을 가리킵니다. 확인 유형과 범위, 정도는 인증 클래스, 신청자 유형 및 기타 요건에 따라 달라집니다. 확인 방법 및 그 방법이 얼마나 엄격히 적용되는 가는

인증 클래스에 따라 결정됩니다. 확인 방법은 CPS § 5에 자세히 설명되어 있습니다.

2.3.2 IA 개인 키 보호

각 IA의 개인 키는 신뢰할 수 있는 하드웨어 제품을 통해 보호됩니다. 그러나 클래스 1 IA(그림 4 *참조*)는 암호화 소프트웨어만을 사용하여 개인 키를 보호합니다. CPS § 4.1(키 생성 및 보호)를 *참조하십시오*..

2.3.3 인증 가입자 및 신청자 개인 키 보호

인증 가입자 및 신청자의 개인 키는 본 CPS에서 지정한 암호화 소프트웨어나 하드웨어 토큰(예: 스마트 카드나 PC 카드)을 사용하여 보호해야 합니다. CPS § 4.1(키 생성 및 보호)과 **https://www.crosscert.com/repository/PrivateKey_FAQ**의 키 보호 FAQ를 *참조하십시오*.

CrossCert는 새 PCS 사용 패턴을 연구하고 있으며, 따라서 그러한 패턴에 적절한 특정 하부 구조 제공을 고려할 것입니다.

발행 기관은 인증 신청자나 등록자의 개인 키를 생성하거나 저장하지 않습니다. 또한 발행 기관은 인증 신청자나 등록자의 특정 개인 키 보호 요구 사항을 확인하거나 적용할 수 없습니다.

2.3.4 운영 제어

운여 제어는 조직의 인적 자원 및 각 인증 클래스를 위해 구현되는 기타 관리 지향 제어를 가리킵니다. 각 제어에는 인증을 얻을 수 있는 사용자 제한, IA 직원의 훈련 및 교육에 관련된 요구 사항, IA 내 업무 분담 정책, 문서 요구 사항 및 규정된 절차와 감사 등이 포함됩니다. 이 중 다수가 CPS § 3(인증 작업의 기초)에 설명되어 있습니다.

2.4 확장 및 확장 명명

2.4.1 확장 메커니즘과 인증 프레임워크

PCS는 X.509 v1, v2 및 v3 인증서를 사용합니다. X.509 v3 인증서는 v1과 v2의 기능을 확장한 것으로 인증서 확장을 추가하는 기능을 포함합니다. CrossCert PCS의 표준 구성 요소인 이 기능은 표준 인증서 서비스 모델을 확장합니다.

2.4.2 표준 및 서비스 정의 확장

X.509 “Amendment 1 to ISO/IEC 9594-8:1995”에서는 여러 확장 필드를 정의합니다. 이러한 확장 필드는 규모가 큰 다용도 인증서에 유용한 여러 가지 관리 제어 기능을 제공합니다. CrossCert PCS는 X.509의 목적에 맞게 이 여러 제어 기능을 사용합니다. (참고:X.509 규격 사용자 소프트웨어는 이 CPS의 유효성 확인 요구 사항에 따르는 것으로 가정합니다. 그러나 IA와 CrossCert가 그러한 소프트웨어가 이 제어 기능들을 지원하고 실행할 것이라고 보증하는 것은 아닙니다.)

이 외에도 이 CPS는 사용자가 자신의 응용 프로그램 환경에 특정한 사용 목적이나 모드를 위한 추가 "개인" 확장 필드를 정의하도록 허용합니다. 서비스 지향 확장 필드에 대한 정의와 인증서 신청, 승인, 발행 중 그러한 정보를 처리하는 방법이 VSP 및 관련 후원 조직에서 공개적으로 제공하는 문서에 명시되어 있습니다. 서비스에 특정한 목적을 위해 PCS 내에 구현되는

개인 확장 필드의 예에는 Microsoft Windows 소프트웨어의 일부 버전에 적용된 소프트웨어 유효성 확인 스킴과 Netscape Communications사의 SSL 보안 기술 스킴이 있습니다. http://microsoft.com/security와 http://home.netscape.com/newsref/ref/netscape-security.html을 *참조하십시오*.

2.4.3 특정 확장의 확인 및 임계값

각 확장의 기능은 표준 OBJECT IDENTIFIER 값(X.509 정의 *참조*)으로 표시됩니다. 이 외에도 인증서의 각 확장에는 "임계" true/false 값이 지정됩니다. 이 값은 IA에서 지정하며 인증 신청자가 인증 신청서에 입력한 정보에 기반할 수 있습니다. 이 값은 확장 정의를 담당하는 조직이 정한 제한 사항을 지켜야 합니다.

특정 확장에 임계값 *true*가 지정되면, 인증서를 확인하는 모든 사람들은 임계값이 *true*인 특정 확장의 목적과 처리 요구 사항에 대해 확실히 알지 못하는 경우 인증서를 유효하지 않은 것으로 처리해야 합니다. 그러한 확장의 임계값이 *false*이면, 유효성 확인 시 모든 사람이 해당 정의에 따라 확장을 처리하거나 또는 확장을 무시합니다.

2.4.4 인증 체인과 IA 유형

CrossCert의 PCS는 인증 체인을 사용합니다. CrossCert 인증 체인의 각 IA는 CrossCert PKI에 지정된 역할(CPS § 2.5 *참조*)에 따라 특정 절차를 수행합니다. 일반적인 IA 역할에는 루트 등록 기관, 다른 IA의 IA, 등록자의 IA 등 세 가지가 있습니다. IA는 다른 IA의 등록자이어야 합니다. IA가 자신의 루트이면 셀프사인된 공용 키는 X.509 v1 형식을 따릅니다. 이것은 전자 서명 검증 중 추가로 유효성을 확인하지 않고(오프라인 인증 메커니즘에 기반하여) 신임될 수 있습니다(CPS § 8 – 인증서 사용 *참조*).그러나 루트 등록 기관에 *등록되면* IA의 인증서는 확장을 포함할 것입니다.

2.4.5 최종 사용자 인증서 확장

최종 사용자를 위한 IA는 X.509 Amendment 1 to ISO/IEC 9594-8:1995뿐 아니라 Microsoft 및 Netscape와 같은 후원 조직에서 정의한 확장 필드가 포함된 인증서를 발행합니다(CPS § 2.4.2 *참조*).CrossCert PCS에 사용되는 ISO 정의 확장 필드는 현재 다음과 같은 확장에 제한됩니다.

- 기본 제한 사항
- 키 사용
- 인증 정책

간단히 말해 이러한 확장을 사용하여 인증서 발행 및 유효성 확인 프로세스를 제어합니다. 표 3은 특정 인증서에 포함되는 확장을 설명합니다.

2.4.6 ISO 정의 기본 제한 확장

기본 제한 사항 확장은 IA 또는 최종 사용자 인증서가 수행하는 역할의 범위를 정하고 인증 체인에서 그 위치를 지정합니다. 예를 들어, CA와 하위 CA에 발행된 인증서에는 그것을 IA 인증서로 식별하는 기본 제한 사항 확장이 포함됩니다. 최종 사용자 인증서에는 IA 인증서가 될 수 없도록 제한하는 확장이 포함됩니다.

2.4.7 ISO 정의 키 사용 확장

키 사용 확장은 유효한 인증서에 첨부된 공용 키가 CrossCert PCS 내에서 특정 용도로만 사용될 수 있도록 기술적 목적을 제한합니다. IA 인증서에는 인증서, 인증 취소 목록 및 기타 데이터에 서명하는 것으로 제한되는 키 사용 확장이 포함될 수 있습니다.

2.4.8 ISO 정의 인증 정책 확장

인증 정책 확장은 신뢰하는 당사자가 요구하는(또는 신뢰하는 당사자에 지정된) 방법으로 인증을 구현하도록 제한합니다. PCS에서 구현되는 인증 정책 확장은 사용자가 이 CPS에 따르도록 하고 인증서를 적절하게 사용하도록 제한합니다(CPS – 2.4.9.1 *참조*).

2.4.9 확장 명명과 CrossCert 확장

특정 S/MIME v1 인증서를 제외한 모든 최종 사용자 인증서에는 X.520 속성인 “Organizational Unit” 필드가 포함되어 있습니다. 여기에는 책임에 관련된 간략한 스테이트먼트가 포함되어 있으며 참조에 의해 “OU=www.crosscert.com/rpc(c)99“와 같은 전체 CPS를 포함합니다(이것은 CPS의 기본 URL를 참조하며, 책임이 제한되어 있음을 고지하고 저작권 표시를 포함합니다).이 정보나 이에 상응하는 정보는 "로컬"(CrossCert 이외의 업체에서 제어하는) 방식으로 사용자에게 보여주기 위해 응용 프로그램에 정의된 X.509 v3 확장에 표시될 수 있습니다. 참고:X.509가 64바이트로 제한되기 때문에 이 Organizational Unit 필드의 내용은 단축형으로 표시됩니다. X.509 v3 확장이 실제로 널리 사용되게 되면 이 Organizational Unit 필드는 사용하지 않게 될 것입니다.

전자 서명 검증 소프트웨어나 하드웨어(통틀어 “검증 소프트웨어”)가 v3 인증서 확장을 받아들여 사용하면 검증 소프트웨어는 CPS의 참조와 그 중요한 부분을 기술하는 확장 집합을 모두 표시할 것입니다. 검증 소프트웨어가 제한되거나 개인적으로 정의된 v3 확장만을 지원하면, 검증 소프트웨어는 그러한 응용 프로그램에 특정한 확장을 이용하여 필요에 따라 해당되는 중요한 수행 명세서 부분을 표시합니다.

그림 3은 CrossCert가 v3 인증서 내에 이러한 방식을 구현하는 방법을 보여줍니다. 그림의 주요 요소는 아래에 설명되어 있습니다.

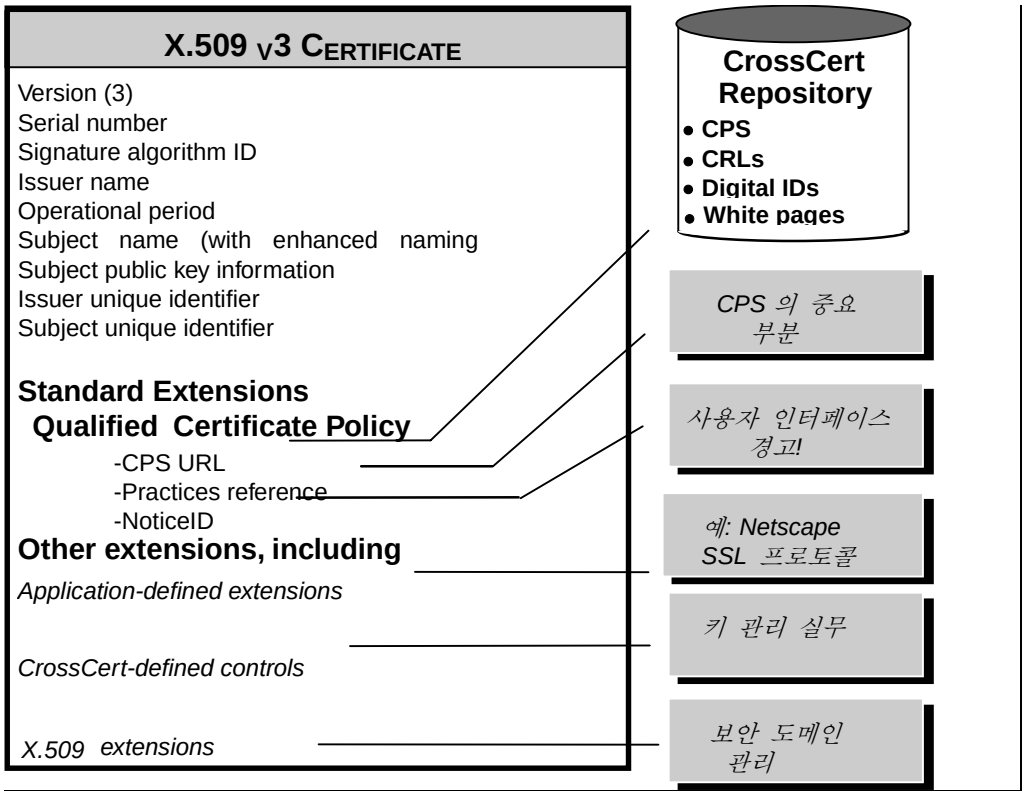

그림 3 – 참조에 포함되는 인증서와 정보

2.4.9.1 참조에 의한 통합

확장과 향상된 명명은 인증서 내에 모두 표시될 수도 있고, 최소한 부분적으로만 인증서 내에 표시되고 나머지는 참조에 의해 인증서에 포함되는 외부 문서에 표시될 수 있습니다(**참조에 의한 포함** 정의 *참조*).

향상된 Organizational Unit 필드에 포함된 정보도 인증서에 표시될 때 certificatePolicy 확장으로 나타날 수 있습니다. 이 CPS는 X.509 Amendment 1 to ISO/IEC 9594-8:1995에 정의된 대로 "인증 정책"을 구성합니다. 정책 정의 기관의 역할을 수행하는 CrossCert는 CPS에 certificatePolicy 확장에 표시될 개체 식별자 값을 지정했습니다. 이 "인증 정책" 정의에서는 표 3과 아래에 설명되어 있는 대로 포인터 값, 경고, 책임 제한, 보증 배제 등이 포함되도록 CrossCert가 정의한 정책 한정자를 사용해야 합니다.

2.4.9.2 CPS에 대한 포인터

컴퓨터 기반 포인터(URL 또는 다른 식별자와 메커니즘 사용)와 영어(해독 가능한) 텍스트 또는 포인터가 모두 사용되므로 인증서 사용자는 쉽게 CPS나 기타 관련 정보를 찾아 액세스할 수 있습니다.

2.4.9.3 경고, 책임 한계, 보증 배제

각 인증서는 CPS에 있는 경고, 제한, 배제 등의 전체 텍스트를 가리키는 포인터를 사용하여 책임 한계와 보증 배제를 명시하는 간략한 스테이트먼트를 포함합니다. 선택적으로 그러한 정보는 인증서에 직접 포함되지 않아도 인증서 보기 기능을 사용하여 사용자나 에이전트가 액세스할 수 있는 메시지로 연결되는 하이퍼텍스트 링크를 따라가 표시할 수 있습니다.

사용자가 볼 수 있도록 정보를 교환하는 방법은 다음과 같습니다. 향상된 명명 organizational unit 속성; CrossCert에서 등록한 인증 정책에 대한 CrossCert 표준 한정자(표준 v3 확장 사용); 다른 업체가 등록한 확장(예: Netscape가 등록한 "Comment" 확장).

"향상된" organizational unit 속성은 문자열 "OU=Terms of use at www.crosscert.com/rpc(a)99" 또는 이와 유사한 문자열을 포함합니다.

표 3은 인증서 확장의 일반적인 내용과 CrossCert CPS 인증 정책 식별자에 대해 정의된 한정자 유형을 설명합니다.

이름/인증서 확장 필드	목적과 설명:	첨부되는 영어(또는 기타 해독 가능한) 텍스트
CA 및 하위 CA에 대한 일반적인 확장: ---------- basicConstraints keyUsage 최종 사용자에 대한 일반적인 확장: ---------- basicConstraints certificatePolicy	 CPS § 2.4.6 *참조* CPS § 2.4.7 *참조* CPS § 2.4.6 *참조* CPS § 2.4.8 *참조*	 중요하지 않음 cA = TRUE 중요하지 않음 keyCertSign (Bit 5 set) cRLSign (Bit 6 set) 중요하지 않음 cA = FALSE 중요하지 않음 CPS § 2.4.9.3 *참조*
CrossCert 표준 식별자 -업무 Reference	CrossCert CPS, CRL 및 기타 정보가 저장되어 있는 CrossCert 저장소(그리고 이 CPS의 다음 버전에서 CrossCert 이외 조직의 저장소)를 참조하는 텍스트 포함	"이 인증서는 참조에 의해 포함되며 이 인증서의 사용은 CrossCert 저장소(https://www.crosscert.com)에서 제공하는 CrossCert 인증 수행 명세서(CPS)를 엄격히 따릅니다. https://www.crosscert.com; 전자우편 CPS-requests@crosscert.com; 또는 우편 번호 137-725 서울시 서초구서초동 1674-4 하림 빌딩 9층 한국전자인증(주) Copyright (c)1999 CrossCert, Inc. All Rights Reserved.일부 사항에 대한 보증 배제와 의무 제한
CrossCert 표준 식별자 -cpsURL	이 CPS의 원본을 가리키는 단일 URL	https://www.crosscert.com/repository/ CPS§ 또는 유사 URL

CrossCert 표준 식별자 -NoticeID	CrossCert PCS 인증서 사용에 관련된 경고, 주의, 보증 배제 및 책임 한계에 대한 정보가 들어 있는 등록된 문자열을 참조하는 개체 식별자.모든 인증서에서 사용자 에이전트(예: 컴퓨터 또는 터미널) 인증서 보기 기능 내에 표시되도록 설계되었으나 모든 인증서에 포함되지는 않습니다.	값 "**경고:이 인증서의 사용은 CrossCert 인증서 수행 명세서를 정확히 따라야 합니다. 발행 기관은 시장성이나 특정 목적에의 적합성을 포함하여 묵시적, 명시적 보증을 배제하며, 결과적 손해, 이에 관련된 손해 및 기타 손해에 대한 책임을 지지 않습니다. 자세한 내용은 CPS를 참조하십시오.**"의 등록된 문자열
CrossCert 표준 식별자 -NSINotice	IA가 정확성을 보증하지 않는 데이터가 인증서에 포함되어 있음을 나타내는 등록된 문자열을 참조하는 개체 식별자	값 **"CrossCert가 등록한 nonverifiedSubjectAttribute 확장값 내용은 IA에서 확인한 정보로 간주되지 않습니다. "**의 등록된 문자열

표 3 – CROSSCERT 인증서 확장

선택적으로 인증서는 사용자 고지 인증 정책 한정자에 특정 제품에서 표시하는 다음과 같은 텍스트에 대한 참조를 포함합니다.

> **이 인증서는 참조에 의해 CrossCert 인증 수행 명세서(CPS)를 포함합니다. 이 인증서의 사용은 CPS에 따릅니다.**
>
> **이 CPS는 CrossCert 저장소 (https://www.crosscert.com/repository/CPS 및** ftp://ftp.crosscert.com/repository/CPS), **전자 우편** CPS-requests@crosscert.com **또는 우편 번호 137-725 서울시 서초구 서초동1674-4 하림 빌딩 9층 한국전자인증(주)를 통해 사용할 수 있습니다.**
>
> **CPS는 결과적 손해와 이에 관련된 손해를 포함하여 특정 책임을 배제하고 제한합니다. 또한 CPS에는 이 인증서에 관련된 책임에 대한 부과금이 포함되어 있습니다. 자세한 내용은 CPS를 참조하십시오.**
>
> **CPS와 이 인증서에 대한 저작권 정보는 다음과 같습니다. Copyright (c) 1999 CrossCert, Inc. All Rights Reserved**

2.5 CrossCert PKI 계층 구조

CrossCert의 공용 인증 서비스는 다음과 같은 IA로 이루어진 PKI 실체 계층 구조 내에서 구현됩니다.

- VeriSign 루트(VR)
- 셋 이상의 CrossCert 공개 기본 인증 기관(PCA)
- 셋 이상의 CrossCert CA(각 CrossCert PCA 아래에 최소한 하나의 CA)
- CrossCert가 인증하는 기타 CA(하위 CA 포함) 또는 이 CPS에 따른 CrossCert PCS 내에서 작동하도록 인증된 IA

PKI 실체 계층 구조에서 IA는 한 IA가 다른 IA를 대신함을 나타내는 "종속하는 위치" 관계를 통해 상호 연결됩니다. IA는 계층 구조의 마지막 IA에서 발행한 최종 사용자 인증서의 인증 클래스에 따라 (IA 유효성 확인을 위한)일반적 또는 향상된 인증 절차를 사용하여 IA 인증서를 발행합니다.

또한 IA는 특정 등록 기능을 하나 또는 여러 LRA로 위임할 수 있습니다. CrossCert PKI는 또한 CrossCert 명명 기관 및 CrossCert 저장소를 포함합니다. 그림 4는 CrossCert PKI의 개요를 보여줍니다. 그림을 단순화하기 위해 그림 4에는 LRA를 표시하지 않았습니다.

참고: 그림 4에는 계층 구조 내 발행 기관 및 기타 실체가 모두 나타나지 않을 수 있습니다.

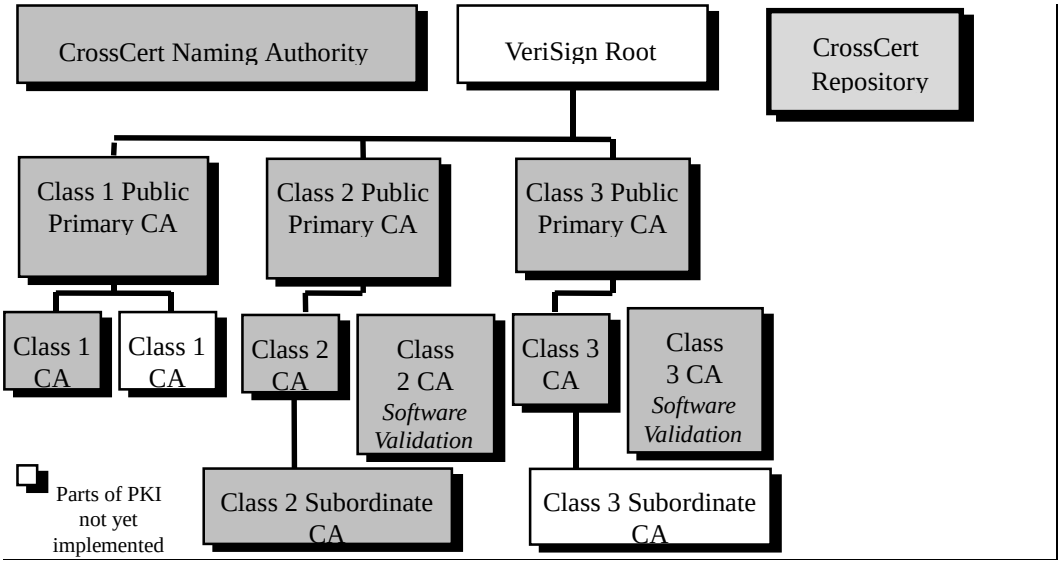

그림 4 – 간략화된 CROSSCERT PKI 계층 구조

2.5.1 VeriSign 루트

VeriSign 루트(VR)는 VeriSign이 소유하고 운영하는 실체로 PCA 공용 키 인증서를 발행합니다. VR은 PCA의 고유 이름을 승인합니다. 또한 VR은 CrossCert PCS 내 신임 구조의 최상단에 위치합니다. 각 PCA는 고유한 공용 키에 셀프사인하고 등록 중에 VR에 셀프사인한 공용 키를 전송합니다. 두 당사자 모두 *CrossCert 보안 정책*(CSP)에 지정되어 있는 해당 시점의 필요한 절차를 완료합니다.

VR의 초기 RSA 키 크기는 2048비트입니다. 신뢰할 수 있는 하드웨어 장치(FIPS 140-1 수준 3으로 보증하는 장치)가 VR의 개인 키를 생성하고 보호하고 파기하는 데 사용됩니다. VR 키 쌍은 교체될 수 있으며 대체 공용 키는 CrossCert 저장소에 발행됩니다. CrossCert 이외 조직의 직원들이 VR의 신뢰도와 보안 수준을 높이기 위해, 이 CPS에 설명되어 있는 비밀 공유 절차에 따라 VR 개인 키의 특정 공유 부분(CPS § 3.17 – 비밀 공유 *참조*)을 사용합니다.

2.5.2 1차 공용 인증 기관(PCA)

PCA는 CrossCert PCS 내에서 최상위 활성 인증 실체의 역할을 합니다. PCA는 CrossCert PCS 내 모든 CA의 인증서를 발행하거나 효력을 중지하거나 취소합니다. 모든 PCA는 CrossCert의 PKI 내에서 VR에 종속되어 있습니다. VeriSign이 각 PCA를 소유하고 운영합니다.

각 CA의 초기 키 크기는 1024비트입니다. 신뢰할 수 있는 하드웨어 장치(FIPS 140-1 수준 3으로 보증하는 장치)가 각 PCA의 개인 키를 생성하고, 보호하고, 파기하는 데 사용됩니다. 각 PCA의 목적, 보증, 서비스 및 책임뿐 아니라 인증 체인 내 인증 신청자, 등록자, 인증서 수신자, 신뢰하는 당사자, CA와 하위 CA 등의 권한과 책임이 이 CPS에 나와 있습니다.

CrossCert PCA와 CrossCert 이외 조직의 PKI 내 해당 실체 간 상호 인증은 다음과 같은 경우 허용됩니다. (i) CrossCert가 CrossCert 이외 조직의 실체가 최소한 유사한 보증 및 신뢰도의 기능과 수준을 제공함을 확인한 경우 (ii) 상호 인증서로 인해 CrossCert 등록자가 CrossCert의 인증에서 더 많은 혜택을 받을 수 있다고 기대되는 경우 (iii) 두 실체가 적절한 CrossCert 상호 인증 계약을 체결한 경우 (iv) CrossCert과 CrossCert 이외의 조직 실체가 상호 인증서를 발행한 경우 (v) 각 당사자가 그러한 인증을 받아들인 경우 (vi) 각 당사자가 취소 및 저장 절차에 동의한 경우

2.5.3 인증 기관(CA)

각 CA는 한 PCA에 종속되며 이 CPS 및 (이 CPS에 따르는)해당 PCA에 지정된 특정 제약 사항에 따라 운영됩니다. 1-클래스 3 CA는 이 CPS에서 허용하는 대로 최종 사용자 인증서를 발행, 관리, 취소할 수 있습니다. 2-클래스 3 CA는 또한 CrossCert 단독 재량으로 하위 CA에 IA 인증서를 발행할 수 있습니다. 하위 CA는 이 CPS에서 허용하는 대로 최종 사용자 인증서를 발행, 관리, 취소할 수 있습니다.

각 CA(및 하위 CA)의 초기 키 크기는 1024비트입니다. 신뢰할 수 있는 하드웨어 장치(FIPS 140-1 수준 3으로 보증하는 장치)가 클래스 2 및 클래스 3 CA의 개인 키를 생성하고, 보호하고, 파기하는 데 사용됩니다. CA와 하위 CA는 대개 CrossCert가 소유하고 운영하지만, CrossCert과 다른 실체가 동의한 경우 CrossCert는 CrossCert 이외 조직의 CA와 그 하위 CA(또는 CrossCert 이외 조직의 하위 CA 중 CrossCert CA에 종속하는 하위 CA)가 CrossCert의 PCS에 참여하도록 인증할 수 있습니다(CPS § 3.1 *참조*).

2.5.4 지역 등록 기관(LRA)과 LRA 관리자(LRAA)

지역 등록 기관(LRA)은 인증 신청을 평가하여 승인하거나 거부하는 실체입니다. LRA는 또한 인증 취소(또는 승인된 경우 효력 정지)를 승인할 수 있습니다. LRA는 LRA 작업을 담당할 LRA 관리자(LRAA)를 고용할 것입니다. LRA 단일 IA(실제로 인증서를 발행하는 VR, PCA 또는 CA)를 대신하거나 (CPS에서 허용하는 대로)단일 IA의 배타적 권한하에 있습니다. IA는 여러 LRA를 가질 수 있습니다.

다르게 권한을 제한하지 않는 경우 LRA는 다음에 의존하여 인증 신청자 정보를 확인할 수 있습니다. (i) 제대로 수행되는 것으로 보이는 공증 행위 (ii) 여권이나 운전 면허증과 같은 인증된 신원 확인 형식.해당 IA가 지정하는 경우 공증인은 LRAA의 역할을 수행할 수 있지만 그렇지 않으면 공증인은 대개 독립적 실체이며(인증 신청자에게 직접 서비스를 제공하므로 LRA의 에이전트가 아님) 인증 신청서의 유효성 확인 기능을 지원합니다.

CrossCert 이외 조직의 LRA은 CrossCert에 가입하지 않은 LRA 중 LRA 조직 내에 가입한 개인에 대한 인증서 발행과 취소를 승인하도록 인증된 LRA입니다. 예를 들어, 특정 회사는 그 회사의 직원과 기타 가입한 개인들에 대한 인증서의 발행을 승인하거나 거부하기 위해 CrossCert 이외 조직의 LRA이 될 수 있지만 일반 사용자에 대한 인증서 발행을 승인할 수는 없습니다.

CrossCert 이외 조직의 LRA에서 발행하는 인증서는 LRAA에서 인사부(HR) 직원 및 독립 계약자 명부와 같은 적절한 내부 문서를 통해 LRA 가입을 확인할 수 있는 개인에게만 발행될 수 있습니다. CrossCert 이외 조직의 LRA이 인증 신청서를 승인하여 발행되는 모든 인증서는 그 주체의 가입을 나타내는 고유 이름을 포함합니다. CrossCert 이외 조직의 LRA에서 인증 신청서의 승인이나 거부를 전적으로 책임집니다. 따라서 CrossCert과 IA는 그러한 책임을 배제합니다.

LRAA 요구 사항은 CPS § 3.20에 나와 있습니다.

2.5.5 명명 기관

CrossCert 명명 기관으로 불리는 명명 기관은 모든 CrossCert IA의 상대 고유 이름(RDN) 발행을 조정합니다. CrossCert 명명 기관은 또한 인증 클래스와 IA에 따라 달라질 수 있는 CrossCert 저장소 내 주체 이름의 명명 규약을 지정합니다. 이러한 명명 규약은 또한 발행 및 재발행/재등록 시 달라질 수 있습니다. CrossCert 이외 조직의 IA는 CrossCert 명명 기관을 사용하거나 또는 CrossCert 명명 기관의 절차와 충돌하지 않고 CrossCert 명명 기관을 사용하여 RDN을 등록하지 않는 절차를 수행하는 명명 기관을 만들거나 사용해야 합니다.

2.5.6 CrossCert 저장소

CrossCert 저장소는 인증서를 저장하고 검색하기 위한 데이터베이스와 인증서에 관련된 기타 정보로 이루어진 공개된 집합입니다. CrossCert PCS 목적에 상관없이 모든 IA는 CrossCert 저장소를 공식적인 기본 저장소로 사용해야 합니다. CrossCert 저장소에는인증서, CRL 및 기타 효력 정지와 취소 정보, CrossCert CPS의 현재 버전과 이전 버전, 때때로 CrossCert에서 지정하는 정보가 포함되며 이외에 다른 정보도 추가될 수 있습니다.

CrossCert 저장소는 IA에서 올바른 형식으로 받은 인증이나 인증서 효력 정지 또는 취소에 대한 고지를 변경하지 않고 정확하게 나타냅니다.

2.5.7 CrossCert 저장소에 의한 발행

CrossCert 저장소는 이 CPS와 해당 법규에 어긋나지 않는 인증, CPS 수정, 인증서 효력 정지나 취소에 대한 고지 및 기타 정보를 신속하게 발행합니다. CrossCert 저장소(https://www.crosscert.com)와 CrossCert가 수시로 지정하는 기타 다른 통신 수단을 통해 액세스할 수 있습니다.

CrossCert는 CrossCert 저장소 내외 모두에 등록자의 인증서와 CRL 관련 데이터를 발행할 수 있습니다. 이 CPS는 CrossCert가 인증하지 않은 경우 CPS 및/또는 CrossCert 저장소에서 기밀로 선언한 저장소의 데이터(또는 IA에서 관리하는 데이터)에 대한 액세스를 금지합니다.

2.6 공증인

공증인은 (이 CPS에서 규정한 경우를 제외하면)일반적으로 CrossCert의 PKI에 포함되지 않습니다. 그러나 공증인은 특정 유형의 인증서(예: 클래스 3 개인 인증서)와 CrossCert 이외 조직

의 CA 신청서(CPS § 3.1.1 *참고*)를 승인하는 등 신원 확인 및 기타 기존의 공증 행위를 수행합니다.

3. 인증 작업의 기초

이 단원에서는 신뢰할 수 있는 PCS 작업을 위한 기초와 제어 방법에 대해 설명하고 레코드 기록, 감사, 인력 요건을 비롯한 CrossCert PCS 운영의 여러 요건을 다룹니다. 아울러 작업 종료나 정지 시 IA가 지켜야 할 의무도 설명합니다.

참고: 인증서 신청 절차는 다음 CPS §4를 참조하십시오.

3.1 PCA 내에서 비CrossCert CA로 승인받기 위한 조건

CrossCert PCS는 CrossCert가 운영하는 IA에 근거합니다. CrossCert의 재량으로 신뢰할 수 있는 실체들은 CA나 하위 CA로서 CrossCert PCS에 참여합니다. PCS 전체에 걸쳐 동일한 신뢰도를 유지하려면 비CrossCert CA와 하위 CA가 CPS의 조건을 준수해야 합니다.

3.1.1 비CrossCert CA 신청서

CA나 하위 CA가 되고자 하는 각 비CrossCert 실체는 발행하고자 하는 인증 클래스에 적용되는 비CrossCert CA 신청서를 작성하게 됩니다. 비CrossCert CA 신청서에 포함되는 내용은 다음과 같습니다.

(a) CA 신청자, 관리 담당자, 권한이 있는 대리인의 이름, 주소, 전화, 팩스, 전자 우편 주소,
(b) CA 신청자의 예정 식별명,
(c) CA 신청자의 공용 키와 개인 키의 생성, 저장, 사용, 파괴 절차,
(d) CPS에 의거한 CA나 하위 CA로 활동할 수 있는 CA 신청자의 능력에 실질적 영향을 미칠 수 있는 사건(현재나 과거의 지급불능 등)에 대한 설명,
(e) CA 신청자에 의한 CPS 및 CA 신청자의 CPS 복사본 분배 절차에 대한 참조 및 옵션 채택 확인,
(f) 예상 인증 기술, 관리, 아웃소싱될 운영의 목적 및 범위를 기술한 문서,
(g) CA 신청자의 승인 또는 확인된 사업자 등록 문서의 복사본.,
(h) CPS의 요구 조건을 최선을 다해 준수하려는 CA 신청자의 의지 표시,
(i) CrossCert에 요구되는 기타 정보.

CA 신청은 공증 전에 승인되어야 합니다.

CA 신청자가 필요한 정보를 제공하지 못하면 CA 신청 처리가 연기되거나 제외됩니다.

3.1.2 CrossCert에 비CrossCert CA 신청서 제출

공증인이 승인한 CA 신청서(필요한 보충 정보 포함)는 다음 CrossCert PCA 주소로 제출해야 합니다.

우편 번호 137-725 서울시 서초구 서초동 1674-4 하림 빌딩 9층 한국전자인증(주)

3.1.3 CA 활동 개시 승인

CA 신청과 심층 조사 검토가 완료되면 해당 CrossCert PCA는 CA 신청자의 CA나 하위 CA 신청을 승인하거나 거부합니다. 해당 CrossCert PCA의 이러한 신청 승인 또는 거부 결정은 3주에서 6주 사이에 내려 집니다.

PCA는 (i) CrossCert PCA-CA 계약 실행 및 (ii) 신청자에 대한 인증서 발행을 통하여 CA 신청이 승인되었음을 표시합니다. CA 신청을 승인할 것인지 또는 거부할 것인지는 해당 CrossCert PCA의 재량에 달려 있으며, 나아가 CA나 하위 CA의 승인을 무효화할 수 있는 권리까지 보유하고 있습니다. CPS 요건을 파기하거나 준수하지 못한 경우에는 승인을 무효화 할 수 있습니다.

3.2 CrossCert의 손상 조사권

IA와 CrossCert는 법적 허용 범위 내에서 모든 손상을 조사할 수는 있으나 조사할 의무는 없습니다. CA 신청서(CPS § 3.1 참조)나 인증 신청서(CPS § 4 참조)를 제출함으로써 모든 신청자는 이러한 조사가 개인 및 데이터 보호법에 위배되지 않는다는 전제 하에 모든 조사를 감수하며 IA와 CrossCert가 CPS에 따라 적절하다고 간주되는 모든 사실과 환경, 기타 정보를 결정하는데 도움을 줄 것에 동의합니다. IA의 조사는 인터뷰 뿐 아니라 해당 책이나 레코드, 절차의 검토 및 관련 시설에 대한 검사와 조사를 포괄합니다. 인증 신청자와 등록자에 대한 조사는 인터뷰와 문서에 대한 평가 및 요청에만 국한되지 않습니다.

3.3 CPS 준수

IA, LRA, CrossCert 저장소는 각 서비스 수행 시 본 CPS를 준수해야 합니다.

3.4 신뢰성

IA, LRA, CrossCert 저장소는 각 서비스 수행 시 신뢰할 수 있는 시스템만 이용해야 합니다.

3.5 재정적 책임

IA는 운영을 유지하고 임무를 수행하는데 충분한 재정적 자원을 갖춰야 하며, 인증 등록자와 수신자, 발행한 인증서 및 타임 스탬프에 의존하는 다른 사람들에 대한 책임 위험도 감수할 수 있어야 합니다. 뿐만 아니라 IA는 오류와 태만에 대한 보험 기능도 갖추고 있어야 합니다.

3.6 레코드 보관 의무

IA는 다음과 같은 레코드를 보관하여 요청을 받는 즉시 CrossCert가 사용할 수 있도록 해야 합니다.

(i) CPS를 준수하는 문서,

(ii) 각 인증 프로그램과 프로그램이 발행한 인증서의 작성, 발행, 사용, 일시 중지, 취소, 만기, 갱신 및 재등록에 대한 자료가 되는 작업과 정보 문서.이러한 레코드에는 다음과 같은 IA 소유의 모든 관련 증거가 들어가야 합니다.

- 각 인증서에 명명된 등록자의 신원(등록자의 이름 레코드만 보관되는 클래스 1 인증서는 제외),
- 인증 일시 중지나 취소를 요청한 사람의 신분(등록자의 이름 레코드만 보관되는 클래스 1 인증서는 제외),
- 인증서에 표시되는 기타 정보,
- 타임 스탬프
- 인증서 발행과 관련된 예측 가능한 특정 소재.

레코드의 색인과 저장, 보존, 복사가 정확하고 완전하다면 컴퓨터 기반 메시지나 종이 문서의 형태로 보존될 수 있습니다. 이를 준수하기 위해 IA는 등록자나 대리인에게 문서 제출을 요구할 수 있습니다.

3.7 타임 스탬프

타임 스탬프는 CrossCert PCS의 무결성과 인증서의 신뢰도를 향상시키고 디지털 서명한 메시지의 부인 방지에 도움이 될 수 있도록 고안된 것입니다. 타임 스탬프는 (명백한 또는 암시적) 작업의 정확한 날짜 및 시간과 사람의 신분, 주석을 작성한 장치를 표시하는 주석을 작성합니다. 모든 타임 스탬프는 그리니치 표준 시간(GMT)을 반영하며 세계시 규칙(UTC)을 채택합니다. CPS 용도의 경우 00-69 범위의 두자리 연도수는 2000-2069를 뜻하며 70-99 범위는 1970-1999를 뜻합니다.

다음 데이터의 경우 해당 IA가 데이터 위에 직접 타임 스탬프를 하거나 신뢰 가능한 해당 감사 자료에 타임 스탬프할 것입니다.

- 인증서,
- CRL과 기타 일시 중지 및 취소 데이터베이스 항목,
- CPS의 각 버전,
- 고객 서비스 메시지,
- 기타 CPS 규정 정보.

3.8 레코드 보유 기간

IA는 클래스 1과 2 인증서와 관련된 레코드를 10년 이상 보유해야 하며, 클래스 3 인증서와 관련된 레코드는 인증서가 취소 또는 만료된 후 적어도 30년간 보유해야 합니다. 이러한 레코드는 검색 가능한 컴퓨터 기반 메시지나 종이 문서로 보존됩니다.

3.9 감사

IA는 신뢰할 수 있는 시스템을 구현하고 유지하여 키 생성이나 인증 신청, 확인, 취소와 같이 중요한 모든 사건에 대한 감사 자료를 보존해야 합니다. 컴퓨터 보안 전문 기술이나 컴퓨터 보안 전문가를 갖춘 공인 회계사가 피감사 대상자의 비용 부담으로 연 1회 이상 감사를 실시하여 IA의 작업 및 해당 LRA가 본 CPS와 기타 관련 계약, 지침, 절차, 규격을 준수하는지 평가해야 합니다. 비CrossCert IA는 이러한 감사 보고서를 즉시 CrossCert에 제출해야 합니다.

이러한 제3자의 감사 보고서는 보고서의 내용과 사실, 추천에 대한 CrossCert 측의 보증이나 승인을 위한 구성 요소가 되지 않습니다. CrossCert는 PCS를 보호하기 위해 이러한 감사 보고서를 검토할 수는 있습니다. 그러나 CrossCert는 감사 보고서의 저자가 아니므로 그 내용에 대한 책임을 지지 않습니다. 아울러 보고서에 대한 의견을 표명하지 않을 뿐더러 감사 보고서로 발생한 피해에 대하여 책임지지 않습니다.

3.10 비상 계획 및 재난 복구

IA는 적절한 비상 계획과 재난 복구의 능력과 절차를 본 CSP 및 VSP에 따라 구현하고 기록하며 정기적으로 테스트해야 합니다.

3.11 IA 인증서 가용성

IA는 자체 인증서(IA가 주체인 인증서)와 이러한 인증서로 입증할 수 있는 디지털 서명을 보유한 사람 및 확인하려는 사람들이 사용할 수 있도록 취소 데이터의 복사본을 만들어야 합니다.

3.12 발행 기관의 발행

IA는 인증서와 취소 데이터, 본 CPS를 발행해야 합니다.

3.13 기밀 정보

다음 정보는 CrossCert과 해당 IA가 기밀로 받고 생성한 것으로서 다음 경우가 아니면 발표되지 않습니다.

- 승인 또는 승인 거부된 CA 신청 레코드,
- 가입자 계약과 인증 신청 레코드(본 CPS의 인증서나 보관소에 포함된 정보는 예외),
- 트랜잭션 레코드(전체 레코드 및 트랜잭션 감사 자료 모두),
- CrossCert나 IA가 작성했거나 보유한 PCS 감사 자료 레코드,
- CrossCert, IA, CrossCert 저장소가 작성한 PCS 감사 레코드(이러한 보고서가 유지되는 수준까지), 각 (내부나 공식) 감사자,
- 비상 계획과 재난 복구 계획,
- IA 하드웨어 및 소프트웨어의 작업과 인증서 서비스 및 지정된 등록 서비스 작업을 통제하는 보안 수단.

IA나 CrossCert는 CPS에 의하지 않고는 신청자의 이름이나 기타 식별 정보를 발표하거나 매각하지 못하며 그러한 정보를 공유하지도 못합니다. 그러나 CrossCert 저장소에는 인증서 뿐 아니라 취소와 기타 인증 상태 정보가 포함되어야 합니다(*참조* CrossCert 저장소에 대한 CPS §§ 2.5.6, 2.5.7).

자발적 공개 / 기밀 정보 발표.
IA와 CrossCert는 인증된 경우나 다음과 같은 사람의 구체적 요청에 의하지 않고는 기밀 정보를 공개해서는 안되며 공개 요구를 받지 않습니다. (I) IA와 CrossCert가 정보를 비밀로 유지해 주어야 할 의무를 가진 사람 (ii) 기밀 정보를 요청하는 사람(동일인이 아닌 경우)이나 법원의 명령.IA와 CrossCert는 요청인에게 정보를 공개하기 전에 타당한 요금 지불을 요구할 수도 있습니다.

3.14 인사 관리 업무

IA는 직원들의 신뢰도와 능력, 직원의 만족스러운 임무수행을 보증하는 인사 관리 업무를 공식화하여 이에 따라야 합니다. 이러한 업무는 본 CPS를 준수해야 합니다.

3.14.1권한을 위임받은 지위

CrossCert 저장소의 제한된 작업에 대한 액세스를 포함한 IA의 발행, 사용, 일시 중지나 취소에 중요한 영향을 미칠 수 있는 암호화 작업에 대한 액세스나 제어권을 보유한 IA의 모든 직원, 계약자, 컨설턴트(집합적으로 "직원")는 이 CPS의 목적에 있어 권한을 위임받은 위치에서 서비스하는 것으로 간주됩니다. 이러한 직원은 고객 서비스 담당 직원, 시스템 관리 담당 직원, 엔지니어링 담당 직원, IA의 시스템 하부구조를 관장하는 경영진을 비롯한 모든 직원을 포괄합니다.

3.14.2조사와 준수

IA는 권한을 위임받은 위치에서 서비스할 가능성이 있는 모든 직원들에 대한 초기 조사를 실시하여 그들의 신뢰도와 능력을 결정합니다. IA는 권한을 위임받은 위치에서 서비스하는 모든 직원에 대해 정기적인 조사를 실시하여 CrossCert의 인사 기준에 적합한 신뢰도와 능력을 갖추고 있는지 확인합니다.

3.14.3권한을 위임받은 지위의 직원 해임

초기 조사 또는 정기 조사에 통과하지 못한 직원은 권한을 위임받은 위치에 있을 수 없습니다. 권한을 위임받은 위치에 있는 직원을 해임하는 것은 해당 IA의 재량입니다(CrossCert 직원인 경우에는 CrossCert의 재량).

3.15 신임

3.15.1소프트웨어 및 하드웨어 장치의 승인

모든 PCS 관련 하드웨어와 소프트웨어에 대한 승인은 CrossCert나 권한을 위임받은 CrossCert 컨설턴트, 기타 공인 기관(CrossCert가 지정하기도 함)이 해야 합니다.

3.15.2권한을 위임받은 지위의 직원

권한을 위임받은 위치에 있는 직원들은 모두 외부 신임 기관이 신임해야 합니다. PCS에서 운영 가용 인력으로 지정한 사람을 제외하고 CrossCert나 IA의 이사회 위원은 이 규정에 포함되지 않습니다.

3.15.3조직적 조화

IA는 법이나 계약에서 요구하는 대로 IA의 신뢰도에 실질적 영향을 미치는 법률과 규칙을 갖는 해당 대리인 및 기관과 조화를 이루어야 합니다.

3.16 IA 키 생성

IA는 신뢰할 수 있는 시스템을 사용하여 자체 개인 키를 안전하게 생성 및 보호하고 손실, 유출, 변경, 무단 사용을 방지할 수 있는 예방책을 강구해야 합니다.

3.17 비밀 공유

IA는 권한을 위임 받은 비밀 공유 홀더를 사용한 비밀 공유로(용어 정의 *참조*) 개인 키에 대한 신뢰도를 강화하고 다음과 같은 복구 기능을 제공해야 합니다.

실체	IA의 개인 키를 활성화하여 최종 사용자 인증서를 서명하는데 필요한 비밀 공유	IA 인증서 서명에 필요한 비밀 공유	배포된 전체 비밀 공유	재난 복구 공유* 필요한 총계	
VR	TBD	TBD	TBD	TBD	TBD
클래스 1 PCA	해당 없음	5	9	3	4
클래스 2 PCA	해당 없음	5	9	3	4
클래스 3 PCA	해당 없음	5	9	3	4
클래스 1 CA	2 (+1 CK) *	3 (+1 CK)	6	2 (+1 CK)	3 (+1 CK)
클래스 2 CA와 하위 CA	2 (+1 CK)	3 (+1 CK)	6	2 (+1 CK)	3 (+1 CK)
클래스 3 CA와 하위 CA	2 (+1 CK)	3 (+1 CK)	6	2 (+1 CK)	3 (+1 CK)

* CA와 하위 CA에 필요한 위 숫자 만큼의 공유 비밀 외에 공통 키("CK")가 있어야 합니다(비밀 공유 용도로 사용되는 모든 CA와 하위 CA에 필요한 총 키 숫자를 하나씩 효과적으로 증가).그러나 할당된 비밀 공유는 공통 키를 대신하여 사용할 수 있습니다. 공통 키는 할당된 공유 비밀을 이러한 암호 모듈에 둠으로써 발생할 수 있는 보안 위험 없이 특정 하드웨어 암호 모듈을 운영 모드로 보존하는 데 사용됩니다.

표 4 – 공유 비밀 배포

3.17.1 하드웨어 보호

IA는 신뢰할 수 있는 소프트웨어를 공유 비밀로 사용하는 클래스 1 CA를 제외하고 개인 키를 사용해야 하는 모든 작업에 대하여 신뢰할 수 있는 하드웨어 암호 모듈을 사용해야 합니다. 개인 키 작성 절차는 CrossCert 저장소에 공개될 수 있습니다.

3.17.2 IA의 대표성

개인 키의 공유 비밀을 분배하는 IA는 비밀 공유될 개인 키를 법적으로 소유한 모든 해당 실체를 대표하여 CPS에 따라 권한을 위임받은 비밀 공유 홀더에게 이를 전송할 것을 보증합니다.

3.17.3 공유 비밀 홀더의 비밀 공유 승인

공유 비밀 홀더가 비밀 공유를 승인하기 위해서는 대다수의 지정된 공유 공유 홀더가 공유의 작성, 재작성, 분배 및 향후 보관 체인을 개인적으로 감시해야 합니다.

각 공유 비밀 홀더는 CrossCert 승인 하드웨어 토큰과 같은 물리적 매체 내에서 공유 비밀을 받아야 합니다. 공유 비밀 홀더가 수신된 공유 비밀에 대한 조사를 마치면 홀더는 IA가 제공한 비밀 공유 승인 형식에 서명하고 이를 해당 IA로 돌려 보내 비밀 공유 수락을 승인하게 됩니다.

3.17.4공유 비밀 보호

공유 비밀 홀더는 신뢰할 수 있는 시스템을 사용하여 공유 비밀이 손상되지 않도록 보호해야 합니다. 본 CPS에서 제공된 경우를 제외하고 비밀 공유 홀더는 다음과 같은 행위를 하지 않을 것을 동의합니다.

• 협력 업체에 기밀을 누설, 폭로, 복사, 사용 허락 하거나 공유 비밀의 무단 사용하는 행위.

• 비밀 공유 홀더가 자신 혹은 타인이 비밀 공유 홀더임을 (명백하게 또는 암묵적으로) 폭로하는 행위.

• 비밀 공유 홀더의 자격이 없어지거나 비밀 공유 홀더를 이용할 수 없는 경우 복구 불가능한 장소에 비밀 공유를 저장하는 행위(권한 위임된 목적으로 사용되는 경우 제외).

3.17.5공유 비밀의 가용성과 공개

비밀 공유 홀더는 권한을 위임받은 레코드(다음 단락 참조)가 적절한 권한을 제공한 경우에만 권한을 위임받은 실체(비밀 공유 홀더 인증 형식에 표시되어 있음)가 공유 비밀을 사용할 수 있게 합니다. 재난이 발생한 상황인 경우(비밀 공유 발행자가 선포한 경우) 비밀 공유 홀더는 비밀 공유 발행자의 지시에 따라 재난 복구 사이트에 이를 보고해야 합니다. 공유 비밀 홀더는 비상/재난 복구 사이트로 가서 공유 비밀을 공개하기 전에 공유 비밀 발행자의 선언을 비밀 공유 승인 형식에서 지정한 대로 승인해야 합니다(법률이나 특정 범죄 조사에 관한 법적 절차로 금지된 경우 제외).이 절차에는 비밀 공유 홀더의 이동 위치가 잘못되어 비밀 공유 발행자의 복구 능력이 불능 상태가 되지 않도록 암호(비밀 공유 발행자에서 비밀 공유 홀더로 전달됨)가 사용됩니다. 재난 복구 절차에 참가하려면 비밀 공유 홀더는 재난 복구 사이트에서 공유 비밀을 물리적으로(직접) 전달해야 합니다.

비밀 공유 홀더는 앞 단락에 제시된 방법으로 비밀 공유 발행자의 선언 권한을 위임한 경우 진실로 믿어지는 지시, 문서, 메시지, 레코드, 증서나 서명을 신뢰할 수 있습니다. 비밀 공유 발행자는 비밀 공유 홀더에게 비밀 공유 발행자의 권한을 인증하는데 사용하는 일단의 샘플 서명 집합을 제공하게 됩니다.

3.17.6공유 비밀 발행자 및 홀더의 레코드 기록

비밀 공유 발행자 및 홀더는 비밀 공유 요소에 관련된 모든 작업 레코드를 기록해야 합니다. 비밀 공유 홀더는 요청이 있을 경우 비밀 공유 발행자나 피지명인에게 비밀 공유 상태에 관한 정보를 제공해야 합니다.

3.17.7공유 비밀 홀더의 의무

비밀 공유 홀더는 CPS에 따라 의무를 수행하며 모든 면에서 적절한 방법으로 작업해야 합니다. 비밀 공유 홀더는 비밀 공유의 손실, 도난, 부당한 폭로나 손상을 감지할 경우 곧바로 비밀 공유 발행자에게 이 사실을 통보해야 합니다. 비밀 공유 홀더는 능력 밖의 원인으로 인하여 의무를 다하지 못했을 경우에는 책임을 지지 않으나, 공유 비밀의 부당한 폭로나 태만 혹은 부주의와 같은 자신의 실수로 인한 손상을 통보하지 않은 경우에는 그에 대한 책임을 져야 합니다.

3.17.8비밀 공유 발행자의 배상

비밀 공유 발행자는 태만이나 부주의 같은 비밀 공유 홀더의 실수로 인해 발생하지 않은 비밀 공유와 관련하여 비밀 공유 홀더가 초래한 모든 항의, 작업, 손해, 판결, 중재 요금, 지출, 비용, 변호사 비용 등을 배상하고 비밀 공유 홀더에게 피해가 가지 않도록 할 것을 동의합니다.

3.18 운영 기간 제한 준수

CA 신청자는 IA 인증서에 지정된 운영 기간이 이를 설정한 상위 IA가 부과한 제한을 준수토록 해야 합니다.

3.19 보안 요건

3.19.1통신 보안 요건

CrossCert과 PCS 상대방 가운데 본 CPS를 준수하는 모든 통신은 수반되는 위험에 비례하는 적절한 보안 메커니즘을 제공하는 응용 프로그램을 사용해야 합니다. 뿐만 아니라 컴퓨터 기반 통지와 이에 상응하는 통지 승인, PCS 보안에 영향을 주는 기타 통신에도 적절한 보안 조치를 취해야 합니다.

3.19.2설비 보안 요건

IA는 VSP나 그에 상응하는 기준에 부합하는 신뢰 가능한 설비를 운영해야 합니다.

3.20 지역 등록 기관 관리자(LRAA) 요건

LRAA는 권한을 위임받은 위치에 있습니다(참조 CPS § 3.14 - 인사 관리 준칙).LRAA에 대한 최소 요건은 LRAA가 권한을 위임받은 신청을 바탕으로 발행된 인증서의 클래스에 따라 다릅니다. 특정 비CrossCert 조직 LRA에는 일반 대중에 대한 인증서를 발행하지 않고 식별 문서의 일반 확인에 대한 경험이 덜 요구되므로 정상적인 LRAA보다 요건이 덜 엄격하다는 사실을 유의하십시오.오히려 비CrossCert 조직 LRA는 권한을 위임받은 직원 및 기타 “관계자” 또는 비즈니스 레코드의 간단한 내부 목록을 바탕으로 인증 승인 결정을 내립니다. LRAA 요건은 표 5에 수록되어 있습니다.

	LRAA 클래스 1과 2	비CrossCert 단체의 LRAA 클래스 2	LRAA 클래스 3
교육	해당 없음 - LRAA 기능이 자동화되었습니다.	기업의 기밀 인사 기록을 처리하는 인사 담당자에 대한 요구조건과 같음	2년제 대학 졸업 이상, 법률 보조원이나 공증인 교육 과정 수료 또는 그에 상응하는 경력
훈련	해당 없음 - LRAA 기능이 자동화되었습니다.	온라인 LRAA 시범 프로그램 수료 및 3개월 이상의 LRA 근무 경력	2주 간의LRAA 수습 과정 수료 후 3달 이상 LRA 근무한 경험.LRAA 근무 시작 6개월 내에 공증 훈련 과정 수료
신임장	해당 없음 - LRAA 기능이 자동화되었습니다.	해당 없음 - LRA와 좋은 관계를 유지하고 있어야 함	법률 보조원 면허나 공증 위임장 또는 그에 상응하는 신임장LRA 및 고용인과 좋은 관계를 유지하고 있어야 함.
초기 조사	해당 없음 - LRAA 기능이 자동화되었습니다.	해당 권한을 위임받은 위치가 필요할 때마다 (CPS § 3.14.1 *참조*)	해당 권한을 위임받은 위치가 필요할 때마다 (CPS § 3.14.1 *참조*)
정기 조사	해당 없음 - LRAA 기능이 자동화되었습니다.	매년 (권장 사항)	매년
결합	해당 없음 - LRAA 기능이 자동화되었습니다.	아니오	예
레코드 기록	Per CPS § 3.6	예, CPS § 3.6에 의거.CrossCert에서 소유하거나 운영하는 IA와 관련이 없는 LRAA는 CPS에 따라 해당 레코드를 보유해야 합니다.	Yes, per CPS § 3.6

표 5 – LRAA 요건

3.21 IA 운영 만료 또는 중지

다음에 나오는 의무 사항은 적기 통보 및 후임 실체에 대한 책임 이전, 레코드 유지, 특정 구제책 제공으로 서비스 중지에 따른 영향을 최소화하는데 목적이 있습니다.

3.21.1중지 사전 요건

IA 역할을 중지하기 전에 IA는 다음과 같은 조치를 취해야 합니다.

(i) 상위 IA에(CrossCert가 소유하거나 운영하는 상위 IA가 없는 경우에는 CrossCert에도) IA로서의 역할 중지 의사를 통보해야 합니다. 그러한 통보는 IA로서의 역할을 중지하기 90일 전에 해야 합니다. 상위 IA가 이 규정을 준수하려면 추가 준칙이 필요할 수도 있습니다.

(ii) 취소 또는 만기되지 않은 인증서 등록자에게 IA로서의 역할을 중지할 의사를 90일 전에 통보해야 합니다.

(iii) 90일의 통보 기간이 끝나는 시점에는 등록자의 취소 요구에 관계없이 취소되지 않거나 만기 되지 않은 모든 인증서를 취소해야 합니다.

(iv) CPS § 9에 따라 영향을 받게 되는 모든 등록자에게 인증서 취소를 통보해야 합니다.

(v) 인증 서비스 중지로 인해 등록자 및 인증서에 포함된 공용 키를 참조하여 디지털 서명을 확인해야 하는 사람들이 겪게 될 불편을 최소화할 수 있도록 노력해야 합니다.

(vi) 레코드 보존을 위한 적절한 준비를 해야 합니다.

(vii) 만기일 전에 인증서를 취소한 등록자에게 적절한 손해배상(인증서 구입 비용을 초과하면 안됨)을 해야 합니다.

3.21.2승계 IA의 인증서 재발행

인증서 신청자와 등록자에게 중단없는 IA 서비스를 제공하려면 권한이 종료되는 IA는 다른 IA의 사전 서면 승인에 따라 등록자의 인증서 재발행 기관을 지정해야 합니다. 인증서 재발행 시 후임 IA(하위 IA와 혼동하지 말 것)는 서비스 중지 IA와 후임 IA간에 서면 동의에 따라 중지되는 IA의 권리를 대신하며 인증에 관한 모든 의무와 책임을 떠맡습니다. 서비스를 중지하는 IA와 등록자간의 계약이 후임 IA의 서면 승인에 종속되지 않은 경우에 CPS는 원래 IA의 후임 IA 하에서 효력이 있는 채로 남아 있습니다.

이러한 수정 사항이 계약 당사자에게만 영향을 미칠 경우 이 요건은 계약에 따라 다를 수 있습니다.

4. 인증서 신청 절차

이 단원에서는 인증서 신청 프로세스에 대해 설명합니다. 여기에는 키 쌍의 생성 및 보호에 대한 요구 사항이 포함되며 각 인증 클래스에 필요한 정보의 목록이 나와 있습니다.

인증서를 원하는 모든 사용자(IA 제외)는 각 인증 신청서에 대해 다음과 같은 일반적인 절차를 동시에 완료해야 합니다.

- 키 쌍을 생성하고 생성한 키 쌍이 함수 키 쌍이라는 것을 해당 IA에 증명합니다.
- (이 키 쌍의)개인 키가 손상되지 않도록 보호합니다.
- 제안된 식별명을 확인합니다.
- 이 키 쌍의 공용 키를 포함하고 있는 인증 신청서(및 가입자 계약서)를 해당 IA에 제출합니다.

4.1 키 생성 및 보호

다음 절차는 이 CPS에서 명시된 대로 키를 생성하는 모든 주체에 적용될 수 있습니다.

4.1.1 소유자의 배타적 책임; 개인 키에 대한 액세스 제어

이 CPS에 따로 언급되어 있지 않으면 각 인증 신청자는 신뢰할 수 있는 시스템을 사용하여 보안이 유지된 상태에서 자신의 개인 키를 생성하고 이 개인 키가 손상, 분실, 유출, 변형 및 무단 사용되지 않도록 필요한 조치를 취해야 합니다. 가입자(및 인증 신청자)는 일반적으로 키를 적절히 보호하는 비CrossCert 제품을 사용합니다. https://www.crosscert.com/repository/PrivateKey_FAQ에서 가입자 개인 키 보호 FAQ를 *참조*하십시오.

각 인증 신청자(및 인증이 승인된 경우의 각 등록자)는 자신의 개인 키가 손상, 분실, 유출, 변형 또는 무단 사용되지 않도록 보호하는 것에 대한 전적인 책임은 CROSSCERT(또는 해당 IA)이 아닌 자신에게 있음을 인정합니다.

사용자와 IA는 CrossCert으로부터 사전 서면 승인을 받거나 이 CPS에서 명시적으로 허용한 경우를 제외하면 PCS 기술 구현을 모니터하거나 방해 또는 분해 분석하지 않는다는 것에 동의합니다.

4.1.2 개인 키 책임의 위임

개인 키에 대한 책임을 위임하는 경우에도 위임자는 개인 키의 생성, 사용, 유지 또는 적절한 폐기와 관련한 책임과 의무를 다해야 합니다.

4.2 인증 신청서 정보와 전달 방법

인증 신청서 정보에는 다음의 표 6에 나와 있는 항목이 포함되어 있습니다. *하지만 다음 정보의 모든 항목이 인증서에 표시되는 것은 아닙니다*(그림 3 - 참조에 의해 포함되는 인증서와 정보 *참조*). *참고*: 인증서에 포함되지 않은 이러한 정보 항목은 IA가 기밀로 보호하는 항목입니다 (CPS § 3.13 *참조*).비CrossCert 조직 LRA에 가입한 개인의 클래스 2 정보는 신청서에는 없어도 되지만 그러한 LRA에 필요할 수 있습니다.

인증 클래스	인증 신청서에 필요한 정보
클래스 1	**개인:** *필수 정보* (a) 이름(또는 별칭) (b) 주체의 공용 키 (c) 전자 우편 주소 (d) 승인된 가입자 계약서 (e) 신용 카드 정보(해당되는 경우) (f) 암호(추후에 IA가 가입자를 인증하는 데 필요) (g) 기타 IA나 CrossCert가 정한 정보 *선택 사항* (h) 인구 통계 데이터(등록 필드 정보) ***신청서 전달 방법:*** IA는 (서명되지 않은)인증서 원본과 가입자 계약서를 인증 신청자에게 전달합니다. 인증 신청자는 보안 웹 채널을 통해 이러한 온라인 대화를 완료하여 (i) 인증 신청자 정보가 정확하고, (ii) 인증 신청자가 가입자 계약서를 읽고, 이해하고, 그 조건에 동의함을 승인할 수 있습니다. 지정된 확인 절차가 끝나면 IA는 인증 신청자가 인증 신청서에 기재한 주소로 전자 우편을 보냅니다. 이 전자 우편 메시지에는 PIN(및 선택 사항으로 인증서에 포함될 정보 내용의 초안)이 포함되어 있습니다. 이 PIN은 IA로부터 인증서를 받을 인증 신청자를 인증합니다. **사업자:** 해당 없음

클래스 2	**개인:** *필수 정보* (a) 공식 이름(이름 형식) (b) 제안된 식별명 (c) (거주)국가, 시, 구/군, 동/면, 번지, 우편 번호 (d) (거주지의)전화 번호 (e) 전자 우편 주소 (f) 주체의 공용 키 (g) 신용 카드 정보 (h) 배우자 이름(해당되는 경우) (i) 주민 등록 번호 (j) 생일 (k) 고용주(해당되는 경우) (l) 암호(추후에 IA가 등록자를 인증하는 데 필요) (m) 승인된 가입자 계약서 (n) 이전 주소(최근 2년 이내에 주소가 변경된 경우) (o) 운전 면허증 정보(해당되는 경우) 기타 IA나 CrossCert가 정한 정보 *선택 사항* (p) 인구 통계 데이터(등록 필드 정보) ***신청서 전달 방법:*** 클래스 1과 동일 ***대리자/권한을 부여받은 담당자:***해당 없음 **사업자:** 해당 없음

클래스 3	개인: *필수 정보 – 클래스 2와 동일하며 다음 항목이 추가됩니다.* (a) 공증인 또는 LRA가 세 가지 형태로 인증 신청자의 신원을 확인하여 승인하는 가입자 계약서("직접 대면" 요구 사항을 충족시킴) *선택 사항* (b) 이전 고용주 *대리인/권한을 부여받은 담당자:* 클래스 3에서는 (개인이 아닌)회사를 대신하여 대리자가 인증서를 신청하고 해당 회사를 가입자로 지정할 수 있습니다. *신청서 전달 방법*: TBD 사업자: *필수 정보* (a) 도메인 이름 (b) 단체 (c) 부서(해당되는 경우) (d) 기술 및 대금 결제 담당자 (e) 시, 구/군, 국가, 우편 번호 (f) 이름을 사용할 수 있는 권한 입증(제3자의 데이터베이스 확인 및 대역외 검증을 통해) (g) 단체 상태 입증(예: 가능한 경우 회사 소개 또는 이에 상당하는 입증) (h) 대리자의 권한 입증 *선택 사항* (i) KSIC(Korean Standard Industrial Classification) 번호 *대리인/권한을 부여받은 담당자: 위의 내용 참조* *신청서 전달 방법*: 작성한 신청서(및 가입자 계약서)를 전자 우편으로 제출해야 합니다.

표 6 – 인증서 신청에 필요한 정보

5. 인증 신청서 확인

이 단원에서는 해당 IA나 권한을 위임 받은 지역 등록 기관이 인증 신청서를 확인하는 데 필요한 요구 사항을 제시하며 확인에 실패하는 경우를 설명합니다.

5.1 인증 신청서 확인 요구 사항

인증 신청서를 받으면(CPS § 4 – 인증서 신청 절차) IA는 다음과 같이 인증서 발행(CPS § 6 – 인증서 발행) 전 필수 사항으로 요구된 확인을 모두 수행해야 합니다.

IA는 다음을 확인해야 합니다.

(a) 인증 신청자는 인증 클래스 설명에 나온 범위에 따라 식별된 사람이어야 합니다. CPS § 2와 아래의 설명을 참조하십시오.

(b) 인증 신청자는 인증서의 공용 키에 대응되는 개인 키를 가집니다. 인증 신청자가 준칙을 지킬 때 이러한 의무를 다할 수 있습니다.

(c) 인증서의 정보는 확인되지 않은 가입자 정보(NSI)를 제외하고 정확해야 합니다.

(d) 인증 신청자의 공용 키(클래스 3 인증서와 사업자만 허용)를 제출하며 인증서를 신청하는 대행사에게는 그러한 요청을 할 수 있는 권한이 부여됩니다.

인증서가 발행되면 IA는 CPS에 따라 인증서의 손상에 대한 통보를 받는 경우 외에는 인증서의 정보가 정확한지 모니터하고 검사해야 할 의무가 없습니다.

표 7(인증 신청서 확인 요구 사항)에서는 각 인증 클래스의 확인 요구 사항 간의 차이점을 보여줍니다. CrossCert는 확인 프로세스를 향상시키기 위하여 이러한 확인 절차를 갱신할 권한을 갖습니다. 확인에 대한 자세한 내용은 다음을 참조하십시오. 갱신된 확인 절차(배포되는 경우)는 CrossCert 저장소(https://www.crosscert.com/repository/updates)에 발행되며, 우편 번호 137-725 서울시 서초구 서초동 1674-4 하림 빌딩 9층 한국전자인증(주)를 통해서도 확인할 수 있습니다.

확인 요구 사항	클래스 2	클래스 3
개인 출석	아니오	예 – 개인:공증인 또는 LRA(비CrossCert 단체 LRA 신청자 제외) 앞 단체:선택 사항
개인 조사 (개인의 경우)	아니오	예 – 개인:공증인에 의한 인증 신청서 승인
제3자에 의한 개인 데이터 자동 확인	예	예(아래 설명 *참조*)
제3자에 의한 사업자 확인	해당 없음	예(아래 설명 *참조*)
주소 확인	예(아래 참조)	해당 없음
INTERNIC 도메인 이름 확인	해당 없음	예(아래 설명 *참조*)

표 7 – 인증 신청서 확인 요구 사항

5.1.1 개인 출석

지원자와 지원자의 공용 키를 적절하게 바인드하려면 공증인이나 LRA와 같은 권한을 부여 받은 기관이 개별적으로 클래스 3 인증을 신청하는 개인의 신분을 확인해야 합니다. 개인 정보 요구 사항은 특정 개인 정보 문서, 인증 클래스나 종류에 따라 다릅니다.

5.1.2 제3자에 의한 개인 데이터 확인

필요하면 제3자는 인증 신청자가 제공한 개인 정보를 제3자의 데이터베이스와 비교하여 확인합니다. 인증 지원자의 데이터가 CrossCert의 사용자 정의 검사 알고리즘이나 기타 적절한 확인 프로세스를 사용해 비교할 때 데이터베이스 정보와 일치하면 확인이 완료됩니다.

온라인 조사는 인증 신청자의 개인 정보와 신용 기관의 데이터베이스를 비교하여 동일성을 확인합니다. 이러한 데이터베이스를 사용하면 신청자의 주소도 확인할 수 있습니다. 그러나 온라인 조사의 범위는 각 나라의 데이터 보호법에 따라 다릅니다. 특정 절차는 인증 신청자와 발행될 인증 클래스의 요구 사항에 따라 IA가 실행할 수 있습니다.

5.1.3 제3자에 의한 사업자 정보 확인

필요한 경우 제3자가 자신의 데이터베이스와의 비교 및 기타 적절한 정부 기관으로의 질의를 통해 사업자 이름, 주소 및 기타 등록 정보를 확인할 수 있습니다. 회사, 은행 및 해당 대리인에 대한 정보 확인에는 특정 사업과 관련, 해당 기준(예:해당 사업 등록)에 따르는 일부 임의적인(그리고 지역화된) 절차가 필요할 수도 있습니다. 제3자는 또한 해당 사업자와의 중립적인 통신에 사용되는 전화 번호를 제공함으로써 특정 정보(예: 사업자 내에서 해당 대리인의 직위나 신청서에 기재된 특정 개인의 실재 존재 여부)를 확인할 수 있습니다. 필요한 모든 정보가 해

당 데이터베이스에 포함되어 있지 않으면, IA가 요청할 경우, 제3자는 해당 정보에 대한 조사를 수행하거나 인증 신청자에게 추가 정보 및 입증 자료 제출을 요구할 수도 있습니다.

5.1.4 우편 주소 확인

클래스 2의 임시 인증서를 발행할 때 IA는 인증 신청서에 표시되어 있고 제3자 데이터베이스를 통해 확인(CPS § 5.1.2 참조)된 주소로 확인서(제 1종 우편 사용)를 보내야 합니다. 이러한 확인 절차는 가입자의 주소가 인증 신청서의 주소와 일치하는 지의 여부를 확인하여 가입자가 동일하다는 것을 확인해 줍니다.

확인서에는 인증 신청자의 승인을 확인하기 위한 개인 식별 번호(PIN)가 포함되어 있습니다. 확인서에는 인증 신청서를 다른 사람이 제출했다면 수령인이 신청서 처리와 인증서 취소를 요청하도록 지시합니다. 이러한 취소 절차는 임시 인증 기간 동안만 사용할 수 있으며 인증 취소 절차와 다른 것입니다. 임시 기간 동안에 취소하지 않으면 임시 인증서가 일반 인증서로 사용됩니다. 주소 확인은 CrossCert 이외의 단체 LRA가 승인한 클래스 2 인증서에 적용되지 않습니다.

5.1.5 도메인명 확인 및 일련 번호 지정

IA와 CrossCert는 상대적 식별명(RDN)과 자체 발행한 인증서의 일련 번호를 임의로 지정할 수 있습니다. IA는 적절한 곳에 RDN을 지정하기 위해 InterNIC을 사용합니다.

5.1.6 수출 제어 확인

클래스 3 인증서에 사용된 기타 인증 외에 CrossCert는 서버에 설치하기 위한 수출 제어 인증서 발행 조건으로 다음을 확인합니다.

(i) CrossCert는 인증 신청자가 인증 신청서에 해당 서버가 있는 국가를 확인하도록 합니다. 인증 신청자가 해당 국가를 확인하면 서버가 실제로 해당 국가에 있다고 표시하며 이를 보증하게 됩니다.

(ii) 인증 신청자가 그러한 서버가 대한민국에 있다는 것을 주장하고 보증하는 경우 CrossCert는 인증 신청서의 국가 필드에 ROK가 지정되어 있는지와, 신뢰할만한 제3자 데이터베이스(CPS § 5.1.3 *참조*)에서 얻은 정보를 통해 인증 신청서의 단체 연락 정보 필드에 지정된 자가 한국에 있다는 것을 확인합니다. CrossCert는 또한 등록 과정 중 기재하는 인증 신청자의 표준 산업 코드(KSIC)가 은행, 금융 기관, 보험 회사 또는 건강이나 의료 단체를 나타내는지 확인합니다. 대체 수단으로 해당 국가의 법률에 따라 적법하게 설립 허가를 증명할 수 있는 기타 문서 자료를 제공하여 한국의 법률에 따라 은행, 금융 기관, 보험 회사 또는 건강이나 의료 단체로서 운영되는지 확인할 수도 있습니다.

5.2 클래스 1 또는 3 인증 신청서 승인

CPS § 5.1에 따라서 클래스 1또는 클래스 3 인증 신청서에 필요한 확인을 모두 성공적으로 수행하면 해당 IA가 신청서를 승인합니다. CPS § 6의 인증서 발행에 따라 일반 인증서를 발행하여 승인을 명시합니다.

5.3 클래스 2 인증 신청서 승인

CPS § 5.1에 따라서 클래스 2 인증 신청서에 필요한 IA 내부 확인을 모두 성공적으로 수행하면 적용할 수 있는 IA가 임시로 인증 신청서를 승인합니다. CPS § 6.2.(임시 인증서)에 따라 IA가 임시 인증서를 발행하여 승인을 명시합니다.

5.4 인증 신청서 거부

확인에 실패하면 해당 IA는 인증 지원자에게 확인에 실패한 것을 즉시 통지하고 법으로 금지된 부분을 제외한 실패의 원인 코드를 제공하여 인증 신청서를 거부합니다. 제3자의 데이터베이스 정보 때문에 확인에 실패한 경우 해당 IA는 인증 신청자에게 제3자 데이터베이스 회사의 연락처를 제공해 실패의 원인을 알 수 있도록 하여 분쟁을 해결합니다. 이러한 통지는 인증 신청자를 IA나 LRA에 알리는 데 사용한 것과 동일한 방법으로 인증 신청자에게 전달됩니다.

인증 신청서가 거부된 지원자는 다시 지원할 수 있습니다.

6. 인증서 발행

이 단원에서는 인증서 발행 요건을 설명하고 발행 기관이 인증서 발행에 사용하는 구체적 사항들을 다룹니다.

6.1 일반 인증서

인증서 신청(CPS 5)이 승인되면 IA가 인증서를 발행합니다. 일반 인증서가 발행되면 IA가 인증 프로그램을 최종 승인했다는 것을 의미합니다. 일반 인증서는 가입자의 승인을 받으면 유효한 인증서가 됩니다. CPS § 7의 승인 관련 사항을 참조하십시오.

6.2 임시 인증서

임시 인증서는 가입자의 주소를 확인하는 동안 특정 인증서 클래스(현재는 클래스 2)로 발행됩니다. 임시 인증서는 취소되지 않으면 임시 기간이 끝날 때 "일반" 인증서가 됩니다. 표 9를 참조하십시오.

6.3 IA의 인증서 발행에 대한 가입자 동의

IA는 인증 신청자의 동의가 없으면 인증서를 발행하지 않습니다. 인증서가 아직 승인되지 않아도 신청자가 인증서를 제출하면 발행에 동의한 것으로 가정됩니다.

6.4 인증서 발행 거부

IA는 신청자에 대한 인증서 발행을 임의로 거부할 수 있으며 이러한 거부로 인해 발생하는 손실이나 비용 부담에 대한 의무나 책임을 지지 않습니다. IA가 인증서 발행을 거부하면 IA는 인증 신청자가 잘못된 정보를 제출한 경우를 제외하고 모든 인증 신청자의 인증서 등록 비용을 즉시 반환해야 합니다.

6.5 인증서 발행에 대한 IA의 확인 사항

6.5.1 가입자에 대한 IA의 확인 사항

(i) CPS에 따로 제시하거나 IA와 가입자가 인증된 기록으로 서로 동의하지 않는 이상 IA는 인증서에 기록된 가입자에게 다음을 약속합니다.

(a) 인증서에는 IA가 알고 있거나 IA로부터 비롯된 사실에 대한 허위 사실이 없습니다.

(b) IA는 인증을 발행할 때 합리적인 보호를 하지 못한 결과로 인하여 인증 신청자의 정보에 오류를 범하지 않습니다.

(c) 인증서는 CPS의 실질적 요구 사항을 모두 충족시킵니다.

(ii) CPS에 따로 제시하거나 IA와 가입자가 인증된 기록으로 서로 동의하지 않는 이상 IA는 가입자에게 다음의 CPS 조건에 따라 그에 상응하는 노력을 할 것을 약속합니다.

(a) CPS § 9에 따라 인증서를 즉시 취소하거나 일시 중지합니다.

(b) IA가 해당 가입자에게 발행한 인증서의 유효성과 신뢰성에 실질적으로 영향을 주는 사실을 가입자에게 통보합니다.

(iii) CPS § 6.5.1 (i)과 (ii)의 의무 사항과 관련 사실은 가입자의 이익을 위해 만들어 지고 시행되며, 다른 관계자의 이익을 위하거나 강요에 의하지 않습니다. IA는 CPS 및 해당 법률을 준수하며 CPS § 6.5.1(ii)을 위해 적절한 조치를 취합니다.

6.5.2 당사자에 대한 IA의 확인 사항

인증서를 발행함으로써 IA는 디지털 서명(CPS에 따르는 인증서의 공용 키로 확인 가능)을 신뢰하는 모든 당사자에게 다음을 확인합니다.

(i) 미확인 가입자 정보(NSI)를 제외하고 인증서의 모든 참조 정보는 정확합니다.
(ii) IA는 CPS에 따라 인증서를 발행합니다.

6.6 발행에 대한 IA의 확인 사항

인증서(CPS § 7.5참조)를 발행함으로써 IA는 CPS § 7.1에서 설명한 것처럼 가입자에게 인증서를 발행하고 가입자가 인증서를 승인했음을 CrossCert 저장소에 보증하며, 인증서의 정보를 신뢰하는 당사자 모두에게 보증합니다.

6.7 IA 확인 사항의 제한

앞에서 설명한 CPS § 6.5와 6.6의 확인 사항은 (i) CPS § 11.3, 11.4, 11.5의 보증 배제와 의무의 제한 중 하나를 조건으로 합니다.

6.8 인증서 발행 시기

다음 기간 내에 IA가 관련 정보를 모두 접수하면 IA는 인증 신청서 정보를 확인하고 사용자 등록 인증서를 발행합니다.

	클래스 1	클래스 2	클래스 3
시간 기간	2시간 이내에 "즉시"	하루 이내에 "즉시"	1-5일 이내

표 8 - 인증서 발행 기한

CrossCert와 IA는 인증 신청자가 완벽하고 정확한 정보를 제 때 제출하고 CrossCert와 IA의 관리상 요청 사항에 대해 적절히 응답할 경우 이러한 기한을 따르며, 여기에는 적절하고 정확한 지불 정보의 제출과 이의 승인 기간이 포함됩니다.

6.9 인증서 효력 및 운영 기간

해당 IA가 발행하고 가입자(CPS § 7 *참조*)가 승인하는 즉시 모든 인증서는 유효하게 됩니다. 다양한 인증 클래스의 표준 운영 기간은 다음과 같으며 일시 중지나 취소로 인해 운영 기간이 조기 종료될 수 있습니다.

인증서 발행 기관:	클래스 1	클래스 2	클래스 3
VR이 PCA에 발행 시	3년	3년	2년
PCA가 CA에 발행 시	2년	2년	2년
CA가 종속 CA에 발행 시	해당 없음	TBD	TBD

CA가 최종 사용자에게 발행 시	1년	임시 인증서: 21일	표준 인증서: 1년	1년

표 9 – 인증서 운영 기간

인증서에 날짜와 시간(발행일로부터 60일 이내)이 별도로 표시되어 있지 않으면 모든 인증서는 발행한 날짜와 시간으로부터 운영 기간이 계산됩니다. 인증서가 승인되지 않아서 아직 유효하지 않은 경우에도 인증서를 발행한 날짜와 시간으로부터 운영 기간이 시작됩니다.

6.10 발행된 비승인 인증서의 제한

승인되지 않아 유효하지 않은 인증서에 대해 신뢰할 수 있는 경우에도 가입자는 인증서의 공용키에 대응하는 개인 키를 사용하거나 해당 개인 키를 사용하여 디지털 서명을 작성하면 안됩니다.

7. 가입자의 인증서 승인

이 단원에서는 가입자의 인증서 승인 시 요구 사항, 승인에 대한 가입자의 확인 사항, 가입자의 개인 키 보호 의무, 인증서 발행 절차에 대해 설명합니다.

7.1 인증서 승인

CPS § 4.2에 따른 다음 신청 승인이 표 10의 설명대로 증명되면 가입자가 인증서를 승인한 것으로 간주됩니다.

클래스	승인 획득 방법
클래스 1	**개인:** **온라인(웹 이용):**인증 신청자는 자신의 PIN을 입력하여 인증서를 취득하고 승인합니다. 참고:인증 신청자는 인증서를 수신하거나 저장소에 발행한 후 또는 인증서에 들어가는 정보를 통지받은 즉시 인증서의 불일치나 결함을 IA에 통지해야 합니다. **전자 우편(S/MIME):** 인증 신청자는 IA에 CSR을 제출하여 인증서를 승인받습니다. 정해진 확인 절차가 완료되면 IA는 인증 신청서가 제출된 전자 우편 주소로 인증서를 보냅니다. 참고:인증 신청자는 인증서나 저장소에 인증서를 발행하거나 인증서에 포함시킬 정보를 사전 통지받는 즉시 인증서의 불일치나 결함을 IA에 통지해야 합니다. **사업자:** 해당 없음
클래스 2	**개인:** **온라인(웹 이용):***온라인 클래스 1과 동일합니다.* 추가로, 인증 신청자가 IA로부터 확인서를 받게 되면 인증 신청자는 CPS § 5.1.4(우편 번호 확인)에 따라 확인서의 내용을 검토하고 해당 확인서에 잘못된 점이 있을 경우 IA에 문의합니다. **전자 우편(S/MIME):** *전자 우편 클래스 1과 동일합니다.* **사업자:**해당 없음
클래스 3	**개인:** **온라인(웹 이용):** *온라인 클래스 1과 동일합니다.* **전자 우편(S/MIME):** *전자 우편 클래스 1과 동일합니다.* **사업자:** **온라인(웹 이용):** *온라인 클래스 1과 동일합니다.* **전자 우편(S/MIME):**TBD

표 10 - 인증서 승인 방식

7.2 승인 시의 가입자 확인 사항

가입자는 IA가 발행한 인증서를 승인함으로써 승인 시점부터 인증서의 유효 기간 동안 및 가입자의 통지가 있을 때까지 인증서에 포함된 정보를 신뢰하는 IA와 모든 사용자를 확인 및 승인합니다.

(i) 인증서에 표시된 공용 키에 해당하는 개인 키로 작성된 디지털 서명은 가입자의 디지털 서명이며, 디지털 서명이 작성된 시점에 인증서는 만기, 일시 중지 또는 철회되지 않고 운영됩니다.

(ii) 권한을 부여받지 못한 사용자는 가입자의 개인 키에 액세스할 수 없습니다.

(iii) 인증서에 포함된 정보와 관련하여 가입자가 IA에 확인한 모든 사항은 사실입니다.

(iv) 인증서에 포함된 모든 정보는 가입자가 승인하거나 통지한 범위까지 사실이며, CPS § 6.1에 명시된 중요한 정보의 허위 사항도 IA에 즉각 통지하지 않습니다.

(v) 인증서는 이 CPS에 따라 허가된 법적 용도로만 사용됩니다.

(vi) 가입자는 IA가 아닌 최종 사용자이며, 따라서 가입자는 IA와의 명시적 서면 동의 없이 인증서에 표시된 공용 키에 해당하는 개인 키를 사용하여 인증서(또는 기타 인증된 공용 키 서식)나 CRL에 서명할 수 없습니다.

인증서를 승인함으로써 가입자는 본 CPS와 해당 가입자 계약에 포함된 계약 조건과 규정에 동의할 것을 약속합니다.

7.3 가입자의 개인 키 누설 방지 의무

인증서를 승인하면 가입자는 개인 키 제어, 신뢰할 수 있는 시스템 사용을 비롯하여 개인 키 손실, 누설, 수정 또는 무단 사용 방지를 위한 적절한 예방 조치를 강구할 의무를 지게 됩니다.

7.4 가입자에 의한 배상

인증서를 승인함으로써 가입자는 IA, CROSSCERT와 VERISIGN, 그들의 대리인 및 계약자가 인증서의 사용이나 게시로 인하여 발생시키거나, 다음의 요건으로 인하여 발생시키는 책임을 초래하는 행동 및 생략, 손실, 피해, 그리고 모든 소송 및 합리적인 변호 비용을 포함하는 모든 비용에 대하여 IA, CROSSCERT와 VERISIGN, 그들의 대리인 및 계약자에게 배상하고 이들에게 피해가 가지 않도록 보호할 것을 약속합니다. I) 가입자나 가입자가 인증한 사람의 지시에 따르는 사람의 거짓 또는 잘못된 진술을 한 경우, II) 가입자가 부주의로 혹은 IA, CROSSCERT와 VERISIGN, 또는 인증서를 수신하거나 신뢰하는 사람을 속이기 위해 고의로 진술 및 생략을 하여 중요한 사실을 밝히지 않는 경우, III) 가입자의 개인 키 보호나 신뢰할 수 있는 시스템 사용을 하지 못한 경우 또는 그 외에 가입자의 개인 키 손상, 손실, 누설, 수정, 무단 사용을 예방하기 위한 필요한 조치를 취하지 못한 경우.

등록 대리인의 요청에 의해 인증서가 발행될 경우 대리인과 가입자 쌍방은 본 조항의 내용에 의거하여 IA, CrossCert와 VeriSign, 그들의 대리인과 계약자들에게 연대 배상합니다. 가입자는 대리인이 잘못 진술하거나 생략한 내용을 발행자에게 통지할 의무를 지속적으로 갖습니다.

7.5 발행

가입자가 인증서를 승인하면 IA는 IA와 CrossCert가 지정한 CrossCert 저장소를 비롯한 기타 저장소에 인증서 사본을 발행합니다. 가입자는 다른 저장소에 자신들의 CrossCert PCS 인증서를 발행할 수 있습니다.

8. 인증서 사용

이 단원에서는 디지털 서명 사용과 CrossCert 발행 인증서와 일치하는 디지털 서명 메시지와 관련하여 본 CPS("당사자" 정의 *참조*)의 제어를 받는 실체의 인증서 사용자의 권리와 의무에 대해 설명합니다.

인증서 "사용자" 즉, 가입자와 신뢰 당사자로 구성된 양 당사자에게는 각자의 권리와 의무에 적용되는 다음 규정이 통지됩니다. 다음과 같은 경우 이 규정은 쌍방이 합의한 것으로 간주되어 효력을 갖습니다. (i) IA가 CPS를 발행할 때, (ii) 신청자나 가입자가 인증 신청서를 제출할 때, (iii) 인증서 수신자나 상대방이 인증서의 공용 키를 참조하여 인증서의 신뢰성이나 디지털 서명을 확인할 수 있을 때.

8.1 디지털 서명 확인

디지털 서명 확인은 (i) 디지털 서명이 서명자의 인증서에 표시된 공용 키에 해당하는 개인 키로 작성되었는지 그리고 (ii) 디지털 서명 작성 후 관련 메시지가 변경되지 않았는지를 확인하기 위해 실행합니다.

이러한 확인은 CPS에 의거한 다음과 같은 방법으로 실행됩니다.

• **디지털 서명 인증 체인 구축** – 디지털 서명은 인증 체인 확인으로 입증됩니다.

• **식별된 인증 체인이 디지털 서명에 가장 적합함을 보증** – 교차 인증처럼 주어진 인증서에서 해당 루트로 가는 하나 이상의 유효한 인증 체인을 끌어낼 수 있습니다. 해당 루트로 가는 인증 체인이 한 개 이상일 경우 디지털 서명을 확인하는 사람은 인증 체인을 선택 및 확인에 대한 여러 가지 선택권을 갖습니다. 예를 들어, "신뢰도가 낮은" PCA가 "신뢰도가 높은" PCA를 인증할 수도 있습니다. 이 경우 디지털 서명 확인자는 신뢰도가 낮은 PCA보다 신뢰도가 높은 PCA, 혹은 VR에서 인증 체인을 종료하는 것을 선호할 수 있습니다.

• **체인에 있는 인증서의 취소나 일시 정지에 대해 CrossCert 또는 기타 저장소 점검** – 수신자는 취소나 일시 정지를 확인할 수 있는 디지털 서명이 작성되는 동안 운영 기간을 일찍 종료하는 효과가 있으므로 서명자에서 PCS 내부의 승인 가능한 루트로 이어지는 체인이 있는 인증서를 일부 취소하거나 일시 정지 여부를 지정해야 합니다. 이것은 두 가지 방법으로 확인할 수 있습니다. CrossCert 저장소의 최근 취소 상태를 조회하거나 인증 체인에서 CRL을 제공할 수 있습니다. 이러한 CRL은 체인의 인증서 취소 상태를 결정하는데 사용됩니다.

• **디지털 서명이 첨부된 데이터 삭제** – 디지털 서명을 확인하려면 서명된 데이터를 정확하게 알아야 합니다. 공용 키 암호화 표준(PKCS)에서 서명된 표준 메시지 서식은 서명된 데이터를 정확하게 나타내도록 지정됩니다.

• **디지털 서명 작성 시간과 날짜 표시** – 디지털 서명이 부인 방지를 지원하려면 해당 디지털 서명에 첨부되는 데이터에는 타임 스탬프가 들어가거나 참조되어야 합니다. 타임 스탬프는 디지털 서명이 첨부된 날짜와 시간을 나타냅니다.

• **서명자에 의한 보증 구축** – 서명자에 의한 디지털 서명의 용도나 의미 지정에 여러 가지 기술적 수단을 사용할 수 있습니다. EDI와 같은 형식 프로토콜에서 디지털 서명은 정확한 의미 전달을 위해 정의된 의미 규칙으로 지정된 보안 서비스로 분류됩니다. 확인자는 인증서를 표준과 임시 중 한가지로 지정해야 합니다.

• **체인의 모든 인증서가 최종 사용자의 개인키 사용을 인증하도록 보증** – IA는 인증서와 인증서를 발행한 공용 키의 용도를 제한할 수 있습니다. 이러한 제한은 인증서 참조에 의해 표시되거나 통합되고 인증서를 신뢰할 수 없는 상황에서 수신자에게 경고 수단을 제공합니다. 인증서 확인자는 체인의 인증서가 적절한 최종 사용자의 인증서 사용을 거부하지 않도록 경고와 제한 사항에 대해 인증서 내용을 검토합니다.

• **인증 체인 확인** – 각 IA는 자체 서명된 공용 키를 가진 VR이나 기타 루트를 제외한 상위 IA에 의해 인증되고, 해당 상위 IA와 관련된 신뢰성을 계승합니다. 각 IA는 최소한 해당 상위 IA와 동일한 수준의 신뢰성을 가지는 것으로 간주됩니다. 인증 체인 확인은 인증 체인에 이어 최종 사용자의 인증서를 확인하는 절차입니다.

8.2 최종 사용자 인증서 확인의 효과

디지털 서명은 (i) 유효한 인증서의 운영 기간 중에 작성되었고 그러한 서명이 (ii) 인증 체인의 확인으로 적절하게 검증될 수 있으며, (iii) 신뢰 당사자가 서명자의 CPS 요건 불이행 사실을 모르고 있거나 통보 받지 못하고, (iv) 신뢰 당사자가 본 CPS의 모든 요구 사항을 준수한 경우 작성자를 구속합니다.

인증서 사용은 사용자 측의 어떤 사람을 대신하여 행동하거나 또는 특정 동작을 수행할 *권한*을 입증하지 않습니다. 디지털 서명된 메시지의 확인자는 인증서와 디지털 서명의 신뢰에 앞서 정당한 의무 이행과 합리적인 판단 실행을 할 전적인 책임이 있습니다. 인증서는 이 CPS에 특별히 제공된 경우를 제외하면 IA의 권리나 권한 양도가 아닙니다.

8.3 디지털 서명 확인 실패에 따른 절차

확인할 수 없는 디지털 서명을 신뢰하는 사용자는 관련된 모든 위험을 부담하며, 디지털 서명이 CPS §§ 8.4 – 8.6 이하의 가입자 서명으로 유효하다는 어떠한 가정을 할 권한도 없습니다.

8.4 디지털 서명의 신뢰

가입자의 디지털 서명이 있는 메시지 수신자는 다음과 같은 경우 가입자에 대한 바인드로 해당 디지털 서명을 신뢰할 수 있습니다.

(i) 유효한 인증서의 운영 기간 중에 디지털 서명을 작성했고 유효한 인증 체인으로 확인할 수 있는 경우

(ii) 신뢰성이 해당 환경에서 합리적인 경우.사용자 환경에서 추가 보증이 필요한 경우 신뢰 당사자는 해당 신뢰성에 합당한 보증을 획득해야 합니다.

또한 확인자는 인증서의 클래스와 상태(표준 또는 임시)를 고려해야 합니다. 확인된 디지털 서명의 신뢰 여부에 대한 최종 결정은 전적으로 확인자의 몫입니다.

8.5 작성

유효한 인증서에 나열된 공용 키가 확인한 디지털 서명 메시지는 용지에 작성하고 서명한 메시지와 마찬가지로 유효하며 강제성을 띕니다.

8.6 서명

법 규정이나 적용 가능한 업무 준칙이 서명을 요구하거나 서명하지 않으면 특정 결과를 나타내는 부분에 대해 메시지는 메시지 서명을 위해 서명자가 첨부하고 이어서 유효한 인증서에 나열된 공용 키 참조가 확인한 디지털 서명을 사용하여 규정을 충족시킵니다.

8.7 보안 방책

메시지가 있는 CrossCert PCS 발행 인증서 사용자는 메시지에 적절한 보안 방책을 적용하여 요청 시 메시지 인증을 제공하고 데이터 신뢰성을 지원할 수 있습니다.

8.8 인증서 발행

인증된 IA만 인증서를 발행할 수 있습니다.

9. 인증서 일시 중지 및 취소[1]

이 단원에서는 인증서를 일시 중지 하거나 취소할 수 있는(또는 해야 하는) 상황에 대해 설명하며 인증서의 일시 중지 및 취소, 재시작 절차에 대해서도 자세히 설명합니다.

9.1 일반적인 일시 중지나 취소 사유

다음과 같은 경우 인증서는 일시 중지되거나 취소됩니다.

- 인증 주체의 개인 키가 손실, 도난, 수정, 유출 또는 기타 손상된 경우
- IA나 가입자 등 인증 주체가 CPS의 중요 의무를 이행하지 않은 경우
- 천재지변, 자연 재해, 컴퓨터나 통신 장애, 법령이나 규제 또는 기타 관련 법률의 변경, 수출 통제 관리 담당 부서 및 기타 정부의 공식적인 조치, 또는 기타 사용자의 합리적인 통제 수준을 넘어서는 사유로 인해 이 CPS에 명시된 사용자 의무 이행이 지연되거나 이행되지 못하고 그 결과로 다른 사용자의 정보가 심각하게 위협받거나 손상될 소지가 있는 경우
- 가입자나 위임받은 대리인이 정당하게 요청한 경우

9.2 IA 인증서의 일시 중지 또는 취소

다음 사항의 경우 IA는 하위 IA의 동의 여부와 상관없이 하위 IA 인증서를 일시 중지하거나 취소해야 합니다.

- IA가 인증서에 표시된 중요 사항을 허위로 판명하는 경우
- 인증서 발행의 중요한 선행 조건이 충족되지 않거나 보류된 경우
- 하위 IA의 개인 키나 신뢰할 수 있는 시스템이 인증서의 신뢰성에 심각한 영향을 미칠 정도로 손상된 경우
- 인증 주체(여기서는 IA)가 이 CPS의 중요 의무를 이행하지 않은 경우

IA는 이러한 일시 중지나 취소 사실을 즉시 하위 IA에 통지해야 합니다.

참고:현재는 사용자 등록 인증서를 일시 중지할 수 없습니다. 일시 정지는 추가 서비스로 제공될 예정입니다. CrossCert는 일시 중지 서비스를 제공하게 되는 경우 웹 사이트의 ***업무 갱신 및 통지*** *섹션에 해당 사실을 고시합니다. 취소의 경우는 최종 사용 등록자와 IA 인증서에 모두 사용할 수 있습니다.*

9.3 IA의 요청에 의한 일시 중지

IA는 정당한 권한이 있는 하위 IA의 대표 또는 하위 IA에 상당하거나 하위 IA 개인 키의 손상을 알 수 있는 사용자(예:하위 IA의 대리인 또는 고용인 등)가 요청 할 때 하위 IA 인증서를 일시 중지시킵니다. 이러한 일시 중지는 다음의 표 11에 설명된 일시 중지 선행 조건에 따라 실행되어야 합니다.

	IA 인증서 일시 중지 선행 조건
VR	해당 없음

[1] 인증서 유효에 필요한 중요한 사항이 손상된 경우 직접 서명한 취소 절차를 처리합니다.

PCA와 CA	• IA의 요청 • 주요 IA나 그 대리인(등록 정보로 미리 제출된 음성이나 암호를 통해 인증된)이 인증된 녹음이나 팩스 또는 음성 메시지 형식으로 요청 **참고:** IA 발행에는 그러한 일시 정지를 요청하는 사람의 신분 또는 대리인 확인에 대한 추가 확인 작업이 필요 없습니다. 인증서가 인증된 지시에 따라 하자 없이 작동된 경우 CPS § 9.3에 의해 하위 IA 인증서를 일시 정지시키는 IA는 해당 인증서의 권한 없는 일시 중지에 대해 책임지지 않습니다.

표 11 – 일시 중지 선행 조건

하위 IA 인증서를 일시 중지시키는 IA는 일시 중지 요청이 있을 경우 CPS § 9.1에 열거된 일시 중지나 취소 사유를 확인한 다음 해당 인증서를 일시 중지하거나 취소하게 됩니다.

9.4 IA의 인증서 일시 중지 종료

(i) 주요 IA가 일시 중지 종료를 요청하고 해당 IA가 주요 IA의 신분을 확인한 경우, (ii) 일시 중지 요청이 일시 중지된 IA의 인증 없이 이루어졌다고 IA가 판단한 경우, 또는 (iii) 일시 중지의 정당한 사유가 없다고 IA가 판단한 경우에 IA는 인증서 일시 중지를 종료(즉, 인증서를 복원)할 수 있습니다.
IA에서 취소

9.5 가입자의 요청에 의한 취소

취소 요청자가 실제 가입자임을 확인하는 즉시 IA는 가입자 요청에 따라 인증서를 취소해야 합니다.

9.6 잘못된 발행에 의한 취소

IA는 인증서가 CPS 요청 절차에 따라 발행되지 않았음을 발견하고 확인하는 즉시 인증서를 취소해야 합니다. IA가 취소 사유를 확인하기 위해 조사하는 동안 인증서는 일시 중지됩니다. 표 12는 취소의 선행 조건입니다.

	IA 인증서 취소 선행 조건
VR	해당 없음
PCA와 CA	• 하위 IA의 인증서 취소 요청 • 주요 IA나 그 대리인이 인증된 녹음이나 팩스 또는 음성 메시지 형식(등록 정보로 미리 제출된 음성이나 암호를 통해 인증된)으로 요청

표 12 – 취소의 선행 조건

9.7 일시 중지나 취소 통지 및 확인

인증서를 일시 중지하거나 취소할 경우 IA는 CrossCert 저장소에 일시 중지나 취소 통지를 게시해야 합니다. IA는 다음 중 하나 이상을 게시할 수 있습니다.

• 보안 채널에서 확인할 수 있는 취소 및 일시 중지된 인증서 목록

• 취소 및 일시 중지된 인증서를 지정하는 인증서 취소 목록(CRL).CrossCert 저장소에 관련 사항에 대한 특별한 언급이 없으면 IA는 클래스 2와 클래스 3 CA 및 하위 CA에 대한 CRL의 경우 하루 한 번 이상, PCA에 대한 CRL의 경우 한 달에 한 번 이상 게시해야 합니다. CRL은 IA가 지정하는 비상 사태의 경우에도 게시될 수 있습니다.

• PCA에 의해 발행된 복합 CRL. 이 PCA는 해당 IA가 CrossCert 저장소에 게시한 CRL에서 생성됩니다.

IA는 요청자가 해당 서비스에 필요한 요금을 지불하고 요청할 경우 다음의 일시 중지 및 취소 통시 서비스도 제공할 수 있습니다.

• 해당 인증서의 주체가 생성한 디지털 서명 메시지 수신자가 요청하는 경우 인증서의 일시 중지나 취소를 확인

• 지정된 인증서의 일시 중지나 취소 시 IA가 요청자에게 해당 내용을 통지하는 “푸시 서비스”

9.8 일시 중지나 취소의 결과

9.8.1 인증서 관련 내용

가입자 인증서를 일시 중지 하거나 영구 취소하면 인증서의 운영 기간은 즉시 종료됩니다. 이와 유사하게, IA에 발행된 인증서의 경우 IA 인증서의 운영 기간을 종료하면 해당 IA의 인증서 발행 권한은 취소되지만 해당 IA가 이미 발행한 인증서는 운영 기간이 종료되지 않은 한 그 유효성에 영향을 미치지 않습니다.

9.8.2 기본 의무 관련 내용

인증서의 일시 중지나 취소는 이 CPS에 작성 또는 전달된 어떠한 계약상의 기본 의무에도 영향을 미치지 않습니다.

9.9 일시 중지나 취소에 대한 개인 키 보호

일시 중지나 취소된 인증서에 포함된 공용 키에 대응하는 개인 키는 일시 중지 기간과 적용 가능한 보유 기간의 취소 시, 삭제되지 않는 한 신뢰할 만한 방법으로 가입자에 의해 보호됩니다.

10. 인증서 만료

이 단원에서는 인증서 만료와 관련한 당사자 간의 의무에 대해 설명합니다. 인증서 만료는 일시 중지나 취소와는 다릅니다(CPS § 9*참조*).CPS § 6.9에 인증서의 유효 기간 및 운영 기간에 대해 설명되어 있습니다.

10.1 만료전 통지

IA는 E-mail을 통해 가입자에게 인증서 만료가 임박했음을 알립니다. 이러한 만료 전 통지는 가입자의 재등록이나 갱신 처리 편의를 위한 것입니다.

10.2 인증서 만료가 기본 의무에 미치는 영향

인증서 만료는 이 CPS에서 작성 또는 전달된 기본 의무의 효력에 영향을 미치지 않습니다.

10.3 재등록과 가입자 갱신

가입자 갱신과 재등록은 각각 다음 과정으로 시작됩니다.

클래스 1	클래스 2	클래스 3
초기 신청서와 동일한 과정.	초기 신청서와 동일한 과정.그러나 인증 신청자는 변경되거나 새로운 정보만 제출하면 됩니다.	초기 신청서와 동일한 과정.그러나 인증 신청자는 변경되거나 새로운 정보만 제출하면 됩니다.

표 13 – 갱신 및 재등록 요청

갱신과 재등록에 대한 요구 사항은 CrossCert의 판단에 따라 달라집니다. 재등록 및 갱신에 대한 최신 요구 사항은 https://www.crosscert.com의 CrossCert 저장소에서 확인할 수 있습니다.

11. 발행 기관과 CROSSCERT의 의무 및 동 의무에 대한 제한

본 조항은 CrossCert의 환불정책, 발행 기관과 CrossCert가 행한 보증과 약속 그리고 동 의무에 대한 면책과 제한을 요약하여 참고로 제공합니다.

11.1 환불 정책

CrossCert 는 인증의 운용과 인증서 발행을 시행함에 있어 매우 엄격한 관행과 정책을 고집합니다. 그럼에도 불구하고 가입자가 자신에게 발행된 인증서에 완전하게 만족하지 못하는 경우 가입자는 CrossCert에 발행일로부터 30일내에 인증서 의 발행 취소 및 환불을 요청할 수 있습니다. 최초 30일의 기간 이후 가입자는 CrossCert가 가입자 또는 가입자의 증명서와 관련된 본 CPS에 의한 보증이나 기타 중대한 의무를 위반한 경우 그 인증서의 취소를 요구하여 환불을 요구할 수 있습니다. CrossCert가 가입자의 인증서를 취소한 이후 CrossCert는 그 인증서에 대하여 지급한 해당 요금전액을 가입자의 신용카드구좌에 신속하게 크레딧을 주거나 (만일 인증서가 신용카드로 지불된 경우) 또는 수표로 환불합니다. 환불요청을 하기위해서는 https//www.crosscert.com/repository/refund 주소로 들어가서 환불요청서 양식을 기입하여야 합니다. 본 환불정책은 유일한 구제책은 아니며 가입자들이 이용 가능한 다른 법적구제수단을 제한하지 아니합니다.

11.2 제한된 보증과 기타 의무들

발행 기관 (그리고 참조된 CPS조항에 명시한 범위 내에서 CrossCert)은 다음을 보증하고 약속합니다.

. CPS 제2조 (CrossCert 인증 하부구조)에 기술된 CrossCert 저장소의 설치 및 운용을 포함한 하부구조 및 인증서비스를 제공하는것,

. CPS 제3조 (인증 운용을 위한 기초)에 제시된 발행 기관의 키 생성, 키 보호 및 비밀공유절차를 포함한 CrossCert의 PKI를 위한 통제와 기초를 제공하는 것,

. CPS 제5조 (인증서 신청확인)에 규정된 바와 같이 지시된 인증서의 종류에 대한 신청확인절차를 수행하는 것,

. CPS 제6조에 의하여 인증서를 발행하는 것과 CPS 제6.5조 (인증서 발행 시의 발행기관 진술)에 제시된 가입자와 신뢰 당사자에의 각종 진술에 대한 보장을 하는 것,

. CPS 제6.6조 (공표시의 IAS 요건) 및 CPS 제7.5조(공표)에 의하여 승인된 인증서를 공표하는 것,

. CPS 제8조 (인증서의 사용)에 의하여 발행 기관의 의무를 수행하고 인증서를 사용하는 가입자와 신뢰 당사자의 권리를 지원하는 것,

. CPS 제9조 (인증서 정지 및 취소)에서 요구된 바와 같이 인증서를 정지하고 취소하는 것,

. CPS 제10조 (인증서 만료)에 기술된 바와 같이 인증서의 만료, 재등록 및 갱신을 규정하는 것과

. CPS 제12조 (기타 규정)에 포함된 규정을 준수하는 것.

추가로 발행 기관과 CrossCert는 그들이 CrossCert 저장소를 통하여 반대의 통지를 하지 않는 한 그들 자신의 개인 키가 손상되지 않는다는 것을 보증합니다.

발행 기관과 CrossCert는 본 CPS에 의하여 추가의 보증을 하거나 추가 의무를 지지 아니합니다.

11.3 발행 기관과 CrossCert의 의무에 대한 면책과 제한

전술 (CPS 제11.2조) 규정에 명시적으로 규정한 것을 제외하고는, 발행 기관과 CrossCert는 상품성, 특정목적에의 적합성, 그리고 제공된 정보의 정확성을 포함하여 여하한 형태의 보증과 의무를 지지 아니하며, 과실이나 상당한 주의의 결여로 인한 여하한 책임도 지지 아니합니다.

전술한 CPS 제11.2조에서 명시적으로 기술된 것을 제외하고는, 발행 기관과 CrossCert는

. 인증서에 포함된, 또는 기타 발행 기관이나 CrossCert가 혹은 이들을 위하여 편찬, 발행, 또는 배포된 정보의 정확성, 진정성, 신뢰성, 완결성, 현재성, 상품성 또는 적합성을 보장하지 아니하며

. 인증서의 내용이 본 CPS의 내용을 근본적으로 준수하는 한 인증서에 포함된 정보의 진술에 대한 책임을 지지 아니합니다.

. 여하한 인증서나 전언문의 용인도 보증하지 아니합니다 (용인은 오직 법률과 당해 분쟁해결기구에 의해서만 결정되기 때문입니다). 그리고

. 여하한 소프트웨어의 보증도 하지 아니합니다.

11.4 손해의 특정 부분에 대한 배제

발행 기관이나 CrossCert는 본 CPS에 의하여 제공되거나 고려된 인증서, 디지털서명, 또는 기타 거래나 서비스의 사용, 인도, 이행 또는 불이행으로 인하여 발생한 간접적, 특별한, 부수적

또는 결과적 손해배상액, 또는 이익의 상실, 자료의 상실 기타 간접적, 결과적 또는 징벌적 손해배상액에 대하여는 비록 발행 기관이나 CrossCert, 혹은 양자 모두가 그러한 손해의 발생가능성을 통지받았다 하더라도 책임을 지지 아니합니다.

11.5 손해와 손실의 제한

인증에 있어서 발행 기관 및 발행 기관의 인증서가 속한 인증체계의 모든 상위 발행 기관(그리고 CrossCert, 명시된 바와 같이)은 모든 당사자 (가입자, 신청인, 수령인 또는 신뢰당사자를 포함하여, 그러나 이에 한정되지 아니하고)에게 총계적으로 아래의 표14에 정해진 해당 책임한도액을 초과하여 배상책임을 지지 아니합니다.

발행 기관과 CrossCert로부터의 특정한 인증서에 관련된 모든 당사자에 대한 전체적인 책임총액은 디지털서명 및 당해 인증서에 관련된 거래 전체에 대하여 다음의 한도액을 초과하지 아니합니다.

	배상책임한도액
종류 1	120,000원
종류 2	6,000,000원
종류 3	12,000,000원

표 14 – 배상 책임 한도표

손해 배상액에 대한 본 제한은 발행 기관 또는 CrossCert가 발행 , 관리, 사용, 정지 또는 취소하는 인증서 또는 만료되는 인증서를 신뢰 또는 사용함으로써 가입자, 신청인, 수령인 또는 신뢰 당사자를 포함하나나 이에 한정되지 아니하는 모든 사람에게 , 야기되는 직접적, 보상적, 간접적, 특별한, 결과적, 예시적, 또는 부수적인 것을 포함하나 이에 한정되지 아니하는 모든 종류의 손실 또는 손해에 적용됩니다.

손해 배상액에 대한 본 제한은 계약, 불법행위 또는 기타 여하한 형태의 책임청구에도 적용됩니다. 매 인증서에 대한 배상한도액은 그러한 인증서에 관련된 디지털서명, 거래, 또는 청구의 수에 관계없이 적용됩니다. 배상한도액을 초과하는 경우에는 관할 법원의 명령이 달리 없는 한, 이용 가능한 책임한도액은 최종적인 분쟁의 해결을 가장 빨리 이룬 청구에 먼저 할당됩니다. 청구자간의 책임한도액에 대한 할당방법에 관계없이 CrossCert는 어떠한 경우에도 각 인증서에 규정된 책임한도액총계를 초과하여 지급할 의무는 없습니다.

11.6 신뢰 당사자에 대한 가입자의 배상 책임

본 CPS에 기술된 가입자의 기타 의무를 제한함이 없이, 가입자는 그들이 인증서에 하나 이상의 디지털 서명을 확인하고 그 인증서에 포함된 진술을 합리적으로 신뢰한 제3자에게 행한 인증서의 잘못된 진술에 대하여 책임을 집니다.

11.7 신뢰 관계의 부재

발행 기관과 CrossCert는 가입자나 신뢰 당사자의 대리인, 신뢰관계인, 수탁자 또는 기타 대표자가 아닙니다. 발행 기관 (또는 CrossCert)과 가입자간의 관계 또는 발행 기관 (또는 CrossCert)과 신뢰 당사자간의 관계는 대리인과 당사자의 관계가 아닙니다. 가입자나 신뢰 당사자는 발행 기관 (또는 CrossCert)을 계약이나 다른 방법으로 구속할 권한이 없습니다. 발행 기관과 CrossCert는 명시적 또는 묵시적으로, 외관상 또는 다른 방법으로 어긋나는 진술을 하지 아니합니다.

11.8 위험한 활동

CrossCert의 공적 인증서비스는 위험한 상황에서의 통제장치로서의 사용 또는 재판매, 또는 그 운용의 실패가 직접적으로 사망, 상해 또는 심각한 환경파괴를 초래하는 핵시설의 운용, 항공기 운항 또는 통신 시스템, 항공교통통제 시스템, 또는 무기통제 시스템과 같은 절대 안전한 수행을 요하는 용도로 구상, 의도, 또는 허가되지 아니하였습니다.

12. 기타 규정들

본 조항은 다른 조항에서 취급하지 않은 본 CPS의 일반적 내용과 조건을 제시합니다.

12.1 규정의 상충

본 CPS와 다른 규칙, 기준 또는 계약서간에 상충이 있는 경우, 가입자는 본 CPS의 규정에 구속을 받습니다. 다만 다음의 계약 즉 (i) 본 CPS의 최초 공개 이전에 체결된 계약 또는 (ii) 계약당사자에 대하여 그 계약서가 적용되는 본 CPS를 명시적으로 무용화 시키는 계약의 그리고 법률에 의하여 본 CPS의 규정이 금지되는 한도에서는 예외입니다.

12.2 수출 법규의 준수

CrossCert의 PCS와 관련하여 사용된 특정 소프트웨어의 수출은 해당 정부기관의 승인을 필요로 할 수 있습니다. 당사자들은 해당 수출법규를 준수해야 합니다.

12.3. 준거법

대한민국의 법률은 계약 또는 다른 법률의 선택규정의 실체 여부를 불문하고 본 CPS의 집행가능성, 구성, 해석, 및 유효성을 지배합니다.

12.4 분쟁 해결, 법정지 선택 및 추정

12.4.1 분쟁 당사자 간의 통지

본 CPS 또는 발행 기관이 발행 한 인증서와 관련한 분쟁에 대하여 분쟁해결조치 (아래에 자세히 기술한, 소송 또는 중재를 포함하여)를 강구하기 이전에, 피해자는 그 분쟁해결을 신의성실로 협상할 목적으로 CrossCert, 해당 발행 기관 및 분쟁의 타방 당사자에게 이를 통지해야 합니다. 만약 당사자가 회합 후 30일 이내에 그 분쟁해결을 위한 협상에 실패하면 당사자는 그 분쟁을 조정에 회부하고 그 조정비용은 균등하게 분담한다. 당사자는 쌍방이 인정하는 조정자를 공동으로 선정하고 신의성실로 조정에 참여하며 30일 동안 협상하기로 합의합니다.

12.4.2 공식적 분쟁 해결

본 CPS의 규정을 시행하기 위한 소송 또는 본 CPS또는 본 당사자간의 관련 영업관계와 관련하여 발생하는 소송은 서울지방법원에 제기되어야 합니다. 이에 각자는 그러한 법원이 그러한 사람에 대하여 독점적인 대인 관할권을 가지고 재판지가 됨을 합의하고 각자는 그러한 법원이 독점적인 관할권 및 재판지를 가진 것으로 합니다.

12.5 승계인과 양수인

본 CPS는 명시적, 묵시적 또는 명백한 당사자의 승계인, 집행인, 상속인, 대표인, 관리인 및 양수인을 위하여 효력을 발생하며 이들을 구속합니다. 본 CPS에 상세히 규정된 권리와 의무는 그러한 양도가 발행 기관 운용의 해지나 중지에 관한 CPS 제3.21조항에 부합하는 조건으로 그리고 또한 그러한 양도 당사자가 양도시에 타방 당사자에게 지닌 기타 채무 또는 의무의 갱신에 영향을 미치지 않는 것을 조건으로 법의 운용 (합병또는 의결권있는 증권에 대한 지배력의 양도의 결과를 포함하여) 또는 다른 방법으로 당사자에 의하여 양도 가능합니다.

12.6 합병

해당 당사자로부터 인증된 전언문이나 문서에 의한 경우와 본 CPS에서 달리 규정된 범위외에는 CrossCert나 모든 발행 기관의 각각의 권리와 의무에 직접적으로 영향을 미치는 본 CPS의 어떤 조건이나 규정도 구두로 변경, 포기, 보완, 수정 또는 해지될 수 없습니다.

12.7 가분성

본 CPS의 어떤 규정이, 또는 그 적용이 어떤 이유로 또는 어떤 범위에서 무효 또는 집행불능인 것으로 발견되면, 본 CPS의 나머지 규정 (그리고 타인 또는 다른 상황에 대한 무효 또는 집행불능인 규정의 적용)은 당사자의 의사를 가장 합리적으로 실행할 수 있도록 해석되어야 합니다. **책임제한, 보증책임이나 다른 채무에 대한 제한 또는 면책, 또는 손해배상의 배제에 대한 본 CPS의 각 규정 및 모든 규정은 가분적이고 타규정으로부터 독립적이며 그 자체로 효력을 가지는 것으로 명시적으로 이해하며 합의합니다.**

12.8 해석 및 번역

달리 규정되지 아니하는 한, 본 CPS는 주어진 상황에서 상업적으로 합리적일 수 있도록 해석되어야 합니다. 본 CPS를 해석함에 있어서는 본 CPS의 국제적인 범위와 적용, 적용에 있어서

통일성 조성의 이익 및 신의성실의 준수에 대한 주의가 주어져야 합니다.

본 CPS의 번역본은 저장소에서 (특정한 비영어본을 입수할 수 있으며) 영어와 비영어가 상충하는 경우에는, 해석의 목적으로, CPS의 본 영어본이 우선합니다.

12.9 불포기

본 CPS규정을 어떠한 사람이 이행하지 못하는 것이, 그 규정이나 다른 규정의 추후 이행을 포기하는 것으로 간주되지 아니합니다.

12.10 통지

본 CPS에 관련된 사람이 본 CPS와 관련하여 통지, 요구 또는 요청을 하기 원하거나 해야 할 경우에는, 그러한 통신은 본 CPS의 요구에 부합하는 전자적으로 서명된 전언문에 의하거나 또는 서면으로 하여야 합니다. 전자통신은 발송인이 수령인으로부터 유효하고 전자적으로 서명된 수령의 확인을 수령함과 동시에 유효합니다. 그러한 확인은 5일내에 수령되거나 또는 서면통지가 그 후에 통보되어야 합니다. 서면 통보는 배달을 서면으로 확인하는 급송배달서비스에 의하여 교부되거나 또는 배달증명을 요구하는 선불의 증명 또는 등기우편으로 다음의 주소에 교부되어야 합니다.

CrossCert에게 발송할 경우:
우편 번호 137-725
서울시 서초구 서초동 1674-4
하림 빌딩 9층
한국전자인증㈜
(TEL: 02-3019-5500)

CrossCert 또는 발행 기관에 의하여 다른 사람의 기록상의 최근의 주소로 보낼 경우:
한국전자인증㈜에 기록되어 있는 주소

CrossCert가 아닌 발행 기관은 CrossCert 발행 기관에게 CrossCert 발행 기관이나 CrossCert에게 영향을 미치는 CrossCert 아닌 발행 기관에게 행하여진 여하한 법적통지를 즉시 알려야 합니다.

12.11 본 CPS의 제목과 부록

표제, 부표제 및 본 CPS에 있는 기타 표제는 편의와 참조 목적만을 가지며, 본 CPS의 규정을 해석, 파악, 또는 시행하기 위하여 사용되지 아니 합니다. 본 CPS의 정의를 포함한 부록은 모든 목적으로 본 CSP의 구속력 있는 불가분적 일부분입니다.

12.12 발행 기관에 기록되어 있는 가입자 정보의 변경; CPS의 변경

12.12.1 발행 기관이 유지 관리 하는 가입자 정보의 변경

가입자는 인증서에는 나타나지 않으나 발행 기관에 기록되어 있는 특정정보 (전형적으로는 가입자 계약서나 인증신청서에 제공된 정보)를 CPS 제12.10조 (통지)규정에 의하여 30일전에 사전 통지를 함으로써 변경할 수 있습니다. 그러한 정보의 변경은 해당 30일의 기간이후부터 지나면 유효합니다.

12.12.2 CPS의 변경

12.12.2.1 일반적 변경

CrossCert는 수시로 본 CSP를 변경(미래에 적용되도록 그러나 소급적으로 안됨)할 권리가 있습니다. CrossCert는 변경사항을 CrossCert저장소에 CPS의 변경본 형태로 또는 CrossCert 저장소의 업무갱신 및 통지부분에 보관할 권리가 있습니다.

12.12.2.2 업무 갱신 및 통지

CrossCert 저장소의 업무갱신 및 통지부분에 보관되는 본 CPS의 변경본 (https//www.crosscert.com/repository/updates 참조)은 CPS를 변경하는 효과를 가집니다. 그러한 변경은 CPS 참고본의 상충되거나 지정된 규정들을 대체합니다.

12.12.2.3 중요 변경

CPS의 중요 변경은 CrossCert가 15일의 기간 종료이전에 저장소의 변경에 대한 취소통지를 공표하지 않는 한, CPS 제12.12.2.1조항에 의하여 CrossCert 저장소의 변경을 공표한 후 15일의 경과로 발효합니다.

12.12.2.4 중요 변경의 예외

(CrossCert가 CPS를 변경하지 아니하는 것이 CPS 또는 그 일부분을 위태롭게 한다면) CPS의 제12.12.2.3조항에도 불구하고 CrossCert가 CPS에 중요 변경본을 공표할 경우, CPS 제12.12.2.1조항에 의하여 CrossCert 저장소에의 공표와 동시에 즉시 효력을 발생할 것입니다.

12.12.2.5 중대하지 않은 변경

CPS에 대한 비중요 변경은 CPS 제12.12.2.1조항에 의하여 CrossCert 저장소에의 공표와 즉시 유효합니다. 변경을 비중요 변경으로 지정하는 CrossCert의 결정은 전적으로 CrossCert의 재량사항입니다.

12.12.2.6 변경에 대한 동의

변경본 발행후 15일 이내에 자신들의 인증서 취소청구를 하지 않는 인증서 신청인 또는 가입자의 결정은 변경에 대한 계약으로 간주합니다. CrossCert 저장소의 https://www.crosscert.com/repository/updates에 위치한 “업무갱신관행 및 통지”부분을 참조하시기 바랍니다.

12. 13 보안 자료에 대한 소유권

달리 합의하지 않는 한, 다음의 보안관련 정보자료 및 데이터는 아래에 지명된 당사자의 재산으로 간주됩니다.

. 인증서: 인증서는 각 발행 기관의 사유 재산입니다.

CrossCert CA나 CrossCert 부속 CA가 발행한 인증서는 다음과 같은 저작권표시를 합니다: CrossCert과 관련하여 “Copyright (c) 1999 CrossCert, Inc., 모든 저작권 본사 보유함” 또는 "(c) 99". CrossCert의 명시적인 서면 허가없이 그대로 있는 저장소나 디렉토리에 공표될 수 없는 것을 제외하고는, 인증서는 전부 복제되어 배포되는 조건으로 비독점적으로 기술료 지급 없이 복제하고 배포할 허가가 주어집니다. 본 제한은 부분적으로는 그들의 인증서를 무단 발행하는 것에 대한 가입자의 사생활을 보호하고자 함에 그 뜻이 있습니다. 본 저작권 통지에 관한 문의는 CPS 제12.10 (통지)에 열거된 CrossCert 또는 practices@crosscert.com으로 하시면 됩니다.

.CPS: 본 CPS는 CrossCert의 사유재산입니다.

.저명한 이름: 저명한 이름은 당사자 (그들의 고용주 또는 본인)의 사유 재산입니다.

.개인 키: 개인 키는 그것들이 저장되고 보호되는 물리적 매체의 종류를 불문하고 그들 (또는 고용주 또는 본인)을 정당하게 사용하거나 또는 사용할 수 있는 가입자의 사유 재산입니다.

.공용 키: 공용 키는 그것들이 저장되고 보호되는 물리적 매체의 종류를 불문하고 그들 (또는 고용주 또는 본인)을 정당하게 사용하거나 또는 사용할 수 있는 가입자의 사유 재산입니다.

.CrossCert 공용 키: 모든 PCA 공용 키를 포함한 CrossCert 루트 공용 키는 CrossCert 회사의 재산입니다. CrossCert는 신뢰할만한 당사자에게 루트 공용 키가 CrossCert의 권한으로 배포되는 신용할 수 있는 하드웨어 또는 소프트웨어와 관련하여서만 그러한 키를 사용할 수 있도록 허가합니다.

.개인 키의 비밀 지분: 발행 기관의 개인 키에 대한 비밀 지분은 해당 발행 기관의 사유재산입니다.

12.14. 침해 및 기타 손해를 끼치는 자료

인증서 신청자 (그리고 가입이후 가입자)는 신청과 도메인명 및 저명한 이름 (또한인증서의 모든 다른 신청정보)의 사용이 그들의 상표, 서비스표, 상호, 회사명, 또는 다른 지적재산권에 관하여 어떠한 관할권내의 제3자의 권리도 간섭 또는 침해하지 않으며, 도메인명이나 저명한 이름을 계약이나 유망한 영업 이점에 대한 불법적인 방해, 부당 경쟁, 타인의 명예훼손, 자연인 또는 법인을 오인 또는 혼동케 하는 것을 포함하나 이에 한정되지 않는 불법목적으로 사용하지 않음을 (발행 기관에) 진술하며 보증합니다. 인증서 신청자 (그리고 가입이후, 가입자)는 발행 기관을 그러한 방해나 침해로부터 초래되는 손실이나 손해에 대하여 변호, 면책 또는 손해가 없도록 합니다.

발행 기관 및 CrossCert는 인증서에 포함시키기 위하여 CrossCert, 발행 기관 또는 CrossCert 저장소에 제출된 또는 달리 제출되었으나 확인되지 않은 가입자정보 (NSI)에 대하여는 책임을 지지 않습니다. 특히, 가입자는 본 CPS에 의하여 발행된 인증서에 사용하기 위하여 그들이 제출하는 정보의 합법성에 대하여 그 내용이 사용 또는 검토되는 관할지역내에서 전적으로 책임을 집니다. 정보내용의 전송 및 가용성에 관한 법률은 끊임없이 변하고 광범위하게 다를 수 있기 때문에, 인증서 신청자나 가입자의 책임은 발행 기관이 인증서 신청자에게 인증서를 발행하는 당시에 실체하는 법률 뿐만 아니라 그 이후에 제정될 법률에 의해서도 결정됩니다. 인증서 신청자와 가입자는 데이터의 전송 특히 암호화되거나 암호 알고리즘에 관계된 데이터에 관한 다수의 법률이 있으며 이러한 법률은 주마다 또는 국가마다 대폭적으로 상이할 수 있다는 점을 주의해야 합니다. 또한 인터넷이나 사용자/관찰자가 기타 소재한 지역의 통신망에서 내용의 배포를 제한하는 것은 일반적으로 가능하지 않기 때문에 인증서 신청자나 가입자로 하여금 그 내용이 그대로 되거나 사용되는 각 관할지역내의 법률을 준수할 것을 요구합니다.

인증서 신청인 또는 가입자는 CrossCert, 발행 기관 또는 CrossCert 저장소에 (i) 모욕적, 명예훼손적, 외설의, 음란한, 남용적인, 편협한, 증오의, 또는 인종적으로 무례하거나, (ii) 불법행위를 지원하거나 불행행위를 행할 의도로 토의하거나 또는 (iii) 달리 법률을 위반하는 내용을 포함하는 어떤 자료도 제출하지 않습니다.

12.15 요금

CrossCert는 가입자에게 CrossCert의 서비스를 이용한 수수료로서 가입자에게 요금을 청구할 수 있습니다. 그러한 수수료에 대한 현행 요금표는 CrossCert 저장소인 https://www.crosscert.com에 등재되어 있습니다.

12.16 암호 해독 방법의 선택

모든 사람은 그들이 (CrossCert와 발행 기관이 아닌) 그들 각자의 변수, 절차 및 기술을 포함

하여 보안 소프트웨어, 하드웨어 및 암호/전자 서명 알고리즘의 선택을 독자적으로 판단하여서 했으며 그에 전적으로 책임을 지는 것을 인정합니다.

12.17 존속 규정

CPS 제3.9조 (감사), 제3.13조 (기밀정보), CPS 제11조 (발행 기관 및 CrossCert의 의무 및 그러한 의무에 대한 제한) 및 CPS 제12조 (기타 규정)은 본 CPS가 종료된 후에도 존속합니다.

12.18 불가항력

발행 기관이나 CrossCert는 천재지변, 전쟁행위, 전염병, 정전, 화재, 지진 및 기타 재해와 같은 그들의 통제를 벗어난 사건으로부터 초래된 본 CPS하의 의한 보증위반, 이행지체, 또는 불이행에 대하여 책임을 지지 아니합니다.

***

13. 부록

13.1 용어 정의

가

가용성

권한 있는 실체가 필요에 따라 적합하게 정보나 프로세스에 액세스하고 사용함으로써 자원에 정당하게 액세스하여 신속하게 작업을 수행할 수 있는 정도.

가입 인증

개인 가입자에게 발행되는 인증.(*비교:* **개인 가입자**)

가입자

인증에 표시된 공용 키에 대응하는 개인 키의 주체로서 이 키를 사용할 수 있도록 사용 권한을 부여 받은 사람.(*참조:* **주체**; *비교:* **인증 신청자; 사용자**)

가입자 계약

CPS에 따른 지정 공용 인증 서비스 조건에 대해 가입자와 IA 간에 체결된 계약서.

가입자 정보

인증서 신청의 일부로 인증 기관에 제공되는 정보.(*비교:* **인증서 신청**)

감사

제어가 적재적소에서 정확하게 이루어지고 있는지를 확인하는 데 사용되는 절차로정보 시스템에 대한 침입 및 오용을 감지하기 위한 기록 및 분석 작업이 여기에 포함됩니다. 감사 작업으로 발견된 부적합성은 담당 관리 직원에게 보고됩니다.

개인 가입자

단체와 다음 관계를 맺고 있는 사람 (i) 관리자, 임원, 직원, 파트너, 도급 업체, 인턴 및 기타 단체 내부인 (ii) 단체와 계약 관계를 맺고 있는 자로서 단체와의 비즈니스에서 신분이 확실하게 보장되는 거래 기록이 있는 사람.(*비교:* **가입 인증**)

개인 키

디지털 서명 작성 및 알고리즘에 따라 기밀성 보호를 위해 대응 공용 키로 암호화된 메시지나 파일의 암호를 해독하는데 사용되는 (홀더가 비밀로 하는) 수학적 키.(*참조:* **공용 키 암호화; 공용 키**)

갱신

기존 인증이 만료된 다음 동일한 클래스 및 주체에 대한 동일 종류의 새로운 인증을 획득하는 절차.

검증(디지털 서명)

지정된 디지털 서명, 메시지, 공용 키와 관련하여 (i) 인증서에 포함된 공용 키에 대응하는 개인 키로 유효 인증서의 운영 기간 중에 디지털 서명을 작성했고 (ii) 디지털 서명을 작성한 이후 관련 메시지가 변경되지 않았다는 것을 확인하는 것.(*비교:* **인증**; **확정**)

공용 인증 서비스(*참조:* **CrossCert 공용 인증 서비스**)

공용 키

공용으로 사용할 수 있는 키로서 대응하는 개인 키로 작성된 서명을 검증하는 데 사용되는 수학적 키.알고리즘에 따라서는 대응하는 개인 키로 암호 해독이 가능한 메시지나 파일을 암호화하는 데도 공용 키를 사용할 수 있습니다. (*참조:* **공용 키 암호화; 개인 키**)

공용 키 구조(PKI)

인증 기반 공용 키 암호 체제의 실행과 운영을 선택적으로 지원하는 구조, 단체, 기술, 업무 및 절차.PKI는 PCS 및 기타 관련 서비스를 공동으로 제공하고 수행하는 시스템으로 구성됩니다.

공용 키 암호화(*비교:* **암호화**)

수학적으로 연관된 한 쌍의 암호화 키를 사용하는 암호화 형태.공용 키는 원하는 사람이면 누구나 사용할 수 있으며 정보를 암호화 하거나 디지털 서명을 검증하는 데 사용할 수 있는 반면, 개인 키는 홀더만 아는 비밀 키로서 정보의 암호를 해독하거나 디지털 서명을 만드는 데 사용할 수 있습니다.

공용 키 인증(*참조:* **인증**)

공용/개인 키 쌍(*참조:* **공용 키; 개인 키; 키 쌍**)

공유 비밀

암호 작성법 비밀 가운데 여러 개의 토큰에 분할된 부분.

공유 비밀 발행자

공유 비밀을 작성하고 배포하도록 IA에서 지정한 사람.

공유 비밀 홀더

공유 비밀이 들어 있는 물리적 토큰의 권한을 부여 받은 소유자.

공증인

감독 정부 기관으로부터 승인, 서약 및 확인, 증인 또는 증명을 위한 서명, 협상 증서 불복 고지와 같은 공증 서비스를 실행하도록 권한을 부여 받은 자연인.일본의 경우 법무부 장관이 임명하고 권한을 부여한 자연인이 공증법에 명시된 이러한 의무를 수행하도록 되어 있습니다.

공통 키

암호화 하드웨어의 일부 시스템은 비밀 공유 과정에서 보안이 유지되어야 하며, 이 공유 과정에서 보안 상태를 유지하려면 마지막 부분이 하드웨어에 물리적으로 연결되어 있어야 합니다. 이 경우 "공통 키"는 이 마지막 공유를 가리키는 것입니다. 이 키는 한 개인이 지속적으로 소유하는 것이 아니므로 비밀로 간주되지 않습니다.

교차 인증

CrossCert PCA와 다른 인증 도메인을 대표하는 비CrossCert 인증서 발행 실체 중 어느 한 쪽 또는 양쪽 모두가 서로를 주체로 하는 인증을 발행하는 경우.

권한 위임

특정 정보나 자원에 액세스할 수 있는 능력을 포함하는 권리 부여.

기밀성

중요한 데이터가 기밀 상태를 유지하고 권한을 부여 받은 당사자에게만 허용되는 상태.

다

단체

사용자가 가입한 대상 실체.단체도 사용자가 될 수 있습니다.

당사자

CPS에 의해 권리와 의무가 통제되는 실체.인증서 신청자, IA, 가입자, 관련 당사자가 여기에 포함됩니다. (*참조:* **사용자; 발행 기관; 신뢰 당사자**)

대응

동일한 키 쌍에 귀속되는 것.(*참조:* **공용 키; 개인 키**)

데이터

컴퓨터에서 저장, 통신, 처리되는 프로그램, 파일, 기타 정보.

데이터 기밀성(*참조:* **기밀성**)

데이터 무결성

무단으로 데이터가 변경되거나 훼손되지 않은 상태.(*참조:* **위협;** *비교:* **손상**)

데이터베이스

컴퓨터화된 정보 관리 시스템으로 작성, 저장, 처리되는 일련의 관련 정보.

등록

인증 신청자의 인증 신청 과정.

등록 기관

다른 실체를 등록하고 이들 실체에 식별 이름이나 인증 해쉬와 같이 상대적인 식별 값을 지정하도록 신임된 실체.각 등록 도메인에 대한 등록 스키마로 인해 등록된 값은 해당 도메인 내에서 명백해 집니다. (*비교:* **인증 기관**)

등록 문자열

등록 기관의 레코드 내에서 값이 명확하게 나타나는 객체 군으로 등록 및 기록 절차를 조건으로 합니다. 기록된 값은 문자열 형태로 되어 있습니다.

등록 필드 정보
가입자 옵션에 지정된 인증에 들어가는 국가, 우편 번호, 연령, 성 데이터.

디렉토리(*비교:* 저장소)

디지털 서명
최초 메시지와 서명자의 공용 키를 가진 사람이 서명자의 공용 키에 대응하는 개인 키로 변형이 작성되었는지, 변형을 작성한 이후에 메시지가 변경되었는지를 정확히 확인할 수 있는, 비대칭적 암호 시스템을 사용한 메시지 변형.

라

레코드
실체적 매체(문서)에 기록되어 있거나 전자 및 기타 매체에 저장되어 있어 인식 가능한 형태로 복원할 수 있는 정보.“레코드”란 “문서”와 “메시지”라는 두 가지 개념의 상위 집합입니다. (*비교:* **문서; 메시지**)

로컬 등록 기관 관리자 (LRAA)
LRA의 기능을 수행할 책임이 있는 LRA 직원.(*비교:* **로컬 등록 기관**)

로컬 등록 기관(LRA)
IA에서 개인의 인증 지원, 취소 및 이러한 승인을 보조하는 작업을 하도록 승인하는 기관.LRA는 인증 신청자의 대리인이 아닙니다. 따라서 LRA는 LRA의 권한을 위임 받은 LRAA 외의 다른 곳에 인증서 지원을 승인할 권한을 위임하지 못합니다. (*비교:* **로컬 등록 기관 관리자**)

루트
인증 체인 가운데 최초로 인증을 발행하는 IA.사용자는 사전에 루트의 공용 키를 알고 있어야 인증 체인을 확인할 수 있습니다. 루트의 공용 키는 안전한 물리적 배포와 같이 인증을 제외한 몇 가지 메커니즘으로 만들어 집니다.

마

메시지
정보의 디지털 표현; 컴퓨터에 기반을 둔 레코드.**레코드**의 하위 집합.(*비교:* **레코드**)

메시지 무결성 (*참조:* **데이터 무결성**)

명명 기관
명명 규칙 및 절차를 실행하고 특정 부류의 객체에 우선(기본) 이름을 등록 및 지정하

는 통제권을 가진 단체.(*비교:* **명명; CROSSCERT 명명 기관**)

명명

명명이란 확인된 등록 절차에 적합한 구체적 정보를 보관하는 권한 있는 기관이 구체적 발행 절차에 따라 특정 형태의 객체에 설명적 식별자를 지정하는 것을 말합니다. (*비교:* **명명 기관; CROSSCERT 명명 기관**)

무결성(*참조:* **데이터 무결성**)

무료 인증서

IA에서 가입자에게 인증 요금을 부과하거나 보상금을 받지 않고 발행하는 인증서.

문서

컴퓨터 기반의 정보가 아닌 종이 등 실체적 매체에 쓰여진 정보가 들어 있는 레코드.(*비교:* **메시지; 레코드**)

미확인 가입자 정보(NSI)

인증 신청자가 IA에 제출한 정보와 IA의 확정을 받지 못한 인증서에 포함된 정보. IA에서 인증 신청자가 정보를 제출했다는 사실 외에 아무 것도 보증하지 않는 정보.제목이나 전문성 등급, 인가, 등록 필드 정보 등은 별도의 언급이 없는 한 NSI로 간주됩니다.

바

바인딩

지정 실체와 공용 키 간의 관계에 대한 IA(또는 LRA)의 확인.

발행 기관(IA)

CrossCert의 PCS 내에서 인증서를 발행, 일시 중지, 취소하는 VR, PCA, CA(또는 하위 CA).IA는 자체에서 발행하는 모든 인증서와 CRL 상의 식별 이름으로 확인됩니다. IA는 CrossCert의 사전 승인을 받아 인증서 신청의 평가, 승인, 거부 책임을 IA가 CPS §2.1.3에 따라 소유 및 운영하지 않는 하나 이상의 LRA에 위임할 수 있습니다. 이러한 위임이 발생하는 경우 문맥상 필요한 곳에 CPS의 “IA” 조항에 IA의 의무, 대표성, 보증, 부인에 관한 내용이 들어갑니다.

발행

CrossCert 저장소 및 기타 저장소에 정보를 기록하거나 파일화 함으로써 CPS 및 관련 법률에 적합한 방법으로 정보를 공개하고 공용할 수 있게 만드는 것.

발행자(*참조:* **발행 기관**)

별칭

가명.

보안

권한을 부여 받지 않은 액세스나 통제권 상실 또는 영향으로부터 보호되는 상태.완벽한 보안이란 사실상 불가능하며 주어진 보안 시스템의 품질은 상대적입니다. 상태-모델 보안 시스템에서 보안은 다양한 운영에서 보호되는 구체적 "상태"를 말합니다.

보안 서비스

일련의 보안 구조로 제공되고 특정 보안 메커니즘 도구로 실행되는 서비스.액세스 통제와 데이터의 기밀성, 무결성 등이 여기에 포함됩니다.

보안 정책

PCS를 지원하는 신뢰할 만한 시스템으로 보호 방법에 대한 요건과 방법으로 구성된 문서.

보안 채널

보안 위협에 대해 메시지를 보호하기 위해 암호로 강화된 통신 경로.

보증

선의지적 노력을 바탕으로 지정된 서비스의 제공 및 유지에 대한 보편적 의지를 나타내는 IA의 말이나 행동. 그러나 "보증"은 반드시 완전하고 만족스러운 서비스 실행이 보장됨을 암시하지는 않습니다. 보증은 별도의 명백한 설명이 없는 한 보호(insurance), 약속(promise), 보장(guarantee), 서약(warranty) 등과는 구별됩니다.

부인(*참조:* 부인 방지)

전체 혹은 일부 통신 과정에 관련된 실체의 부인 혹은 부인 시도.

부인 방지

데이터의 출처 및 배달 정보를 제공하여 수취인이 데이터를 받았다는 사실을 부인하지 못하게 함으로써 송신인을 보호하고 송신인이 데이터를 보낸 사실을 부인하지 못하도록 하여 수취인을 보호하는 기능.참고:실질 심판관(분쟁 해결 권한을 가진 사람)만이 부인 방지를 최종 확정할 수 있습니다. 실례로 CPS에 부합하는 디지털 서명 확인을 통해 실질 심판관에 의한 부인 방지 확정을 증명할 수 있습니다.

비밀 공유(*참조:* **공유 비밀**)

개인 키의 공유 비밀을 여러 명의 공유 비밀 홀더들에게 배포하는 작업; 임계 값에 기반한 키 분할.

비CrossCert 단체 LRA

CrossCert가 소유하지는 않지만 운영하는 LRA로 LRA에 가입되지 않은 개인 가입자에게 발행된 인증서와 관련된 LRA 기능을 수행하는 것으로만 기능이 제한됩니다. (*참조:* CPS § 2.5.4; *비교:* **로컬 등록 기관; 개인 가입자**)

비CrossCert IA

CrossCert가 소유하거나 운영하지 않는 IA.(*참조:* CPS § 3.1; *비교:* **발행 기관**)

사

사람

법적 또는 사실적으로 메시지에 서명하거나 검증할 수 있는 사람 또는 단체(또는 인간이나 단체의 통제를 받는 장치).(**실체**의 동의어.)

사용자

신청자나 가입자, 수취인, 신뢰 당사자의 위치에서 인증서를 사용할 수 있는 권한을 부여 받은 실체로 인증을 발행하는 IA는 사용자에 포함되지 않습니다. (*비교:* **인증 신청자; 실체; 사람; 가입자**)

상대적 식별 명(RDN)

동일한 유형의 다른 실체와 해당 실체를 구별하는 실체 식별 이름을 구성하는 속성 집합.

상업적 타당성

전자 상거래 차원에서 기술, 제어 기능, 시스템, 메시지를 신뢰할 수 있게 만드는 관리 및 운영 절차의 실행과 사용.

상위 IA

IA의 CrossCert PKI 구조 계층 내에서 각 IA는 VR, PCA, CA 또는 "하위 CA"입니다. 하위 CA의 상위 IA는 또 다른 하위 CA나 CA이며, CA의 상위는 PCA, PCA의 상위는 VR이나 그 자신입니다. VR은 자체 상위 IA입니다. **(***비교:* **하위 IA)**

서명

문서 작성자가 자신을 확인하기 위해 사용 또는 채택하는 방법으로 수취인이 인정하거나 그 상황에서 관습적으로 사용되는 방법.(*비교:* **디지털 서명**)

서명자

메시지의 디지털 서명이나 문서의 서명을 작성한 사람.

서명하다

메시지에 디지털 서명을 작성하거나 문맥에 따라 문서에 서명을 첨부하는 행위.

서버

클라이언트 시스템의 요청에 대응하는 컴퓨터 시스템.
서비스 거부(*참조:* 가용성)

손상

중요한 정보의 무단 발표나 통제력 상실과 같은 보안 정책 위반(또는 위반 추정) 상황이 발생한 경우.(*비교:* **데이터 무결성**)

수출 제어 인증

승인 서버 인증 가입자로 하여금 강력한 암호화 모드로 운영하게 만듦으로써 이러한 서버에 액세스하는 브라우저가 강력한 암호화 모드로 운영할 수 있게 하는 인증 기반 서비스.

수취인(디지털 서명)

디지털 서명을 받는 사람으로서 신뢰 관계의 발생 여부가 이 서명에 따라 결정되는 위치에 있는 사람.(*비교:* **신뢰 당사자**)

스마트 카드

한 개 이상의 집적 회로(IC) 칩을 통합하여 암호화 기능을 수행하며 간섭에 대한 고유 저항력을 가진 하드웨어 토큰.

승인(인증)

인증 신청자가 인증서의 내용을 알거나 통지 받은 상태에서 CPS에 따라 인증에 대한 동의를 표시하는 것.

시범 인증서

안전한 통신이나 기밀 통신용이 아닌 시범 또는 프리젠테이션 용도로만 사용하도록 IA가 발행하는 인증.권한을 부여 받은 사람만 시범 인증서를 사용할 수 있습니다.

식별 이름

컴퓨터 기반의 컨텍스트 상에 있는 사람 등 존재의 실재를 확인하는 데이터 집합.(예: countryName=US, state=California, organizationName=Electronic Inc., commonName=JohnDoe).

식별

사람의 신분을 확정하는 과정.공용 키 암호화에서 인증서를 통해 식별 과정이 촉진됩니다.

식별자(*참조:* **CROSSCERT 식별자**)

신뢰 당사자

인증 및 디지털 서명에 의존하여 행동하는 수취인.(*비교:* **수취인; 신뢰(인증서** 및 **디지털 서명**에 대하여))

신뢰

신뢰의 당사자가 신뢰하는 당사자의 예상 대로 행동할 것이라는 일반적인 가정.신뢰는 구체적 기능에만 적용됩니다. 인증 체제에서 신뢰의 핵심 역할은 인증 실체와 IA 간의 관계를 설명하는 것입니다. 인증 실체는 IA가 유효하고 신뢰할 수 있는 인증만 작성한다는 것과 이러한 인증서의 사용자는 인증 실체의 신임 결정을 신뢰한다는 사실을 확인해야 합니다.

신뢰(인증서 및 **디지털 서명**에 대하여)

디지털 서명을 승인하고 자신에게 손해가 될 수도 있는 방법으로 행동하는 것은 디지털 서명을 무효로 만들 수 있습니다. (*비교:* **신뢰 당사자; 수취인**)

신뢰된 개인

신임된 위치에서 CPS에 따라 임무를 수행하도록 선정된 사람.(*비교:* **신임; 신임된 위치; 제 3 신임자; 신뢰할 만한 시스템**)

신뢰된 루트

신뢰된 루트는 사용자나 시스템 관리자에 의해 IA로 귀속되도록 확정된 공용 키입니다. 공용 암호 및 인증서를 바탕으로 인증을 실행하는 소프트웨어와 시스템은 이 값이 정확하게 얻어졌다고 가정합니다. 이 루트는 항상 신뢰된 시스템 저장소로부터 확인되고 신뢰된 관리자만이 수정 권한을 가진 시스템으로 액세스함으로써 확정됩니다.

신뢰된 위치

IA 내에서 저장소 액세스 제한 운영을 비롯한 인증서의 발행과 사용, 일시 중지, 취소에 실질적으로 영향을 끼칠 수 있는 암호 운영 액세스나 통제를 포함하는 역할.

신뢰할 만한 시스템

침입과 오용으로부터 안전한 컴퓨터 하드웨어와 소프트웨어, 절차를 말합니다. 합리적인 수준의 가용성과 신뢰도, 정확한 운영을 제공하는 이 시스템은 계획된 기능을 수행하는 데 적합하며, 적절한 보안 정책을 실행하도록 고안되었습니다. 신뢰할 만한 시스템은 반드시 정부 지정 용어집에 나온 "신뢰된 시스템"일 필요는 없습니다.

신분

도메인의 특정 실체를 표시하고 구분하는 고유의 정보.이러한 정보는 특정 도메인 내에서만 고유성을 갖습니다.

신임

특정 정보 시스템, 전문가, 직원, 도급 업체, 단체가 특정 임무를 수행하고, 사전에 지정된 안전 장치를 사용하는 안전 모드에서 운영하도록 승인하는 CrossCert 지정 승인 기관의 공식 확인.
신청자(*참조*: CA 신청자; 인증 신청자)

실체(*참조:* **사람**)

쓰기

추후 참조를 위해 액세스하여 사용할 수 있는 레코드의 정보.

아

암호 모듈

데이터의 암호화 및 해독을 안전하게 실행하는 신뢰할 만한 암호법 구현.

암호

인증 신청자가 선택하여 인증 지원서와 함께 IA에 전송하는 일련의 숫자 및 문자 집합으로 CPS에 규정된 다양한 목적에 맞게 IA가 가입자를 인증하는 데 사용됩니다. 또한 공유 비밀 홀더는 암호를 써서 공유 비밀 발행자에 대해 자신을 인증합니다.

암호(암호문; 핀 번호)

컴퓨터 자원을 액세스하는 데 사용되는 문자열로 구성된 비밀 인증 정보.

암호화 알고리즘

명확하게 지정된 수학적 계산 프로세스; 계획된 결과를 도출하는 일련의 규칙.

암호화

평문 데이터를 읽을 수 없는 형태(암호문)로 변형함으로써 원래 데이터를 복구할 수 없게 만들거나(일방 암호화) 역 암호 해독 과정을 거치지 않고는 데이터를 복구할 수 없게(쌍방 암호화) 만드는 과정.

암호화(*비교:* **공용 키 암호화**)

(i) 데이터를 적절한 암호화 알고리즘과 키를 보유한 사람만이 볼 수 있는 변형된 버전으로 교체함으로써 데이터의 기밀성과 인증을 보호하는데 사용되는 수학적 과학. (ii) 데이터 전송 시에 데이터에 담긴 정보 내용을 감춤으로써 미처 감지하지 못한 수정이나 무단 사용을 예방하기 위한 원칙 및 수단, 방법 등을 포함하는 규칙.

액세스

전송과 통신 간 또는 정보 자원 간에 이루어지는 특정한 형태의 상호 작용으로 정보 흐름이나 제어 실행, 프로세스 활성화를 유발.

예비 인증서

(CPS § 5.1에 적합한) 클래스 2 인증서 신청에 필수적인 모든 IA 내부 타당성 검사 절차를 성공적으로 마침에 따라 발행되는 운영 기간 첫 21일 동안의 클래스 2 인증서.예비 상태란 가입자의 동일성에 대한 인증서 신청의 타당성 검사가 주소 "회신" 절차를 통해 향후에 완료될 것임을 의미합니다(*참조:* CPS § 5.1.4 - 주소 확정; *비교:* **인증**).

온라인

CrossCert PCS에 대한 실시간 연결을 제공하는 통신 방법.

운영 기간

인증 발행 날짜와 시간으로 개시되어(또는 인증서에 언급된 특정 날짜 및 이후 날짜) 인증 만료나 조기 중지, 취소 날짜와 시간으로 종료되는 기간.

운영 인증서

현재 날짜 및 시간, 또는 문맥에 따른 특정 날짜 및 시점에 운영 중인 인증서.

월드 와이드 웹(WWW)

사용자들이 하이퍼텍스트 문서를 작성, 편집, 검색할 수 있는 하이퍼텍스트 기반의 분산 정보 시스템.그래픽 문서의 발표와 검색이 가능한 매체로서 인터넷에 들어 있는 상호 연결된 문서들의 조합입니다.

위협

데이터 파괴나 무단 발표, 수정이나 서비스 거부 등, 시스템에 위해를 발생시킬 여지가 있는 환경이나 사건.

유효 인증서

IA가 발행하고 그 안에 표시된 가입자가 동의한 인증서.

이름

특정 형태의 실체를 설명하는데 사용되는 일련의 확인 속성.

인증

사용자의 신분이나 특정 정보의 무결성을 확정하는 데 사용되는 절차.메시지 인증에는 메시지 자원 결정 및 메시지가 전송되는 과정에서 수정되거나 교체되지 않았음을 검증하는 과정이 포함됩니다. (*비교:* **검증**(디지털 서명))

인증

IA에 의한 인증 발행 프로세스.

인증 (공용 키 인증)

이름을 지정하거나 IA를 확인하는 메시지로 가입자를 확인하는 공용 키를 포함하고 있으며, 인증에 필요한 작업 기간을 확인하고 인증 일련 번호가 들어간 IA의 디지털 서명이 들어 있는 메시지(**메시지** 정의 *참조*). 한정 형용사가 없는 "클래스 [1, 2, 3] 인증"이나 "인증"은 문맥상 다른 의미를 갖지 않는 한 "일반" 및 "예비" 인증을 나타내는 것입니다. 인증은 IA가 발행하는 인증만을 의미합니다(*비교:* **예비 인증**)

인증 계층

하위 IA의 "트리 구조"에서 역할에 따라 구분되는 IA의 CrossCert PCS 도메인. IA는 최종 사용 가입자 및 다음 단계의 IA중 한 개 이상의 IA에 대한 인증을 발행하고 관리합니다. 참고:도메인의 무결성을 확실히 하고 신뢰할 만한 운영 절차로 신뢰도 및 감사도를 관리하려면 신임 계층의 IA는 이름 지정이나 레벨 최대 수 처리에 동일한 기준을 적용해야 합니다.

인증 관리

인증의 보관, 배포, 발행, 취소, 일시 중지를 비롯한 포괄적인 인증 관리 작업.IA는 가입자 인증 등록 기관으로서 각종 인증서 관리 기능을 수행합니다. IA는 발표를 통해 인증을 유효한 것으로 발행 및 승인합니다.

인증 기관(CA)

인증 발행 권한을 부여 받은 사람(*참조:* **사람** 정의). CrossCert PCS에서 CA는 PCA의 하위에 위치합니다. (*비교:* **등록 기관; 제 3 신임자**)

인증 레코드

적절한 인증 보증을 받은 서명된 문서 또는 신뢰의 당사자가 유효한 클래스 3 인증으로 확인한 디지털 서명이 들어간 메시지.그러나 일시 중지 및 취소 통보를 목적으로 사용되는 이러한 통보 메시지에 포함된 디지털 서명은 해당 인증 클래스의 인증에 들어 간 공용 키에 대응하는 개인 키로 작성된 것이어야 합니다.

인증 목록 확정

인증 목록 확인 및 추후 최종 사용 가입자 인증의 타당성 검사 작업.

인증 발표(*참조:* **인증 발표**)

인증 발효(*예:* **최종 가입자 인증**의 발효)

수취인 혹은 신뢰 당사자가 최종 사용 가입자 인증이 유효하며, 적절한 디지털 서명이 작성된 날짜와 시간에 운영되었다는 사실을 확정하기 위해 실행하는 작업.

인증서 만료

일시 중지나 취소와 상관없이 인증서에 명시된 운영 기간 만료일 및 시간.

인증 서명 요청서(CSR)

컴퓨터로 판독할 수 있는 인증 신청서의 형태.(*비교:* **인증 신청서**)

인증서 신청

IA에 인증을 발행해 달라는 인증 신청자(또는 권한을 부여 받은 대리인)의 요청.(*비교:* **인증서 신청자; 인증 승인 요청서**)

인증서 신청자

IA의 공용 키 인증서 발행을 요청하는 사람이나 권한을 부여 받은 대리인(*비교:* **CA 신청자; 가입자)**

인증 업무 준칙(CPS)

이 문서는 가끔 개정 됩니다(인증을 발행함에 있어 IA 직원들이 지켜야 할 CrossCert 업무 준칙).

인증서 일련 번호

IA가 발행한 인증임을 명백하게 확인하는 값.

인증서 일시 중지

영구적인 인증서의 취소 없이 인증의 운영 기간의 유효성에 내려지는 일시적인 "중지". 인증서의 일시 중지는 원인 코드가 있는 CRL 항목 등에 의해 실행됩니다. (*비교:* **인증 취소**)

인증 일시 중지(*참조:* 인증을 일시 중지)

인증 체인 발효

체인의 각 인증에 대해 수취인이나 신뢰 당사자가 (각 인증의) 공용 키를 인증하고 각 인증이 타당성이 있으며, 대응하는 IA 인증 운영 기간 내에 발행되었다 것, 모든 당사자(IA, 최종 사용자 가입자, 수신자, 관련 당사자)들이 체인의 모든 인증에 대해 CPS에 따라 운영했다는 사실을 확정하기 위해 수행하는 작업.

인증 체인

최종 사용 가입자 인증서 및 IA 인증서를 포함하는 인증 차례 목록(*참조:* **유효 인증**)

인증 취소 목록(CRL)

만료일 전에 일시 중지 또는 취소된 인증에 대하여 IA가 디지털 서명하여 정기적으로 발행하는 목록입니다. 일반적으로 이 목록에는 CRL 발행자 이름과 발행일, 다음 CRL 발행 예정일, 일시 중지 또는 취소된 인증의 일련 번호, 일시 중지 및 취소의 구체적 시간과 원인이 표시됩니다.

인증 취소

이미 지정된 시간에서 인증 운영 기간을 영구적으로 종료하는 작업.

인증서 취소(*참조:* 인증을 취소)

인증 코드(*참조*: Microsoft Authenticode™; **소프트웨어 타당성 검사**)

인증 확인서
미 국무부 장관 등 권한 있는 공증인의 확인과 함께 공식 기관에서 발행된 문서.

인증 확장
인증된 공용 키 및 가입자, 인증서 발행자, 인증 프로세스에 대한 추가 정보를 나타내는 인증 확장 필드.표준 확장은 ISO/IEC 9594-8:1995 (X.509) 수정 제1조에 규정되어 있으며, 사용자 정의 확장은 관계자들도 정의할 수 있습니다.

인증서 발행
인증서 작성 및 인증서에 수록된 인증 신청자(예정 가입자)에게 이를 통지하는 과정에서 IA가 수행하는 작업.

인증의 유형
의도된 용도를 해당 유형과 독특하게 연관된 일단의 신청으로 제한하는 인증의 한정성.

인증의 주체
공용 키에 대응하는 개인 키의 소유자."주체"란 개인 키를 소유한 장치나 도구 뿐 아니라 이 장치나 도구를 제어하는 개인을 의미할 수도 있습니다. 각 주체에는 인증에 포함된 공용 키에 구속되는 확실한 이름이 지정됩니다.

인증자(*참조:* 발행 기관)

인증하다. (*참조:* **인증**)

일련 번호(*참조:* **인증 일련 번호**)

일반 인증(*참조:* **인증)**

일차 인증 기관(PCA)
모든 인증 기관과 사용자에 대한 업무를 도메인 내에 설정해 두고 있는 개인.

자

자체 서명 공용 키
인증과 동일한 이름으로 구성되었지만 그 주체가 서명한 데이터 구조.인증과 달리 자체 서명 공용 키는 다른 당사자에게 공용 키를 인증하는 방법으로 사용할 수 없습니다. VR이 디지털 사인을 한 PCA 자체 서명 공용 키는 하나의 인증을 구성합니다. (*비교:* **인증**)

재등록 (*비교:* **갱신**)

저장

보안, 백업, 감사로 지정된 시간 동안 레코드나 관련 저널을 보관하는 것.

저장소

인증 및 온라인으로 액세스 할 수 있는 기타 관련 정보의 데이터베이스.

전자 메일("E-MAIL")

컴퓨터 기반 통신 메커니즘을 통해 디지털 형식으로 전송 또는 수신되는 메시지.

정직원

자격이 만료 또는 중지되지 않은, 수습이 아닌 직원. 훈련 조치의 계류 여부와는 큰 상관이 없습니다.

제 3 신임자

컴퓨터를 통한 전송의 보안 및 신뢰 가능성의 극대화에 기여하는 독립적이고 공평한 제3자.제 3 신임자는 신임자-피신임자의 관계나 기타 신용 관계가 존재한다는 것을 의미하지 않습니다. (*비교:* **신임**)

제어

프로세스의 무결성과 품질을 보증하는 방법.

주체 이름

공용 키에 구속되는 인증의 주체 이름 필드에 들어가는 확실한 값.

차

참조에 의한 통합

통합될 메시지가 수신 상대방이 전체에서 액세스하고 확보할 수 있는 정보와 동일한 것임을 확인하고 이를 통합 메시지의 일부로 하고자 하는 의사를 표현함으로써 하나의 메시지를 다른 메시지의 일부로 통합하는 작업.이렇게 통합된 메시지는 법률이 허용하는 범위 내에서 메시지에 언급된 것과 같은 효과를 발휘합니다.

창시자

데이터 메시지를 생성, 저장, 통신하기 시작한 사람(또는 대표자).중개자 역할을 하는 사람은 여기에 포함되지 않습니다.

최종 사용 가입자

IA가 아닌 가입자.

출현

특정 조건에서 인증 발행의 선행 조건으로서 개인의 동일성을 증명하기 위해 LRA나 그 피지명자 앞에 (가상적 혹은 상징적이 아닌 신체적으로) 나타나는 행위.

카

클래스 [1, 2, 3] 인증
특정 신뢰 수준의 인증. (*참조:* CPS § 2.2)

키 생성
신뢰할 만한 개인 키 및 공용 키 작성 과정.인증 신청 과정이 진행되는 동안 IA에 공용 키가 제공됩니다.

키 쌍 생성
신청자의 개인 키 사용 용량을 표시하는 방법으로 인증 신청이 실행되는 동안 개인 키에 대응하는 공용 키를 해당 IA에 등록하면서 인증 신청이 이루어지는 개인 키 작성 프로세스.

키 쌍
개인 키와 이에 대응하는 공용 키.공용 키는 대응하는 개인 키를 써서 작성된 디지털 서명을 검증할 수 있습니다. 아울러 실행 알고리즘의 종류에 따라 키 쌍의 구성 요소는 기밀성 확보를 위해 정보를 암호화 하고 해독할 수 있는데, 이 경우 개인 키는 대응하는 공용 키로 암호화된 정보를 해독할 수 있습니다.

타

타당성 검사(소프트웨어) (*참조:* **소프트웨어 타당성 검사**)

타당성 검사(인증서 신청)
인증서 신청의 승인 및 인증서 발행의 선행 조건으로 IA(또는 그 LRA)가 인증 신청서 제출에 이어 수행하는 작업.(*비교:* **인증; 소프트웨어 타당성 검사**)

타임 스탬프
행동의 정확한 날짜와 시간 뿐 아니라 타임 스탬프를 보내거나 받은 사람 및 장치의 신분을 표시하는 표기법.

테스트 인증서
내부 기술 상의 시험이라는 제한적 용도로 IA가 발행하는 인증서.테스트 인증서는 권한을 부여 받은 사람만 사용할 수 있습니다. (*참조:* CPS § 2.2.4).

토큰
사용자의 개인 키와 공용 키 인증 및 선택 사항으로 사용자의 인증 체인에 들어 있는 모든 인증을 비롯한 기타 인증 캐시를 포함하는 하드웨어 보안 토큰.

통지
CPS에 따른 고지의 결과. (*참조:* CPS § 12.10)

통지하다

CPS 및 기타 적용 법률이 요구하는 다른 사람에게 특정 정보를 알리는 것.

트랜잭션

컴퓨터를 통한 사업 정보의 전송. 이 트랜잭션에는 글로벌 네트워크를 통해 통신을 촉진하는 특정 프로세스가 포함되어 있습니다.

특정 레코드 및 World Wide Web 상에 위치한 기타 자원을 확인하고 찾는 데 사용되는 표준 장치.

파

파일 전송 프로토콜(FTP)

인터넷 프로토콜 수트로부터의 파일 시스템 액세스를 제공하는 응용 프로그램 프로토콜.

하

하위 IA

IA의 CrossCert PKI 구조 계층 내에서 각 IA는 VR, PCA, CA 또는 "하위 CA"입니다. VR의 하위 IA는 PCA, PCA의 하위 IA는 CA, CA의 하위 IA는 하위 CA입니다. CA의 하위 IA가 있다면 또 다른 하위 CA입니다. (*비교:* **상위 IA**)

해시(해시 기능)

하나의 비트 집합을 다음과 같은 방법으로 다른(일반적으로 크기가 더 작은) 집합에 매핑하거나 해석하는 알고리즘. i. 입력된 것과 동일한 메시지를 사용하여 알고리즘을 실행했을 때 메시지는 매번 동일한 결과를 도출합니다. ii. 알고리즘으로 생성된 결과로부터 메시지를 도출 또는 재설정하기 불가능합니다. iii. 같은 알고리즘을 써서 같은 해시 결과를 생산하는 두 개의 상이한 메시지를 발견하는 것은 불가능합니다.

확실한 이름(*참조:* **식별 이름**)

확인

데이터의 정확성 및 정보의 사실성을 말이나 행동으로 나타내는 것.

확장 명명

X.509 v3 인증의 확장 단체 필드(OU=)의 사용.

확장

X.509 v3 인증의 확장 필드.(*참조:* **X.509**)

확정

적절한 조회나 조사를 통한 확인 작업.(*비교:* **인증; 디지털 서명 검증**)

C

CA 신청(비CrossCert CA 신청)
인증 기관 또는 하위 인증 기관이 되려고 하거나 CrossCert의 공용 인증 서비스 가운데 IA 인증서를 요청하기 위해 비CrossCert 실체가 해당 CrossCert CA에 제출하는 신청.(*참조:* CPS § 3.1.1)

CA 신청자
CA나 하위 CA가 되기 위해 CrossCert에 CA 신청서를 제출하는 사람.(*비교:* **가입자**)

CrossCert 공용 인증 서비스(PCS)
CPS에 언급된 CrossCert 및 CrossCert이 권한을 부여한 모든 IA.

CrossCert 명명 기관
모든 IA(최종 사용 가입자의 경우는 아님)에 대한 상대적 식별 이름의 발행과 관련하여 통제력을 행사하며 의사 결정 권한을 지닌 CrossCert 등록 기관.(*비교:* **명명 기관**).

CrossCert 보안 정책(CSP)
CrossCert의 내부 보안 정책을 설명하는 문서.

CrossCert 식별자
CrossCert CPS의 의미를 한정하는 일련의 값이 갖는 표현을 촉진하는 데이터 구문.식별자 값은 해당 확장 형태에 대해 X.509로 한정된 규칙에 따라 모든 인증서에 나타나는 표준 인증 정책 확장을 증가시킵니다.

Digital ID℠(*참조:* 인증서)
인증서에 사용된 CrossCert의 서비스 마크 및 상표 이름.

FTP(*참조:* 파일 전송 프로토콜)

I

IA 인증서
권한을 부여 받은 상급 IA에서 하위 IA에 발행하는 인증서(*참조:* **상급 IA; 하위 IA**; *비교:* **인증**).

IA(*참조:* **발행 기관**)

P

PC 카드(*참조:* **스마트 카드**)

컴퓨터에 정보 보안 강화를 비롯한 여러 가지 확장 기능을 제공하는 Personal Computer Memory Card International Association(PCMCIA)의 표준에 부합하는 하드 웨어 토큰.

PKI 계층

권한 대표의 원칙에 따라 기능이 구성되고 하위 또는 상위 IA로 서로 연관된 일련의 IA.

R

RSA

Rivest, Shamir 및 Adelman이 창안한 공용 키 암호 시스템.

S/MIME

인터넷 MIME 환경에서 암호 메시지 구문을 이용하는 전자 우편 보안 규격.

U

URL(웹 주소)

V

VERISIGN 루트(VR)

각 PCS의 자체 서명 공용 키를 등록함으로써 PCA를 등록하는 IA.

X

X.509

인증에 대한 ITU-T(International Telecommunications Union-T) 기준.X.509 v3은 확장을 포함하고 있거나 포함할 수 있는 인증을 나타냅니다.

***

13.2 색인

가

다

라

마

바

사

아

자

차

카

타

파

하

C

I

P

V