CrossCert
인증업무준칙

버전 2.0

발효일: 2003 년 4 월 21 일

서울 서초구 서초동 1674-4 하림빌딩 9 층
한국전자인증㈜
(우) 137-725
http://www.crosscert.com

CrossCert 인증업무준칙

© 2001 VeriSign, Inc. All rights reserved.
Printed in the United States of America.

수정일: 2003 년 4 월

상표 관련 공지사항

VeriSign 과 Managed PKI 는 VeriSign, Inc.의 등록 상표입니다. VeriSign 의 로고인 VeriSign Trust Network 및 Go Secure!는 VeriSign, Inc 의 상표 및 서비스 상표입니다. 이 문서의 다른 상표 및 서비스 상표는 해당 소유권자의 자산입니다.

위 저작권을 제한하지 않는 범위에서, VeriSign, Inc.의 사전 서면 허가 없이 이 자료를 복제하거나 컴퓨터 시스템에 저장 또는 삽입할 수 없으며 어떤 형태나 방법(전자, 기계, 복사, 기록 등)으로도 배포할 수 없습니다. 단 아래와 같은 경우는 예외로 합니다.

(i) 상기 저작권 조항과 첫 단락을 각 사본의 첫 부분에 명시하고 (ii) 문서에 대한 권한을 VeriSign. Inc.에 귀속한 상태에서 정확히 완전 복제한다는 조건으로 CrossCert 인증업무준칙의 비독점적인 무료 복제와 배포가 허용됩니다.

이 CrossCert 인증업무준칙의 다른 복제 권한을 요청하거나 CrossCert 에 사본을 요청하려면 다음으로 문의하십시오.
서울 서초구 서초동 1674-4 하림빌딩 9 층 한국전자인증(주)
(우) 137-725 수신: Practices Development
전화: (02)3019-5500
팩스: (02)3019-5678
인터넷: practices@crosscert.com

감사의 말씀

VeriSign 은 인증업무준칙(CPS) 발행을 위한 자문을 제공하신 비즈니스, 법률, 정책 및 기술 분야 전문가 여러분들께 감사 드립니다.

목차

1. 소개

참고 사항: 본 CPS 에서 대문자로 표시된 용어는 특수한 의미로 정의된 용어입니다. 정의 목록은 9 항을 참조하십시오.

CrossCert 인증업무준칙("CPS")은 VeriSign의 인증업무준칙(https://www.verisign.com/cps 참조)을 기반으로 하며,[1] VeriSign Trust Network 인증서 정책("CP")의 세부 요구 사항에 따라 인증서의 발행, 관리, 폐지 및 갱신을 포함한(이에 제한되지는 않음) 인증 서비스 제공 시 CrossCert 인증 기관("CA")이 사용하는 준칙을 다루고 있습니다. VeriSign, Inc.("VeriSign")는 웹 사이트, 기업, 전자 상거래 서비스 제공업체 및 개인에게 신뢰할 수 있는 기반구조 서비스를 제공하는 선두 업체입니다. VeriSign은 도메인 이름, 디지털 인증서 및 결제 서비스를 통해 온라인 기업들이 안전한 전자 상거래 활동을 수행하기 위해 필요로 하는 웹 상의 신원 조회, 인증 및 거래 기반구조를 제공합니다.

CP 에서는 VeriSign Trust Network^{SM}("VTN")에 대해 설명합니다. VTN 은 유무선 애플리케이션을 위한 디지털 인증서("인증서")를 제공하는 글로벌 공개키기반구조("PKI")입니다. VTN 은 통신 및 정보 보안과 관련하여 다양한 요구 사항을 가진 세계 곳곳의 수 많은 사용자들에게 적용할 수 있도록 설계되었습니다. VeriSign 은 CrossCert 를 비롯한 전세계 여러 회원사("회원사")들과 함께 VTN 관련 서비스를 제공하는 업체 중 하나입니다.

CP는 VTN에 적용되는 정책의 주요 준칙을 다루고 있습니다. CP는 VTN 내에서 디지털 인증서의 허가, 발행, 관리, 사용, 폐지 및 갱신을 수행하고 관련된 인증 서비스를 제공하기 위한 비즈니스, 법률 및 기술 요구 사항을 설정합니다. "VTN 표준"이라고 하는 이러한 요구 사항은 VTN의 보안 및 무결성을 보장하고 모든 VTN 참여자들에게 적용되기 때문에 전체 VTN에 걸쳐 일관성 있는 신뢰도를 제공합니다. VTN 및 VTN 표준에 대한 자세한 내용은 CP[2]를 참조하십시오.

VeriSign 과 각 회원사는 VTN 의 일부에 대해 권한을 갖고 있습니다. VTN 에서 VeriSign 또는 CrossCert 의 제어를 받는 부분을 VTN 의 "하위 도메인"이라고 합니다. 회원사의 하위 도메인은 VTN 중 해당 회원사의 제어를 받는 부분으로 구성되어 있습니다. CrossCert 의 하위 도메인에는 고객, 가입자 및 신뢰 당사자 등과 같은 CrossCert 의 종속 개체가 포함됩니다.

CrossCert, VeriSign 및 각 회원사는 VTN 내의 해당 하위 도메인을 담당하는 CPS를 가지고 있습니다. CP는 VTN 참여자들이 준수해야 하는 요구 사항을 명시하고, CPS는 주로

---

[1] CPS 섹션에 대한 내부 상호 참조("CPS §"의 형태)는 이 문서의 섹션을 의미합니다. "CPS"는 인증업무준칙을 의미하며 본 CPS 나 VTN 회원사 등과 같은 다른 회사의 CPS 를 나타냅니다. CPS § 9 (정의)를 참조하십시오.

[2] CP 는 **https://www.verisign.com/CP**의 VeriSign 저장소에 전자 형태로 나와 있습니다. 필요할 경우 VeriSign, Inc., 487 East Middlefield Road, Mountain View, CA 94043 USA, Attn: Practices Development – CP 로 요청하시면 VeriSign Trust Network 정책 관리 기관("PMA")에서 문서 형태로 제공합니다.

한국에 위치한 VTN의 CrossCert 하위 도메인 내에서 CrossCert가 이러한 요구 사항을 충족하는 방법을 설명합니다. 보다 구체적으로 말하자면 이 CPS는 CrossCert가 CP 및 해당 VTN 표준의 요구 사항에 따라 VTN의 CrossCert 하위 도메인 내에서 다음을 수행하기 위해 적용하는 준칙에 대해 설명합니다.[3]

- VTN 을 지원하는 핵심 기반구조를 안전하게 관리
- VTN 인증서 발행, 관리, 폐지 및 갱신

1.1 개요

이 CPS 의 적용 대상은 다음과 같습니다.

- VeriSign 의 공식 주요 인증 기관(PCA), CrossCert 기반구조 CA, VeriSign Trust Network 를 지원하는 CrossCert 관리 CA
- CrossCert의 공식 CA, VTN 내에서 인증서를 발행하는 Managed PKI[4] 고객의 CA

보다 넓은 의미에서 CPS 는 CrossCert 의 하위 도메인 내에서 모든 개인 및 단체(즉 CrossCert 하위 도메인 참여자)가 VTN 의 CrossCert 하위 도메인 내에 있는 VTN 서비스를 사용하는 것에도 적용됩니다. 개인 CA 나 CrossCert 가 관리하는 하위 기관의 경우 이 CPS 의 적용을 받지 않습니다.
VTN 에는 세 가지 클래스의 인증서가 포함되어 있으며, CP 에는 이러한 세 가지 클래스가 공통 보안 요구 사항을 지닌 세 가지 애플리케이션 클래스에 대응하는 방식을 설명합니다. CP 는 각 클래스에 적용되는 세 가지 인증 정책을 정의하고 각 클래스에 대한 VTN 표준을 설정하는 하나의 문서입니다.

CrossCert 는 VTN 의 하위 도메인 내에 있는 세 가지 인증서 클래스를 모두 제공합니다. 본 CPS 는 CrossCert 가 하위 도메인 내의 각 클래스별 CP 요구 사항을 충족하는 방식을 설명합니다. 따라서 이 CPS 에는 세 가지 인증서 클래스의 발행 및 관리와 관련된 준칙과 절차가 모두 나와 있습니다.

(a) CrossCert CPS 및 다른 준칙 문서의 역할

CP 에는 VTN 의 전반적인 비즈니스, 법률 및 기술 기반구조에 대한 일반 수준의 설명이 나와 있습니다. 본 CPS 는 CP 의 VTN 표준을 CrossCert 하위 도메인 참여자에게 적용하고 CP 에 대한 CrossCert 의 구체적인 준칙에 대해 설명합니다. 구체적으로 CPS 에는 다음에 대한 설명이 나와 있습니다.

---

[3] VeriSign CA 는 회원사의 CA 를 인증하지만 회원사와 관련된 준칙은 이 CPS 가 아닌 해당 회원사 CPS 의 적용을 받습니다.

[4] Managed PKI 서비스의 원래 명칭은 OnSite 였습니다. 본 CPS 의 모든 OnSite 는 Managed PKI 로 변경되었습니다. Server OnSite 의 경우 SSL 용 Managed PKI 로, Global Server OnSite 의 경우 SSL Premium Edition 용 Managed PKI 로 각각 변경되었습니다. 다른 Managed PKI 문서나 URL 에서는 아직 OnSite 를 사용할 수도 있습니다. OnSite 서비스는 이름만 바뀌었을 뿐 서비스 자체는 변경되지 않았습니다.

- VTN 의 CrossCert 하위 도메인 내에서 인증 기관, 등록 기관, 가입자 및 신뢰 당사자의 의무 사항
- CrossCert 하위 도메인 내의 가입 계약서와 신뢰 당사자 계약서에서 다루는 법적 문제
- CrossCert 및 CrossCert 하위 도메인 참여자가 수행하는 감사와 관련 보안 및 준칙 검토
- 각 인증서 클래스에 대한 인증서 신청자 신원 확인을 위해 CrossCert 하위 도메인 내에서 사용되는 방법
- CrossCert 하위 도메인에서 수행되는 인증 주기 서비스를 위한 시행 절차: 인증서 신청, 발행, 승인, 폐지 및 갱신
- 감사 기록, 기록 보존 및 재난 복구를 위해 CrossCert 하위 도메인에서 사용되는 보안 시행 절차
- CrossCert 하위 도메인 참여자들의 물리적, 논리적, 인원 관리 및 키 관리 보안 준칙
- CrossCert 하위 도메인 내의 인증서 및 인증서 폐지 목록
- 수정 방법을 포함한 CPS 관리

그러나 CPS 외에도 VTN 의 CrossCert 하위 도메인에 대한 관련 문서는 많습니다. 이러한 기타 문서 중 일부는 다음과 같습니다.

- 다음은 보다 자세한 요구 사항을 제공하여 CP 와 CPS 를 보완하는 보안 및 운영 보조 문서입니다.
    - VeriSign Security Policy(VeriSign 보안 정책): VTN 기반구조에 적용되는 보안 원칙 설정
    - Security and Audit Requirements Guide(보안 및 감사 요구 사항 가이드): CrossCert 의 인원 관리, 암호 키 관리, 통신, 물리적 및 논리적 보안을 위한 세부 요구 사항 설명
    - Enterprise Security Guide(기업 보안 가이드): Managed PKI 사용자의 인원 관리, 암호 키 관리, 통신, 물리적 및 논리적 보안을 위한 세부 요구 사항 설명
    - Key Ceremony Reference Guide(키 형식 참조 가이드): 구체적인 키 관리 요구 사항 설명
- CrossCert 가 제공하는 보조 계약서입니다. 이러한 계약서는 CrossCert 의 고객, 가입자 및 신뢰 당사자에게 구속력을 갖습니다. 특히 VTN 참여자에게 VTN 표준을 적용하며, 일부 경우에는 이들 참여자가 VTN 표준을 준수하기 위해 지켜야 하는 준칙을 구체적으로 명시합니다.

CPS 의 세부 사항이 VTN 의 CrossCert 하위 도메인 보안에 해가 될 경우 CPS 는 VTN 표준 이행 시 구체적인 세부 준칙을 위해 위의 보조 문서를 참조하는 경우가 많습니다.

표 1 에는 다양한 VTN 및 CrossCert 준칙 문서와 이들의 공개 상태 및 해당 위치가 나와 있습니다. 모든 문서가 이 표에 나와 있는 것은 아니며, 공개 상태가 아닌 문서는 VTN 보안을 위한 기밀 문서입니다.

문서	*상태*	*문서 위치*
VeriSign Trust Network 인증 정책	공개	CrossCert 저장소(CP § 8.2.2), https://www.crosscert.com/repository 참조
VTN 보안 및 운영 보조 문서		
CrossCert Security Policy(CrossCert 보안 정책)	대외비	해당 없음
Security and Audit Requirements Guide(보안 및 감사 요구 사항 가이드)	대외비	해당 없음
Key Ceremony Reference Guide(키 형식 참조 가이드)	대외비	해당 없음
Managed PKI Administrator's Handbook(Managed PKI 관리자 핸드북)	공개	https://www.crosscert.com/enterprise/library/index.html
Managed PKI Key Management Service Administrator's Guide(Managed PKI 키 관리 서비스 관리자 가이드)	공개	https://www.crosscert.com/enterprise/library/index.html
Enterprise Security Guide(기업 보안 가이드)	대외비	해당 없음
VeriSign 관련 문서		
CrossCert 인증업무준칙	공개	CrossCert 저장소(CPS § 2.6.1.), https://www.crosscert.com/Repository 참조
CrossCert 의 보조 계약서(Managed PKI 계약서, 가입 계약서 및 신뢰 당사자 계약서)	Managed PKI Lite 계약서를 포함하여 모두 공개(기밀 문서인 Managed PKI 계약서는 제외)	CrossCert 저장소(CPS § 2.6.1.), https://www.crosscert.com/Repository 참조

표 1 – 준칙 문서 공개 여부

(b) 디지털 인증서 및 VTN 하위구조에 대한 배경

이 CPS에서는 독자가 대체적으로 디지털 서명, PKI 및 VTN에 익숙한 것으로 간주합니다. 따라서 익숙하지 않은 경우에는 VTN에 적용하기 전에 공개키 암호화 및 공개키기반구조의 사용에 관한 교육을 받는 것이 좋습니다. 일반 교육 정보는 CrossCert 웹 페이지 **http://www.crosscert.com**에 나와 있습니다. 또한 VTN 참여자 간의 역할에 대한 간략한 설명은 CP의 1.1(b)항에서 확인할 수 있습니다.

(c) 해당 표준 준수

본 CPS 에 명시된 준칙은 CA 를 위한 AICPA/CICA WebTrust 프로그램, ANS X9.79:2001 PKI 준칙 및 정책 프레임워크, 기타 CA 운영과 관련된 다른 업계 표준 등을 포함하여 일반적으로 사용되고 있는 업계 표준의 요구 사항 이상을 충족하도록 구성되었습니다.

이 CPS 의 구조는 일반적으로 인터넷 표준 단체인 IETF(Internet Engineering Task Force)의 RFC 2527(*Internet X.509 공개키기반구조 인증서 정책 및 인증 업무 프레임워크*)을 따르고 있습니다. RFC 2527 은 PKI 업계 표준이 되었습니다. 이 CPS 는 VeriSign 서비스 사용자나 사용을 고려 중인 잠재 고객이 정책 매핑, 비교, 평가 및 상호운용을 보다 간편하게 수행할 수 있도록 하기 위해 RFC 2527 을 준수합니다.

CrossCert 는 가능한 경우 CPS 를 RFC 2527 구조에 맞추었지만 CrossCert 비즈니스 모델이 매우 복잡하기 때문에 제목이나 세부 내용이 약간 다를 수도 있습니다. CrossCert 는 앞으로도 RFC 2527 을 준수하는 정책을 고수할 것입니다. 그러나 CPS 의 품질을 개선하거나 CrossCert 하위 도메인 참여자에게 맞추는 등의 경우에는 필요에 따라 RFC 2527 구조와 약간 달라질 수 있습니다. 또한 CPS 구조는 향후 RFC 2527 버전과 맞지 않을 수도 있습니다.

1.1.1 정책 개요

CrossCert 는 유무선 인터넷 및 다른 네트워크용으로 세 가지 클래스의 인증 서비스를 제공하고 있으며, 이러한 인증 서비스는 CP 에 해당 정책이 설명되어 있는 세 가지 클래스의 인증서에 대응됩니다. 인증서의 각 레벨 또는 클래스는 특정 기능 및 보안 특징이 있으며 특정 수준의 신뢰도를 제공합니다. CrossCert 하위 도메인 참여자는 이들 중 자신에게 맞는 인증서 클래스를 선택할 수 있습니다.

CP의 기능 중 하나는 이 세 가지 인증서 클래스에 대한 자세한 설명을 제공하는 것입니다.[5] 여기에서는 CrossCert가 해당 하위 도메인 내에서 제공하는 인증서 클래스에 대해 간략히 설명합니다.

클래스 1 인증서는 CrossCert 의 하위 도메인 내에서 가장 낮은 수준의 보증을 제공합니다. 이 인증서는 개인에게 발행되며, 확인 절차의 기준은 가입자의 식별명(DN)이 CA 의 하위 도메인 내에서 고유하고 명확한지 여부와 특정 E-mail 주소가 공개키와 연관되어 있는지 여부입니다. 이 인증서는 신원 확인이 필요 없는 비상업적 또는 소규모 거래의 디지털 서명, 암호화 및 액세스 제어에 적합합니다.

클래스 2 인증서는 다른 두 가지 클래스 인증서와 비교할 때 중간 수준의 보증을 제공하며 이 인증서 또한 개인에게 발행됩니다. 확인 절차 기준은 클래스 1 의 확인 절차 기준에,

[5] CP § 1.1.1 을 참조하십시오.

인증서 신청자가 제출한 정보를 비즈니스 기록이나 데이터베이스 또는 CrossCert 신원 확인 서비스의 데이터베이스에 있는 정보와 비교하는 절차가 추가됩니다. 이 클래스의 인증은 중간 규모의 거래를 위한 신원 확인, 디지털 서명, 암호화 및 액세스 제어에 사용할 수 있습니다.

클래스 3 인증서는 CrossCert 의 하위 도메인 내에서 가장 높은 수준의 보증을 제공합니다. 이 인증서는 개인 및 단체는 물론 CA 와 RA 의 관리자에게 발행됩니다. 클래스 3 개인 인증서는 대규모 거래를 위한 신원 확인, 디지털 서명, 암호화 및 액세스 제어에 사용할 수 있습니다. 이 개인 인증서는 가입자가 신원을 확인하는 담당자에게 일반적 종류의 정부 발행 ID 와 다른 하나의 신분 증명서를 직접 제출해야 발행됩니다. 클래스 3 의 다른 단체 인증서는 장치를 대상으로 발행되며 메시지, 소프트웨어 및 컨텐트 무결성 등에 대한 인증과 비밀 암호화를 제공합니다. 클래스 3 단체 인증서는 해당 가입 단체가 실제로 존재하는지 여부와 이 단체가 인증 신청서를 승인했는지 여부 및 가입 단체를 대표하여 인증 신청서를 제출한 사람이 해당 권한을 부여받았는지 여부를 기준으로 발행됩니다. 서버용 클래스 3 단체 인증서(시큐어 서버 ID 및 글로벌 서버 ID)는 또한 가입자가 인증 신청서에 명시된 도메인 이름을 사용할 권한이 있음을 보증합니다.

아래 표 2 에는 CrossCert 가 CP 에 따라 제공하는 인증서 클래스의 요약 설명이 나와 있습니다. 이 표에서는 각 인증서 클래스의 발행 대상(개인 또는 단체) 및 인증서 종류(리테일, Managed PKI 용 또는 관리자용) 등과 같은 특징을 설명합니다.

이 CPS 의 요약 설명과 같이 인증서 클래스의 명세서에는 각 클래스에 대한 최소 보증 수준이 명시되어 있습니다. 예를 들어, 클래스 1 인증서는 신원 증명이 필요 없는 낮은 보증 수준의 적용을 위한 디지털 서명, 암호화 및 액세스 제어에 사용됩니다. 그러나 계약서나 특정 환경(예: 사내)에 따라 CrossCert 하위 도메인 참여자는 CP 에 명시된 수준 이상의 검증 절차를 사용하거나, CPS §§ 1.1.1, 1.3.4.1 에 명시된 것보다 높은 보안 수준으로 적용하기 위한 인증서를 사용할 수도 있습니다. 이러한 변경은 CrossCert 하위 도메인 참여자에게만 허용되며 CPS §§ 2.2.1.2, 2.2.2.2 의 적용을 받습니다. 또한 CrossCert 하위 도메인 참여자는 이러한 변경으로 인해 생긴 손해에 대해 전적인 책임이 있습니다.

클래스	*발급 대상*	*인증서 사용이 가능한 서비스 종류* [6]	*인증 신청자 신원 확인 방법(CPS §§ 3.1.8.1, 3.1.9)*	*사용자의 적용 용도 (CPS § 1.3.4.1)*

[6] 리테일 인증서는 CA 역할을 하는 CrossCert 가 해당 웹 사이트에서 CrossCert 에 하나씩 신청하는 개인 또는 단체에게 발행하는 인증서입니다. 반면 Managed PKI 인증서는 특정 수량의 인증서 발행을 위해 CrossCert 와

클래스	*발급 대상*	*인증서 사용이 가능한 서비스 종류*[6]	*인증 신청자 신원 확인 방법(CPS §§ 3.1.8.1, 3.1.9)*	*사용자의 적용 용도 (CPS § 1.3.4.1)*
클래스 1	개인	리테일	CA 의 하위 도메인 내에서 식별명(DN)이 고유하고 명확한지 확인하기 위해 이름과 E-mail 주소를 확인합니다.	신원 증명이 필요 없는 경우 암호화, 디지털 서명 및 웹 기반 액세스 제어를 통해 E-mail 보안을 향상합니다. 비상업적 웹 검색 및 E-mail 과 같이 다른 클래스에 비해 요구되는 보안 수준이 낮은 경우에 적용됩니다.
클래스 2	개인	Managed PKI	클래스 1 Managed PKI 와 동일하며 여기에 추가로 인증 신청자의 신원 확인을 위해 인사부 문서 등의 내부 문서나 데이터베이스를 확인합니다.	암호화, 디지털 서명 및 웹 기반 액세스 제어 등을 통해 E-mail 보안을 향상합니다. 개인, 사내 및 회사간 E-mail, 온라인 가입, 계정 신청, 패스워드 변경, 중간 규모의 거래를 위한 신원 증명 등과 같이 다른 클래스에 비해 보안 수준이 중간인 경우에 적용됩니다.
클래스 3	개인	관리자	관리자 유형에 따른 특별 확인 절차로서, 관리자의 신원과 관리자를 활용하는 단체의 신원을 확인합니다. CPS § 5.2.3 을 참조하십시오.	관리자 기능에 적용됩니다.

계약을 맺은 Managed PKI 고객이 승인하는 인증서 신청을 기반으로 발행됩니다(CP § 1.1.2.1.1 참조). 또한 VTN 인증서는 CA 및 RA 의 관리자를 대상으로 ASB(Authentication Service Bureau)를 통해 발행됩니다. ASB(Authentication Service Bureau)에 대한 자세한 내용은 CP § 1.1.2.2.1 을 참조하십시오. 관리자 인증서는 CA 또는 RA 관리자들이 CA 또는 RA 를 대표하여 관리 기능을 수행할 수 있도록 발행됩니다.

클래스	발급 대상	인증서 사용이 가능한 서비스 종류[6]	인증 신청자 신원 확인 방법(CPS §§ 3.1.8.1, 3.1.9)	사용자의 적용 용도 (CPS § 1.3.4.1)
	기업	리테일	해당 단체의 이름에 대한 사용권을 증명하는 제 3 의 데이터베이스나 다른 문서를 확인합니다. 인증 신청 후 내용 확인과 승인을 위해 전화 또는 이와 유사한 방법으로 확인합니다. 웹 서버 인증서의 경우 해당 도메인 이름에 대한 인증 신청자의 사용 권한이 인증서에 명시되어야 합니다.	서버 인증, 암호화, 다른 서버와의 통신 시 클라이언트 인증(시큐어 서버 ID, 글로벌 서버 ID, WTLS(Wireless Transport Layer Security) 인증서), 메시지 무결성 인증, 소프트웨어 및 다른 컨텐트 무결성 인증에 적용됩니다.
		Managed PKI	클래스 3 단체 리테일 인증에서와 같이 SSL 고객용 Managed PKI 또는 SSL Premium Edition 고객용 Managed PKI 를 확인하고 여기에 추가로 Managed PKI 관리자를 확인합니다.	서버 인증, 암호화, 다른 지원 서버와의 통신 시 클라이언트 인증(시큐어 서버 ID 및 글로벌 서버 ID)에 적용됩니다.

표 2 – 신뢰도에 영향을 미치는 인증서 특징

1.1.2 VeriSign 의 VTN 서비스

CP § 1.1.2 의 설명과 같이 VTN은 인증서의 설치, 관리 및 사용을 위해 일련의 서비스를 제공합니다. 여기서는 CrossCert가 CP § 1.1.2 에 따라 제공하는 서비스를 설명합니다. 이런 서비스에 대한 자세한 내용은 **http://www.crosscert.com**을 참조하십시오. 이러한 모든 서비스는 CrossCert와 맺은 계약서의 적용을 받습니다. 표 3 에는 CrossCert가 제공하는 VTN 서비스의 요약 설명이 나와 있습니다.

VTN 서비스	CP 내의 해당 위치	CrossCert 제공 서비스
인증서 배포 서비스		
VeriSign Managed PKI	CP § 1.1.2.1.1	Managed PKI
		Managed PKI Lite
		SSL 용 Managed PKI
부가가치 서비스		
VeriSign 디지털 공증 서비스	CP § 1.1.2.2.2	CrossCert 디지털 공증 서비스
CrossCert 에서 현재 제공되지 않음		
특별 인증서 유형		
CrossCert Key Manager 서비스가	CP § 1.1.2.3.2	Managed PKI Key Manager 이중 키 시스템

VTN 서비스	*CP 내의 해당 위치*	*CrossCert 제공 서비스*
제공하는 VeriSign Managed PKI		Managed PKI Key Manager 단일 키 시스템
CrossCert 가 제공하는 VeriSign 로밍 서비스	CP § 1.1.2.3.3	기업이 기업 로밍 서버를 보유하는 로밍 서비스
		공인된 제 4 의 기관이 기업 로밍 서버를 보유하는 로밍 서비스

표 3 – CrossCert 가 제공하는 VTN 서비스

1.1.2.1 인증서 배포 서비스

1.1.2.1.1 CrossCert 가 제공하는 VeriSign Managed PKI

CrossCert 가 제공하는 VeriSign Managed PKI 는 완전 통합된 Managed PKI 서비스로서, CrossCert 의 기업 고객은 이 서비스를 통해 서버, 라우터 및 방화벽 등의 장치는 물론 직원, 제휴업체, 공급업체 및 고객 등의 개인에게 인증서를 제공합니다. CrossCert 가 제공하는 VeriSign Managed PKI 에 대한 보다 자세한 내용은 CP § 1.1.2.1.1 에 나와 있으며, CrossCert 의 하위 도메인 내에서 Managed PKI 에 필요한 보안 요구 사항은 Enterprise Security Guide(기업 보안 가이드)에 명시되어 있습니다. Managed PKI 는 아웃소싱 서비스입니다. CrossCert 가 제공하는 VeriSign Managed PKI 를 사용하는 CrossCert 고객("Managed PKI 고객")은 다음 세 가지 범주로 구분됩니다.

첫번째 범주는 VTN 의 CrossCert 하위 도메인 내에서 인증 기관이 되어 클라이언트 인증서를 제공하는 일부 Managed PKI 고객("Managed PKI 고객")입니다. Managed PKI 고객은 인증 신청을 승인 또는 거부하는 RA 의 "프론트엔드" 기능을 수행하며 Managed PKI 기능을 사용하여 인증서를 폐지 또는 갱신하기도 합니다. RA 기능은 CA 기능의 하위 기능입니다. Managed PKI 고객은 또한 인증서 발행, 관리, 폐지 및 갱신 등의 모든 "백엔드" 작업을 CrossCert 에 아웃소싱하여 VeriSign Trust Network 의 안전한 PKI 구조를 이용할 수 있습니다.

두번째 범주의 Managed PKI 고객("Managed PKI Lite 고객")은 일반 Managed PKI 고객에 비해 작은 규모의 기업 및 단체에 보안을 제공하는 Managed PKI Lite 를 사용합니다. Managed PKI Lite 고객은 CrossCert CA 와 연관된 등록 기관이 됩니다. 여기서 CrossCert CA 는 특정 인증서 클래스의 CrossCert Managed PKI Lite 고객 간에 공유됩니다. Managed PKI 고객과 마찬가지로 Managed PKI Lite 고객은 Managed PKI 기능을 사용하여 인증 신청을 승인 또는 거부하고 인증서 폐지 또는 갱신을 요청하기도 합니다. CrossCert 는 Managed PKI 고객에서와 마찬가지로 모든 백엔드 인증서 발행, 관리, 폐지 및 갱신 기능을 수행합니다.

마지막 범주의 Managed PKI 고객은 시큐어 서버 ID("SSL 고객용 Managed PKI")라는 서버 인증서와 글로벌 서버 ID("SSL Premium Edition 고객용 Managed PKI")라는 서버 인증서에 대한 인증 신청을 승인합니다. 시큐어 서버 ID 와 글로벌 서버 ID 간의 차이점에 대해서는 "CPS 정의"를 참조하십시오. SSL 고객용 Managed PKI 와 SSL Premium Edition 고객용 Managed PKI 는 CrossCert CA 와 연관된 등록 기관이 됩니다. 여기서 CrossCert CA 는 모든 VTN(CrossCert 포함)의 SSL 고객용 Managed PKI 또는 SSL Premium Edition 고객용 Managed PKI 간에 공유됩니다. SSL 고객용 Managed PKI 와 SSL Premium Edition 고객용 Managed PKI 는 다른 Managed PKI 고객에서와 마찬가지로 Managed PKI 기능을 사용하여 인증 신청을 승인 또는 거부하고 인증서의 폐지 및 갱신을 요청하기도 합니다. 또한 CrossCert 는 다른 Managed PKI 인증서에서와 마찬가지로 모든 백엔드 인증서 발행, 관리, 폐지 및 갱신 기능을 수행합니다.

CrossCert 의 Managed PKI 고객 및 Managed PKI Lite 고객은 다음 경우를 제외하고 해당 개인 회원이 아니면 어떠한 인증 신청도 승인할 수 없습니다. Managed PKI 고객은 일반인에게 발행된 VTN 인증 신청을 승인할 수 없습니다. 그러나 ASB(Authentication Service Bureau)에서는 회원이 아닌 개인 및 단체 대표를 위한 인증서를 얻으려는 단체를 위해 한가지 솔루션을 제공합니다. CPS § 1.1.2.2.1 을 참조하십시오.

SSL 고객용 Managed PKI 와 SSL Premium Edition 고객용 Managed PKI 는 해당 단체 내의 서버에 대한 인증 신청만 승인할 수 있으며, 해당 단체 외부의 어떠한 서버에 대해서도 클래스 3 인증 신청을 승인할 수 없고 일반인에게 인증서를 발행할 수도 없습니다.

1.1.2.1.2 VeriSign 회원 프로그램

CP §1.1.2.1.2 에 나온 설명과 같이 CrossCert 는 리테일 인증서나 Managed PKI 인증서의 경우 인증 신청을 승인 또는 거부할 수 있고, 프로세싱 센터와 함께 Managed PKI 고객에게 백엔드 인증 주기 서비스를 제공할 수 있는 서비스 센터입니다. 클라이언트 인증서를 제공하는 서비스 센터 지사("클라이언트 서비스 센터")는 VTN 내에서 CA 가 되지만 백엔드 기능은 VeriSign 이나 다른 프로세싱 센터에 아웃소싱합니다. 그러나 서비스 센터는 서버 인증서를 제공할 때 VeriSign CA 를 위한 VTN 내에서 RA 가 되어 시큐어 서버 ID 또는 글로벌 서버 ID 를 발행합니다. 이러한 서비스 센터는 유효성 확인 기능을 수행하여 시큐어 서버 ID 또는 글로벌 서버 ID 를 위한 인증 신청을 승인하거나 거부합니다. 또한 해당 Managed PKI 고객에게 VeriSign Managed PKI 를 제공할 수도 있습니다. 이러한 Managed PKI 고객은 서비스 센터 Managed PKI 규약의 적용을 받으며, 이 경우 프로세싱 센터는 서비스 센터가 CrossCert 나 다른 프로세싱 센터와 맺은 계약에 따라 이들 Managed PKI 고객에게 백엔드 인증 주기 서비스를 제공합니다. CP § 1.1.2.1.2 의 설명과 같이 CrossCert 는 "프로세싱 센터"이기도 합니다. 즉 CrossCert 는 안전한 설비 보관 기능 외에도, 인증서 발행에 사용되는 개인키가 들어 있는 암호 모듈을 포함하여 CA 시스템을 구축했습니다. CrossCert 는 VTN 에서 CA 의 역할을 수행하며 인증서 발행, 관리, 폐지 및 갱신 등의 모든 인증 주기 서비스를 제공합니다. CrossCert 는 또한 Managed PKI 고객이나 CrossCert 하위 서비스 센터의 Managed PKI 고객을 대신하여 CA 키 관리 및 인증 주기 서비스를 제공합니다. CP § 1.1.2.1.2 의 설명과 같이 CrossCert 는

소비자(클래스 1 및 2 클라이언트 리테일 인증서), 웹 사이트(시큐어 서버 ID 및 글로벌 서버 ID) 및 기업(Managed PKI 서비스 제공) 모두에 인증서를 제공합니다. 회원사가 제공하는 서비스나 VeriSign 이 회원사에 제공하는 서비스와 관련된 업무는 본 CPS 에서 다루지 않습니다.

1.1.2.1.3 제공되지 않음

1.1.2.1.4 CrossCert 에서 현재 제공하지 않음

1.1.2.2 부가가치 인증 서비스

1.1.2.2.1 CrossCert 에서 제공하지 않음

1.1.2.2.2 CrossCert 가 제공하는 VeriSign 디지털 공증 서비스

CP § 1.1.2.2.2 에 명시된 것과 같이 CrossCert 는 "CrossCert 가 제공하는 VeriSign 디지털 공증 서비스"를 제공합니다. 이러한 CrossCert 의 서비스는 CrossCert 와, CrossCert 가 제공하는 VeriSign 디지털 공증 서비스의 고객 간에 맺어진 계약 조항의 적용을 받습니다.

1.1.2.2.3 CrossCert 에서 제공하지 않음

1.1.2.3 특별 인증서 유형

1.1.2.3.1 CrossCert 에서 현재 제공하지 않음

.

1.1.2.3.2 CrossCert 가 제공하는 VeriSign Managed PKI Key Manager 서비스

Managed PKI Key Manager 를 통해 Managed PKI 고객은 인증 신청 승인 대상인 가입자를 대신하여 키 쌍을 생성할 수 있습니다. 또한 Managed PKI 고객은 이 Key Manager 를 사용하여 해당 가입자에게 개인키를 안전하게 전송하고 가입자 개인키의 백업 사본을 안전하게 보관할 수 있으며 필요할 경우 개인키를 복구할 수도 있습니다. Managed PKI Key Manager 는 단일 키 쌍 시스템과 이중 키 쌍 시스템을 모두 지원합니다. 단일 키 쌍 시스템은 최종 사용 가입자가 디지털 서명 및 기밀 기능 모두에 사용할 키를 생성합니다. 가입자는 하나의 인증서를 통해 두 가지 기능 모두를 획득하게 됩니다 반면 이중 키 쌍 시스템은 최종 사용 가입자가 기밀을 위해 사용하는 키 쌍만 생성합니다. 디지털 서명

기능을 위한 키 쌍은 가입자가 스스로 생성해야 합니다. 이중 키 쌍 시스템에서 가입자는 각 공개키에 대한 인증서를 하나씩 총 두개를 받게 됩니다. Managed PKI Key Manager 소프트웨어는 CrossCert 가 제공하는 VeriSign 키 복구 서비스와 함께 작동합니다. Managed PKI Key Manager 에 대한 자세한 내용은 CP § 1.1.2.3.2 를 참조하십시오.

Managed PKI Key Manager 소프트웨어는 개인키의 백업 사본을 Managed PKI 고객 사이트에 암호화 형태로 저장합니다. 각 가입자의 개인키는 고유한 키 암호화 키를 사용하여 개별적으로 암호화됩니다. 키 복구 블록("KRB")은 키 복구 기술을 사용하여 이 암호화 키에서 생성되며 KRB 가 생성된 후 암호화 키는 삭제됩니다. 가입자의 암호화된 개인키와 KRB 는 모두 Managed PKI 고객 시스템의 Key Manager 데이터베이스에 저장됩니다.

Managed PKI Key Manager 소프트웨어는 CrossCert 가 제공하는 VeriSign 키 복구 서비스와 함께 작동합니다. 개인키를 복구하려면 일단 Managed PKI Key Manager 가 필요하며, Managed PKI 고객의 관리자 지시에 따라 데이터베이스에서 KRB 를 가져온 후 CrossCert 의 안전한 데이터 센터 외부에서 작동하는 키 복구 서비스로 온라인 전송해야 합니다. KRB 잠금을 해제하고 내장된 암호화 키를 복구할 수 있는 개인키는 CrossCert 만 보유합니다. CrossCert 가 수신하는 복구 요청에는 KRB 잠금 해제를 허용하는 데 필요한 기업 비상 복구 코드가 포함됩니다. 유효한 KRB 가 전송되고 정확한 비상 복구 코드가 제공되면 키 복구 서비스는 Managed PKI Key Manager 소프트웨어에 암호화 키를 반환하여 해당 사용자 개인키를 복구하도록 합니다.

1.1.2.3.3 CrossCert 가 제공하는 VeriSign 로밍 서비스

CrossCert 의 Managed PKI 고객에 나온 것과 같이 "CrossCert 가 제공하는 VeriSign 로밍 서비스"를 사용할 경우, 가입자는 주식 거래와 같은 중요 거래에 디지털 서명을 사용하여 해당 개인키가 상주하는 단일 클라이언트 터미널에 접속할 필요 없이 기밀 정보에 액세스할 수 있습니다. CrossCert 의 로밍 서비스를 사용하는 가입자("로밍 가입자")는 자신의 개인키를 안전하게 다운로드하여 다른 클라이언트 터미널에서 사용할 수 있습니다. 로밍 가입자는 모든 클라이언트 터미널에서 자신의 개인키를 사용할 수 있습니다.

CrossCert 가 제공하는 VeriSign 로밍 서비스는 분리되어 각기 다른 위치의 두 서버에 저장된 대칭 키를 사용하여 로밍 가입자의 개인키를 암호화함으로써 단일 인증 서버에 대한 공격을 방지합니다. 즉 이런 대칭 키의 컴포넌트는 Managed PKI 고객("기업 로밍 서버") 또는 Managed PKI 고객을 대신하는 제 4 공인 단체의 사이트에 위치한 서버와 CrossCert("CrossCert 로밍 서버")에 위치한 다른 서버로 각각 분리됩니다. 개인키 자체는 기업 로밍 서버에 암호화된 형태로 저장됩니다. 로밍 가입자는 패스워드가 서버에 제대로 제공되었다는 가정 하에 이 패스워드를 사용하여 스스로 이들 서버에 대해 인증을 승인합니다. 그러면 암호화된 개인키와 가입자의 개인키를 해독하는 데 필요한 대칭 키의 컴포넌트가 클라이언트 터미널에 다운로드됩니다. 클라이언트 터미널에서 이 대칭 키가 재구성되고 가입자의 개인키가 해독되면 단일 세션 동안 이 개인키를 사용할 수 있게

됩니다. 이 세션이 끝나면 클라이언트 터미널의 개인키는 복구가 불가능하도록 영구 삭제됩니다.

1.2 신원 확인

본 문서는 CrossCert 인증업무준칙입니다. VTN 인증서에는 해당 VTN 인증 클래스에 대응되는 객체 식별자 값이 포함되어 있습니다. 따라서 CrossCert 는 이 CPS 에서 객체 식별자 값을 지정하지 않았습니다. 인증서 정책 객체 식별자는 CPS § 7.1.6 에 따라 사용됩니다.

1.3 커뮤니티 및 적용

본 CPS 가 적용되는 커뮤니티는 VeriSign Trust Network 내의 CrossCert 하위 도메인입니다. VTN 은 통신 및 정보 보안에 대해 다양한 요구 사항을 갖고 있는 전세계 수 많은 유무선 사용자들에게 서비스를 제공하는 PKI 입니다. VTN 의 CrossCert 하위 도메인은 VTN 중 본 CPS 가 적용되는 부분이며, CPS 는 VTN 의 CrossCert 하위 도메인을 제어하는 문서입니다. 대부분의 CrossCert 하위 도메인 참여자는 한국에 있습니다.

1.3.1 인증 기관

인증 기관(CA)이란 용어는 VTN 내에서 인증서를 발행하는 모든 개체를 포괄적으로 일컫는 용어입니다. "CA"는 주요 인증 기관(PCA)이라고 하는 하위 범주의 발행 기관을 포함합니다. PCA는 각 인증서 클래스에 속한 총 세 가지 도메인의 루트 역할을 합니다.[7]각 PCA는 VeriSign 개체입니다. 현재 각 인증서 클래스별로 세 가지 세대의 VeriSign PCA(G1, G2 및 G3)가 있습니다. PCA 아래에는 최종 사용 가입자나 다른 CA에 인증서를 발행하는 인증 기관이 있습니다. CrossCert 하위 도메인 내의 CA는 (1) CrossCert (2) Managed PKI 고객의 두 가지 범주로 나뉩니다. VeriSign은 모든 VTN PCA를 호스트하는 프로세싱 센터이고, CrossCert는 해당 CA와 안전한 CA내의 일부 다른 CA를 모두 호스트하는 프로세싱 센터입니다.

CrossCert CA 는 RA 기능을 포함하여 모든 CA 기능을 수행하지만 Managed PKI Lite 고객 및 SSL 고객용 Managed PKI 가 인증 신청을 승인한 후 인증서를 발행하는 CA 의 기능은 수행하지 않습니다. Managed PKI 고객은 VTN 내에서 CA 가 되며, RA 기능은 유지하면서 백엔드 기능을 프로세싱 센터에 아웃소싱합니다.

CP § 1.3.1 의 설명과 같이 VeriSign 이 RSA Security Inc.로부터 인수한 RSA 시큐어 서버 인증 기관은 클래스 3 단체 인증서인 시큐어 서버 ID 를 발행합니다. VeriSign 은 RSA 시큐어 서버 인증 기관을 VTN 의 CrossCert 하위 도메인 내에서 클래스 3 CA 로 승인 및 지정했습니다. RSA 시큐어 서버 인증 기관이 발행하는 인증서와 시큐어 서버 ID 는 다른 클래스 3 단체 인증서에 상응하는 보증 수준을 제공하는 것으로 간주됩니다.

1.3.2 등록 기관

VTN 의 CrossCert 하위 도메인 내에서 RA 는 (1) Managed PKI Lite 고객 (2) SSL 고객용 Managed PKI (3) SSL Premium Edition 고객용 Managed PKI (4) ASB 공급업체 역할을 하는 CrossCert 의 네 가지 범주로 나뉩니다. 다른 유형의 RA 는 CrossCert 의 사전 서면 동의를 받아야 합니다. 이러한 RA 가 Managed PKI 고객의 의무 사항을 충족할 경우, Managed PKI 기술과 이들 RA 가 사용하는 기술 간의 차이를 해결하기 위해 변경 작업이 필요하며 해당 계약서의 조건이 충족되어야 합니다. RA 는 신원 확인, 인증 신청 승인 또는 거부, 인증서 폐지 요구, 갱신 요구 승인 또는 거부 등의 프론트엔드 기능을 수행하여 CA 를 지원합니다.

Managed PKI Lite 고객은 RA 가 되어 CrossCert CA 가 최종 사용 가입자에게 클라이언트 인증서를 발행하도록 지원합니다. 마찬가지로 SSL 고객용 Managed PKI 또한 Managed PKI 를 사용하는 RA 가 되어 RSA 시큐어 서버 CA, VeriSign 국제 서버 CA – 클래스 3 또는 유사한 CrossCert CA 가 시큐어 서버 ID 나 글로벌 서버 ID 를 발행하도록 지원합니다.

1.3.3 최종 개체

표 4 는 각 클래스별 가입자 종류와 VTN 의 CrossCert 하위 도메인 내에서 제공되는 인증서 종류를 보여줍니다.

클래스	발급 대상	인증서 사용이 가능한 서비스 종류	가입자 유형
클래스 1	개인	리테일	모든 일반인입니다.
클래스 2	개인	Managed PKI	2 단계 인증 서비스의 경우를 제외하고 Managed PKI 고객과 관련이 있는 개인 회원입니다. 2 단계 인증 서비스에서 서비스를 획득한 Managed PKI 고객은 RA 기능을 관련 단체로 위임합니다. Managed PKI 인증서를 취득한 개인은 이러한 RA 기능을 위임받은 단체의 개인 회원이 되어야 합니다.
클래스 3	개인	관리자	관리자 역할을 하는 개인입니다(CrossCert, Managed PKI 고객 또는 제 3 공인 기관을 대신하여 인증서 또는 인증 서비스 관리 기능을 수행하는 권한을 부여받은 개인).
	단체	리테일	장치를 제어하는 단체는 다음을 포함하며 이에 제한되지는 않습니다. • 웹 서버 또는 웹 트래픽 관리 장치(시큐어 서버 ID 및 글로벌 서버 ID) • WTLS 서버 • EDI(Electronic Data Interchange) 서버 • OFX 서버 • 코드 또는 기타 컨텐트에 디지털 서명을 사용하는 장치
		Managed PKI	다수의 웹 서버를 제어하며, 해당 Managed PKI 관리자가 시큐어 서버 ID 및/또는 글로벌 서버 ID 발행을 승인하는 단체입니다.

표 4 – VTN 의 CrossCert 하위 도메인에 있는 가입자 종류

CA 는 엄밀히 말하면 인증서의 가입자입니다. 자신이 서명한 인증서를 스스로에게 발행하는 PCA 가 되거나, 상위 CA 가 발행한 인증서를 받는 CA 가 되기 때문입니다. 그러나 본 CPS 에서 "가입자"라고 하면 최종 사용 가입자만 해당됩니다.

1.3.4 적용 가능성

본 CPS 는 CrossCert, 고객, 리셀러, 가입자 및 신뢰 당사자 등을 포함하여 모든 CrossCert 하위 도메인 참여자에 적용되며, VTN 의 CrossCert 하위 도메인과 VTN 을 지원하는 CrossCert 의 핵심 기반구조에도 적용됩니다. 이 CPS 에서는 CP 의 설명과 같이 각 클래스 1-3 의 CrossCert 하위 도메인 내에서 인증서 사용에 적용되는 준칙에 대해 설명하고 있습니다. 각 클래스의 인증서는 일반적으로 CP § 1.3.4.1 및 CPS § 1.1.1(표 2)에 명시된 경우에 대해 사용하기에 적합합니다 그러나 계약 또는 특정 환경(예: 사내)에 따라 VTN 참여자들은 CPS §§ 1.1.1, 1.3.4.1 에 명시된 것보다 높은 보안 수준의 인증서를 사용할 수도

있습니다. 이러한 변경은 해당 개체에만 제한되며 CPS §§ 2.2.1.2, 2.2.2 의 적용을 받습니다. 이런 변경으로 인한 모든 손해에 대해서는 이러한 개체가 전적인 책임을 갖습니다.

1.3.4.1 적절한 적용

적절한 활용에 대한 내용은 CP § 1.3.4.1 및 CPS § 1.1.1(표 2)을 참조하십시오. 표의 항목은 요약본입니다. 개인 인증서와 일부 단체 인증서는 신뢰 당사자가 디지털 서명을 확인할 수 있도록 허용합니다. 해당 법규가 허용하는 범위 내에서, CrossCert 하위 도메인 참여자는 거래가 서면으로 이루어져야 하는 경우 VTN 인증서를 통해 확인 가능한 디지털 서명이 포함된 메시지 또는 기타 기록이 실제 서면 위에 서명한 같은 메시지 또는 기록과 동일한 유효성과 효과를 나타낸다는 것을 인정하고 동의합니다. 해당 법규의 범위 내에서, 디지털 서명이나 거래가 VTN 인증서를 통해 이루어지는 경우 VTN 인증서의 발행 장소, 디지털 서명 생성 및 사용 장소, CA 나 가입자의 장소 등과 관계 없이 유효합니다.

1.3.4.2 제한된 적용

일반적으로 VTN 인증서는 일반 목적을 지닌 인증서입니다. VTN 인증서는 전세계적으로 사용되며 다양한 신뢰 당사자와 호환도 가능합니다. VTN 인증서 사용은 시험 프로젝트, 금융 서비스 시스템, 수직적 시장 환경, 가상 시장 등과 같은 특정 비즈니스 환경에 국한되지 않습니다. 그러나 이러한 환경 속에서 인증서를 사용하는 고객들은 인증서 사용에 추가 제약 사항을 더할 수도 있습니다. 이 경우 CrossCert 와 CrossCert 하위 도메인 참여자는 이러한 추가 제약 사항을 감시 및 실행할 책임을 지지 않습니다.

일부 VTN 인증서는 기능면이 제한됩니다. 예를 들어, CA 인증서는 CA 기능을 제외한 어떤 기능에도 사용되지 못할 수 있습니다. 또한 클라이언트 인증서는 클라이언트에만 적용되어야 하며 서버나 단체 인증서로 사용할 수 없습니다. 장치에 대해 발행되는 클래스 3 단체 인증서의 기능은 웹 서버나 웹 트래픽 장치(시큐어 서버 ID 및 글로벌 서버 ID 의 경우) 및 객체 서명(객체 서명 인증서의 경우)에 한정되며, 관리자 인증서는 관리자 기능 수행에만 사용됩니다.

또한 X.509 버전 3 VTN 인증서의 경우, 인증서에서 공개키에 해당하는 개인키가 VTN 내에서 사용되도록 하기 위한 기술적 목적으로 키 사용 범위가 확장됩니다. CP § 6.1.9 를 참조하십시오. 사용자 등록 인증서는 CA 인증서로 사용되지 않습니다. 이러한 제한은 기본 규제(Basic Constraints)가 확장되지 않는 것으로 확인할 수 있습니다. CP § 7.1.2.4 를 참조하십시오. 그러나 확장 기반 제한의 효과는 CrossCert 이외의 업체가 개발 또는 제어하는 소프트웨어의 영향을 받습니다.

일반적으로 인증서는 해당 법규를 준수하는 범위 내에서, 특히 해당 수출입법이 허용하는 범위 내에서만 사용됩니다.

1.3.4.3 금지된 적용

VTN 인증서는 위험한 환경이나 이중 안전 장치가 필요한 경우에 적합하도록 설계되지 않았습니다. 즉, 핵 시설물, 항공기 운항 또는 통신 시스템, 항공 교통 제어 시스템, 무기 관리 시스템 등과 같이 잘못될 경우 인명 피해나 심각한 환경 손상이 따르는 경우에 대해서는 사용할 수 없습니다. 또한 CPS § 1.3.4 에 따라 클래스 1 인증서는 신원 증명 또는 신원 확인의 근거로 사용할 수 없습니다.

1.4 연락처

1.4.1 담당 조직

본 CPS 는 CrossCert 준칙 개발 부서에서 담당하고 있습니다. 문의 사항은 아래 연락처로 해주시기 바랍니다.

CrossCert
서울 서초구 서초동 1674-4
하림빌딩 9 층 한국전자인증 (우) 137-725
수신: Practices Development – CPS
CrossCert 전화 (02)3019-5500
CrossCert 팩스 (02)3019-5678
practices@crosscert.com

1.4.2 담당자

CPS에 관한 문의 사항은 cps-requests@CrossCert.com 또는 아래 주소로 연락하십시오.

CrossCert
서울 서초구 서초동 1674-4
하림빌딩 9 층 한국전자인증 (우) 137-725
수신: Practices Development – CPS
(02)3019-5563 (02)3019-5678
practices@crosscert.com

1.4.3 정책에 대한 CPS 적합성 여부 판단

CPS § 1.4.2 에 명시된 조직은 본 CPS 를 비롯하여 인증업무준칙과 관련된 보조 문서나 CPS 보조 문서가 CP 및 본 CPS 에 적합한지 여부를 판단할 책임이 있습니다.

2. 일반 조항

2.1 의무 사항

2.1.1 CA 의무 사항

CA 는 본 CPS 에 명시된 의무 사항을 이행합니다. CPS 의 각 조항은 CrossCert 프로세싱 센터, 서비스 센터 및 Managed PKI 고객 등과 같은 각 범주의 CA 에 대한 의무 사항을 명시하고 있습니다.

CrossCert 는 상업적으로 합당한 노력을 통해 가입 계약서 및 신뢰 당사자 계약서가 CrossCert 하위 도메인 내에서 가입자와 신뢰 당사자에게 구속력을 갖도록 보장합니다. 예를 들면 가입 계약서에 등록 조건으로 동의 조항을 넣거나, 신뢰 당사자 계약서에 인증서 상태 정보를 받는 조건으로 동의 조항을 넣습니다. 마찬가지로 리셀러는 계약상 필요한 경우 CrossCert 의 요구 사항에 따라 가입 계약서 및 신뢰 당사자 계약서를 사용해야 합니다. VeriSign 과 리셀러가 사용하는 가입 계약서 및 신뢰 당사자 계약서에는 CPS §§ 2.2-2.4 에 명시된 조항이 포함되어야 합니다.

Managed PKI 고객은 자신에게 해당되는 가입 계약서를 사용할 수 있으며 이것이 의무 사항은 아닙니다. 가입 계약서를 사용하는 Managed PKI 고객은 CP §§ 2.2-2.4 에서 요구하는 조항을 포함해야 합니다. Managed PKI 고객이나 리셀러가 가입 계약서를 사용하지 않는 경우, CrossCert 의 가입 계약서가 적용됩니다. 리셀러에게 신뢰 당사자 계약서가 없는 경우에는 CrossCert 의 신뢰 당사자 계약서가 적용됩니다.

2.1.2 RA 의무 사항

RA 는 확인 기능 수행, 인증 신청 승인 또는 거부, 인증서 폐지 요구, 갱신 요구 승인 등을 수행하여 프로세싱 센터 또는 서비스 센터 CA 를 지원합니다. CPS 에는 Managed PKI Lite 고객, SSL 고객용 Managed PKI 등과 같은 각 범주의 RA 에 대한 의무 사항이 명시되어 있습니다.
.

2.1.3 가입자 의무 사항

CP 의 가입자 의무 사항은 이 CPS 상에서 VeriSign 이 승인한 가입 계약서를 통해 CrossCert 하위 도메인 내의 가입자에게 적용됩니다. CrossCert 하위 도메인 내에서 유효한 일부 가입 계약서가 다음 주소에 나와 있습니다.
http://www.crosscert.com/Repository

CrossCert 하위 도메인 내의 가입 계약서 상에서 인증 신청자들은 인증 신청에 대한 정확하고 완전한 정보를 제공하고, 인증서 취득 조건으로 해당 가입 계약서에 대해 명백히 동의해야 합니다.

가입 계약서는 CP 및 CPS 에 명시된 세부 의무 사항을 CrossCert 하위 도메인의 가입자에게 적용합니다. 가입 계약서에 따라 가입자는 자신의 인증서를 CPS § 1.3.4 에 준하여 사용해야 하며, CPS §§ 6.1-6.2, 6.4 에 따라 자신의 개인키를 보호해야 합니다. 이러한 가입 계약서에 따라, 가입자는 자신의 개인키 또는 개인키를 보호하는 활성 데이터가 손상되었다고 판단될 경우 또는 인증서 내의 정보가 부정확하거나 변경된 경우에 즉각 다음과 같은 조치를 취해야 합니다.

- CPS § 4.4.1.1 에 따라 가입자의 인증 신청을 승인한 조직(CA 또는 RA)에 통보하고 CPS §§ 3.4, 4.4.3.1 에 준하여 인증서 폐지를 요청합니다.
- 가입자가 신뢰할 수 있는 담당자, 또는 가입자의 인증서나 가입자 인증서를 통해 확인 가능한 디지털 서명을 지원하는 서비스를 제공하는 담당자에게 통보합니다.

가입 계약서에 따라 가입자는 CPS § 6.3.2 에 명시된 키 사용 기간이 만료되면 본인의 개인키 사용을 중지해야 합니다.

가입자는 VeriSign 의 사전 서면 허가 없이 VTN 의 기술적 수행을 감시, 방해 또는 분석할 수 없으며 VTN 의 보안을 고의로 손상해서도 안됩니다.

2.1.4 신뢰 당사자 의무 사항

CP의 신뢰 당사자 의무 사항은 이 CPS 상에서 CrossCert의 신뢰 당사자 계약서를 통해 CrossCert 하위 도메인 내의 신뢰 당사자에게 적용됩니다. CrossCert 하위 도메인 내에서 유효한 신뢰 당사자 계약서는 다음 주소에 나와 있습니다.
http://www.crosscert.com/Repository/rpa/index.html

CrossCert 하위 도메인의 신뢰 당사자 계약서에 따라, 신뢰 당사자는 인증서 사용이 모든 목적에 적합한지 여부를 독립적으로 평가한 후 인증서가 합당한 목적에 사용되도록 결정해야 합니다. 또한 CrossCert, CA 및 RA 는 인증서 사용의 적합성 여부를 판단할 책임이 없습니다. 신뢰 당사자 계약서는 신뢰 당사자가 인증서를 CPS § 1.3.4.2 에 명시된 제한 범위를 벗어나는 목적이나 CPS § 1.3.4.3 에 명시된 금지 사항에 해당되는 목적으로 사용할 수 없도록 규정하고 있습니다.

신뢰 당사자 계약서에 따라 신뢰 당사자는 또한 적합한 소프트웨어/하드웨어를 사용하여 디지털 서명을 확인하거나 기타 원하는 암호화 방법을 통해 인증서 신뢰 조건을 구축해야 합니다. 이러한 암호화 방법의 예로는 인증 체인 확인, 해당 인증 체인의 모든 인증서에 대한 디지털 서명 확인 등이 있습니다. 이러한 계약서에 따라 신뢰 당사자는 위의 확인 절차가 성공적이지 않을 경우 인증서를 신뢰해서는 안됩니다.

또한 신뢰 당사자 계약서 상에서 신뢰 당사자는 CPS §§ 4.4.10, 4.4.12 에 따라, 신뢰하려는 인증서의 상태는 물론 해당 인증 체인의 모든 인증서 상태를 확인해야 합니다. 인증

체인의 인증서 중 하나라도 폐지된 경우, 신뢰 당사자는 신뢰 당사자 계약서에 따라 사용자 등록 인증서 또는 해당 인증 체인의 다른 폐지된 인증서를 신뢰해서는 안됩니다.

마지막으로 신뢰 당사자 계약서에서는 해당 계약서의 조건에 동의해야 인증서를 사용 또는 신뢰할 수 있음을 명시하고 있습니다. 신뢰 당사자인 동시에 가입자인 경우, 가입 계약서에 동의하면 신뢰 당사자 계약서 조건, 보증 부인 및 의무 조건을 준수할 의무가 생깁니다.

위에 명시된 모든 확인 사항이 통과되면 합당한 환경에서 신뢰 당사자는 인증서를 신뢰할 수 있습니다. 추가 보증이 필요한 경우에는 신뢰 당사자가 필요한 추가 보증을 획득해야 합니다.

신뢰 당사자 계약서에 따라 신뢰 당사자는 VeriSign 의 사전 서면 허가 없이 VTN 의 기술적 수행을 감시, 방해 또는 분석할 수 없으며 고의로 VTN 의 보안을 손상시켜서도 안됩니다.

2.1.5 저장소 의무 사항

CrossCert 는 해당 CA 및 Managed PKI 고객의 CA 를 위한 저장소 기능에 대해 책임이 있습니다. CrossCert 는 CPS § 2.6 에 따라 표 5 에 명시된 저장소에 발행한 인증서를 게시합니다.

CA	*CA 대신 인증서를 발행하는 기관*	*해당 저장소*
모든 CrossCert CA	CrossCert	CrossCert 저장소
Managed PKI 고객	CrossCert	CrossCert 저장소

표 5 – CA 유형별 해당 저장소

사용자 등록 인증서를 폐지할 때 CrossCert 는 표 5 에 나와 있는 저장소에 폐지 사실을 공지합니다. CrossCert 는 CPS §§ 2.6, 4.4.9, 4.4.11 에 따라 해당 CA, 서비스 센터의 CA 및 Managed PKI 고객을 위해 CRL 을 발행합니다. 또한 온라인 인증 상태 프로토콜("OCSP") 서비스에 계약한 Managed PKI 고객을 위해 CrossCert 는 CPS §§ 2.6, 4.4.9, 4.4.11 에 따라 OCSP 서비스를 제공합니다.

2.2 책임

2.2.1 인증 기관 책임

CrossCert 의 하위 도메인 내에서 CrossCert, 리셀러 및 각 해당 고객 간의 보증, 보증 부인 및 의무 제한은 이들 서로 간에 맺은 계약서의 적용을 받습니다. 이 CPS § 2.2.1 항은 특정

CA(CrossCert 및 Managed PKI 고객)가 인증서를 받는 최종 사용 가입자 및 신뢰 당사자에 대해 제공해야 하는 보증과, 이러한 가입자 및 신뢰 당사자에 대한 보증 부인 및 의무 제한에만 관련이 있습니다. CrossCert 와 리셀러(필요한 경우)는 CPS § 2.1.1 에 따라 가입 계약서 및 신뢰 당사자 계약서를 사용합니다. Managed PKI 고객의 경우 가입 계약서 사용은 선택 사항입니다. 이러한 가입 계약서는 CrossCert(리셀러의 경우)의 요구 사항을 충족해야 합니다. 요구 사항에 따라 가입 계약서에는 보증, 보증 부인 및 의무 제한이 포함되어야 하며, 이러한 요구 사항은 가입 계약서를 사용하는 리셀러와 Managed PKI 고객에 적용되어야 합니다. CrossCert 는 가입 계약서에서 이와 같은 요구 사항을 충족합니다. 신뢰 당사자 계약서에서 보증, 보증 부인 및 의무 제한과 관련된 CrossCert 의 업무 준칙은 {회원사}에 적용됩니다. 가입자는 신뢰 당사자 역할도 하는 경우가 많기 때문에 신뢰 당사자에 적용 가능한 조항은 신뢰 당사자 계약서뿐만 아니라 가입 계약서에도 포함되어야 합니다.

2.2.1.1 가입자 및 신뢰 당사자에 대한 인증 기관 보증

CrossCert 의 가입 계약서 및 다른 가입 계약서는 가입자에 대해 다음과 같은 내용을 보증해야 합니다.

- 인증 신청을 승인하거나 인증서를 발행하는 기관의 인증서에 내용 상의 오류가 없습니다.
- 인증 신청 관리 또는 인증서 작성을 적절히 수행하지 못했을 때 인증 신청을 승인하거나 인증서를 발행하는 기관이 제출하는 인증서 정보에 어떤 오류도 없습니다.
- 인증서가 본 CPS 의 모든 요구 사항을 충족합니다.
- 폐지 서비스 및 저장소 사용이 본 CPS 를 완전히 준수합니다.

CrossCert 의 신뢰 당사자 계약서는 인증서를 신뢰하는 신뢰 당사자에 대해 다음과 같은 내용을 보증합니다.

- 미확인 가입자 정보를 제외하고 인증서의 모든 정보와 참조 정보는 정확합니다.
- CrossCert 저장소에 있는 인증서의 경우, 인증서는 인증서에 '가입자'로 명명된 개인 또는 단체에 발행된 것이며 가입자는 CPS § 4.3 에 준하여 인증서를 받아들인 것입니다
- 인증 신청을 승인하거나 인증서를 발행하는 기관은 인증서 발행 시 본 CPS 를 준수하였습니다.

2.2.1.2 인증 기관의 보증 부인

해당 법규가 허용하는 범위 내에서 CrossCert 의 가입 계약서, 신뢰 당사자 계약서 및 다른 가입 계약서는 상품성이나 특정 목적에의 적합성을 포함하여 CrossCert 의 보증을 부인할 수 있습니다.

2.2.1.3 인증 기관의 의무 제한

해당 법규가 허용하는 범위 내에서 CrossCert 의 가입 계약서, 신뢰 당사자 계약서 및 다른 가입 계약서는 CrossCert 의 의무를 제한할 수 있습니다. 의무 제한에는 간접적, 특수적, 우발적 및 결과적 손해의 제외가 포함됩니다. 또한 각 인증서 클래스별 CrossCert 의 배상 책임 한도액은 다음과 같습니다.

클래스	*배상 책임 한도액*
클래스 1	₩120,000
클래스 2	₩6,000,000
클래스 3	₩120,000,000

표 6 – 배상 책임 한도액

CrossCert 는 동양화재 보험에 가입되어 있어 CrossCert 의 인터넷 및 네트워크 활동으로 인해 발생한 배상액에 대해 최대 1 백만 달러를 지급받습니다.

2.2.1.4 불가항력

해당 법규가 허용하는 범위 내에서 CrossCert 의 가입 계약서, 신뢰 당사자 계약서 및 다른 가입 계약서에는 CrossCert 를 보호하는 불가항력 조항이 포함되어 있습니다.

2.2.2 등록 기관 책임

RA, 인증서 발급을 지원하는 CA 및 해당 리셀러 간의 보증, 보증 부인 및 의무 제한은 이들 간에 맺은 계약서의 적용을 받습니다. CrossCert 는 해당 보증, 보증 부인 및 의무 제한 조항이 명시되어 있는 CPS §§ 2.1.1-2.1.2 에 따라 가입 계약서 및 신뢰 당사자 계약서를 사용합니다.

Managed PKI Lite 고객과 SSL 고객용 Managed PKI 는 가입 계약서와 신뢰 당사자 계약서를 사용하지 않으므로 이 항에 나온 준칙의 적용을 받지 않습니다. 대신 CrossCert 의 가입 계약서가 적용됩니다.

2.2.3 가입자 책임

2.2.3.1 가입자 보증

CrossCert 의 가입 계약서에 따라 가입자는 다음과 같은 내용을 보증해야 합니다.

- 인증서의 공개키에 대응되는 개인키를 사용하여 생성된 각 디지털 서명은 가입자의 디지털 서명이며, 인증서는 디지털 서명이 생성될 때 승인되어 만료 또는 폐지되지 않고 작동합니다.
- 가입자의 개인키에 무단 사용자가 액세스한 적이 없습니다.
- 가입자가 인증 신청서에 기재한 내용은 모두 사실입니다.
- 가입자가 제공한 정보와 인증서에 포함된 정보는 모두 사실입니다.
- 인증서는 본 CPS 에 준하여 승인된 합법적 목적으로만 사용됩니다.
- 가입자는 CA 가 아닌 최종 사용 가입자이며, 인증서의 공개키에 대응하는 개인키를 인증서(또는 기타 형식의 인증된 공개키)에 CA 로서 디지털 서명하는 데 사용하지 않습니다.

다른 가입 계약서에도 이러한 요구 사항이 포함되어 있습니다.

그러나 Managed PKI 고객이 Managed PKI Key Manager 를 사용하여 가입자의 인증 신청을 승인한 경우, 가입자는 가입자의 하드웨어/소프트웨어 플랫폼에서 가입자의 개인키 사본에 무단 사용자가 액세스한 적이 없다는 사실만 보증합니다. 이러한 가입자는 Managed PKI Key Manager 를 사용하는 Managed PKI 고객이 소유한 개인키 사본에 대해서는 어떠한 보증도 제공하지 않습니다.

2.2.3.2 개인키 손상

CP 는 가입자의 개인키 보호를 위해 VTN 표준을 마련해 놓고 있으며 이러한 표준은 CPS § 6.2.7.1 에 따라 가입 계약서에 포함되어 있습니다. 가입 계약서에 따르면 이러한 VTN 표준을 충족하지 못한 가입자는 이로 인해 발생한 모든 손실에 대해 전적인 책임이 있습니다.

2.2.4 신뢰 당사자 책임

가입 계약서 및 신뢰 당사자 계약서에 따라 신뢰 당사자는 인증서 상의 정보를 신뢰할 정도로 확실한 결정을 내리기에 충분한 정보를 가지고 있고, 이러한 정보의 신뢰 여부 판단에 대해 전적인 책임을 지며, CPS § 2.1.4 에 명시된 신뢰 당사자 의무 사항을 준수하지 않을 경우 따를 법적 결과에 책임질 것에 동의해야 합니다.

2.3 금전적 책임

2.3.1 가입자 및 신뢰 당사자의 배상

2.3.1.1 가입자의 배상

해당 법규가 허용하는 범위 내에서 CrossCert 의 가입 계약서 및 다른 가입 계약서에 따라 가입자는 다음과 같은 경우에 CrossCert 및 CrossCert 이외의 CA 나 RA 에 배상해야 합니다.

- 가입자가 인증 신청 시 사실을 잘못 기재한 경우

- 가입자가 인증 신청 시 실수로 또는 고의로 잘못된 내용을 기재하거나 중요한 내용을 생략한 경우
- 가입자가 자신의 개인키를 보호하지 못했거나 신뢰할 만한 시스템을 사용하지 않은 경우, 또는 사용자의 개인키가 손상, 분실, 공개, 수정 또는 무단 사용되지 않도록 필요한 예방조치를 취하지 않은 경우
- 가입자가 제 3 자의 지적 재산권을 침해하는 이름(일반 이름, 도메인 이름, E-mail 주소 등)을 사용한 경우

2.3.1.2 신뢰 당사자의 배상

해당 법규가 허용하는 범위 내에서 CrossCert 의 가입 계약서, 신뢰 당사자 계약서 및 다른 가입 계약서에 따라 신뢰 당사자는 다음과 같은 경우에 CrossCert 및 CrossCert 이외의 CA 나 RA 에게 배상해야 합니다.

- 신뢰 당사자가 자신의 의무 사항을 이행하지 않은 경우
- 신뢰 당사자가 부적합한 상황에서 인증서를 신뢰한 경우
- 신뢰 당사자가 인증서의 만료 또는 폐지 여부를 판단하기 위해 해당 인증서의 상태를 확인하지 않은 경우

2.3.2 신용 관계

해당 법규가 허용하는 범위 내에서 CrossCert 의 가입 계약서, 신뢰 당사자 계약서 및 다른 가입 계약서는 CrossCert 또는 CrossCert 이외의 CA 나 RA 와 가입자 또는 신뢰 당사자 간의 신용 관계를 부인할 수 있습니다.

2.3.3 행정 절차

Managed PKI 고객은 운영을 유지하고 의무를 이행하기에 충분한 만큼의 재원을 보유해야 하며, 가입자 및 신뢰 당사자에 대해 타당한 책임 관련 위험을 감수해야 합니다. 또한 Managed PKI 고객은 오류 및 태만에 관한 적정 수준의 보험에 가입하거나 자가 보험을 유지해야 합니다. 정부 기관의 경우에는 이 보험 요구 사항이 적용되지 않습니다. CrossCert 는 이러한 오류 및 태만에 대해 보험에 가입되어 있습니다.

2.4 법의 해석 및 집행

2.4.1 적용 법률

본 CPS 의 실행, 해석 및 유효성과 관련해서는 한국 법이 적용됩니다. 이때 계약이나 다른 법 조항 선택은 무시되며 한국에 관련 상업 조직을 설립할 의무는 없습니다. 이러한 법규 선택은 위치에 상관없이 CrossCert 하위 도메인의 모든 참여자에 대해 일관성있는 절차 및 해석을 수행하기 위한 것입니다.

이 법률 조항은 본 CPS 에만 적용됩니다. 해당 법규의 제한에 따라 이 CPS § 2.4.1 이 CPS 조항의 실행, 해석 및 유효성을 계약서의 나머지 조항과 별도로 적용하는 경우, CPS 가 포함된 계약서는 자체의 적용 법률 조항을 가지고 있을 수 있습니다.

본 CPS 는 하드웨어/소프트웨어 또는 기술 정보에 대한 수출입 제한을 비롯하여 국내법, 주법, 지방법, 외국법, 규칙, 규제, 조례, 명령 등의 적용을 받습니다.

2.4.2 잔여부분 유효 조항, 존속 조항, 완전 합의 조항, 통지 조항

해당 법규가 허용하는 범위 내에서 CrossCert 의 가입 계약서, 신뢰 당사자 계약서 및 다른 가입 계약서는 잔여부분 유효 조항, 존속 조항, 완전 합의 조항 및 통지 조항을 포함합니다. 잔여부분 유효 조항은 특정 조항의 무효화로 인해 계약의 나머지 조항이 무효화되지 않도록 보호합니다. 존속 조항은 계약이 종료 또는 만료된 후에도 계속 유효한 조항이고, 완전 합의 조항은 계약의 주된 내용에 관한 모든 합의 사항이 계약서에 포함되도록 하는 조항이며, 통지 조항은 당사자간 통지 방법에 관한 조항입니다.

2.4.3 분쟁 해결 절차

2.4.3.1 CrossCert 와 고객 간의 분쟁

CrossCert 와 해당 고객 간의 분쟁은 당사자 간에 맺은 계약서의 조항에 따라 해결되어야 합니다.

2.4.3.2 최종 사용 가입자 또는 신뢰 당사자와의 분쟁

해당 법규가 허용하는 범위 내에서 CrossCert 의 가입 계약서, 신뢰 당사자 계약서 및 다른 가입 계약서에는 분쟁 해결 조항이 나와 있습니다. 해당 조항에 따르면 분쟁을 해결하기 위해서는 60 일 간의 초기 협상 기간이 지난 후 당사자가 한국에 거주하는 경우 서울 지방법원에 소송을 제기하고, 한국에 거주하지 않는 경우에는 국제 상공 회의소("ICC")가 ICC 조정 및 중재 규정에 따라 중재 역할을 수행해야 합니다.

2.5 요금

2.5.1 인증서 발급 또는 갱신 요금

CrossCert 와 고객은 최종 사용 가입자에게 인증서의 발행, 관리 및 갱신 요금을 청구할 수 있습니다.

2.5.2 인증서 액세스 요금

CrossCert 와 고객은 인증서를 저장소에 두거나 신뢰 당사자에게 제공하는 경우에는 요금을 청구하지 않습니다.

2.5.3 폐지 또는 상태 정보 액세스 요금

CrossCert 는 CPS § 4.4.9 에 따라 요구되는 CRL 을 저장소에 두거나 신뢰 당사자에게 제공하는 경우에 요금을 청구하지 않습니다. CrossCert 는 그러나 사용자 정의 CRL, OCSP 서비스 또는 기타 부가가치 폐지 및 상태 정보 서비스를 제공하는 경우에는 요금을 청구합니다. CrossCert 는 CrossCert 의 사전 서면 동의 없이 인증서 상태 정보를 사용하는 제품이나 서비스를 공급하는 제 3 자가 폐지 정보, 인증서 상태 정보 또는 저장소의 Time Stamping 에 액세스하지 못하도록 금지합니다.

2.5.4 정책 정보 등의 기타 서비스 요금

CrossCert 는 CP 또는 본 CPS 에 대한 액세스에 요금을 부과하지 않습니다. 복제, 재배포, 수정, 파생물 생성 등과 같이 열람 이외의 목적으로 이 문서를 사용하는 것은 해당 문서의 저작권 소유자와의 라이센스 계약에 대한 적용을 받습니다.

2.5.5 환불 정책

CrossCert 하위 도메인에서는 다음과 같은 환불 정책이 적용됩니다(**http://www.crosscert.com/Repository/refund/** 참조).

CrossCert 는 인증 수행 및 인증서 발행에 있어 매우 엄격한 정책을 고수합니다. 그럼에도 불구하고 가입자가 자신에게 발행된 인증서에 대해 완전히 만족하지 못할 경우에는 발행일로부터 30 일 이내에 CrossCert 에 인증서 폐지 및 환불을 요청할 수 있습니다. 최초 30 일이 지난 후 CrossCert 가 가입자 또는 가입자의 인증서와 관련하여 본 CPS 상의 보증이나 기타 중대한 의무 사항을 위반한 경우 가입자는 해당 인증서의 폐지 및 환불을 요구할 수 있습니다. CrossCert 는 가입자의 인증서를 폐지한 후 해당 인증서에 대해 지급된 요금 전액을 가입자의 신용카드 계좌로(인증서가 신용카드로 지불된 경우) 즉시 입금하거나 수표로 환불합니다. 환불을 요청하려면 고객 서비스 센터 (02)3019-5500 으로 문의하십시오. 이 환불 정책은 유일한 구제책은 아니며 가입자들이 이용할 수 있는 다른 구제 수단을 제한하지 않습니다.

2.6 게시 및 저장소

2.6.1 CA 정보 게시

VeriSign 은 다음에 대해 저장소 기능을 담당합니다.

- VTN 을 지원하는 VeriSign 공식 기본 인증 기관(PCA) 및 VeriSign 기반구조/관리 CA
- CrossCert 는 CrossCert 의 기반구조 및 관리 CA 에 대한 저장소 기능을 담당합니다.

- VTN 의 CrossCert 하위 도메인 내에서 인증서를 발행하는 CrossCert CA 및 Managed PKI 고객 CA

아래 설명과 같이 CrossCert는 CrossCert 웹 사이트의 저장소 섹션 http://www.crosscert/com/Repository에 특정 CA 정보를 게시합니다.

CrossCert 는 CrossCert 웹 사이트의 저장소 섹션에 VeriSign VTN CP, CPS, 가입 계약서 및 신뢰 당사자 계약서를 게시합니다.

CrossCert 는 아래 표 7 과 같이 인증서를 발행합니다.

인증서 유형	*발행 요구 사항*
VeriSign PCA 및 VeriSign 발행 루트 CA 인증서	현재 브라우저 소프트웨어에 포함시켜 아래 설명된 질의 기능을 통해 사용자 등록 인증서와 함께 획득할 수 있는 인증 체인의 일부로 신뢰 당사자에게 제공할 수 있습니다.
CrossCert 발행 CA 인증서	아래 설명된 질의 기능을 통해 사용자 등록 인증서와 함께 획득할 수 있는 인증 체인의 일부로 신뢰 당사자에게 제공할 수 있습니다.
Managed PKI Lite 인증서와 Managed PKI 고객의 CA 인증서를 지원하는 CrossCert CA 의 인증서	directory.crosscert.com 에서 CrossCert LDAP 디렉토리 서버 질의를 통해 얻을 수 있습니다.
VeriSign OCSP Responder 인증서	directory.crosscert.com 에서 CrossCert LDAP 디렉토리 서버 질의를 통해 얻을 수 있습니다.
사용자 등록 인증서	다음 주소의 CrossCert 저장소에서 질의 기능을 통해 신뢰 당사자에게 제공할 수 있습니다. • https://digitalid.crosscert.com/Repository • directory.verisign.com 에서 VeriSign LDAP 디렉토리 서버 질의를 통해 얻을 수 있습니다.
Managed PKI 고객을 통해 발행된 사용자 등록 인증서	위에 나온 질의 기능을 통해 제공할 수 있습니다. Managed PKI 고객의 자유 재량이지만 인증서는 인증서의 일련 번호를 사용한 검색에서만 액세스가 가능합니다.

표 7 – 인증서 게시 요구 사항

CrossCert 는 CPS § 4.4.11 에 따라 인증서 상태 정보를 게시합니다.

2.6.2 게시 주기

CPS § 8 에 따라 본 CPS 에 대한 업데이트가 게시됩니다. 가입 계약서 및 신뢰 당사자 계약서의 업데이트는 필요에 따라 게시되고, 인증서는 발행 시 게시됩니다. 인증서 상태 정보는 CPS §§ 4.4.9 및 4.4.11 에 따라 게시됩니다.

2.6.3 액세스 제어

CrossCert 웹 사이트의 저장소 섹션에 게시된 정보는 액세스가 가능한 공개 정보입니다. 이런 정보에 대한 읽기 전용 액세스는 제한이 없습니다. 인증서, 인증서 상태 정보 또는 CRL 로 액세스하려는 경우 CrossCert 는 신뢰 당사자 계약서에 동의할 것을 요구합니다. CrossCert 는 권한이 없는 사람이 저장소 정보를 추가, 삭제 또는 수정하지 못하도록 논리적이고 물리적인 보안 장치를 구축해 놓았습니다.

2.6.4 저장소

CPS § 2.1.5 를 참조하십시오.

2.7 준수성 감사

CrossCert 의 공용 서비스 및 Managed PKI CA 서비스를 지원하여 CrossCert 의 데이터 센터 운영과 키 관리 운영에 대해 SAS 70 Type II 또는 이와 비슷한 수준의 감사가 매년 1 회 수행됩니다. 또한 CPS § 1.3.1 에 명시된 VTN 루트 CA, 클래스 3 단체 CA, 클래스 2 단체 및 개인 CA, 클래스 1 개인 CA 에 대해 인증 기관용 WebTrust 검사가 매년 1 회 수행됩니다. VeriSign 고객별 CA 는 고객이 요구하지 않는 한 CrossCert 작업 감사의 일부로 특별히 감사되지는 않습니다. CrossCert 는 Managed PKI 고객에게 본 CPS § 2.7 에 따른 준수성 감사와 이런 유형의 고객을 위한 감사 프로그램을 받도록 요구할 권리가 있습니다.

CrossCert 는 준수성 감사뿐만 아니라 다른 검사나 조사를 수행하여 VTN 의 CrossCert 하위 도메인에 대한 신뢰도를 보증할 수 있습니다. 다음에는 해당 예가 나와 있습니다.

- CrossCert 또는 CrossCert 로부터 권한을 부여받은 기관은 감사 대상이 VTN 표준을 충족하지 못했거나, 손상을 입었거나 또는 적절한 작업을 수행하지 못함에 따라 VTN 의 보안이나 무결성에 실제적 또는 잠재적인 위협을 제공한다고 판단될 경우 단독 재량에 따라 언제든지 자체 기관이나 고객에 대해 "긴급 감사/조사"를 수행할 권리가 있습니다.
- CrossCert 또는 CrossCert 로부터 권한을 부여받은 기관은 준수성 감사에서 문제점이 발견된 경우 또는 일상 업무 진행 중 전반적 위험 관리 프로세스의 일환으로 실행하려는 경우 자체 기관이나 고객에 대해 "추가 위험 관리 검토"를 수행할 권리가 있습니다.

CrossCert 또는 CrossCert 로부터 권한을 부여받은 기관은 이러한 감사, 검토 및 조사 작업을 제 3 의 감사 업체에 위임할 수 있습니다. 감사, 검토 또는 조사의 대상은 CrossCert 및 감사를 수행하는 직원들에게 필요한 협조를 제공해야 합니다.

2.7.1 준수성 감사 주기

준수성 감사는 매년 1 회 수행되며 비용은 감사 대상이 전적으로 부담합니다.

2.7.2 감사 기관 자격 요건

CrossCert 의 CA 준수성 감사는 다음과 같은 요건을 갖춘 공인 회계 법인에서 수행합니다.

- 공개키기반구조 기술, 정보 보안 도구 및 기술, 보안 감사, 제 3 자 인증 기능 등에 대해 탁월한 능력
- 미국 공인회계사 협회(AICPA)나 이와 유사한 기관으로부터 승인된 업체로서 특정 기술을 비롯하여 동료 검토, 능력 검증, 적절한 직원 배정 능력, 지속적인 전문 교육 등의 조건을 모두 충족시키는 업체

2.7.3 감사자와 피감사자 간의 관계

CrossCert 의 운영에 대한 준수성 감사는 CrossCert 와 아무런 관계가 없는 공인 회계 법인이 수행합니다.

2.7.4 CrossCert 의 운영에 대한 준수성 감사는 CrossCert 와 아무런 관계가 없는 공인 회계 법인(또는 이와 상응하는 기관)이 수행합니다. 감사 대상 항목

CrossCert 의 연례 SAS 70 Type II 감사 또는 이와 수준이 유사한 감사의 범위에는 CA 환경 제어, 키 관리 운영 및 기반구조/관리 CA 제어가 포함됩니다.

2.7.5 결함 발견 시 조치

CrossCert 의 운영에 대한 준수성 감사 결과 중대한 결함이 발견될 경우에는 단호한 조치가 취해집니다. 이러한 결단은 감사 기관의 자료를 바탕으로 CrossCert 의 경영진이 수행하게 됩니다. CrossCert 경영진은 운영 수정안을 작성 및 이행할 책임이 있습니다. 발견된 결함이 VTN 의 보안 및 무결성에 즉각적 위협이 될 것으로 판단될 경우, CrossCert 경영진은 30 일 이내에 운영 수정안을 작성하여 가능한 빠른 시일 내에 이행합니다. 결함의 정도가 크지 않은 경우에는 문제의 심각성을 평가한 후 적절한 조치를 취하게 됩니다.

2.7.6 결과 통보

CrossCert 의 운영에 대한 준수성 감사의 결과는 CrossCert 경영진의 자유재량에 따라 공개됩니다.

2.8 비밀 보장 및 개인 정보 보호

CrossCert 는 CP § 2.8 에 따라 개인 정보 보호 정책을 준수합니다.
http://www.CrossCert.com/privacy 를 참조하십시오.

2.8.1 비밀 보장 및 개인 정보 보호가 필요한 유형의 정보

CPS § 2.8.2 에 따라 다음과 같은 가입자 정보는 비밀이 보장됩니다("기밀/개인 정보").

- CA 신청 기록(승인 여부와 무관)
- 인증 신청 기록(CPS § 2.8.2 에 준함)
- Managed PKI 고객이 Managed PKI Key Manager 를 사용하여 보유하고 있는 개인키 및 이러한 개인키를 복구하는 데 필요한 정보
- 거래 기록(전체 기록 및 거래 감사 기록)
- VeriSign, 회원사 또는 고객이 생성했거나 보유하고 있는 VTN 감사 기록
- CrossCert 또는 해당 감사자(내부 또는 외부)가 작성한 CrossCert 감사 보고서
- 비상 계획 및 재해 복구 계획
- CrossCert 의 하드웨어/소프트웨어 운영과 인증 및 등록 서비스 관리를 제어하는 보안 조치

2.8.2 비밀 보장 및 개인 정보 보호가 필요 없는 유형의 정보

CrossCert 하위 도메인 참여자는 인증서, 인증서의 폐지, 기타 상태 정보, CrossCert 저장소 및 저장소 내의 정보는 기밀/개인 정보로 간주되지 않음을 인정합니다. CPS § 2.8.1 에 따라 기밀/개인 정보로 명시되지 않은 정보는 기밀/개인 정보로 취급되지 않습니다. 이 조항은 해당 개인정보 보호법의 적용을 받습니다.

2.8.3 인증서 폐지/일시 중지 정보의 공개

CPS § 2.8.2 를 참조하십시오.

2.8.4 법 집행 기관에 공개

CrossCert 하위 도메인 참여자는 CrossCert 가 소환장이나 수색 영장에 의해 정보 공개가 필요한 경우 기밀/개인 정보를 공개할 권한이 있음을 인정합니다. 이 조항은 해당 개인정보 보호법의 적용을 받습니다.

2.8.5 심리 과정에서 공개

CrossCert 하위 도메인 참여자는 소송이 발생했을 때 소환장, 심문서, 승인 요청, 자료 요청 등의 민사상 또는 행정상 절차에 필요한 경우 기밀/개인 정보를 공개할 권한이 있음을 인정합니다. 이 조항은 해당 개인정보 보호법의 적용을 받습니다.

2.8.6 정보 소유자의 요청에 의한 공개

CrossCert 의 개인정보 보호 정책에는 기밀/개인 정보를 CrossCert 에 공개한 소유자에게 이러한 정보를 공개하는 것과 관련된 조항이 포함되어 있습니다. 이 조항은 해당 개인정보 보호법의 적용을 받습니다.

2.8.7 기타 정보 공개 상황

해당 조항 없음

2.9 지적 재산권

가입자 및 신뢰 당사자가 아닌 CrossCert 하위 도메인 참여자 간의 지적 재산권 배당은 CrossCert 하위 도메인 참여자 간에 맺은 계약의 적용을 받습니다. 다음 CPS § 2.9 하위 조항은 가입자 및 신뢰 당사자와 관련된 지적 재산권에 적용됩니다.

2.9.1 인증서 및 폐지 정보에 대한 지적 재산권

CA 는 자사가 발행한 인증서와 폐지 정보에 대해 모든 지적 재산권을 보유합니다. CrossCert 와 고객은 인증서가 전체 복제되고 인증서에 언급된 신뢰 당사자 계약서에 준하여 사용될 경우 무료로 인증서 복제 및 배포 권한을 허용합니다. CrossCert 와 고객은 해당 신뢰 당사자 계약서 또는 다른 계약서에 따라 신뢰 당사자의 기능을 수행하는 데 폐지 정보를 사용할 수 있도록 허용합니다.

2.9.2 CP 에 대한 지적 재산권

CrossCert 하위 도메인 참여자는 CrossCert 가 본 CPS 에 대해 모든 지적 재산권을 보유함을 인정합니다.

2.9.3 이름에 대한 지적 재산권

인증 신청자는 인증 신청서 내의 모든 해당 상표, 서비스 상표 및 상호는 물론 이 인증 신청자에게 발행된 인증서 내의 식별명(DN)에 대한 권리를 보유합니다.

2.9.4 키 및 키 재료에 대한 지적 재산권

CA 및 최종 사용 가입자의 인증서에 해당하는 키 쌍은 키 쌍이 저장되어 있는 물리적 매체와 상관없이, Managed PKI Key Manager 를 사용하는 Managed PKI 고객의 권리에 따라 이러한 인증서의 주체인 CA 및 최종 사용 가입자의 재산이며 이러한 키 쌍에 대한 지적 재산권도 이들 CA 및 최종 사용 가입자가 보유합니다. 그러나 모든 PCA 공개키와 자체 서명한 인증서를 포함하여 VeriSign 의 루트 공개키 및 해당 루트 인증서는 VeriSign 의 재산입니다. VeriSign 은 소프트웨어 및 하드웨어 제조업체가 루트 인증서를 복제하여 신뢰할 수 있는 하드웨어 장치나 소프트웨어에 내장할 수 있도록 라이센스를 제공합니다. 마지막으로 위 모든 사항의 보편성을 제한하지 않는 범위 내에서, CA 개인키의 Secret Shares 는 CA 의 재산이며 CA 는 이러한 Secret Shares 에 대한 모든 지적 재산권을 보유합니다.

3. 식별 및 인증

3.1 최초 등록

3.1.1 이름 유형

CrossCert CA 인증서의 발행자 및 피발행자 필드에는 X.501 식별명(DN)이 포함되며, CrossCert CA DN 은 아래 표 8 에 지정된 구성 요소로 이뤄집니다.

속성	*값*
국가(C) =	["KR"],"US" 또는 사용하지 않음
단체(O) =	"VeriSign, Inc." 또는 CrossCert - "RSA Data Security, Inc.", 즉 현재의 VeriSign CA 를 나타냄(Secure Server CA 제외)
부서(OU) =	CrossCert CA 인증서에는 여러 가지 OU 속성이 포함될 수 있습니다. 이러한 속성에는 다음과 같은 항목이 하나 이상이 포함됩니다. • CA 이름 • VeriSign Trust Network • 인증서 사용에 관한 약관을 지정하는 해당 신뢰 당사자 계약에 관한 고지문 • 저작권 고지
시/도(S) =	사용하지 않음
행정 구역(L) =	"인터넷"을 사용하는 VeriSign Commercial Software Publishers CA 이외에는 사용하지 않음
일반이름(CN) =	CA 이름 포함(OU 속성에 CA 이름이 지정되지 않은 경우) 또는 CA 이름이 사용되지 않음

표 8 – CA 인증서의 식별명(DN) 속성

사용자 등록 인증서의 피발행자 이름 필드에는 X.501 식별명(DN)이 포함되며, 아래의 표 9 에 지정된 구성 요소로 이뤄집니다.

속성	*값*
국가(C) =	"[KR]" 또는 사용하지 않음
단체(O) =	단체 속성은 다음과 같이 사용됩니다. • "CrossCert" - CrossCert OCSP 응답자 인증서 및 개별 인증서인 경우 • 가입자 단체 이름 - 웹 서버 인증서인 경우

속성	값
	• 사용되지 않음 - 코드/객체 서명 인증서인 경우
부서(OU) =	CrossCert 사용자 등록 인증서에는 여러 OU 속성이 포함될 수 있습니다. 이러한 속성에는 다음과 같은 항목이 하나 이상이 포함됩니다. • 가입자 부서(단체 인증서인 경우) • VeriSign Trust Network • 인증서 사용에 관한 약관을 지정하는 해당 신뢰 당사자 계약에 관한 고지문 • 저작권 고지 • CrossCert 가 인증한 애플리케이션 인증서의 “Authenticated by CrossCert” 및 “Member, VeriSign Trust Network” • 클래스 1 개인 인증서의 “Persona Not Validated” • 인증서 유형에 대한 설명 텍스트
시/도(S) =	가입자의 시/도를 나타내거나 사용되지 않음
행정 구역(L) =	가입자의 행정 구역을 나타내거나 사용되지 않음
일반이름(CN) =	이 속성에는 다음이 포함됩니다. • OCSP 응답자 이름(OCSP 응답자 인증서의 경우) • 도메인 이름(웹 서버 인증서의 경우) • 단체 이름(코드/객체 서명 인증서의 경우) • 이름(개인 인증서의 경우)
E-mail 주소(E) =	클래스 1 개인 인증서의 E-mail 주소

표시 9 – 사용자 등록 인증서의 식별명(DN) 속성

사용자 등록 인증서의 피발행자 식별명(DN)의 일반이름(CN=) 구성 요소는 클래스 2-3 인증서인 경우에 인증됩니다.

- 단체 인증서의 피발행자 식별명(DN)에 포함된 인증된 일반이름(CN) 값은 단체나 단체내 부서의 도메인 이름(보안 서버 ID 및 글로벌 서버 ID 인 경우) 또는 공식 이름입니다.
- 개인 인증서의 피발행자 식별명(DN)에 포함된 일반이름(CN) 값은 개인의 이름을 나타냅니다.

3.1.2 유의미한 이름의 필요성

클래스 2 및 3 사용자 등록 인증서에는 인증서 피발행자인 개인이나 단체의 신원 판별이 가능한 이름이 포함되어 있습니다. 이러한 인증서에서는 최종 사용 가입자의 가명(가입자의 실제 이름이나 단체 이름이 아닌 이름)을 사용할 수 없습니다.

가명은 클래스 1 사용자 등록 인증서에만 사용할 수 있습니다.

CrossCert CA 인증서에는 인증서의 피발행자인 CA 의 신원을 판별하는 의미 규칙을 갖는 이름이 포함되어 있습니다.

3.1.3 다양한 이름 형식의 해석 규칙

해당 조항 없음

3.1.4 이름의 고유성

CrossCert 는 가입자 등록 프로세스의 자동 구성 요소를 통해 특정 CA 의 도메인 내에서 피발행자 식별명(DN)이 고유한지 확인합니다.

3.1.5 이름 분쟁 해결 절차

인증 신청자는 인증 신청서에 타인의 지적 재산권을 침해하는 이름을 사용할 수 없습니다. 하지만 CrossCert 는 인증 신청자가 인증 신청서에 표시될 이름의 지적 재산권을 소유하고 있는지 여부를 확인하지 않으며 도메인 이름, 상표 이름, 상표 또는 서비스 표시의 소유권에 관련한 어떠한 분쟁도 중재 또는 해결하지 않습니다. CrossCert 는 인증 신청자에 대한 의무 없이 이러한 분쟁을 이유로 인증 신청서를 거부 또는 보류할 수 있습니다.

3.1.6 상표의 인식, 인증 및 역할

CPS 3.1.5 항 참조

3.1.7 개인키 소유 증명 방법

CrossCert 는 PKCS #10 이나 다른 암호화 데모 또는 기타 CrossCert 승인 방식에 따른 디지털 서명 인증서를 사용하여 개인키의 소유를 확인합니다.

CrossCert 가 가입자 대신 키 쌍을 생성하는 경우, 예를 들어 사전 생성된 키가 스마트 카드에 있는 경우에는 이 요건이 적용되지 않습니다.

3.1.8 단체 신원 인증

CrossCert 는 클래스 3 단체 최종 사용 가입자와 기타 등록 정보(미확인 가입자 정보 제외)를 제공한 인증 신청자의 신원을 다음 단원에 정해진 절차에 따라 확인합니다. 아래의 절차 이외에도 인증 신청자는 CPS 3.1.7 항에 따라 인증서에 표시될 공개키에 대응하는 개인키를 정당하게 소유하고 있음을 증명해야 합니다.

3.1.8.1 단체 사용 등록자 인증

3.1.8.1.1 리테일 단체 인증서 인증

CrossCert 는 다음과 같은 방법으로 리테일 단체 인증서의 인증 신청자 신원을 확인합니다.

- 하나 이상의 제 3 의 신원 확인 서비스나 데이터베이스 또는 해당 정부가 발행 또는 보고한 단체의 존재를 확인하는 공식 문서를 통해 단체의 존재 여부 확인
- 전화나 우편, 단체에 대한 특정 정보를 비교하는 절차를 통해 해당 단체 담당자를 확인하고, 단체가 인증 신청서를 승인했으며 단체를 대표하여 인증 신청서를 제출한 사람이 정당한 권한이 있는지 확인

인증서 유형에 따라 아래 표 10 에 나와 있는 추가 절차를 수행합니다.

인증서 유형	*추가 절차*
모든 서버 인증서	CrossCert 는 인증 신청자가 인증서의 피발행자인 서버의 도메인 이름을 소유하고 있거나, 도메인을 사용할 수 있도록 승인되었는지 확인합니다.
글로벌 서버 ID	CrossCert 는 미국 수출 관련 법규 및 미국 BIS(Bureau of Information and Science)에서 발행한 라이센스를 충족시키는 데 필요한 추가 검사를 수행합니다.

표 10 – 특수 인증 절차

3.1.8.1.2 Managed PKI for SSL 인증

Managed PKI for SSL 고객의 경우, 신원 확인 절차는 CrossCert 가 CPS 3.1.8.2 항에 따라 Managed PKI for SSL 고객의 신원을 확인하는 것으로 시작됩니다. 확인이 끝나면 Managed PKI for SSL 고객은 다음과 같은 방법으로 해당 단체 내의 서버에 대한 인증서 발행을 승인해야 합니다.

- 보안 서버 ID 나 글로벌 서버 ID 의 피발행자로 지정된 서버가 실제로 존재하는지 확인합니다.
- 단체가 서버에 보안 서버 ID 나 글로벌 서버 ID 를 발행할 권한이 있는지 확인합니다.

3.1.8.1.3 CrossCert 에서 제공하지 않음

3.1.8.2 CA 및 RA 신원 인증

CrossCert CA 인증 신청서의 경우, 권한 있는 CrossCert 담당자가 여러 CrossCert 직원들이 참여하는 엄격한 절차를 거쳐 인증서 요청을 작성, 처리 및 승인합니다.

CA 나 RA 가 되려는 Managed PKI 고객은 CrossCert 와 계약을 체결합니다. CrossCert 는 CA 나 RA 최종 승인에 앞서 CPS 3.1.8.1 항에 지정된 단체 최종 사용 가입자의 신원 확인에 필요한 검사를 수행하여 잠재 Managed PKI 고객이나 ASB 고객의 신원을 인증합니다(인증 신청서가 아닌 Managed PKI 고객이 되기 위한 신청에 대한 확인이라는 점이 다름). 또한 Managed PKI 고객에 대해 VeriSign 은 Managed PKI 관리자로 신원이 확인된 사람이 법률적 권한이 있는 사람인지 확인합니다. CrossCert 는 신청 단체의 권한 있는 대표자에게 CrossCert 담당 직원 앞에 직접 출두하도록 요구할 수도 있습니다.

경우에 따라 CrossCert 는 잠재 Managed PKI 고객에 대한 인증 책임을 위임할 수 있습니다. 리셀러의 단체 신원 인증 절차는 반드시 CrossCert 에 제출되어 승인을 받아야 하며, 승인이 있어야만 리셀러는 Managed PKI 의 공급자로서 업무를 시작할 수 있습니다. 이러한 인증 절차는 앞 단락에 정의된 요건에 부합해야 합니다.

3.1.9 개인 신원 인증

모든 클래스의 개인 인증서에 대해 Managed PKI 고객인 CrossCert 는 CA 를 대신하여 다음 사항을 확인합니다.

- 인증 신청자가 인증 신청서에 표시된 사람인지 확인합니다(클래스 1 인증 신청자 제외).
- CPS 3.1.7 항에 따라 인증 신청자가 인증서에 표시된 공개키에 대응하는 개인키를 정당하게 소유하고 있는지 확인합니다.
- 인증서에 수록된 정보가 정확한지 확인합니다(미확인 가입자 정보 제외).

또한 CrossCert 는 각 인증서 클래스에 대해 아래에 설명된 보다 세부적인 절차를 수행합니다.

3.1.9.1 클래스 1 개인 인증서

클래스 1 인증서에 대한 개인 인증은 피발행자의 식별명(DN)이 고유하며, 피발행자의 이름이 CrossCert 클래스 1 CA 서브도메인 내에서 명백한지 확인하는 절차로 이뤄집니다. 클래스 1 인증에서는 신원 확인, 즉 가입자가 본인이 주장하는 사람이 맞는지 확인하는 절차가 없습니다. 가입자의 일반이름(CN)은 미확인 가입자 정보입니다. 클래스 1 인증에서는 인증 신청자의 E-mail 주소에 대한 제한된 확인이 이뤄집니다.

3.1.9.2 클래스 2 개인 인증서

클래스 2 인증서에 대한 인증 절차는 두 가지 방식으로 이뤄집니다. 클래스 2 Managed PKI 인증서의 경우, Managed PKI 고객 및 Managed PKI Lite 고객은 CPS 3.1.9.2.1 항에 따라 비즈니스 레코드나 비즈니스 정보 데이터베이스를 사용하여 인증 신청을 승인 또는 거부합니다.

3.1.9.2.1 클래스 2 Managed PKI 인증서

클래스 2 Managed PKI 인증서의 경우, Managed PKI 고객은 다음에서 설명하는 수동 또는 자동 인증 절차나 암호 코드를 사용하여 인증 신청을 승인합니다.

Managed PKI 고객 및 Managed PKI Lite 고객은 등록 정보를 기존의 비즈니스 레코드나 비즈니스 정보 데이터베이스와 비교하여 개인의 신원을 확인합니다. 즉, 예를 들어 등록 정보를 인사부 데이터베이스의 직원 또는 독립 계약자 레코드와 비교합니다. 등록 정보가 인증에 사용된 레코드나 데이터베이스와 일치할 경우, Managed PKI 고객 또는 Managed PKI Lite 고객은 Managed PKI 제어 센터를 사용하여 인증 신청을 수동으로 승인할 수 있는데, 이 프로세스를 일컬어 “수동 인증”이라고 합니다.

Managed PKI 의 자동관리소프트웨어모듈(AA 모듈)을 비롯한 이와 유사한 CrossCert 소프트웨어에는 Managed PKI 고객이 각 인증 신청서를 수동으로 인증할 필요 없이, 기존 관리 시스템이나 데이터베이스에서 직접 사용자나 장치를 자동으로 승인 및 거부할 수 있는 기능이 있습니다. Managed PKI 자동관리소프트웨어모듈(AA 모듈)을 사용하면 잠재 인증 신청 정보를 데이터베이스에 저장하기 전에 신청자의 신원을 인증할 수 있습니다. 인증 신청자가 인증 신청서를 제출하면 자동관리소프트웨어모듈(AA 모듈)은 인증 신청서의 정보와 데이터베이스의 정보를 비교하여 정보가 일치할 경우 CrossCert 가 인증서를 즉시 발행할 수 있도록 인증 신청을 자동으로 승인합니다. 이 프로세스를 일컬어 “자동 관리”라고 합니다.

CrossCert 인증에 사용되는 VeriSign Managed PKI “암호 코드”(“암호 코드 인증”) 인증에서는 인증 신청자의 등록 데이터와 Managed PKI 고객의 Managed PKI 관리자가 제공하는 사전 구성된 인증 데이터를 비교하여 인증 신청을 자동으로 승인 또는 거부합니다. 암호 코드 인증에서 Managed PKI 고객은 적절한 인증 레벨에 부합하는 잠재 인증 신청자에게 오프라인 방식으로 "암호 코드"를 배포합니다. 암호 코드를 받은 인증 신청자는 다른 인증 정보와 함께 인증 신청서를 제출할 때 이 암호 코드를 제공합니다. 암호 코드와 추가 인증 정보는 Managed PKI 관리자가 미리 구성한 암호 코드 데이터베이스와 비교되고, 모든 필드가 일치하면 인증서가 발행됩니다.

모든 Managed PKI Lite 고객과 자동 관리나 암호 코드 인증을 사용하지 않는 Managed PKI 고객은 반드시 수동 인증 절차를 사용해야 합니다.

3.1.9.2.2 CrossCert 에서 현재 제공하지 않음

.

3.1.9.3 클래스 3 개인 인증서

3.1.9.3.1 CrossCert 에서 현재 제공하지 않음

.

3.1.9.3.2 클래스 3 관리자 인증서

CrossCert CA 시스템에 대한 액세스를 제어하고 VTN 내에서의 특정 작업을 인증하는데 사용되는 관리자 인증서의 종류는 다양합니다. 클래스 3 관리자 인증서의 구체적인 종류는 CPS 1.3.1 항을 참조하십시오.

CrossCert 는 Managed PKI 고객 및 신임된 제 4 자 직원에 대한 클래스 3 관리자 인증 신청을 다음과 같이 인증합니다.

- CrossCert 는 CPS 3.1.8.2 항에 따라 해당 관리자를 고용 또는 유지하고 있는 실체의 존재 및 신원을 인증합니다.
- CrossCert 는 인증 신청서에 관리자로 지정된 사람의 고용 및 권한 부여를 확인합니다.

또한 CrossCert 는 자사 관리자에 대한 인증 신청도 승인합니다. 관리자는 소속 단체에서 "권한을 부여받은 사람"을 말합니다(CPS 5.2.1 항 참조). 이 경우, 독립 계약자로서의 고용이나 유지와 관련된 신원 확인(CPS 5.2.3 항 참조), 백그라운드 검사 절차(CPS 5.3.2 항 참조), 관리자 역할 인증을 기반으로 인증서 인증이 진행됩니다.

3.2 정기적 키 재발급 및 갱신

인증서를 계속 사용하려면 기존 인증서가 만료되기 전에 새 인증서를 발급 받아야 합니다. 보통의 경우 CrossCert 는 가입자에게 만료되는 키 쌍을 대체할 새 키 쌍을 생성하도록 요구하는데, 이를 기술적으로 "키 재발급"이라고 합니다. 하지만 특별한 경우, 즉 웹 서버 인증서와 같은 경우에는 기존 키 쌍에 대한 새 인증서를 요청할 수 있도록 하고 있는데, 이를 기술적으로 "갱신"이라고 합니다. 아래의 표 11 에서는 정기적 키 재발급(기존 키 쌍을 대체하는 새 키 쌍에 대한 새 인증서 발행)과 갱신(기존 키 쌍에 대한 새 인증서 발행)에 대한 설명이 나와 있습니다.

일반적으로 말해 새 키 쌍의 생성 여부는 차치하고 기존 인증서를 새 인증서로 대체한다는 점에서만 보면 “키 재발급”과 “갱신”은 모두 “인증서 갱신”에 들어갑니다. 클래스 3 서버 인증서를 제외한 모든 CrossCert 인증서 클래스 및 유형에 있어서 이러한 구분은 중요치 않습니다. CrossCert 의 사용자 등록 인증서 대체 프로세스에서 새 키 쌍이 항상 생성되기 때문입니다.

하지만 클래스 3 서버 인증서의 경우에는 가입자 키 쌍이 웹 서버에서 생성되고, 대부분의 웹 서버 키 생성 도구를 사용하여 기존 키 쌍에 대한 새 인증서 요청을 생성을 할 수 있기 때문에 "키 재발급"과 "갱신"은 구분됩니다. 또한 아래 표 11 에 나와 있는 제약 조건에 따라 기존 CrossCert CA 키 쌍에 대해 새로운 CA 인증서를 발행할 수 있습니다.

인증서 클래스 및 유형	*정기적 키 재발급 및 갱신 요건*
클래스 1, 클래스 2, 클래스 3 코드 및 객체 서명, 클래스 3 관리자 인증서	이 인증서 유형의 가입자 키 쌍은 온라인 등록 프로세스에서 생성되는 브라우저입니다. 가입자는 기존 키 쌍에 대한 "갱신"을 제출할 수 없습니다. 따라서 이 인증서 유형에 대해서는 키 재발급만 지원되고, 인증서 갱신은 지원되지 않습니다.
클래스 3 서버 인증서	보안 서버 ID 나 글로벌 서버 ID 의 경우 가입자 키 쌍은 온라인 등록 프로세스가 아닌, 웹 서버에서 생성됩니다. 대부분의 서버 키 생성 도구를 사용하여 가입자는 기존의 키 쌍에 대해 새로운 인증서 서명 요청(CSR)을 생성할 수 있습니다. 따라서 보안 버서 ID 와 글로벌 서버 ID 의 경우 키 재발급과 인증서 갱신이 모두 지원됩니다.
CA 인증서	CA 인증서 갱신은 CA 키 쌍의 누적 인증서 유효 기간이 CPS 6.3.2 항에 지정된 최대 CA 키 쌍의 유효 기간을 초과하지 않을 경우에 한해 허용됩니다. CrossCert CA 는 CPS 4.7 항에 따라 키를 재발급 받을 수 있습니다. CrossCert CA 인증서에 대해서는 키 재발급과 인증서 갱신이 모두 지원됩니다.

표 11 - 정기적 키 재발급 및 갱신 요건

3.2.1 사용자 등록 인증서의 정기적 키 재발급 및 갱신

가입자 인증서는 폐지되지 않는 한 아래 표 12 에 따라 대체(키 재발급 또는 갱신)할 수 있습니다.

기간	요건
인증서 만료전 30 일, 만료후 30 일 이내	모든 CrossCert 인증서에 대해 CrossCert 또는 Managed PKI 고객은 암호를 사용하여 인증서 대체를 요청하는 가입자를 인증합니다. 가입자는 최초 등록 프로세스에서 등록 정보와 함께 암호를 제출하게 됩니다. 지정된 기간 내에 인증서에 대한 키 재발급이나 갱신을 신청할 경우, 가입자가 재등록 정보와 함께 제출한 암호가 정확하고 연락처 정보를 제외한 등록 정보가 변경되지 않았으면 새 인증서가 자동으로 발행됩니다. 이 방식으로 키 재발급이나 갱신이 수행된 이후, 한번 이상 후속 키 재발급이나 갱신이 일어나면 CA 나 RA 는 CPS 3.1.8.1 항에 지정된 원본 인증 신청서 인증과 관련한 요건에 따라 가입자의 신원을 재확인합니다.
인증서 만료후 30 일 이후	이 시나리오에서는 CPS 3.1.8.1 항 및 3.1.9 항에 지정된 원본 인증 신청서 인증에 관한 요건이 사용자 등록 인증서 대체에 사용됩니다.

표 12 – 사용자 등록 인증서의 정기적 키 재발급 및 갱신 요건

3.2.2 CA 인증서의 정기적 키 재발급 및 갱신

CrossCert CA 는 CPS 4.7 항에 따라 정기적으로 키를 재발급 받을 수 있습니다.

CrossCert CA 인증서는 CPS 6.3.2 항에 지정된 매개 변수 내에서 갱신될 수 있습니다. 예를 들어, 최초 PCA 인증서가 10 년 유효 기간으로 발행된 경우 갱신되는 인증서는 CA 키 쌍의 유효 기간을 20 년까지 연장하여 최대 허용 유효 기간인 30 년 동안 사용할 수 있게 발행될 수 있습니다. 만료 기간이 경과하면 CA 인증서를 갱신할 수 없습니다.

VeriSign 자체 서명 PCA 인증서와 기타 CrossCert 루트 CA, CrossCert CA 인증서의 경우, 권한 있는 VeriSign 담당자가 여러 관계자가 참여하는 엄격한 절차를 거쳐 갱신 요청을 생성 및 승인합니다.

VeriSign PCA 와 연관된 비 CrossCert CA 인증서의 경우, CrossCert 는 Managed PKI 고객이 CA 인증서의 실제 가입자인지 확인하는 적절한 절차를 수행하게 됩니다. 인증 절차는 CPS 3.1.8.3 항에 나와 있는 원본 등록 절차와 동일합니다.

3.3 폐지 후 키 재발급

다음과 같은 경우 인증서가 폐지된 후에 키를 재발급할 수 없습니다.

- 인증서 피발행자로 명명된 사람이 아닌 사람에게 인증서(클래스 1 인증서 제외)가 발행되어 폐지된 경우
- 인증서의 피발행자로 명명된 사람에 대한 인증 없이 인증서(클래스 1 인증서 제외)가 발행된 경우

- 가입자의 인증 신청을 승인하는 실체가 인증 신청서의 중대한 사실이 거짓임을 발견하거나 그렇게 믿을만한 근거가 있는 경우

앞에서 설명한 바와 같이 폐지된 가입자 인증서는 아래 표 12 에 따라 대체(키 재발급)할 수 있습니다.

기간	*요건*
인증서 만료 전	인증서 폐지 후 단체 또는 개인 인증서를 대체하는 경우 CrossCert 는 CPS 3.2.1 의 설명에 따라 암호를 사용하여 인증서를 대체하려는 가입자(개인)나 권한 있는 단체 대표(단체의 경우)의 신원을 확인합니다. 이 절차 이외에는 폐지 후 인증서 교체에 CPS 3.1.8.1 항 및 3.1.9 항의 원본 인증 신청서 확인 요건이 적용됩니다. 이러한 인증서에는 교체되는 인증서의 피발행자 식별명(DN)과 동일한 피발행자 식별명(DN)이 사용됩니다.
인증서 만료 후	이 시나리오에서는 사용자 등록 인증서 대체에 CPS 3.1.8.1 항 및 3.1.9 항에 지정된 원본 인증 신청서 인증 요건이 사용됩니다.

표 13 – 폐지 후 인증서 교체의 요건

3.4 폐지 요청

인증서를 폐지하기 전에 CrossCert 는 인증 신청을 승인한 실체인 인증서 가입자가 폐지를 요청했는지 확인합니다. 가입자 폐지 요청 인증은 다음과 같은 절차로 진행됩니다.

- 가입자에게 가입자 암호를 제출하게 하여 이것이 레코드의 암호와 일치하면 인증서를 자동으로 폐지합니다.
- 가입자로 자칭하는 사람으로부터 폐지를 요청하는 메시지를 수신합니다. 이 메시지에는 폐지할 인증서에 대한 참조로 확인할 수 있는 디지털 서명이 있습니다.
- 가입자에게 연락하여 인증서 클래스를 고려하여 폐지를 요청하는 개인이나 단체가 실제 가입자임을 합리적인 방법으로 보증하도록 요구합니다. 환경에 따라 이러한 연락은 전화, 팩스, E-mail, 우편, 택배 등의 방법으로 이루어질 수 있습니다.

CrossCert 관리자는 CrossCert 서브도메인 내에서 사용자 등록 인증서의 폐지를 요청할 수 있습니다. CrossCert 는 관리자에게 폐지 기능을 허용하기 전에 SSL 을 사용한 액세스 제어와 클라이언트 인증을 통해 관리자 신원을 인증합니다. .

Managed PKI 고객은 자동관리소프트웨어모듈(AA 모듈)을 사용하여 VeriSign 에 일괄 폐지 요청을 제출할 수 있습니다. 이러한 요청은 Managed PKI 고객의 자동 관리 하드웨어 토큰에 있는 개인키로 디지털 서명된 요청을 통해 인증됩니다.

CrossCert 는 Managed PKI 고객의 CA 인증서 폐지 요청이 실제 CA 가 요청한 것인지 확인한 후 인증합니다.

4. 운영 요건

4.1 인증 신청서

4.1.1 사용자 등록 인증용 인증 신청서

CrossCert 인증서를 신청하고자 하는 모든 사용자 등록 인증 신청자는 다음과 같은 등록 절차를 거쳐야 합니다.

- 인증 신청서를 작성하고 필요한 정보를 입력합니다.
- CPS 6.1 항에 따라 키 쌍을 생성하거나 생성되도록 조치를 취합니다.
- CPS 6.1.3 항에 따라 자신의 공개키를 직접 또는 Managed PKI 고객을 통해 CrossCert 로 보냅니다.
- CPS 3.1.7 항에 따라 CrossCert 로 전달된 공개키에 대응하는 개인키를 소유하고 있음을 CrossCert 에 입증합니다.
- 관련 가입 계약에 동의함을 명시합니다.

웹 호스트는 웹 호스트 프로그램에 따라 고객을 대신하여 인증 신청서를 제출할 수 있습니다(CPS 1.1.2.6 항 참조).

인증 신청서는 Managed PKI 고객인 CrossCert 로 보내져 승인 또는 거부 처리됩니다. 인증 신청서를 처리하는 실체와 CPS 4.2 항에 따라 인증서를 발행하는 실체는 다음 표에서 보듯이 서로 다를 수 있습니다.

인증서 클래스/범주	*인증 신청서 처리 실체*	*인증서 발행 실체*
클래스 1 개인 리테일 인증서	CrossCert	CrossCert
클래스 2 개인 Managed PKI 인증서	클래스 2 Managed PKI 고객, Managed PKI Lite 고객	CrossCert
클래스 3 관리자 인증서	CrossCert	CrossCert
클래스 3 단체 리테일 인증서	CrossCert	CrossCert
클래스 3 단체 Managed PKI 인증서(Managed PKI for SSL)	Managed PKI for SSL 고객	VeriSign
CA, 기반구조, CrossCert 직원 인증서	CrossCert	CrossCert

표 14 – 인증 신청 처리 실체

4.1.2 CA, RA, 기반구조 및 직원 인증서용 인증 신청서

4.1.2.1 CA 인증서

VeriSign PCA 는 VeriSign, Affiliate, Managed PKI 고객을 비롯한 하위 CA 에만 인증서를 발행합니다. CA 인증서 가입자인 CrossCert CA 의 경우, 권한 있는 CrossCert 담당자가 여러 명의 관계자가 참가하는 엄격한 절차를 거쳐 인증 신청을 생성 및 승인합니다.

CA 인증서 가입자인 Managed PKI 고객은 공식 인증 신청서를 작성할 필요가 없습니다. 대신 CrossCert 와 계약을 체결합니다. CA 인증 신청자는 CPS 3.1.8.2 항에 따라 계약 과정에서 자신의 신원을 증명하고 연락처 정보를 제공하는 증명서를 제출해야 합니다. 이 계약 과정에서 또는 적어도 Managed PKI 고객의 인증서를 생성하는 키 생성 절차가 시작되기 전까지 신청자는 CrossCert 와 협력하여 적절한 식별명(DN)과 신청자에게 발행될 인증서 내용을 결정해야 합니다. 이러한 CA 의 인증서 요청은 권한 있는 CrossCert 담당자가 여러 명의 관계자가 참가하는 엄격한 절차를 거쳐 생성 및 승인합니다.

4.1.2.2 RA 인증서

CrossCert 는 다음과 같이 구성되는 RA 및 RA 시스템에 인증서를 발행하는 몇 개의 관리 CA 를 운영합니다.

- CrossCert CA 를 대신하여 인증 신청을 처리하는 CrossCert 담당자(CrossCert RA 관리자)
- 단체 내의 Managed PKI 고객 및 서브 도메인 내의 서버를 대신하여 인증 신청을 처리하는 Managed PKI 고객 담당자(Managed PKI 관리자)

- 자동 관리 인증 프로세스를 수립한 Managed PKI 고객에 대한 인증 신청을 처리하는 Automated Administration 서버

해당 관리 CA 의 가입자이기도 한 이 모든 RA 에 대해서는 CPS 4.1.1 항에 지정된 클래스 3 관리자 인증서 요건이 적용됩니다.

4.1.2.3 기반구조 인증서

CrossCert 는 CrossCert 기반구조 구성 요소(예: 인증서 상태 정보를 제공하는 OCSP 응답자, CrossCert 로밍 서비스를 지원하는 로밍 서버)에 인증서를 발행하는 몇 개의 기반구조 CA 를 운영합니다.

4.1.2.4 VeriSign 직원 인증서

CrossCert 는 인증 신청서를 제출한 소속 직원에 대해 처리 절차를 거쳐 클래스 2 인증서를 발행합니다.

4.2 인증서 발행

4.2.1 사용자 등록 인증서 발행

인증 신청자가 인증 신청서를 제출하면 Managed PKI 관리자(CPS 4.1.1 항 참조)인 CrossCert 는 CPS 3.1.8.1 항 및 3.1.9 항에 따라 인증 신청서(미확인 가입자 정보 제외)의 정보를 확인합니다. CPS 3.1 에 따라 필요한 인증 절차가 성공적으로 처리되면 Managed PKI 관리자인 CrossCert 는 인증 신청을 승인합니다. 인증 절차가 성공하지 못하면 Managed PKI 관리자인 CrossCert 는 인증 신청을 거부합니다.

인증 신청이 승인되거나 또는 RA 의 인증서 발행 요청이 수신되면 인증서가 생성 및 발행됩니다. CrossCert 는 인증 신청이 승인된 후 인증 신청서의 정보를 기반으로 인증서를 생성하여 신청자에게 발행합니다. Managed PKI 고객이 인증 신청을 승인하고 이 사실을 CrossCert 에 통보하면 CrossCert 는 인증서를 생성하여 인증 신청자에게 발행합니다. 이 단원의 절차는 인증서 교체(갱신. 키 재발급) 요청 제출과 관련된 인증서 발행에도 사용됩니다.

4.2.2 **CA, RA 및 기반구조 인증서 발행**

CrossCert 는 CPS 3.1.8.2 항에 따라 고객이 되고자 하는 실체의 신원을 인증하고, 신청이 승인되면 CA 나 RA 기능을 수행하는 데 필요한 인증서를 발행합니다. CrossCert 가 CPS 4.1.2 항에 따라 고객 신청자와 계약을 체결하는 경우, 먼저 제출된 증명서를 기반으로 한 잠재 고객의 신원 확인 절차가 진행됩니다. 이 계약이 실행되면 CrossCert 가 신청서를 확인하여 최종 승인했음을 의미합니다. 고객 신청서에 대한 승인이나 거부 결정은 전적으로 CrossCert 의 재량입니다. 승인이 완료되면 CrossCert 는 CPS 6.1 항에 따라 고객 CA 나 RA 에 인증서를 발행합니다.

CrossCert 기반구조 구성 요소(예: OCSP 응답자)에 대한 인증서 요청은 권한 있는 CrossCert 담당자에 의해 여러 관계자가 참여하는 엄격한 절차를 거쳐 생성 및 승인됩니다.

4.3 인증서 승인

인증서가 생성되면 CrossCert 는 가입자에게 인증서가 발행된 사실과 이를 실제로 발급 받는 방법을 알립니다. Managed PKI 고객은 Managed PKI 관리자를 통해 가입자에게 이러한 사실을 통보합니다.

인증서가 발행되면 최종 사용 가입자는 웹 사이트에서 이를 다운로드하거나 전송된 인증서 포함 메시지를 통해 인증서를 사용할 수 있습니다. 예컨대 CrossCert 의 경우는 가입자에게 등록 웹 페이지에 입력하면 인증서를 받을 수 있는 PIN 을 보냅니다. 인증서를 E-mail 메시지로 보낼 수도 있습니다. 가입자가 인증서를 다운로드하거나 메시지 첨부된 인증서를 설치하면 인증서를 수락하는 것이 됩니다.

4.4 인증서 일시 중지 및 폐지

4.4.1 폐지 조건

4.4.1.1 사용자 등록 인증서 폐지 조건

사용자 등록 인증서는 다음과 같은 경우 폐지됩니다.

- CrossCert, 고객 또는 가입자가 가입자의 개인키가 손상되었다고 판단하거나, 그렇게 믿을만한 근거가 있는 경우
- CrossCert 또는 고객이 가입자가 해당 가입 계약에 명시된 중요한 의무나 진술, 보증을 중대하게 위반했다고 믿을만한 근거가 있는 경우
- 가입자와의 가입 계약이 만료된 경우
- Managed PKI 고객과의 제휴가 만료 또는 종료된 경우

- CrossCert 또는 고객이 인증서가 해당 CPS 에 정해진 절차에 따라 발행되지 않았거나, 인증서(클래스 1 인증서 제외)가 인증서 피발행자가 아닌 사람에게 발행되었거나, 인증서(클래스 1 인증서 제외)가 해당 인증서 피발행자의 허가 없이 발행되었다고 판단하는 경우
- CrossCert 또는 고객이 인증 신청서에 수록된 중요한 사실이 거짓이라고 믿을만한 근거가 있는 경우
- CrossCert 또는 고객이 인증서 발행의 주요 사전 전제 조건이 충족되지 않았거나 면제되지 않았다고 판단한 경우
- 클래스 3 단체 인증서의 경우 가입자의 단체 이름이 변경된 경우
- 미확인 가입자 정보 이외의 인증서 내용이 부정확하거나 변경된 경우
- 가입자가 CPS 3.4 항에 따라 인증서 폐지를 요청한 경우

CrossCert 는 관리자가 관리자 역할을 수행할 수 있는 권한이 만료 또는 종료된 경우에도 관리자 인증서를 폐지할 수 있습니다.

CrossCert 가입 계약에 따르면 최종 사용 가입자는 개인키의 손상이 알려지거나 의심되는 경우 CPS 4.4.3.1 항에 따라 즉시 CrossCert 에게 이를 통보해야 합니다.

4.4.1.2 CA, RA 또는 기반구조 인증서 폐지 조건

CrossCert 는 다음과 같은 경우 CA, RA 또는 기반구조 인증서를 폐지합니다.

- CrossCert 가 CA, RA 또는 기반구조 개인키가 손상되었음을 발견하거나, 그렇게 믿을만한 근거가 있는 경우
- CA 또는 RA 와 CrossCert 간의 계약이 만료된 경우
- CrossCert 가 인증서가 이 CPS 에 정해진 절차에 따라 발행되지 않았거나, 인증서가 인증서 피발행자가 아닌 실체에게 발행되었거나, 인증서가 해당 인증서

피발행자의 허가 없이 발행되었음을 발견하거나 그렇게 믿을만한 근거가 있는 경우
- CrossCert 가 인증서 발행의 중요한 사전 전제 조건이 충족되지 않았거나 면제되지 않았다고 판단하는 경우
- CA 또는 RA 가 인증서 폐지를 요청하는 경우

CrossCert 는 인증서를 폐지해야 하는 경우 CPS 4.4.3.1 항의 절차에 따라 Managed PKI 고객에게 폐지를 요청합니다.

4.4.2 인증서 폐지 요청자

4.4.2.1 사용자 등록 인증서의 폐지 요청자

다음 실체는 사용자 등록 인증서의 폐지를 요청할 수 있습니다.
- 가입자의 인증 신청을 승인한 CrossCert 나 고객은 CPS 4.4.1.1 항에 따라 사용자 등록 인증서나 관리 인증서의 폐지를 요청할 수 있습니다.
- 개인 가입자는 자신의 개인 인증서 폐지를 요청할 수 있습니다.
- 단체 인증서의 경우, 해당 단체의 권한 있는 대표만 인증서의 폐지를 요청할 수 있습니다.

- 관리자 인증서를 받은 CrossCert 나 Managed PKI 고객의 정당한 권한 있는 대표가 관리자 인증서 폐지를 요청할 수 있습니다.

4.4.2.2 CA, RA 또는 기반구조 인증서 폐지 요청자

다음 실체는 CA, RA 또는 기반구조 인증서의 폐지를 요청할 수 있습니다.
- CrossCert 는 자체 CA, RA 또는 기반구조 구성 요소에 발행된 인증서의 폐지를 요청하거나 시행할 수 있습니다.
- VeriSign, CrossCert 하위 기관 및 CrossCert 는 CPS 4.4.1.2 항에 따라 모든 Processing Center, Service Center, Managed PKI 고객, RA 또는 기반구조 인증서 폐지를 시행할 수 있습니다.
- Processing Centers, Service Centers, Managed PKI 고객은 정당한 권한 있는 대표를 통해 자체 CA, RA 및 기반구조 인증서의 폐지를 요청할 수 있습니다.

4.4.3 폐지 요청 절차

4.4.3.1 사용자 등록 인증서의 폐지 요청 절차

폐지를 요청할 최종 사용 가입자는 가입자의 인증 신청 승인을 담당한 CrossCert 나 고객에게 폐지 요청을 보내야 하며, 이들은 요청을 받은 즉시 인증서 폐지를 시행합니다. Managed PKI 고객의 가입자는 Managed PKI 관리자에게 요청을 보내야 하며, 관리자는

CrossCert 에 폐지 요청을 전달하여 처리합니다. 이러한 폐지 요청 전달은 CPS 3.4 항에 따라 이뤄집니다.

Managed PKI 고객은 자체 재량으로 사용자 등록 인증서를 폐지하거나 CrossCert 에 인증서 폐지를 지시할 수 있습니다.

4.4.3.2 CA 또는 RA 인증서의 폐지 요청 절차

CA 또는 RA 인증서 폐지를 요청하는 CA 나 RA 는 CrossCert 에 폐지 요청을 보내야 합니다. 요청을 받은 CrossCert 는 인증서를 폐지합니다. CrossCert 는 CA 또는 RA 의 요청 없이 인증서를 폐지할 수도 있습니다.

4.4.4 폐지 요청 기간

폐지 요청은 합리적인 시간 내에 가능한 즉각적으로 제출해야 합니다.

4.4.5 일시 중지 조건

CrossCert 는 보통 CA 또는 사용자 등록 인증서의 일시 중지 서비스를 제공하지 않습니다.

4.4.6 일시 중지 요청자

해당 없음

4.4.7 일시 중지 요청 절차

해당 없음

4.4.8 일시 중지 기간 제한

해당 없음

4.4.9 CRL 발행 빈도

CrossCert 는 CrossCert 인증서 폐지 목록을 보여주고 상태 확인 서비스를 제공하는 CRL 을 발행합니다. 사용자 등록 인증서를 발행하는 CA CRL 은 매일 발행됩니다. CA 인증서만 발행하는 CA CRL 은 분기별로 발행되며 CA 인증서가 폐지될 때마다 발행됩니다. 만료된 인증서는 인증서 만료 후 30 일이 지나면 CRL 에서 삭제됩니다.

4.4.10 인증서 폐지 목록 확인 요건

신뢰 당사자는 신뢰하는 인증서의 상태를 확인해야 합니다. 신뢰 당사자가 인증서 상태를 점검하는 데 사용할 수 있는 한 가지 방법은 신뢰 대상 인증서를 발행한 CA 에서 발행한 최신 CRL 을 검토하는 것입니다.

- VeriSign PCA 및 클래스 1-3 인증 기관의 CRL은 VeriSign 저장소인 **http://crl.crosscert.com**에 게시됩니다.
- Managed PKI Lite 고객 CA의 CRL은 **http://onsitecrl.crosscert.com/OnSitePublic/**에 게시됩니다.
- Managed PKI 고객 CA 의 CRL 은 Managed PKI 고객에게 통보된 고객별 저장소에 게시됩니다.

저장소에는 신뢰 당사자가 관련 CA 의 CRL 위치를 확인할 수 있는 "CRL 참조 테이블"도 게시됩니다.

4.4.11 온라인 폐지/상태 확인 기능

CRL 발행 외에도 CrossCert 는 CrossCert 저장소의 질의 기능을 통해 인증서 상태 정보를 제공합니다.

인증서 상태 정보는 다음의 CrossCert 저장소에서 액세스할 수 있는 웹 기반 질의 기능을 사용하여 확인할 수 있습니다.

- **https://www..crosscert.com/Repository** (개인 인증서)
- **https://www..crosscert.com/Repository** (서버 및 개발자 인증서)

CrossCert 는 OCSP 인증서 상태 정보도 제공합니다. OCSP 서비스 계약을 체결한 Managed PKI 고객은 OCSP 를 사용하여 인증서 상태를 점검할 수 있으며, 관련 OCSP 응답자의 URL 이 Managed PKI 고객에게 통보됩니다.

4.4.12 온라인 폐지 확인 요건

신뢰 당사자가 최신 관련 CRL 을 점검하여 신뢰 대상 인증서의 상태를 확인하지 않는 경우에는 CPS 4.4.11 항에 정해진 방법 중 하나를 사용하여 인증서 상태를 확인해야 합니다.

4.4.13 사용 가능한 기타 폐지 광고 형태

해당 조항 없음

4.4.14 기타 폐지 광고 형태에 대한 확인 요건

해당 조항 없음

4.4.15 키 손상에 관한 특수 요건

CPS 4.4.9 – 4.4.14 항에서 설명한 절차 외에 CrossCert 는 CrossCert CA 의 개인키 손상을 발견하였거나 그렇게 믿을만한 근거가 있는 경우 이를 잠재적 신뢰 당사자에게 통보하기 위한 합리적인 노력을 다합니다.

4.5 보안 감사 절차

4.5.1 기록 이벤트 유형

CrossCert 는 다음 주요 이벤트를 자동 또는 수동으로 기록합니다.

- 다음을 포함한 CA 키 유효 주기 관리 이벤트
  - 키 생성, 백업, 저장, 복구, 저장 및 해제
  - 암호화 장치 유효 주기 관리 이벤트
- 다음을 포함한 CA 및 가입자 인증서 유효 주기 관리 이벤트
  - 인증 신청서, 갱신, 키 재발급 및 폐지
  - 성공하거나 성공하지 못한 요청 처리
  - 인증서와 CRL 의 생성 및 발행
- 다음을 포함한 보안 관련 이벤트
  - 성공하거나 성공하지 못한 PKI 시스템 액세스 시도
  - CrossCert 담당자가 수행하는 PKI 및 보안 시스템 동작
  - 보안에 민감한 파일이나 레코드의 읽기, 쓰기 또는 삭제
  - 보안 프로파일 변경
  - 시스템 중단, 하드웨어 고장 및 기타 이상 증상
  - 방화벽 및 라우터 동작
  - CA 시설 방문자 출입

로그 항목에는 다음 요소가 포함됩니다.

- 입력 날짜 및 시간
- 항목의 일련번호 또는 시퀀스 번호(자동 저널 항목의 경우)
- 저널을 입력하는 실체의 신원
- 항목의 종류

CrossCert RA 및 Managed PKI 관리자는 다음을 포함한 인증 신청 정보를 기록합니다.

- 인증 신청자가 제출한 신별 문서의 종류
- 식별 문서의 고유 식별 데이터, 번호 또는 그 조합(예: 인증서 요청자의 운전면허증 번호)
- 신청서 및 식별 문서의 사본 저장 위치
- 신청서를 승인하는 실체의 신원
- 식별 문서 확인에 사용되는 방법(해당되는 경우)
- CA 수신 또는 RA 제출 이름(해당되는 경우)

4.5.2 로그 프로세싱 빈도

주 단위로 감사 로그를 조사하여 중요 보안 및 운영 이벤트를 점검합니다. 또한 CrossCert 는 감사 로그를 검토하여 CrossCert CA 및 RA 시스템 내의 특이 상황이나

사건으로 인해 생성된 경고에 대한 응답으로 수행된 의심스럽거나 비정상적 동작이 있는지 확인합니다.

감사 로그 프로세싱은 감사 로그의 검토와 감사 로그 요약의 주요 이벤트에 대한 문서화로 이뤄집니다. 감사 로그 검토에는 로그의 침해 여부 확인, 모든 로그 항목의 간단한 검사 및 로그의 비정상적 동작에 대한 자세한 검토가 포함됩니다. 감사 로그 검토에 따른 조치도 문서화됩니다.

4.5.3 감사 로그 보유 기간

감사 로그는 처리 후 2 개월 이상 온사이트에 보관되며 그 이후에는 CPS 4.6.2 항에 따라 보관됩니다.

4.5.4 감사 로그 보호

전자 및 수동 감사 로그 파일은 물리적, 논리적 액세스 제어를 통해 무단 보기나 수정, 삭제, 기타 침해 행위로부터 보호됩니다.

4.5.5 감사 로그 백업 절차

감사 로그에 대한 증분 백업은 매일 수행되며 전체 백업은 매주마다 수행됩니다.

4.5.6 감사 수집 시스템

자동 감사 데이터는 애플리케이션, 네트워크 및 운영 체제 수준에서 생성 및 기록됩니다. 수동으로 생성되는 감사 데이터는 CrossCert 직원에 의해 기록합니다.

4.5.7 이벤트 발생 주체에 대한 통보

감사 수집 시스템에 의해 이벤트가 기록되는 경우 해당 이벤트를 발생시킨 개인, 단체, 장치 또는 애플리케이션에는 통보되지 않습니다.

4.5.8 취약점 평가

감사 프로세스의 이벤트는 시스템 취약성을 모니터하기 위한 목적으로도 기록됩니다. 논리적 보안 취약성 평가(“LSVA”)는 모니터된 이벤트에 대한 검사를 거쳐 수행, 검토 및 개정됩니다. LSVA 는 실시간 자동 로그 데이터를 기반으로 하며 보안 및 감사 요건 가이드의 요건에 따라 매일, 매월 및 매년 단위로 수행됩니다. 연간 LSVA 는 연간 준수 감사(Compliance Audit)를 위한 데이터를 제공합니다.

4.6 기록 보관

4.6.1 기록 이벤트 유형

CrossCert 는 CPS 4.5 항에 지정된 감사 로그 외에도 다음에 관한 문서를 포함하는 기록을 유지합니다.

- 가입자와의 계약에 따른 CrossCert 의 CPS 및 기타 의무 준수 여부
- 각 인증 신청서, CrossCert 프로세싱/서비스 센터에서 발행하는 모든 인증서의 생성, 발행, 사용, 폐지, 만료, 키 재발급 또는 갱신에 관한 중요 동작 및 정보

CrossCert 의 인증서 유효 주기 이벤트 기록에는 다음이 포함됩니다.

- 각 인증서(가입자의 불명확한 이름의 기록만 유지되는 클래스 1 인증서 제외)에 기재된 가입자의 신원
- 인증서 폐지를 요청하는 사람의 신원(가입자의 불명확한 이름의 기록만 유지되는 클래스 1 인증서 제외)
- 인증서에 표시된 기타 내용
- 타임 스탬프
- CPS 2.7 항에 따라 호환성 감사의 성공적 완료에 관련된 정보를 포함한 인증서 발행에 관련된 중요한 사실

정확하고 완벽하게 색인화되고 저장, 보존 및 복제된 기록은 전자적 형태나 하드카피 형태로 보관이 가능합니다.

4.6.2 기록 보존 기간

인증서에 관련된 기록은 인증서가 만료되거나 폐지된 후 적어도 다음 기간 동안 보존됩니다.

- 클래스 1 인증서의 경우 5 년
- 클래스 2 인증서의 경우 10 년
- 클래스 3 인증서의 경우 30 년

필요한 경우 CrossCert 는 적절한 법률을 준수하기 위해 보존 기간을 늘릴 수 있습니다.

4.6.3 기록 보호

CrossCert 는 CPS 4.6.1 항에 따라 인증된 사람만 액세스할 수 있도록 컴파일된 보관 기록을 보호합니다. 전자적으로 보관된 데이터는 물리적, 논리적 액세스 제어를 통해 무단 보기, 수정, 삭제 또는 기타 침해 행위로부터 보호됩니다. 기록 데이터와 이를 처리하는 데 필요한 애플리케이션이 저장된 미디어는 CPS 4.6.2 항에 정해진 기간 동안 액세스할 수 있도록 보존됩니다.

4.6.4 기록 백업 절차

CrossCert 는 발행된 인증서 정보의 전자 기록에 대한 증분 백업을 매일 수행하고 매주 한차례씩 전체 백업을 수행합니다. CPS 4.6.1 항에 따라 작성된 하드카피 사본은 CPS 4.8 에 따라 오프사이트의 재난 복구 설비에 보관됩니다.

4.6.5 레코드 시간 기록 요건

인증서, CRL 및 기타 폐지 데이터베이스 항목에는 시간 및 날짜 정보가 포함됩니다. CrossCert 의 Digital Notarization Service 와 반대로 이러한 시간 정보는 암호화되지 않습니다(CPS 1.1.2.2.2 항 참조).

4.6.6 기록 정보 수집 및 확인 절차

CPS 4.6.3 항 참조

4.7 키 변경

CrossCert CA 키 쌍은 CPS 6.3.2 항에 정해진 최대 사용 기간이 끝나면 더 이상 사용할 수 없습니다. CrossCert CA 인증서는 CA 키 쌍의 누적 인증 사용 기간이 최대 CA 키 쌍 사용 기간을 초과하지 않는 경우에 한해 갱신이 가능합니다. 새로운 CA 키 쌍은 CPS 6.1 항에 따라 폐지된 CA 키 쌍을 대체하거나, 기존의 활성 키 쌍을 보완하거나, 새로운 서비스를 지원하기 위해 생성됩니다.

상위 CA 의 CA 인증서가 만료되기 전에 상위 CA 계층 구조 내의 실체가 기존 상위 CA 키 쌍에서 새 CA 키 쌍으로 자연스럽게 전환되도록 돕는 키 변경 절차가 활성화됩니다. CrossCert 의 CA 키 변경 프로세스가 활성화되려면 다음과 같은 조건이 필요합니다.

- 상위 CA 는 상위 CA 키 쌍의 남은 사용 기간이 상위 CA 의 계층에 속한 종속 CA 가 발행한 특정 유형의 인증서에 대해 승인된 인증서 유효 기간과 동일한 시간("발행 중지 날짜") 이전 60 일이 되기 전에 새로운 종속 CA 인증서 발행을 중지합니다.
- "발행 중지 날짜" 이후 수신된 종속 CA 또는 사용자 등록 인증서 신청에 대한 확인이 끝나면 인증서는 새로운 CA 키 쌍으로 서명됩니다.
- 상위 CA 는 원래의 키 쌍을 사용해 발행된 최종 인증서의 만료일이 될 때까지 원래 상위 CA 개인키로 서명된 CRL 을 계속해서 발행합니다.

4.8 재난 복구 및 키 손상

CrossCert 는 키 손상이나 재난의 위험과 잠재적 영향을 최소화하기 위해 물리적, 논리적, 절차적 제어의 강력한 조합을 구현하고 CPS 4.8.2 항에 설명된 재난 복구 절차와 CPS 4.8.3 항에 설명된 키 손상 응답 절차를 구현했습니다. CrossCert 의 손상 및 재난 복구 절차는 재난 발생에 따르는 잠재적인 영향을 최소화하고 합리적인 시간 내에 CrossCert 를 정상적으로 복원하기 위해 개발되었습니다.

4.8.1 컴퓨팅 리소스, 소프트웨어 및 데이터의 손상

컴퓨팅 리소스, 소프트웨어 및 데이터가 손상되면 CrossCert Security 에 이 사실이 보고되고 CrossCert 의 사고 처리 절차가 시작됩니다. 이러한 절차는 적절한 보고, 사고 조사 및 대응으로 이뤄지며, 필요한 경우 CrossCert 의 키 손상이나 재난 복구 절차가 시작됩니다.

4.8.2 재난 복구

4.8.2.1 VeriSign

인증서를 발행하는 실체가 VeriSign 인 서비스의 경우(CPS 1.1.2.1.2 항 참조)를 위해 VeriSign 은 주 보안 설비에서 1 천 마일 떨어진 곳에 재난 복구 사이트를 만들었습니다. VeriSign 은 모든 종류의 자연 재해와 인간에 의한 재해가 미치는 영향을 최소화하도록 재난 복구 계획을 개발, 구현 및 테스트했으며, 재난 발생 시 작동되도록 주기적인 테스트, 확인 및 업데이트를 실시합니다.

정보 시스템 서비스의 주요 비즈니스 기능을 복구할 수 있도록 상세한 재난 복구 계획이 수립되어 있습니다. VeriSign 의 재난 복구 사이트에는 안전한 백업 설정을 제공하기 위해 보안 및 감사 요건 가이드에서 요구하는 물리적 보호 및 운영적 제어가 구현되어 있습니다.

VeriSign 의 주 설비 운영을 일시적 또는 영구적으로 중지시키는 자연재해나 인간에 의한 재해가 발생하면 VeriSign Emergency Response Team(VERT)에 의해 VeriSign 재난 복구 프로세스가 시작됩니다.

VeriSign 은 재난 발생 후 24 시간 이내에 최소한 다음과 같은 기능이 지원되도록 시스템을 복구 및 복원합니다.

- 인증서 발행
- 인증서 폐지
- 폐지 정보 게시
- Managed PKI Key Manager 를 사용하는 Managed PKI 고객을 위한 키 복구 정보 제공

VeriSign 의 재난 복구 데이터베이스는 보안 및 감사 요건 가이드에 설정된 시간 제한 내에서 프로덕션 데이터베이스와 주기적으로 동기화됩니다. VeriSign 의 재난 복구 장비는 VeriSign CPS 5.1.1 에 지정된 물리적 보안 장치와 비교할 수 있는 물리적 보호 기능으로 보호됩니다.

VeriSign 의 재난 복구 계획은 VeriSign 의 주 사이트에서 재난이 발생한 경우 1 주일 이내에 완전 복구되도록 설계되었습니다. VeriSign 은 전체 설비의 운영이 불가능한 중대한 재난이 발생하는 경우 주 사이트의 장비가 CA/RA 기능을 지원하는지

테스트하는데, 이 테스트 결과는 감사 및 계획 수립을 위해 검토 및 보관됩니다. 따라서 중대한 재난이 발생할 경우 가능한 신속하게 VeriSign 의 주 사이트 운영이 재개됩니다.

VeriSign 은 CA 와 기반구조 시스템 소프트웨어의 백업과 중복 하드웨어를 재난 복구 설비에 유지합니다. 또한 CA 개인키는 VeriSign CPS 6.2.4 에 따라 재난 복구용으로 백업 유지됩니다.

4.8.2.2 CrossCert

인증서를 발행하는 실체가 CrossCert 인 서비스에 대해(CPS 1.1.2.1.2 항 참조) CrossCert 는 2004 년 말까지 재난 복구 계획을 개발, 구현 및 테스트될 예정이며, 이 계획은 재난 발생 시 운영될 수 있도록 주기적으로 테스트, 확인 및 업데이트됩니다. 또한 정보 시스템 서비스와 주요 비즈니스 기능을 복구하기 위한 세부 재난 복구 계획이 수립될 것입니다. CrossCert 의 주 설비 운영이 일시적 또는 영구적으로 중지되는 자연 또는 인간 재해가 발생할 경우 CrossCert Emergency Response Team(CERT)에 의해 CrossCert 의 재난 복구 프로세스가 시작됩니다.

CrossCert 는 재난 발생 후 24 시간 이내에 최소한 다음과 같은 기능이 지원되도록 시스템을 복구 및 복원합니다.

- 인증서 발행
- 인증서 폐지
- 폐지 정보 게시
- Managed PKI Key Manager 를 사용하는 Managed PKI 고객을 위한 키 복구 정보 제공

CrossCert 는 다음과 같은 백업 및 보관 절차를 구현했습니다.

- 야간 데이터 백업
- 매주 오프 사이트(로컬 뱅크) 전체 백업

CrossCert 는 재난 복구 설비에 CA 와 기반구조 시스템 소프트웨어의 백업과 중복 하드웨어를 유지합니다. 또한 CA 개인키는 CPS 6.2.4 항에 따라 재난 복구용으로 백업 및 유지됩니다.

4.8.3 키 손상

CrossCert CA, CrossCert 기반구조 또는 고객 CA 개인키의 손상이 파악되거나 의심되는 경우 Compromise Incident Response Team(CIRT)에 의해 CrossCert 의 키 손상 대응 절차가 시작됩니다. 보안, 암호화 사업, 생산 서비스 담당자와 기타 CrossCert 관리자 대표로 구성된 이 팀은 상황을 분석하여 대처 계획을 수립하고 CrossCert 임원진의 승인을 받아 계획을 실행합니다.

CA 인증서를 폐지해야 하는 경우 다음 절차가 수행됩니다.

- CPS 4.4.9 항에 따라 CrossCert 저장소를 통해 신뢰 당사자에게 인증서 폐지 상태가 통보됩니다.
- 모든 관련 VTN 참여자에게 폐지를 통보하기 위한 합리적인 노력이 진행됩니다.
- CA 가 CPS 4.7 항에 따라 새 키 쌍을 생성합니다(CA 가 CPS 4.9 항에 따라 만료된 경우 제외).

4.9 CA 만료

CrossCert CA, Managed PKI 고객 CA 가 운영을 중지할 필요가 생긴 경우 CrossCert 는 CA 만료 이전에 가입자, 신뢰 당사자 및 기타 영향을 받는 모든 실체에게 이러한 만료 사실을 통보하기 위한 모든 노력을 수행합니다. CA 만료가 필요한 경우 CrossCert 및 고객 CA 의 경우 해당 고객이 고객, 가입자 및 신뢰 당사자에게 미치는 영향을 최소화하기 위한 만료 계획을 개발합니다. 이러한 만료 계획에는 가능한 경우 다음과 같은 사항이 포함됩니다.

- 가입자, 신뢰 당사자, 고객 등 만료의 영향을 받는 당사자에게 CA 상태에 대한 정보 통보
- 통보에 따르는 비용 처리
- CrossCert 가 CA 에 발행한 인증서 폐지
- CPS 4.6 항에 지정된 기간 동안의 CA 기록 및 레코드 보존
- 지속적인 가입자 및 고객 지원 서비스 수행
- CRL 발행, 온라인 상태 확인 서비스 유지 등의 폐지 서비스 수행
- 필요한 경우 만료되지 않고 폐지되지 않은 최종 사용 가입자 및 종속 CA 의 인증서 폐지
- 만료 계획, 준비에 의해 만료되지 않고 폐지되지 않은 인증서가 폐지된 가입자에게 변상 조치를 하거나 후임 CA 에 의한 인증서 대체 발행
- CA 의 개인키 및 이러한 개인키가 포함된 하드웨어 토큰 처분
- CA 의 서비스를 후임 CA 로 이전하기 위해 필요한 준비 수행
-

5. 물리적, 절차상 및 인적 보안 제어

CrossCert 는 본 CPS 의 보안 요구 사항을 지원하는 CrossCert 보안 정책을 이행하고 있습니다.

5.1 물리적 제어

5.1.1 위치 및 구축

CrossCert 의 CA 와 RA 는 보안 및 감사 요구 사항을 충족하는 [해당 국가 및 도시]의 CrossCert 시설 내에서 운영됩니다. 모든 CrossCert CA 와 RA 의 운영은 은밀한 또는 공개적 침투를 감지하여 차단하도록 물리적으로 보호된 환경에서 수행됩니다.

CrossCert 의 주요 시설은 CPS § 5.1.2 의 설명과 같이 7 개 물리적 보안 계층으로 보호되고 있습니다.

- RA 확인 작업은 3 번째 계층에서 수행됩니다.
- CA 기능은 4 번째 계층에서 수행됩니다.
- VeriSign 로밍 서버를 포함하여 기밀 서버는 4 번째 계층에 위치합니다.
- 온라인 CA 암호화 모듈은 5 번째 계층에 저장되어 있습니다.
- 오프라인 CA 암호화 모듈은 7 번째 계층에 저장되어 있습니다.

Managed PKI 고객은 해당 보안 시설이 Enterprise Security Guide(기업 보안 가이드)의 요구 사항을 충족하도록 해야 합니다.

5.1.2 물리적 액세스

CrossCert CA 시스템은 4 개의 물리적 보안 계층으로 보호됩니다. 이때 상위 계층에 액세스하려면 먼저 하위 계층에 액세스해야 합니다. 뿐만 아니라 물리적 보안 시스템에는 키 관리 보안을 위한 3 개의 추가 계층이 포함되어 있습니다. 아래 표 15 에는 각 계층의 특성과 요구 사항이 나와 있습니다.

계층	*설명*	*액세스 제어 메커니즘*
물리적 보안 계층 1	물리적 보안 계층 1 은 시설의 가장 바깥쪽에 있는 물리적 보안을 의미합니다.	이 계층에 액세스하려면 직원 출입 카드가 필요합니다. 계층 1 에 대한 물리적 액세스는 자동으로 기록되며 비디오에 녹화됩니다.
물리적 보안 계층 2	계층 2 는 화장실과 복도 등의 공동 구역을 포함합니다.	계층 2 는 CA 시설의 공동 구역에 출입하는 모든 인원에 대해 직원 출입 카드를 사용하여 개별 액세스 제어를 수행합니다. 계층 2 에 대한 물리적 액세스는 자동으로 기록됩니다.

계층	*설명*	*액세스 제어 메커니즘*
물리적 보안 계층 3	계층 3 은 기밀 CA 활동이 수행되는 첫번째 계층입니다. 기밀 CA 활동이란 인증, 확인, 발행 등의 인증 프로세스 주기와 관련된 모든 활동을 의미합니다.	계층 3 은 생체인식을 포함한 두 가지 요소의 인증을 사용하여 개별 액세스 제어를 수행합니다. 권한이 부여되지 않은 직원이나 방문자를 포함하여 동행 안내되지 않은 사람은 계층 3 보안 구역에 출입할 수 없습니다. 계층 3 에 대한 물리적 액세스는 자동으로 기록됩니다.
물리적 보안 계층 4	계층 4 는 특별히 기밀성이 높은 CA 활동이 수행되는 계층입니다. 계층 4 구역은 온라인 계층 4 데이터 센터와 오프라인 계층 4 키 형식 공간의 두 가지 종류로 나뉩니다.	계층 4 데이터 센터는 개별 액세스 제어를 수행하고, 키 형식 공간은 이중 제어를 수행합니다. 두 구역 모두 생체인식을 포함한 두 가지 요소의 인증을 사용합니다. 동행 안내 없이 계층 4 액세스가 허용된 개인은 직원 승인 정책(Trusted Employee Policy)을 준수해야 합니다. 계층 4 에 대한 물리적 액세스는 자동으로 기록됩니다.
키 관리 계층 5-7	키 관리 계층 5-7 은 CSU 와 키 제작 재료의 온라인 및 오프라인 저장을 보호합니다.	온라인 CSU 는 캐비닛 잠금을 통해 보호되고, 오프라인 CSU 는 금고, 캐비닛 및 용기 잠금으로 보호됩니다. CSU 와 키 제작 재료에 대한 액세스는 CrossCert 의 직무 분리 요구 사항에 따라 제한됩니다. 이들 계층에서 캐비닛이나 용기를 열고 닫는 작업은 감사를 위해 자동으로 기록됩니다. 물리적 액세스 권한을 단계적으로 점차 제한함으로써 각 계층에 대한 액세스가 제어됩니다.

표 15 – 물리적 보안 계층

5.1.3 전원 및 에어컨 설비

CrossCert 의 보안 시설에는 다음과 같은 주요 장치와 보조 장치가 설치되어 있습니다.

- 중단없이 계속되는 전력 공급을 보장하는 전원 시스템
- 온도와 상대 습도를 제어하기 위한 냉난방/환기 시스템

5.1.4 수해 위험

[회원사]는 CrossCert 시스템에 대한 수해 위험을 최소화하기 위해 적절한 예방 조치를 마련해 놓고 있습니다.

5.1.5 화재 예방 및 보호

CrossCert 는 화염이나 연기 등의 화재 위험을 예방하고 화재 발생 시 진화하기 위한 적절한 대책을 마련해 놓고 있습니다. CrossCert 의 화재 예방 및 진화 조치는 해당 지역의 소방 안전 규정을 준수하도록 고안되었습니다.

5.1.6 매체 저장

제작 소프트웨어와 데이터, 감사, 보관 또는 백업 정보 등을 포함하고 있는 모든 매체는 CrossCert 시설 내에 저장되거나, 승인된 사람으로만 액세스를 제한하여 우발적 손상(예: 수해, 화재, 전자기적 피해 등)을 방지하도록 적절한 물리적 및 논리적 액세스 제어 기능을 갖춘 CrossCert 시설 외의 안전한 저장 시설에 보관됩니다.

5.1.7 폐기물 처리

모든 기밀 문서와 자료는 분쇄하여 폐기하고, 기밀 정보를 수집 또는 전송하는 데 사용된 매체는 읽기불능 상태로 만든 후 폐기합니다. 또한 암호화 장치는 폐기하기 전에 물리적으로 파괴하거나 제작 업체의 지침에 따라 모든 값을 0 으로 만들고, 기타 모든 폐기물은 CrossCert 의 일반 폐기 요구 사항에 따라 처리합니다.

5.1.8 별도의 백업

CrossCert 는 중요한 시스템 데이터, 감사 기록 데이터 및 기타 기밀 정보에 대해 정기적인 백업을 수행합니다.

5.2 절차 상의 제어

5.2.1 승인된 역할

다음에 대해 중요한 영향을 미칠 수 있는 인증 또는 암호화 작업을 액세스하거나 제어할 수 있는 모든 직원, 계약직 및 컨설턴트는 승인된 사람에 포함됩니다.

- 인증 신청서의 정보 확인
- 인증 신청서의 승인, 거부 또는 기타 처리, 폐지 요청, 갱신 요청 및 등록 정보
- 저장소의 제한된 일부에 액세스할 수 있는 사람을 포함하여 인증서의 발급 또는 폐지
- 가입자 정보 또는 요청 처리

승인된 사람에는 다음이 포함되며 이에 제한되지는 않습니다.

- 고객 서비스 직원
- 암호화 업무 처리 직원
- 보안 요원
- 시스템 관리자
- 지정된 기술 직원

- 기반구조 신뢰도의 관리를 위해 지정된 임원

CrossCert 는 이 항에 명시된 범주의 인원을 승인된 직책을 가진 승인된 사람으로 간주합니다. 승인된 직책을 획득하여 승인된 사람이 되려면 CPS § 5.3 의 조사 요구 사항을 모두 충족해야 합니다.

5.2.2 작업별 필요한 인원수

CrossCert 는 담당 업무를 기반으로 직무를 명확히 분리하는 엄격한 제어 절차 및 정책을 유지하고 있습니다. CA 암호화 하드웨어(암호화 서명 장치 또는 CSU)와 연관된 키 재료 등에 대한 액세스 및 관리와 같이 기밀성이 매우 높은 작업은 여러 명의 승인된 사람이 필요합니다.

이러한 내부 제어 절차는 장치에 대한 물리적 또는 논리적 액세스를 위해 최소 두 명의 승인된 사람이 필요하도록 구성되었습니다. CA 암호화 하드웨어에 대한 액세스는 접수 및 검사에서 논리적 또는 물리적 최종 파기에 이르기까지 전체 수명에 걸쳐 여러 명의 승인된 사람에 의해 엄격하게 수행됩니다. 운영 키를 통해 모듈이 활성화되고 나면 장치에 대한 물리적 액세스와 논리적 액세스를 분리하여 제어하는 작업을 관리하기 위해 추가 액세스 제어가 실행됩니다. 모듈에 대해 물리적 액세스 권한을 가진 사람은 "Secret Shares"를 보유하지 않으며, "Secret Shares"를 보유한 사람은 모듈에 대해 이러한 권한이 없습니다. CA 개인키 활성화 데이터와 Secret Shares 를 위한 요구 사항은 CPS § 6.2.7 에 명시되어 있습니다.

클래스 3 인증서의 확인 및 발행과 같은 다른 작업을 위해서는 최소 두 명의 승인된 사람이 필요합니다.

5.2.3 각 역할에 대한 식별 및 인증

승인된 사람이 되려는 모든 사람은 CrossCert 의 인사 관리 또는 보안 기능을 수행하는 승인된 사람 앞에 본인이 직접 출두하여 일반적인 형태의 신분증(예: 여권, 운전면허증 등)을 통해 확인을 받습니다. CPS § 5.3.1 의 배경 조사 절차를 통해 추가 신원 확인이 수행됩니다.

CrossCert 는 담당자가 다음을 수행할 권한을 얻기 전에 먼저 승인된 상태 및 부서 승인을 획득하도록 보장합니다.

- 장치 및 필요한 시설에 대한 액세스
- CrossCert CA, RA 및 기타 IT 시스템 상의 특정 기능을 액세스 및 수행하기 위한 전자 인증

5.3 인원 제어

5.3.1 배경, 자격, 경험 및 허가 요구 사항

승인된 사람이 되려면 필수적인 배경 및 자격은 물론 해당 직무를 완벽하게 수행하기에 충분한 경험을 증명하는 자료를 제시해야 하며, 정부와의 계약에 따른 인증 서비스를 수행하는 경우에는 필요한 각종 정부 허가 증명을 제시해야 합니다. 배경 조사는 승인된 사람의 경우 최소 매 5 년에 한 번씩 수행됩니다.

5.3.2 배경 조사 절차

승인된 역할을 위해 사람을 고용하기 전에 CrossCert 는 다음 항목을 포함하는 배경 조사를 실시합니다.

- 이전 경력 확인
- 전문성에 대한 참조 자료 확인
- 최종 학력 또는 가장 관련이 많은 학위 확인
- 범죄 기록 조회(전국 및 지방 범위)
- 신용/재정 상태 조회
- 운전면허 조회
- 주민등록 조회

이 항에서 명시하는 요구 사항 중 하나라도 현지법이나 기타 상황에 의해 충족되지 못할 경우, CrossCert 는 해당 정부 기관에 의한 배경 조사를 포함하여 법이 허용하는 범위 내에서 이와 유사한 정보를 제공하는 대체 조사 방법을 사용합니다.

배경 조사 결과 승인된 직책의 후보자를 거부하거나 기존의 승인된 사람에 대해 조치를 취할 근거로 사용할 수 있는 요소에는 일반적으로 다음이 포함됩니다.

- 후보자 또는 승인된 사람에 의한 허위 진술
- 매우 부정적이거나 신뢰성 없은 신원 증명서
- 특정 범죄 기록
- 재정 능력 미달

인사 관리 및 보안 담당 직원은 이러한 정보가 포함된 보고서를 평가함으로써 배경 조사를 통해 밝혀진 행위의 유형, 범위 및 빈도를 고려하여 적절한 결정을 내립니다. 이런 결정에 따라 승인된 직책 후보자의 자격을 취소하거나 기존의 승인된 사람을 해고할 수도 있습니다.

배경 조사로 밝혀진 정보를 기반으로 이러한 조치를 취하는 것은 해당 국가 및 지역 법규의 적용을 받습니다.

5.3.3 교육 요구 사항

CrossCert 는 직원을 대상으로 완벽한 직무 수행에 필요한 현장 교육을 실시합니다. 이러한 교육 프로그램은 주기적으로 검토되며 필요에 따라 개선됩니다.

CrossCert 의 교육 프로그램은 개별 직원의 직무에 맞게 구성되어 있으며 다음과 같은 내용이 포함됩니다.

- 기본 PKI 개념
- 직무 설명
- CrossCert 보안 및 운영 정책과 절차
- 배치된 하드웨어/소프트웨어의 사용 및 운영
- 사고 및 손상에 대한 보고 및 처리
- 재해 복구 및 업무 연속성 절차

5.3.4 재교육 주기 및 요구 사항

CrossCert 는 재교육 프로그램을 주기적으로 실시하여 해당 직원이 본인의 직무를 완벽히 수행하는 데 필요한 수준의 능력을 유지하도록 보장합니다. 보안 인식 교육은 항상 주기적으로 실시됩니다.

5.3.5 직무 교대 주기 및 순서

해당 조항 없음

5.3.6 무단 행위에 대한 제재

CrossCert 정책과 절차에 위반되는 무단 행위는 적절한 제재 조치가 취해집니다. 이러한 제재 조치로 인해 해고될 수도 있으며, 무단 행위의 심각성이나 빈도에 따라 적절한 조치가 취해집니다.

5.3.7 계약 직원 요구 사항

제한된 상황에서 독립 계약 직원이나 컨설턴트가 승인된 직책을 수행할 수도 있습니다. 이러한 계약 직원이나 컨설턴트는 동등한 직책의 CrossCert 직원에게 적용되는 것과 동일한 기능 및 보안 기준의 적용을 받습니다

CPS § 5.3.2 에 명시된 배경 조사를 완료하지 않은 독립 계약 직원이나 컨설턴트는 승인된 사람이 안내하고 직접 감독하는 범위 내에서 CrossCert 의 보안 시설에 액세스할 수 있습니다.

5.3.8 담당자에게 제공되는 문서

CrossCert 의 PKI 서비스 운영에 관여하는 CrossCert 직원은 본 CPS 와 VTN CP 및 CrossCert 보안 정책을 숙지해야 합니다. CrossCert 는 담당자들에게 완벽한 직무 수행에 필요한 필수 교육과 기타 문서를 제공합니다.

6. 기술 보안 제어

6.1 키 쌍 생성 및 설치

6.1.1 키 쌍 생성

CA 키 쌍은 선발되어 교육을 받은 다수의 승인된 개인이 키에 필요한 암호화 강도와 보안을 제공하는 신뢰할 수 있는 시스템 및 프로세스를 통해 생성합니다. PCA 및 루트 CA 발행의 경우, 키 생성에 사용되는 암호화 모듈은 FIPS 140-1 레벨 3 의 요구 사항을 충족합니다. CrossCert CA 와 Managed PKI 고객 CA 를 포함하여 기타 CA 의 경우, 사용되는 암호화 모듈은 FIPS 140-1 레벨 2 이상의 요구 사항을 충족합니다.

모든 CA 키 쌍은 Key Ceremony Reference Guide(키 형식 참조 가이드), CA Key Management Tool User's Guide(CA 키 관리 도구 사용자 가이드) 및 Security and Audit Requirements Guide(보안 및 감사 요구 사항 가이드)의 요구 사항에 따라 사전 계획된 키 생성 형식으로 생성됩니다. 각 키 생성 형식에서 수행된 활동은 관여한 모든 개인에 의해 기록되고 날짜와 서명이 추가됩니다. 이러한 기록은 감사 및 추적을 위해 CrossCert 경영진이 적절하다고 판단하는 기간 동안 보관됩니다.

RA 키 쌍은 일반적으로 해당 브라우저 소프트웨어와 함께 제공되는 FIPS 140-1 레벨 1 공인 암호화 모듈을 사용하는 RA 에 의해 생성됩니다.

Managed PKI 고객은 자동 관리(AA) 서버가 사용하는 키 쌍을 생성합니다. CrossCert 에서는 FIPS 140-1 레벨 2 공인 암호화 모듈을 사용하여 자동 관리(AA) 서버 키 쌍을 생성할 것을 권장합니다.

최종 사용 가입자 키 쌍은 일반적으로 가입자가 생성합니다. 클래스 1 인증서, 클래스 2 인증서 및 클래스 3 코드/객체 서명 인증서의 경우, 일반적으로 가입자는 해당 브라우저 소프트웨어와 함께 제공된 FIPS 140-1 레벨 1 공인 암호화 모듈을 사용하여 키를 생성합니다. 서버 인증서의 경우, 가입자는 보통 웹 서버 소프트웨어와 함께 제공되는 키 생성 유틸리티를 사용합니다.

6.1.2 해당 개체에 개인키 전달

최종 사용 가입자 키 쌍은 일반적으로 최종 사용 가입자가 생성하므로 이런 경우 개인키가 가입자에게 전달되는 일은 수행되지 않습니다.

RA 또는 최종 사용 가입자 키 쌍이 하드웨어 토큰이나 스마트 카드 상에서 CrossCert 에 의해 사전 생성된 경우, 이러한 장치는 일반 배달 서비스와 개봉 확인 서비스(TEP)를 사용하여 RA 또는 최종 사용 가입자에게 전달됩니다. 장치 활성화에 필요한 활성화 데이터는 대역외 프로세스를 통해 RA 또는 최종 사용 가입자에게 전달됩니다. 이러한 장치의 배포는 CrossCert 에 의해 기록됩니다.

키 복구 서비스를 위해 Managed PKI Key Manager 를 사용하는 Managed PKI 고객의 경우, 인증 신청이 승인된 가입자를 대신하여 암호화 키 쌍을 생성하고 이 키 쌍을 암호로 보호된 PKCS # 12 파일을 통해 가입자에게 전달할 수 있습니다.

6.1.3 인증서 발행자에게 공개키 제출

최종 사용 가입자 및 RA 는 PKCS#10 인증서 서명 요청(CSR)이나 SSL(Secure Sockets Layer)로 보호되는 세션의 디지털 서명 패키지를 통한 전자적 방법으로 CrossCert 로 인증에 필요한 공개키를 제출합니다. 그러나 이는 CrossCert 가 CA, RA, 최종 사용 가입자 키 쌍을 생성하는 경우에는 적용되지 않습니다.

6.1.4 사용자에게 CA 공개키 제공

CrossCert 는 PCA 및 루트 CA 의 CA 인증서를 Microsoft 및 Netscape 웹 브라우저 소프트웨어에 포함시켜 가입자나 신뢰 당사자가 사용할 수 있도록 합니다. 새 PCA 및 루트 CA 인증서가 생성되면 CrossCert 는 브라우저 개발업체에 새 인증서를 제공하여 브라우저 새 버전이나 업데이트에 포함시킵니다.

CrossCert 는 인증서 발행시 최종 사용 가입자에게 발행 CA 를 비롯한 체인 내 모든 CA 를 포함하는 전체 인증 체인을 제공합니다. CrossCert CA 인증서는 CrossCert LDAP 디렉토리인 directory.CrossCert.com 에서도 다운로드할 수 있습니다.

6.1.5 키 크기

키 쌍이 1000 비트 RSA 인 레거시 RSA 시큐어 서버 CA 를 제외한 CrossCert CA 의 키 쌍은 최소 1024 비트 RSA 이상입니다. VeriSign 제 3 세대 PCA 의 키 쌍은 2048 비트 RSA 입니다. CrossCert 는 RA 및 최종 사용 가입자들이 1024 비트 RSA 키 쌍을 생성하도록 권장합니다. 그러나 현재 특정 레거시 애플리케이션이나 웹 서버 지원에는 512 비트 RSA 키 쌍을 사용해야 합니다.

6.1.6 공개키 매개변수 생성

해당 없음

6.1.7 매개변수 품질 검사

해당 없음

6.1.8 하드웨어/소프트웨어 키 생성

CrossCert 는 CPS 6.2.1 항에 따라 해당 하드웨어 암호화 모듈에서 CA 키 쌍을 생성합니다. RA 및 최종 사용 가입자 키 쌍은 하드웨어 또는 소프트웨어에 생성됩니다.

6.1.9 키 용도

X.509 Version 3 인증서의 경우, CrossCert 는 RFC 2459 에 따라 Internet X.509 공개키 기반구조 인증서 및 CRL 프로파일(1999 1 월)과 같은 인증서의 KeyUsage 확장 필드를 자동으로 지정합니다. VeriSign X.509 Version 3 에서 KeyUsage 확장 필드는 다음 경우를 제외하고는 표 16 에 따라 자동으로 지정됩니다.

- 글로벌 서버 ID, 클래스 1 개인 인증서, 클래스 2 개인 인증서에는 KeyUsage 확장 필드가 사용되지 않습니다.
- CrossCert 클래스 3 Managed PKI Authentication Services Bureau CA 에 대한 KeyUsage 확장 필드의 임계는 TRUE 로 설정됩니다.
- Managed PKI Key Manager 를 통한 이중 키 쌍 서명 인증서에 대한 부인 방지 비트를 설정할 수 있습니다.
- 향후 다른 인증서에 대해서도 KeyUsage 확장 필드 임계를 TRUE 로 설정할 수 있습니다.

		CAs	*클래스 3 서버 및 코드/객체 서명 최종 사용 가입자; Automated Administration*	*이중 키 쌍 서명 (Managed PKI Key Manager)*	*이중 키 쌍 암호 (Managed PKI Key Manager)*
임계		FALSE	FALSE	FALSE	FALSE
0	digitalSignature	해제	설정	설정	해제
1	nonRepudiation	해제	해제	해제	해제
2	keyEncipherment	해제	설정	해제	설정
3	dataEnciphermen t	해제	해제	해제	해제
4	keyAgreement	해제	해제	해제	해제
5	keyCertSign	설정	해제	해제	해제
6	CRLSign	설정	해제	해제	해제

서식 있음

		CAs	클래스 3 서버 및 코드/객체 서명 최종 사용 가입자; Automated Administration	이중 키 쌍 서명 (Managed PKI Key Manager)	이중 키 쌍 암호 (Managed PKI Key Manager)
7	encipherOnly	해제	해제	해제	해제
8	decipherOnly	해제	해제	해제	해제

서식 있음

서식 있음

서식 있음

표 16 –KeyUsage 확장 필드 설정

서식 있음

특정 CA 및 사용자 등록 인증서는 X.509 Version 1 인증서(CPS 7.1.1 항 참조)로서 KeyUsage 확장 필드를 지원하지 않습니다. 또한 CrossCert 는 WTLS 인증서에 대해서도 KeyUsage 확장 필드를 사용하지 않습니다.

서식 있음

6.2 개인키 보안

CrossCert 는 CrossCert, Managed PKI, 개인키를 보호하기 위해 물리적, 논리적, 절차적 제어 장치를 마련했습니다. 논리적, 절차적 제어에 대한 자세한 내용은 CPS 6.2 항을, 물리적 액세스 제어에 대한 자세한 내용은 CPS 5.1.2 항을 참조하십시오. 사용자는 계약서에 정해진 대로 개인키의 분실, 공개, 수정, 불법 사용을 막기 위한 필요한 예방 조치를 취해야 합니다.

6.2.1 암호화 모듈 표준

PCA, 인증서 발행 루트 CA 키 쌍 생성과 CA 개인키 저장을 위해 VeriSign 과 CrossCert 는 FIPS 140-1 Level 3 에 지정되었거나 이 요건에 부합하는 하드웨어 암호화 모듈을 사용합니다. 그 외 기타 CA 에 대해서는 FIPS 140-1 Level 2 에 지정된 하드웨어 암호화 모듈이 사용됩니다.

6.2.2 개인키(n/m) 복수 개체 제어

CrossCert 는 권한있는 여러 명의 관계자가 민감한 CA 암호 작업에 참여토록 하는 기술적, 절차적 방법을 사용합니다. CrossCert 는 "비밀 공유" 기법을 사용하여 CA 개인키 사용에 필요한 활성화 데이터를 분할하여 "Shareholder"라는 정당한 권한을 부여 받은 사람이 관리하는 "Secret Shares"라는 별도의 부분에 보관하게 됩니다. 모듈에 저장된 CA 개인키를 활성화하는 데는 특정 하드웨어 암호화 모듈용으로 생성 및 배포된 전체 Secret Shares 수(m) 가운데 임계 수(n)가 사용됩니다.

아래 표 17 은 CrossCert CA 유형별 필요 Secret Shares 임계 수와 총 배포 Secret Shares 수를 보여줍니다. 재해 복구 토큰용으로 배포되는 Secret Shares 수는 운영 토큰용으로 배포되는

Secret Shares 수보다 작으며, 필요한 Secret Shares 의 임계 수는 동일합니다. Secret Shares 는 CPS 6.4.2 항에 따라 보호됩니다.

실체	*CA 개인키로 사용자 등록 인증서 서명하는데 필요한 Secret Shares*	*CA 인증서 서명에 필요한 Secret Shares*	*총 배포 Secret Shares*	*재해복구 Secret Shares CrossCert 에 해당 없음*	
				필요한 Secret Shares	*총 Secret Shares*
클래스 1 PCA	해당 없음	CrossCert 에 해당 없음	CrossCert 에 해당 없음		
클래스 2 PCA	해당 없음	CrossCert 에 해당 없음	CrossCert 에 해당 없음		
클래스 3 PCA	해당 없음	CrossCert 에 해당 없음	CrossCert 에 해당 없음		
클래스 1 CA 및 종속 CA	3	3	4		
클래스 2 CA 및 종속 CA	3	3	4		
클래스 3 CA 및 종속 CA	3	3	4		

표 17 – Secret Shares 배포 및 임계수

6.2.3 개인키 조건부 양도

CrossCert 는 법률에 따른 조회 목적을 위해 제 3 자에게 CA, RA, 최종 사용 가입자 개인키를 조건부 양도(escrow)하지 않습니다.

Managed PKI Key Manager 를 사용하는 Managed PKI 고객은 자신이 인증 신청서를 승인하는 가입자의 개인키 복사본을 조건부 양도할 수 있습니다. CrossCert 는 가입자 개인키 사본을 저장하지 않지만, 다음에서 설명하듯이 가입자 키 복구 프로세스에서 중요한 역할을 수행합니다.

- Managed PKI Key Manager 는 백업된 각 일반 사용자 키 쌍에 대해 백업된 개인키 암호화에 사용되는 대칭 키를 고객 사이트에 무작위로 생성합니다. 이렇게 암호화된 개인키는 고객 사이트의 로컬 데이터베이스에 저장됩니다. 대칭 키 역시 CrossCert 키 복구 서비스에 속한 공개키를 사용하여 암호화된 후 고객 사이트의 로컬 데이터베이스에 저장됩니다.
- 백업한 일반 사용자의 개인키를 복구해야 하는 경우 Managed PKI 관리자는 Key Manager 가 고객 사이트에 저장한 키 사용 기록을 사용하여 해당 키를 식별하고 대응되는 암호화 대칭 키를 CrossCert 복구 서비스로 보냅니다. CrossCert 키 복구

서비스가 대칭 키를 해독하여 반환하면 반환된 키는 해당 지역에서 데이터베이스의 사용자 개인키를 해독하는데 사용됩니다. 이 키와 해당 인증서는 일반 사용자에게 재배포될 수 있습니다.

6.2.4 개인키 백업

CrossCert 는 일상적인 복구 및 재해 복구를 위해 CA 개인키의 백업 복사본을 생성합니다. 이 키는 하드웨어 암호화 모듈이나 관련 키 저장 장치에 암호화된 형태로 저장됩니다. CA 개인키 저장에 사용되는 암호화 모듈은 CPS 6.2.1 항에 정해진 요건의 적용을 받습니다. CA 개인키는 CPS 6.2.6 항에 따라 백업 하드웨어 암호화 모듈에 복사됩니다.

CA 개인키의 온사이트 백업 복사본이 포함된 모듈은 CPS 5.1 항 및 6.2.1 항의 적용을 받으며, CA 개인키의 재해 복구 복사본이 포함된 모듈은 CPS 4.8.2 항에 정해진 요건의 적용을 받습니다.

CrossCert 는 RA 개인키의 복사본을 저장하지 않습니다. 최종 사용 가입자개인키의 백업에 관한 내용은 CPS 6.2.3 항을 참조하십시오.

6.2.5 개인키 저장

CrossCert CA 키 쌍은 유효 기간 만료 후 최소 5 년 동안 저장됩니다. 저장된 CA 키 쌍은 CPS 6.2.1 항에 부합하는 하드웨어 암호화 모듈을 사용하여 안전하게 저장됩니다. 저장 기간 만료 후 저장된 CA 개인키는 CPS 6.2.9 항에 따라 안전하게 파기됩니다.

CrossCert 는 RA 및 가입자 개인키의 복사본을 저장하지 않습니다.

6.2.6 암호화 모듈에 개인키 입력

CrossCert 는 CA 키 쌍이 사용될 하드웨어 암호화 모듈에 대한 CA 키 쌍을 생성하고 일반 복구 및 재해 복에 사용할 CA 키 쌍의 복사본을 만듭니다.CA 키 쌍이 다른 하드웨어 암호화 모듈로 백업되면 이 키 쌍은 암호화된 형태로 모듈간에 이동됩니다.

6.2.7 개인키 활성화 방법

모든 CrossCert 서브도메인 참가자는 개인키가 분실, 절도, 수정, 무단 공개, 불법 사용되지 않도록 활성 데이터를 보호해야 합니다.

6.2.7.1 최종 사용 가입자 개인키

이 단원에서는 최종 사용 가입자의 개인키 활성 데이터 보호에 대한 VTN 표준을 CrossCert 의 서브도메인에 적용합니다. 또한 가입자는 스마트 카드, 생체인식 장비 및 기타 하드웨어 토큰을 비롯한 강화된 개인키 보호 메커니즘을 사용하여 개인키를 저장할

수 있습니다. 두 가지 요소로 구성된 인증 메커니즘(토큰과 암호, 생체인식과 토큰, 생체인식과 암호 등)을 사용하는 것이 바람직합니다.

6.2.7.1.1 클래스 1 인증서

클래스 1 개인키 보호에 대한 VTN 표준은 가입자의 승인 없이 다른 사람이 워크스테이션 및 관련 개인키를 사용하지 못하도록 가입자의 워크스테이션을 실질적으로 보호하기 위한 합리적인 보안 조치를 취하는데 관한 것입니다. CrossCert 는 가입자에게 CPS 6.4.1 항에 따라 패스워드 또는 이에 준하는 보안 기능(개인키 작동 전 패스워드 입력, Windows 로그온 시 또는 화면보호기 해제 시 패스워드 입력, 네트워크 로그온 시 패스워드 입력 등)을 사용하여 개인키 활성화에 앞서 가입자를 인증하도록 권합니다.

6.2.7.1.2 클래스 2 인증서

클래스 2 개인키 보호에 관한 VTN 표준의 내용은 다음과 같습니다.

- 가입자는 CPS 6.4.1 항에 따라 패스워드 또는 이에 준하는 보안 기능(개인키 작동 전 패스워드 입력, Windows 로그온 시 또는 화면보호기 해제 시 패스워드 입력, 네트워크 로그온 시 패스워드 입력, CrossCert 로밍 서비스 사용시 패스워드 입력 등)을 사용하여 개인키 활성화에 앞서 가입자를 인증해야 합니다.
- 가입자는 본인의 승인 없이 다른 사람이 워크스테이션 및 관련 개인키를 사용하지 못하도록 워크스테이션을 실질적으로 보호하기 위해 필요한 보안 조치를 취해야 합니다.

비활성화된 개인키는 반드시 암호화된 형태로 보관해야 합니다.

6.2.7.1.3 관리자 인증서를 제외한 클래스 3 인증서

관리자 인증서를 제외한 클래스 3 개인키 보호에 대한 VTN 표준의 내용은 다음과 같습니다.

- 가입자는 스마트 카드, 암호화 하드웨어 장비, 생체인식 장치, 패스워드(CrossCert 로밍 서비스와 연계) 또는 이에 준하는 보안 기능을 사용하여 개인키 활성화에 앞서 가입자를 인증해야 합니다.
- 가입자는 본인의 승인 없이 다른 사람이 워크스테이션이나 서버 및 관련 개인키를 사용하지 못하도록 워크스테인션을 실질적으로 보호하는 합리적 조치를 취해야 합니다.

CPS 6.4.1 항에 따라 패스워드와 스마트 카드나 암호화된 하드웨어 장비, 생체인식 장치를 함께 사용하십시오. 비활성화하된 개인키는 반드시 암호화된 형태로 보관해야 합니다.

6.2.7.2 관리자 개인키

6.2.7.2.1 관리자

관리자 개인키 보호에 대한 VTN 표준은 다음과 같습니다.

- 관리자는 CPS 6.4.1 항에 따라 스마트 카드, 생체인식 장치, 패스워드 또는 이에 준하는 보안 기능(개인키 작동 전 패스워드 입력, Windows 로그온 시 또는 화면 보호기 해제 시 패스워드 입력, 네트워크 로그온 시 패스워드 입력 등)을 사용하여 개인키 활성화에 앞서 관리자를 인증해야 합니다.
- 관리자는 본인의 승인 없이 다른 사람이 워크스테이션이나 관련 개인키를 사용하지 못하도록 관리자 워크스테이션을 실질적으로 보호하는 합리적 조치를 취해야 합니다.

개인키를 활성화하기 전에 CPS 6.4.1 항에 따라 패스워드와 스마트 카드 또는 패스워드와 생체인식 장치를 함께 사용하여 관리자를 인증하십시오.

비활성화된 개인키는 반드시 암호화된 형태로 보관해야 합니다.

6.2.7.2.2 Automated Administration 또는 Managed PKI Key Manager Service 에 암호화 모듈을 사용하는 Managed PKI 관리자

암호화 모듈을 사용하는 관리자들을 위한 개인키 보호에 관한 VTN 표준은 다음과 같습니다.

- CPS 6.4.1 항에 따라 암호화 모듈과 패스워드를 함께 사용하여 개인키 활성에 앞서 관리자를 인증해야 합니다.
- 관리자는 본인의 승인 없이 다른 사람이 워크스테이션이나 암호화 모듈과 관련된 개인키를 사용하지 못하도록 암호화 모듈 판독기가 포함된 워크스테이션을 실질적으로 보호하는 합리적인 보안 조치를 취해야 합니다.

.

6.2.7.3 **CrossCert 보유 개인키**

CrossCert CA 개인키는 CPS 6.2.2 항에 따라 활성화 데이터(토큰, 암호문)를 제공하는 임계 숫자의 Shareholder 로 활성화됩니다. CrossCert 의 오프라인 CA 의 경우 CA 개인키는 한 세션(종속 CA 인증 또는 PCA 의 CRL 서명 인스턴스 등)에 대해 활성화되었다가 해당 세션이 끝나면 비활성화되고 모듈은 보안 스토리지로 환원됩니다. CrossCert 의 온라인 CA 의 경우, CA 개인키는 지속적인 활성화 상태를 유지하며 모듈은 CA 가 시스템 유지관리 등의 이유로 오프라인될 때까지 생산 데이터 센터에 온라인 상태로 남게 됩니다. CrossCert Shareholder 는 Secret Share 를 보호할 책임이 있으며, Shareholder 의무를 인정하는 계약서에 서명해야 합니다.

6.2.8 개인키 비활성화 방법

CrossCert CA 개인키는 토큰 판독기에서 삭제함과 동시에 비활성화되고, RA 애플리케이션 인증에 사용되는 CrossCert RA 개인키는 시스템 로그오프와 함께 비활성화됩니다. CrossCert RA 는 작업을 마치고 떠날 때 반드시 워크스테이션을 로그오프해야 합니다.

클라이언트 관리자, RA 및 최종 사용 가입자의 개인키는 사용자가 채택한 인증 방식에 따라 매 작동 후 또는 시스템 로그오프 시, 스마트 카드 판독기에서 카드 제거 시 각각 비활성화됩니다. 최종 사용 가입자는 모든 경우에 CPS 2.1.3 항 및 6.4.1 항에 따라 자신의 개인키를 보호해야 할 의무가 있습니다.

6.2.9 개인키 파기 방법

CrossCert CA 의 유효 기간이 만료되면 CPS 6.2.5 항에 따라 하나 이상의 CA 개인키 복사본이 저장되고 나머지 CA 개인키 복사본은 안전하게 파기됩니다. 저장된 CA 개인키는 보존기한이 경과하면 안전하게 파기됩니다. CA 키 파기 작업에는 권한있는 여러 명의 관계자가 참가해야 합니다.

필요할 경우 CrossCert 는 키 재생성에 사용될 수 있는 흔적까지 완벽하게 없애는 방법으로 CA 개인키를 파기해야 합니다. CrossCert 는 CA 개인키의 완벽한 파기를 보장하기 위해 하드웨어 암호화 모듈의 소거 기능을 비롯한 기타 수단을 사용합니다. CA 키를 파기하면 파기 작업에 대한 로그가 기록됩니다.

6.3 키 쌍 관리의 다른 측면

6.3.1 공개키 저장

CrossCert CA, RA, 사용자 등록 인증서는 CrossCert 의 정기 백업 절차에 따라 백업 및 저장됩니다.

6.3.2 공개키 및 개인키의 사용 기간

인증서는 만료 또는 폐지될 때까지 유효합니다. 개인키가 암호 해독에 사용되는 경우와 공개키가 서명 확인에 사용되는 경우를 제외하고 키 쌍의 유효 기간은 관련 인증서의 유효 기간과 동일합니다. 본 CPS 의 유효일 또는 이후에 발행된 CrossCert 인증서의 최대 유효 기간은 아래 표 18 에 나와 있습니다.

또한 CrossCert CA 는 종속 CA 가 발행한 인증서의 만료일이 상위 CA 가 발행한 인증서의 만료일보다 늦어지는 사태를 방지하기 위해 CA 인증서 만료 전 해당일에 인증서 신규 발행을 중단합니다.

인증서 발행자	*클래스 1*	*클래스 2*	*클래스 3*
CrossCert 에 해당 없음			
CrossCert 에 해당 없음			
자체 서명 발행 루트 CA	해당 없음	해당 없음	최대 10 년까지
CrossCert 에 해당 없음			
종속 CA 에 대한 CA	최대 5 년까지	최대 5 년까지	최대 5 년까지
최종 사용 가입자에 대한 CA	최대 2 년까지	보통 최대 2 년이나, 아래 기술된 조건 하에서는 최대 5 년까지 가능	보통 최대 2 년이나, 아래 기술된 조건 하에서는 최대 5 년까지 가능

서식 있음

표 18 – 인증서 유효 기간

이 단원에 언급된 경우를 제외하고 CrossCert 서브도메인 참가자들은 키 쌍 사용 기한이 지나면 키 쌍의 사용을 중지해야 합니다.

CA 가 최종 사용 가입자에게 발행한 인증서의 경우 다음과 같은 조건 하에서는 유효 기간이 최소 2 년에서 최대 5 년이 됩니다.

- 개인 인증서인 경우
- 가입자의 키 쌍이 스마트 카드와 같은 하드웨어 토큰에 저장된 경우
- 가입자가 CPS 3.1.9 항에 따라 매년 재인증 절차를 거쳐야 하는 경우
- 가입자가 인증서 내의 공개키에 대응하는 개인키를 소유하고 있음을 매년 증명해야 하는 경우
- 가입자가 CPS 3.1.9 항에 따라 재인증 절차를 완료하지 못하거나 공개키에 대응하는 개인키의 소유를 증명하지 못할 경우 CA 는 자동으로 가입자의 인증서를 폐지합니다.

또한 CrossCert 는 VeriSign Trust Network 를 구성하는 몇 개의 레거시 자체 서명 발행 루트 CA 를 운영합니다. 이러한 CA 가 발행하는 사용자 등록 인증서는 표 18 에 나와 있는 사용자 등록 인증서에 대한 CA 요구 사항을 충족시킵니다.

CrossCert 에서 제공하지 않음		

서식 있음

6.4 활성 데이터

6.4.1 활성 데이터 생성 및 설치

CrossCert CA 개인키가 포함된 토큰 보호에 사용되는 활성 데이터(Secret Share)는 CPS 6.2.2 항 및 키 형식 참조 가이드(Key Ceremony Reference Guide)의 요구 사항에 따라 생성됩니다. Secret Share 의 생성 및 배포는 로그에 기록됩니다.

CrossCert RA 는 개인키를 보호할 강력한 패스워드를 선택해야 합니다. CrossCert 의 패스워드 선택 지침이 요구하는 패스워드 조건은 다음과 같습니다.

- 사용자가 직접 생성한 것
- 8 문자 이상
- 하나 이상의 알파벳 및 숫자 포함
- 하나 이상의 소문자 포함
- 여러 개의 동일 문자를 사용하지 말 것
- 운영자의 프로파일 이름과 동일하지 않을 것
- 사용자 프로파일 이름의 긴 하위 문자열을 포함하지 말 것

CrossCert 는 Managed PKI 관리자, RA, 최종 사용 가입자에게 위의 조건에 부합하는 패스워드를 선택하도록 강력히 권합니다. 두 가지 요소로 구성된 인증 메커니즘(토큰과 암호문, 생체인식과 토큰, 생체인식과 암호문 등)을 사용하십시오.

6.4.2 활성화 데이터 보호

CrossCert Shareholder 는 Secret Share 를 보호해야 하며 Shareholder 의 의무를 인정하는 계약서에 서명해야 합니다.

CrossCert RA 는 패스워드 보호와 해당 브라우저의 "보안 높음" 옵션을 사용하여 자신의 관리자/RA 개인키를 암호화된 형태로 저장해야 합니다.

CrossCert 는 클라이언트 관리자, RA, 최종 사용 가입자에게 개인키를 암호화된 형태로 저장하고 하드웨어 토큰 및 암호문을 사용하여 보호할 것을 권합니다. 두 가지 요소로 구성된 인증 메커니즘(토큰과 암호문, 생체인식과 토큰, 생체인식과 암호문 등)을 사용하십시오.

6.4.3 활성 데이터의 다른 측면

CPS 6.4.1 및 6.4.2 항 참조

6.5 컴퓨터 보안 통제

CrossCert 는 CrossCert 보안 및 감사 요구 사항 가이드(Security and Audit Requirements Guide)의 요건에 맞는 믿을 수 있는 시스템을 사용하여 CA 및 RA 기능을 수행합니다. Managed PKI 고객은 기업 보안 가이드(Enterprise Security Guide) 요건에 맞는 확실한 시스템을 사용해야 합니다.

6.5.1 컴퓨터 보안의 기술적 요구 사항

CA 소프트웨어 및 데이터 파일이 있는 시스템은 무단 액세스로부터 안전한 믿을 수 있는 시스템입니다. CrossCert 는 생산 서버에 대한 액세스를 업무상 타당한 이유가 있는 개인으로 제한하기 때문에 일반 애플리케이션 사용자들은 생산 서버 계정이 없습니다.

CrossCert 의 생산 네트워크는 다른 구성 요소와 논리적으로 구분됩니다. 따라서 정의된 애플리케이션 프로세스를 통하지 않고는 네트워크를 액세스할 수 없습니다. CrossCert 는 방화벽을 사용하여 내외부 무단 침입으로부터 생산 네트워크를 보호하며 생산 시스템에 액세스할 수 있는 네트워크 작업 속성과 소스를 제한합니다.

사용자는 최소 문자 길이 이상의 알파벳과 특별 문자로 조합된 패스워드를 사용해야 하며, 정기적으로 패스워드를 변경해야 합니다.

CrossCert 저장소를 지원하는 CrossCert 데이터베이스에 대한 직접 액세스는 타당한 업무상의 이유가 있는 CrossCert 의 운영 그룹 내의 권한있는 자로 제한됩니다.

6.5.2 컴퓨터 보안 등급

CrossCert 에서 제공하지 않음

6.6 유효 주기 기술 제어

6.6.1 시스템 개발 제어

CrossCert 는 CrossCert 시스템 개발 및 변경 관리 표준에 따라 애플리케이션을 개발 및 구현하며, Managed PKI 고객에게 RA 나 특정 CA 기능을 수행하는데 필요한 소프트웨어를 제공합니다. 이러한 소프트웨어는 CrossCert 시스템 개발 표준에 따라 개발됩니다.

VeriSign 에서 개발한 소프트웨어를 처음 설치하면 VeriSign 이나 CrossCert 에서 개발한 시스템에 설치된 소프트웨어가 설치 전에 수정이 되었는지 또는 사용 목적에 적합한 버전인지 등을 확인할 수 있습니다.

6.6.2 보안 관리 제어

CrossCert 는 CA 시스템의 구성을 제어 및 감시하는 메커니즘이나 정책을 설치합니다. CrossCert 는 모든 소프트웨어 패키지 및 CrossCert 소프트웨어 업데이트에 대한 해쉬를 작성하는데, 이 해쉬는 소프트웨어의 무결성 확인에 사용됩니다. 설치 시 및 이후 정기적으로 CrossCert 는 CA 시스템의 무결성을 검증합니다.

6.6.3 유효 주기 보안 등급

해당 조항 없음.

6.7 네트워크 보안 제어

CrossCert 는 보안 및 감사 요구 사항 가이드(Security and Audit Requirements Guide)에 따라 보안된 네트워크를 통해 CA 및 RA 기능을 수행하여 무단 액세스 및 기타 악의적 활동을 방지합니다. CrossCert 는 암호와 디지털 서명을 사용하여 기밀 정보의 전송을 보호합니다.

6.8 암호화 모듈 엔지니어링 제어

CrossCert 및 VeriSign 에서 사용되는 암호화 모듈은 CPS 6.2.1 항에 지정된 요건을 준수합니다.

7. 인증서 및 CRL 프로파일

7.1 인증서 프로파일

CPS § 7.1 에는 본 CPS 에 따라 발행된 VTN 인증서의 CrossCert 인증서 프로파일 및 인증서 컨텐트 요구 사항이 정의되어 있습니다.

WTLS 인증서를 제외하고, CrossCert 인증서는 (가) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 및 (나) RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999 ("RFC 2459")를 준수합니다.

WTLS 인증서는 Wireless Application Protocol: WAP Certificate and CRL Profiles Specification, Proposed Version dated March 9, 2000 을 준수합니다. CrossCert 는 상기 프로파일이 발행된 후 1 년 이내에 WAP 포럼의 승인을 받을 경우 해당 사양의 최종 버전을 준수하게 됩니다.

아래 표 20 에는 CrossCert X.509 및 WTLS 인증서의 기본 X.509 버전 1 필드와 규정 값 또는 값 제약 조건이 나와 있습니다.

필드	값 또는 값 제약 조건
버전	CPS §7.1.1 을 참조하십시오. WTLS 인증서에는 해당 사항 없습니다.
일련 번호	발행자 DN 별 고유 값입니다.
서명 알고리즘	인증서 서명에 사용된 알고리즘의 이름입니다(CPS § 7.1.3 참조).
발행자 DN	CPS § 7.1.4 를 참조하십시오.
유효 시작일	협정된 기준 세계시입니다. 미해군 관측소의 표준 시간에 맞추며 RFC 2459 에 따라 암호화됩니다.
유효 만료일	협정된 기준 세계시입니다. 미해군 관측소의 표준 시간에 맞추며 RFC 2459 에 따라 암호화됩니다. 유효 기간은 CPS § 6.3.2 에 지정된 제약 조건에 따라 설정됩니다.
피발행자 DN	CPS § 7.1.4 를 참조하십시오.
피발행자 공개키	CPS § 7.1.3 에 지정된 알고리즘과 CPS § 6.1.5 에 지정된 키 길이를 사용하여 RFC 2459 에 따라 암호화됩니다.
서명	RFC 2459 에 따라 생성 및 암호화됩니다.

서식 있음

표 20 – 인증서 프로파일 기본 필드

7.1.1 버전 번호

CrossCert CA 및 사용자 등록 인증서는 X.509 버전 3 인증서입니다. 단, 다음은 예외입니다.

- VeriSign PCA 및 기타 VeriSign 루트 CA 를 포함하는 VeriSign 루트 CA 인증서는 X.509 버전 1 인증서입니다.
- 일부 시큐어 서버 인증서는 X.509 버전 1 인증서이며, 여기서 특정 웹 서버는 X.509 버전 3 인증서 사용을 지원하지 않습니다.
- 다음과 같은 일부 레거시 VeriSign 발행 CA 인증서는 X.509 버전 1 인증서입니다.

- CrossCert 무선 PKI 서비스를 지원하기 위해 WAP 형식으로 발행된 VeriSign G2 PCA 인증서
- WAP 형식으로 발행된 WTLS 사용자 및 WTLS 서버 인증서

7.1.2 인증서 확장

X.509 버전 3 인증서가 사용되는 경우, CrossCert 는 CPS §§ 7.1.2.1-7.1.2.8 에서 요구하는 확장을 인증서에 적용합니다. VTN CP 와 본 CPS 를 준수하는 한 개인 확장도 허용됩니다.

CrossCert 는 현재 WTLS 인증서용 확장을 사용하지 않습니다.

7.1.2.1 키 용도

X.509 버전 3 인증서가 사용되는 경우, CrossCert 는 CPS § 6.1.9 에 따라 KeyUsage 확장을 적용합니다. 이 확장의 임계 필드는 FALSE 로 설정됩니다.

7.1.2.2 인증서 정책 확장

CrossCert X.509 버전 3 사용자 등록 인증서는 인증 정책 확장을 사용합니다. 인증 정책 확장에는 CP § 7.1.6 에 따른 VTN CP 용 해당 객체 식별자와 CP § 7.1.8 에 지정된 정책 식별자가 포함됩니다. 이 확장의 임계 필드는 FALSE 로 설정됩니다.

7.1.2.3 피발행자 대체 이름

해당 조항 없음

7.1.2.4 기본 제약 조건

CrossCert 는 피발행자 유형이 CA 로 설정된 BasicConstraints 확장을 X.509 버전 3 CA 인증서에 적용합니다. 사용자 등록 인증서에는 또한 피발행자 유형이 최종 개체와 동일한 BasicConstraints 확장도 적용됩니다. CrossCert 클래스 3 Managed PKI Authentication Services Bureau CA 를 제외하고 기본 제약 조건 확장의 임계는 일반적으로 FALSE 로 설정됩니다. 이 확장의 임계는 차후 다른 인증서에서 TRUE 로 설정할 수도 있습니다.

즉 BasicConstraints 확장의 "pathLenConstraint" 필드가 인증 경로에서 이 인증서 뒤에 이어지는 CA 인증서의 최대 수로 설정되도록 발행된 CrossCert X.509 버전 3 CA 인증서에서는 이 값을 TRUE 로 설정할 수 있습니다. 또한 Managed PKI 고객의 온라인 CA 와 CrossCert CA 에 발행된 CA 인증서에서도 이 값을 TRUE 로 설정할 수 있으며 여기서 발행되는 사용자 등록 인증서에서 "pathLenConstraint" 필드는 "0"으로 설정되어 인증 경로에서 사용자 등록 인증서만 뒤에 이어집니다.

7.1.2.5 확장 키 용도

CrossCert 는 아래 표 21 에 나열된 특정 유형의 CrossCert X.509 버전 3 인증서를 위해 ExtendedKeyUsage 확장을 사용합니다. 다른 유형의 인증서에서 CrossCert 는 확장 키 용도 확장을 사용하지 않습니다.

인증서 유형	*인증서 유형*
인증 기관(CA)	클래스 3 국제 서버 CA
OCSP 응답자	클래스 1-3 공식 기본 OCSP 응답자 시큐어 서버 OCSP 응답자
클래스 3 웹 서버 인증서	시큐어 서버 ID 글로벌 서버 ID

표 21 – 확장 키 용도 확장을 사용하는 인증서

서식 있음

CrossCert 는 아래 표 22 에 따라 인증서에 ExtendedKeyUsage 확장을 적용합니다.

		클래스 3 국제 서버 CA	*OCSP 응답자*	*시큐어 서버 ID*	*글로벌 서버 ID*
임계		FALSE	FALSE	FALSE	FALSE
0	ServerAuth	해제	해제	설정	해제
1	ClientAuth	해제	설정	설정	해제
2	CodeSigning	해제	해제	해제	해제
3	EmailProtection	해제	설정	해제	해제
4	ipsecEndSystem	해제	해제	해제	해제
5	ipsecTunnel	해제	해제	해제	해제
6	ipsecUser	해제	해제	해제	해제
7	TimeStamping	해제	해제	해제	해제
8	OCSP 서명	해제	설정	해제	해제
-	Microsoft SGC(Server Gated Crypto) OID: 1.3.6.1.4.1.311.10.3.3	해제	해제	해제	설정
-	Netscape SGC - OID: 2.16.840.1.113730.4.1	설정	해제	해제	설정
-	TBD – OID: 2.16.840.1.113733.1.8.1	설정	해제	해제	해제

서식 있음

서식 있음

서식 있음

서식 있음

서식 있음

서식 있음

서식 있음

서식 있음

서식 있음

서식 있음

서식 있음

서식 있음

서식 있음

표 22 – ExtendedKeyUsage 확장 설정

서식 있음

7.1.2.6 CRL 배포 지점

CrossCert X.509 버전 3 시큐어 서버 및 클래스 1 개인 사용자 등록 인증서는 신뢰 당사자가 CA 인증서의 상태를 점검하기 위해 CRL 을 획득할 수 있는 위치의 URL 이 포함된 cRLDistributionPoints 확장을 사용합니다. 이 확장의 임계 필드는 FALSE 로 설정됩니다. CRL 배포 지점은 차후 다른 CrossCert CA 에서도 지원됩니다.

7.1.2.7 인증 기관 키 식별자

VeriSign 은 VeriSign 상용 소프트웨어 게시자 CA 가 발행한 X.509 버전 3 사용자 등록 인증서의 인증 기관 키 식별자 확장을 적용합니다. 인증 기관 키 식별자는 인증서 발행 CA 공개키의 160 비트 SHA-1 해쉬로 구성되어 있습니다. 이 확장의 임계 필드는 FALSE 로 설정됩니다. 인증 기관 키 식별자 확장은 차후 다른 VeriSign CA 에 대해서도 지원될 수 있습니다.

7.1.2.8 피발행자 키 식별자

CrossCert 가 X.509 버전 3 VTN 인증서에 subjectKeyIdentifier 확장을 적용하는 경우, 인증서 피발행자의 공개키를 기반으로 하는 keyIdentifier 가 생성됩니다. 이 확장을 사용할 때 확장의 임계 필드는 FALSE 로 설정됩니다.

7.1.3 알고리즘 객체 식별자

CrossCert X.509 인증서는 RFC 2459 에 따라 sha1RSA(OID: 1.2.840.113549.1.1.5) 또는 md5RSA(OID: 1.2.840.113549.1.1.4)를 사용하여 서명이 입력됩니다. VeriSign 은 일부 레거시 CA 및 사용자 등록 인증서를 md2RSA(OID: 1.2.840.113549.1.1.2)를 사용하여 서명했습니다

CrossCert WTLS 인증서는 sha1RSA(OID: 1.2.840.113549.1.1.5) 또는 ecdsa-SHA1(OID: 1.2.840.10045.1)을 사용하여 서명이 입력됩니다.

7.1.4 이름 형식

CPS § 3.1.1 에 따라 CrossCert 는 VTN 인증서에 발행자 및 피발행자 식별명(DN)을 적용합니다.

또한 CrossCert 의 사용자 등록 인증서에는 추가 부서 필드가 포함되어 있습니다. 이 필드에는 인증서의 사용 조건이 해당 신뢰 당사자 계약에 대한 포인터인 URL 에 규정되어 있다는 통지가 들어 있습니다. 단, 인증서 내의 공간이나 서식화 또는 상호 운용성 제한 등으로 인해 이러한 부서를 해당 인증서가 의도하는 목적에 사용할 수 없는 경우에는 상기 요구 사항의 예외가 허용됩니다.

7.1.5 이름 제약 조건

해당 조항 없음

7.1.6 인증서 정책 객체 식별자

인증서 정책 확장이 사용되는 경우, 인증서에는 CPS § 1.2 의 규정과 같이 해당 인증서 클래스에 적합한 인증 정책의 객체 식별자가 포함됩니다. 인증 정책 확장이 포함된 VTN CP 가 게시되기 전에 발행된 레거시 인증서의 경우 VeriSign CPS 를 참조하십시오.

7.1.7 정책 제약 조건 확장의 용도

해당 조항 없음

7.1.8 정책 한정자 구문 및 의미 규칙

CrossCert 는 X.509 버전 3 VTN 인증서에 CertificatePolicies 확장 내의 정책 한정자를 적용합니다. 일반적으로 이러한 인증서에는 해당 신뢰 당사자 계약 또는 VeriSign CPS 를 가리키는 CPS 포인터 한정자가 포함되어 있습니다. 또한 일부 인증서에는 해당 신뢰 당사자 계약을 가리키는 사용자 고지 한정자가 포함됩니다.

7.1.9 임계 인증서 정책 확장을 위한 의미 규칙 처리

해당 조항 없음

7.2 CRL 프로파일

CrossCert 는 RFC 2459 를 준수하는 CRL 을 발행합니다. CrossCert CRL 에는 최소한 아래 표 23 에 지정된 기본 필드와 내용이 포함됩니다.

필드	*값 또는 값 제약 조건*
버전	CPS §7.2.1 을 참조하십시오.
서명 알고리즘	CRL 서명에 사용되는 알고리즘입니다. VeriSign CRL 은 RFC 2459 에 따라 md5RSA(OID: 1.2.840.113549.1.1.4) 또는 md2RSA(OID: 1.2.840.113549.1.1.2)를 사용하여 서명을 입력했습니다.
발행자	CRL 을 서명 및 발행한 기관입니다. CRL 발행자 이름은 CPS § 7.1.4 에 지정된 발행자 식별명(DN)을 따릅니다.
발효일	CRL 의 발행일입니다. CrossCert CRL 은 발행 즉시 효력이 발생합니다.
다음 업데이트	다음 CRL 이 발행될 날짜입니다. CrossCert CRL 의 다음 업데이트 날짜는 VeriSign PCA 의 경우 발효일로부터 3 개월, 기타 CrossCert CA 의 경우 발효일로부터 10 일로 설정됩니다. CRL 의 발행 주기는 CPS § 4.4.9 의 요구사항을 따릅니다.
폐지된 인증서	폐지된 인증서의 일련 번호와 폐지 날짜를 포함하는 폐지 인증서 목록을 작성합니다.

표 23 – CRL 프로파일 기본 필드

서식 있음

7.2.1 버전 번호

CrossCert 는 현재 X.509 버전 1 CRL 을 발행합니다.

7.2.2 CRL 및 CRL 엔트리 확장

해당 조항 없음

8. 사양 관리

8.1 사양 변경 절차

본 CPS에 대한 개정은 VeriSign 업무 개발 그룹의 승인을 받아 CrossCert가 수행해야 합니다. 개정 작업은 CPS의 수정 양식을 포함하는 문서나 업데이트 형식이어야 합니다. 개정된 버전이나 업데이트는 https://www.crosscert.com/Repository/updates에 위치한 CrossCert 저장소의 업무 업데이트 및 통지 섹션으로 연결됩니다. 업데이트는 CPS 참조 버전의 모든 지정된 조항이나 상충되는 조항에 우선합니다.

8.1.1 통보 없이 변경 가능한 항목

CrossCert 는 인쇄 오류 수정, URL 변경, 연락처 정보 변경 등을 포함하여(이에 제한되지는 않음) 중요하지 않은 개정 사항에 대해 통보 없이 CPS 를 개정할 권리가 있습니다. 개정 사항이 중요한 것인지 여부에 대한 판단은 CrossCert 의 단독 재량에 따릅니다.

8.1.2 통보 후 변경 가능한 항목

CrossCert 는 본 CPS § 8.1.2 에 따라 CPS 에 대해 중요 사항을 개정할 수 있습니다.

8.1.2.1 항목 목록

중요 개정 사항은 CPS § 8.1.1 에 따라 CrossCert 가 중요한 것으로 간주하는 사항입니다.

8.1.2.2 통보 메커니즘

CrossCert의 업무 개발 그룹은 https://www.crosscert.com/Repository/updates에 위치한 CrossCert 저장소의 업무 업데이트 및 통지 섹션에 제안된 CPS 개정안을 게시합니다. CrossCert는 다른 CrossCert 하위 도메인 참여자의 CPS 개정 요청도 수신합니다. CrossCert는 이러한 개정을 타당한 것으로 간주하여 개정을 제안할 경우 이 섹션에 따라 이러한 개정을 통지해야 합니다.

이에 반하는 CPS 의 규정에도 불구하고 CPS 에 대한 중대한 개정이 VTN 이나 CrossCert 의 하위 도메인 또는 VTN 일부의 보안이 침해되는 것을 예방하거나 즉시 중지시키는 데 필요하다고 판단될 경우, CrossCert 는 CrossCert 저장소에 이를 게시하여 개정을 수행할 권리가 있습니다. 이러한 개정은 게시하는 즉시 효력을 발생합니다.

8.1.2.3 의견 개진 기간

CPS § 8.1.2.2 에 지정된 경우를 제외하고, CPS 의 중요 개정에 대한 의견 개진은 CrossCert 저장소에 게시된 날로부터 15 일 동안 가능합니다. 모든 CrossCert 하위 도메인 참여자는 의견 개진 기간이 끝날 때까지 CrossCert 의 업무 개발 그룹에 의견을 개진할 권리가 있습니다.

8.1.2.4 의견 처리 메커니즘

CrossCert 의 업무 개발 그룹은 제안된 개정안에 대한 모든 의견을 고려합니다. CrossCert 는 (가) 개정 없이 제안된 개정안이 효력을 발생하도록 하거나, (나) CPS § 8.1.2.2 에 따라 제안된 개정안을 수정하여 새로운 개정 사항으로 다시 게시하거나, (다) 제안된 개정안을 철회합니다. CrossCert 는 CrossCert 저장소의 업무 업데이트 및 통지 섹션에 게시하여 제안된 개정안을 철회할 권리가 있습니다. 제안된 개정안은 개정 또는 철회되지 않을 경우 CPS § 8.1.2.3 에 따라 의견 개진 기간이 만료됨과 동시에 효력을 발생합니다.

8.1.3 인증 정책 OID 또는 CPS 포인터가 변경되어야 하는 변경 사항

CP § 8.1.3 *을 참조하십시오.*

8.2 게시 및 통보 정책

8.2.1 CPS 에 게시되지 않는 항목

VeriSign 및 회원사가 기밀로 간주하는 보안 문서는 일반에 공개되지 않습니다. 기밀 보안 문서에는 CPS § 1.1(a)의 표 1 에서 일반에 공개되지 않는 문서로 지정된 문서가 포함됩니다.

8.2.2 CP 배포

https://www.crosscert.com/CPS의 CrossCert 저장소 내에 전자 형태로 게시되는 본 CPS는 CrossCert 저장소에서 Word, Adobe Acrobat pdf 및 HTML 형식으로 제공됩니다. **CPS-requests@crosscert.com**으로 요청을 보낼 경우 CrossCert는 Adobe Acrobat pdf 또는 Word 형식의 CPS를 제공합니다. 또한 CrossCert., [회원사 주소] 수신: CPS로 요청을 보내면 CrossCert의 업무 개발 그룹이 CPS 인쇄본을 제공합니다.

8.3 CPS 승인 절차

해당 없음

두문자어 및 정의

두문자어 표

두문자어	*용어*
ANSI	American National Standards Institute(미국 표준 협회)
ASB	Authentication Service Bureau
B2B	Business-to-business(기업간)

두문자어	용어
BXA	United States Bureau of Export Administration(수출 관리국) - 미 상무성
CA	Certification Authority(인증 기관)
CP	Certificate Policy(인증 정책)
CPS	Certification Practice Statement(인증업무준칙)
CRL	Certificate Revocation List(인증서 폐지 목록)
EAL	Evaluation assurance level(평가 보증 수준) - 국제 공통 평가 기준(Common Criteria)을 따름
EDI	Electronic Data Interchange(전자 문서 교환)
EDIFACT	EDI for Administration, Commerce, and Transport(행정, 상업 및 운송에 관한 EDI) - UN 유럽 경제 위원회가 제정한 국제 표준
FIPS	Federal Information Processing Standards(미 연방 정보처리 표준)
ICC	International Chamber of Commerce(국제 상공 회의소)
KRB	Key Recovery Block(키 복구 블록)
LSVA	Logical security vulnerability assessment(논리적 보안 취약점 평가)
OCSP	Online Certificate Status Protocol(온라인 인증 상태 프로토콜)
OFX	Open Financial Exchange(개방형 금융 교환)
PCA	Primary Certification Authority(기본 인증 기관)
PIN	Personal identification number(개인 식별 번호)
PKCS	Public-Key Cryptography Standard(공개키 암호화 표준)
PKI	Public Key Infrastructure(공개키기반구조)
PMA	Policy Management Authority(정책 관리 기관)
RA	Registration Authority(등록 기관)
RFC	Request for comment
SAS	Statement on Auditing Standards(감사 표준 기준서) - 미국 공인회계사 협회 공표
S/MIME	Secure multipurpose Internet mail extensions(보안 다목적 인터넷 메일 확장)
SSL	Secure Sockets Layer(보안 소켓 레이어)
VTN	VeriSign Trust Network
WAP	Wireless Application Protocol(무선 애플리케이션 프로토콜)
WTLS	Wireless Transport Layer Security(무선 전송 레이어 보안)

정의

용어	정의
관리 인증 기관 (관리 CA)	CrossCert RA, Managed PKI 고객 직원(Managed PKI 관리자), 회원 관리자 및 자동 관리(AA) 서버에 대해 인증서를 발행하는 CrossCert CA 의 유형입니다.

용어	정의
관리자	프로세싱 센터, 서비스 센터 및 Managed PKI 고객 내의 승인된 사람으로서 확인을 비롯한 다른 CA 또는 RA 기능을 수행합니다.
관리자 인증서	관리자에게 발행된 인증서로서 CA 또는 RA 기능을 수행하는 데만 사용됩니다.
회원사	승인된 제 3 의 업체로서, 특정 업계(예: 기술, 통신 또는 금융 서비스)에서 VeriSign 과 계약을 체결하여 특정 지역 내의 VTN 배포 및 서비스 채널 역할을 담당하는 업체입니다.
개인 회원	(i) 해당 조직의 임원, 직원, 제휴 업체, 계약 직원, 인턴 또는 기타 관련자 (ii) 이해 관계에 있는 VeriSign 등록 커뮤니티의 일원 (iii) 해당 당사자에 대해 적절한 신원 증명을 제공할 수 있는 조직과 관계를 유지하고 있는 개인 등으로서 특정 조직과 관련된 자연인입니다.
자동 관리	등록 정보가 데이터베이스에 보관된 정보와 일치하는 경우 인증 신청이 자동으로 승인되는 절차입니다.
자동 관리 소프트웨어 모듈(AA 모듈)	VeriSign 이 제공하는 소프트웨어로서 자동 관리를 수행합니다.
인증서	최소한 이름 명시 또는 CA 확인, 가입자 확인, 가입자의 공개키 포함, 인증서의 유효 기간 확인, 인증서 일련 번호 포함, CA 의 전자 서명 포함 등을 수행하는 메시지입니다.
인증 신청자	CA 의 인증서 발행을 요청하는 개인 또는 단체입니다.
인증 신청서	CA 에게 인증서 발행을 요청하는 인증 신청자(또는 인증 신청자가 승인한 대리인)의 요청서입니다.
인증 체인	사용자 등록 인증서와 CA 인증서를 포함하며 마지막에 루트 인증서로 끝나는 인증서 목록입니다.
인증서 관리 감독 목표	준수성 감사에 통과하기 위해 충족해야 하는 기준입니다.
인증 정책(CP)	"VeriSign Trust Network 인증 정책"이란 이름의 문서로서 VTN 을 규정하는 기본 준칙입니다.
인증서 폐지 목록(CRL)	만료일 이전에 폐지된 인증서의 목록으로서 정기적으로 또는 임시로 발행되며 CA 의 전자 서명이 포함됩니다. 이 목록에는 일반적으로 CRL 발행자의 이름, 발행일, 다음 CRL 발행 예정일, 폐지된 인증서의 일련 번호, 구체적인 폐지 시간 및 사유가 기재됩니다.
인증서 서명 요청	인증서 발행 요청을 담고 있는 메시지입니다.
인증 기관(CA)	VTN 인증서를 발행, 관리, 폐지 및 갱신할 수 있는 공인 기관입니다.
인증업무준칙(CPS)	VeriSign 또는 회원사가 인증 신청을 승인하거나 거부할 때 및 인증서를 발행, 관리 및 폐지할 때 사용하는 업무 준칙으로서

용어	*정의*
	해당 Managed PKI 고객은 이 업무 준칙을 준수해야 합니다. 본 CPS 에서 "CPS"는 이 문서를 의미합니다.
암호	인증서 등록 시 인증 신청자가 선택한 비밀 문구입니다. 인증서가 발행되면 인증 신청자는 가입자가 되며 CA 또는 RA 는 가입자가 자신의 인증서를 폐지하거나 갱신하려고 할 때 이 암호를 사용하여 가입자를 인증할 수 있습니다.
클래스	CP 에 정의된 각 보증 수준입니다. CP § 1.1.1 을 참조하십시오. 각 수준의 차이는 CPS § 1.1.1 에 요약되어 있습니다.
Client OnSite 고객	Managed PKI 고객을 참조하십시오.
Client OnSite Lite 고객	Managed PKI Lite 고객을 참조하십시오.
클라이언트 서비스 센터	소비자 또는 기업에 클라이언트 인증서를 제공하는 회원사 서비스 센터입니다.
준수성 감사	프로세싱 센터, 서비스 센터 또는 Managed PKI 고객이 해당 VTN 표준에 대한 준수성을 확인하기 위해 받는 정기 감사입니다.
손상	기밀 정보에 대한 무단 공개나 통제력 상실이 발생할 수 있는 보안 정책의 위반(또는 위반 혐의)입니다. 개인키의 경우, 손상이란 개인키의 손실, 도난, 공개, 수정, 무단 사용 또는 기타 보안 손상을 의미합니다.
기밀/개인 정보	CPS § 2.8.1 에 따라 기밀 또는 개인 정보로 취급되어야 하는 정보입니다.
소비자(소비자 서비스 센터의 경우)	인증 신청자에게 클라이언트 리테일 인증서를 제공하는 회원사의 업종입니다.
CRL 사용 계약서	CRL 또는 해당 정보의 사용에 대한 조건을 규정하는 계약서입니다.
고객	Managed PKI 고객 또는 ASB 고객인 조직입니다.
디지털 영수증	CrossCert 가 제공하고 Time-Stamping 기관(TSA)의 전자 서명이 포함된 VeriSign 디지털 공증 서비스와 관련하여 작성된 데이터 객체로서, 특정 시점에 해당 문서나 데이터가 존재했음을 보여주는 일련의 문서 또는 데이터 및 time-stamp 가 들어 있습니다.
전자 데이터 교환(EDI)	해당 표준에 따른 구매 주문, 송장 및 지불 통지 등의 컴퓨터간 기업 거래입니다.
전자 데이터 교환 인증서(EDI 인증서)	전자 데이터 교환 메시지의 전자 서명과 EDI 메시지의 암호화를 구현하는 클래스 3 단체 인증서입니다.
기업(기업 서비스 센터의 경우)	Managed PKI 고객에게 Managed PKI 서비스를 제공하는 회원사의 업종입니다.

용어	정의
기업 로밍 서버	CrossCert 가 제공하는 VeriSign 로밍 서비스와 관련하여 사용되는 Managed PKI 고객의 사이트에 설치된 서버로서, 로밍 가입자의 암호화된 개인키와 이런 개인키를 암호화 및 해독하는 데 사용되는 대칭 키 부분을 보관합니다.
Enterprise Security Guide(기업 보안 가이드)	Managed PKI 고객에 대한 보안 요구 사항과 업무 준칙을 규정한 문서입니다.
특별 감사/조사	해당 기관이 VTN 표준을 준수하지 않았거나, 해당 기관과 관련하여 사고나 손상이 발생했거나, 해당 기관이 VTN 보안에 실제적 또는 잠재적 위협을 제공한다고 판단될 경우 VeriSign 이 실시하는 감사 또는 조사입니다.
글로벌 서버 ID	해당 수출 관계법을 준수하는 강력한 암호화 보호를 통해 암호화된 웹 브라우저와 웹 서버 간의 SSL 세션을 지원하는 데 사용되는 클래스 3 단체 인증서입니다.
Global Server OnSite	SSL Premium Edition 용 Managed PKI 를 참조하십시오.
Global Server OnSite 고객	SSL Premium Edition 고객용 Managed PKI 를 참조하십시오.
Go Secure!	Managed PKI 서비스를 기반으로 구축된 플러그 앤 플레이 서비스로서 전자상거래 애플리케이션을 가속화하기 위해 개발되었습니다.
기반구조 인증 기관(기반구조 CA)	특정 CrossCert 서비스를 지원하는 CrossCert 기반구조의 구성 요소에 인증서를 발행하는 CrossCert CA 의 한 유형입니다. 기반구조 CA 는 CA, RA 또는 사용자 등록 인증서를 발행하지 않습니다.
지적 재산권	모든 저작권, 특허, 영업 비밀, 상표 및 기타 지적 재산권과 관련된 권리입니다.
Intermediate Certification Authority(Intermediate CA)	인증서 체인에서 루트 CA 의 인증서와 사용자 등록 인증서를 발행하는 인증 기관의 인증서 사이에 존재하는 인증서의 인증 기관입니다.
Key Ceremony Reference Guide(키 형식 참조 가이드)	키 생성 형식 요구 사항과 업무 준칙을 설명하는 문서입니다.
키 생성 형식	CA 또는 RA 의 키 쌍이 생성되고, 개인키가 암호화 모듈로 전송되며, 개인키가 백업되거나 공개키가 인증되는 절차입니다.
Key Manager 관리자	Managed PKI Key Manager 를 사용하여 Managed PKI 고객의 키 생성 및 복구 기능을 수행하는 관리자입니다.
키 복구 블록(KRB)	암호화 키를 사용하여 암호화되는 가입자의 개인키가 포함된 데이터 구조입니다. KRB 는 Managed PKI Key Manager

용어	정의
	소프트웨어를 사용하여 생성됩니다.
키 복구 서비스	CrossCert 가 제공하는 VeriSign 서비스로서, Managed PKI 고객이 Managed PKI Key Manager 를 사용하여 가입자의 개인키를 복구할 때 키 복구 블록을 복구하는 데 필요한 암호화 키를 제공합니다.
Managed PKI	CrossCert 가 제공하는 VeriSign 의 완전 통합 Managed PKI 서비스로서, CrossCert 의 기업 고객은 이 서비스를 사용하여 직원, 제휴 업체, 공급업체 및 고객 등의 개인은 물론 서버, 라우터 및 방화벽 등의 장치에 인증서를 배포할 수 있습니다. Managed PKI 를 사용하여 기업은 메시지, 인트라넷, 엑스트라넷, VPN, 전자상거래 애플리케이션 등에 보안을 설정할 수 있습니다.
Managed PKI 관리자	Managed PKI 고객에 대한 인증 확인 또는 기타 RA 기능을 수행하는 관리자입니다.
Managed PKI Administrator Handbook(Managed PKI 관리자 핸드북)	Managed PKI 고객의 운영 요구 사항과 업무 준칙을 규정하는 CrossCert 문서입니다.
Managed PKI 계약서	이 계약서를 통해 조직은 Managed PKI 고객이 되고 본 CPS 를 준수하는 데 동의하게 됩니다.
Managed PKI 인증서	Managed PKI 고객이 인증 신청을 승인한 인증서입니다.
Managed PKI 제어 센터	Managed PKI 관리자가 인증 신청의 수동 인증을 수행할 수 있도록 하는 웹 기반 인터페이스입니다.
Managed PKI 고객	CrossCert 에서 Managed PKI 서비스를 취득한 조직으로서, 클라이언트 인증서를 발행하는 VTN 내의 CA 가 되는 조직입니다. Managed PKI 고객은 발행, 관리 및 폐지의 백엔드 기능을 CrossCert 에 아웃소싱하지만 인증 신청을 승인 또는 거부하고 인증서를 폐지 및 갱신하는 RA 기능은 보유합니다.
Managed PKI Key Manager	특별 Managed PKI 계약 하에서 키 복구를 구현하기로 선택한 Managed PKI 고객의 키 복구 솔루션입니다.
Managed PKI Key Management Service Administrator's Guide(Managed PKI 키 관리 서비스 관리자 가이드)	Managed PKI Key Manager 를 사용하는 Managed PKI 고객에 대한 운영 요구 사항과 업무 준칙을 규정한 문서입니다.
SSL 용 Managed PKI	Managed PKI 서비스의 한 유형으로서 이를 통해 조직은 VTN 내의 RA 가 되어 VeriSign 또는 회원사 CA 가 지정된

용어	정의
	도메인에서 시큐어 서버 ID 를 발행하도록 지원합니다. 이 CA 는 인증 신청을 승인 또는 거부하고 시큐어 서버 ID 를 폐지 및 갱신하는 RA 기능을 Managed PKI 고객에게 위임합니다.
SSL 고객용 Managed PKI	VeriSign 또는 회원사로부터 Managed PKI 서비스를 취득한 조직입니다.
Managed PKI Lite 고객	VeriSign 또는 회원사로부터 Managed PKI Lite 서비스를 취득한 조직으로서 이 조직은 VTN 내의 등록 기관이 되어 VeriSign 또는 회원사 CA 가 클라이언트 인증서를 발행하도록 지원합니다. 이 CA 는 인증 신청을 승인 또는 거부하고 인증서를 폐지 및 갱신하는 RA 기능을 Managed PKI Lite 고객에게 위임합니다.
수동 인증	관리자가 웹 기반 인터페이스를 사용하여 인증 신청을 하나씩 직접 검토 및 승인하는 절차입니다.
미확인 가입자 정보	인증 신청자가 CA 또는 RA 에게 제출하는 정보로서 인증서에 포함되어 있으나 CA 또는 RA 가 확인하지 않은 정보입니다. 해당 CA 나 RA 는 이 정보가 인증 신청자에 의해 제출되었다는 사실 이외에 어떤 것도 보증하지 않습니다.
부인 방지	통신 발생지나 제출 또는 전달 사실을 부인하는 통신 상대에 대해 보호를 제공하는 통신 속성입니다. 발생지 부인에는 보낸 사람의 신원을 알 수 없는 경우에도 통신이 하나 이상의 이전 메시지와 동일한 소스에서 시작되었음을 부인하는 것이 포함됩니다. 참고: 법원이나 중재 위원회 및 기타 재판소의 판결을 통해서만 부인을 궁극적으로 방지할 수 있습니다. 예를 들어, VTN 인증서를 근거로 확인된 디지털 서명은 재판소의 부인 방지 결정을 지원하는 증거를 제공할 수 있지만 자체가 부인 방지를 구성하지는 않습니다.
온라인 인증 상태 프로토콜(OCSP)	신뢰 당사자에게 실시간 인증 상태 정보를 제공하는 프로토콜입니다.
OnSite	Managed PKI 를 참조하십시오.
OnSite 관리자	Managed PKI 관리자를 참조하십시오.
OnSite Administrator's Handbook(OnSite 관리자 핸드북)	Managed PKI Administrator Handbook(Managed PKI 관리자 핸드북)을 참조하십시오.
OnSite 계약서	Managed PKI 계약서를 참조하십시오.
OnSite 인증서	Managed PKI 인증서를 참조하십시오.
OnSite 제어 센터	Managed PKI 제어 센터를 참조하십시오.
OnSite Key Manager	Managed PKI Key Manager 를 참조하십시오.

용어	정의
OnSite Key Management Service Administrator's Guide(OnSite 키 관리 서비스 관리자 가이드)	Managed PKI Key Management Service Administrator's Guide(Managed PKI 키 관리 서비스 관리자 가이드)를 참조하십시오.
OnSite Lite	Managed PKI Lite 를 참조하십시오.
유효 기간	인증서가 발행된 날짜 및 시간(또는 인증서에 기재된 경우 발행 이후의 특정 날짜 및 시간)부터 인증서가 만료되거나 조기 폐지되는 날짜 및 시간까지의 기간입니다.
PKCS #10	RSA Security Inc.가 개발한 공개키 암호화 표준 #10 으로서 인증서 서명 요청의 구조를 정의합니다.
PKCS #12	RSA Security Inc.가 개발한 공개키 암호화 표준 #12 로서 개인키를 안전하게 전송하는 방법을 정의합니다.
정책 관리 기관(PMA)	VeriSign 내의 조직으로서 VTN 전체에 이 정책을 배포하는 역할을 담당합니다.
기본 인증 기관(PCA)	특정 인증서 클래스에 대해 루트 CA 역할을 수행하며 해당 하위 CA 에 인증서를 발행하는 CA 입니다.
프로세싱 센터	인증서 발행에 사용되는 암호화 모듈을 보관하는 안전한 시설을 만드는 조직(VeriSign 또는 특정 회원사)입니다. 소비자 및 웹 사이트 부문에서 프로세싱 센터는 VTN 내의 CA 역할을 하며 인증서 발행, 관리, 폐지, 갱신 등의 모든 인증 주기 서비스를 수행합니다. 기업 부문에서 프로세싱 센터는 해당 Managed PKI 고객 또는 하위 서비스 센터의 Managed PKI 고객을 대신하여 주기 서비스를 제공합니다.
공개키기반구조(PKI)	인증서 기반 공개키 암호화 시스템의 구현 및 운영을 전반적으로 지원하는 아키텍처, 조직, 기술, 업무 준칙 및 절차입니다. VTN PKI 는 VTN 을 제공 및 구현하기 위해 함께 작동하는 시스템으로 구성되어 있습니다.
등록 기관(RA)	인증 신청자의 인증 신청을 지원하고 인증 신청의 승인이나 거부 및 인증서 폐지나 갱신을 수행하도록 CA 의 허가를 받은 기관입니다.
신뢰 당사자	인증서 및/또는 디지털 서명에 대한 신뢰를 바탕으로 역할을 수행하는 개인이나 조직입니다.
신뢰 당사자 계약서	CA 가 사용하는 계약서로서 개인이나 조직이 신뢰 당사자 역할을 수행할 때 적용되는 조건을 규정합니다.

용어	정의
리테일 인증서	웹 사이트 상에서 개별적으로 신청하는 개인이나 조직에게 CrossCert 가 CA 로서 발행한 인증서입니다.
로밍 가입자	VeriSign 로밍 서비스를 사용하는 가입자입니다. 이 서비스의 개인키는 VeriSign 로밍 서버와 기업 로밍 서버로 분리된 대칭키를 사용하여 암호화 및 해독됩니다.
RSA	Rivest, Shamir 및 Adelman 이 개발한 공개키 암호화 시스템입니다.
RSA 시큐어 서버 인증 기관(RSA 시큐어 서버 CA)	시큐어 서버 ID 를 발행하는 인증 기관입니다.
RSA 시큐어 서버 계층	PKI 계층은 RSA 시큐어 서버 인증 기관으로 구성됩니다.
Secret Share	CA 개인키의 일부, 또는 공유 비밀 계약에 따라 CA 개인키를 작동하는 데 필요한 실행 데이터의 일부입니다.
비밀 공유	CPS § 6.2.2 에 따라 여러 사람이 CA 개인키 작동을 제어할 수 있도록 하기 위해 CA 개인키 또는 CA 개인키를 작동시키기 위한 활성화 데이터를 분리하는 작업입니다.
시큐어 서버 ID	웹 브라우저와 웹 서버 간의 SSL 세션을 지원하는 데 사용되는 클래스 3 단체 인증서입니다.
SSL(Secure Sockets Layer)	Netscape Communications Corporation 이 개발한 웹 통신 보호용 산업 표준 메서드입니다. SSL 보안 프로토콜은 전송 제어 프로토콜/인터넷 프로토콜 연결에 대해 선택적 클라이언트 인증, 메시지 무결성, 서버 인증 및 데이터 암호화 기능을 제공합니다.
Security and Audit Requirements Guide(보안 및 감사 요구 사항 가이드)	프로세싱 센터와 서비스 센터에 대한 보안 및 감사 요구 사항과 업무 준칙을 규정한 VeriSign 문서입니다.
보안 및 업무 검토	회원사의 운영을 허용하기 전에 VeriSign 이 수행하는 회원사에 대한 검토 작업입니다.
SGC(Server Gated Cryptography)	이 기술을 통해 글로벌 서버 ID 가 발행된 웹 서버는 강력한 암호화 보호 기능을 사용하여 암호화되는 브라우저로 SSL 세션을 생성할 수 있습니다.
Server OnSite	SSL 용 Managed PKI 를 참조하십시오.
Server OnSite 고객	SSL 고객용 Managed PKI 를 참조하십시오.
서버 서비스 센터	웹 사이트 또는 기업에 시큐어 서버 ID 와 글로벌 서버 ID 를 제공하는 회원사 서비스 센터입니다.
서비스 센터	특정 클래스나 유형의 인증서를 발행하기 위해 인증서 서명 장치를 설치하는 대신 이러한 인증서의 발행, 관리, 폐지 및

용어	*정의*
	갱신을 수행하는 데 프로세싱 센터에 의존하는 회원사입니다.
하위 도메인	VTN 중 VTN 계층에서 특정 기관 및 모든 해당 하위 기관의 제어를 받는 부분입니다.
피발행자	공개키에 대응하는 개인키의 소유자입니다. "피발행자"라는 용어는 단체 인증서의 경우 개인키를 소유한 장비나 장치를 의미할 수 있습니다. 피발행자에게는 피발행자의 인증서에 포함된 공개키와 연결된 명확한 이름이 할당됩니다.
가입자	개인 인증서의 경우 인증서를 발행 받은 피발행자이고, 단체 인증서의 경우 인증서가 발행된 장비나 장치를 소유한 조직입니다. 가입자는 인증서에 기재된 공개키에 대응하는 개인키를 사용할 권한이 있습니다.
가입 계약서	CA 또는 RA 가 사용하는 계약서로서 개인이나 단체가 가입자 역할을 수행할 때 적용되는 조건을 규정합니다.
상위 개체	VTN 계층(클래스 1, 2 또는 3)에서 특정 개체 위의 개체를 말합니다.
추가 위험 관리 검토	개체에 대한 준수성 감사에서 불완전하거나 비정상적인 결과를 발견했을 때 또는 일반 업무에 대한 전반적인 위험 관리 프로세스의 일환으로 VeriSign 이 수행하는 검토 작업입니다.
리셀러	특정 시장에서 VeriSign 또는 회원사를 대신하여 서비스를 제공하는 조직입니다.
Time-Stamping 기관	VeriSign 디지털 공증 서비스의 일부로서 디지털 영수증에 서명하는 VeriSign 기관입니다.
Time-Stamping 기관 CA	디지털 영수증의 디지털 서명을 확인하는 데 사용된 Time-Stamping 기관에 특별 클래스 3 단체 인증서를 발행한 VeriSign CA 입니다.
승인된 사람	CPS § 5.2.1 의 세부 정의에 따라 특정 조직과 이 조직의 제품, 서비스, 시설 및 업무의 기반구조에 대한 신뢰 가능성 관리를 담당하는 VTN 내 조직의 직원, 계약 업체 및 컨설턴트입니다.
승인된 직위	VTN 조직 내의 승인된 사람에게 부여된 직위입니다.
신뢰 가능한 시스템	침입 및 오용을 방지하고, 적절한 수준의 가용성, 신뢰성 및 작동의 정확성을 제공하며, 원하는 기능을 제대로 수행하기에 적합하고, 해당 보안 정책을 준수하는 컴퓨터 하드웨어/소프트웨어 및 절차입니다. 신뢰 가능한 시스템이 항상 분류된 정부 용어법에서 인정되는 "승인된 시스템"은 아닙니다.
CrossCert 가 제공하는 VeriSign 디지털 공증 서비스	Managed PKI 고객에게 제공되는 서비스로서 특정 문서나 데이터 세트가 특정 시점에 존재했음을 전자 서명으로 증명합니다(디지털 영수증).

용어	*정의*
CrossCert 저장소	온라인에서 액세스할 수 있는 관련 VTN 정보와 인증서가 들어 있는 CrossCert 데이터베이스입니다.
CrossCert 가 제공하는 VeriSign 로밍 서비스	CrossCert 가 제공하는 VeriSign 로밍 서비스와 관련하여 사용되는 CrossCert 프로세싱 센터의 서버로서 로밍 가입자의 개인키를 암호화 및 해독하는 데 사용되는 대칭 키의 일부가 저장되어 있습니다.
CrossCert 가 제공하는 VeriSign 로밍 서비스	가입자가 자신의 개인키를 다운로드하고 다른 클라이언트 터미널에서 개인키 작동을 수행할 수 있도록 CrossCert 가 제공하는 서비스입니다.
CrossCert Security Policy(CrossCert 보안 정책)	CrossCert 의 보안 정책을 설명하는 최상위 설명서입니다.
CrossCert 하위 도메인 참여자	VTN 의 CrossCert 하위 도메인에 속하는 하나 이상의 개인 또는 조직으로서 CrossCert, 고객, 리셀러, 가입자 또는 신뢰 당사자가 포함됩니다.
VeriSign Trust Network(VTN)	VTN 인증 정책이 적용되는 인증서 기반의 공개키기반구조(PKI)입니다. 이를 통해 전세계 VeriSign 과 해당 회원사, 각 고객, 가입자 및 신뢰 당사자는 인증서를 배치 및 사용할 수 있습니다.
CrossCertVTN 참여자	VTN 내의 개인 또는 조직으로서 VeriSign, 회원사, 고객, 리셀러, 가입자, 신뢰 당사자 등이 포함됩니다.
VTN 표준	VTN 에서 인증서의 발행, 관리, 폐지, 갱신 및 사용에 대한 비즈니스, 법률 및 기술 요구 사항입니다.
웹 호스트	인터넷 서비스 제공업체, 시스템 통합업체, 리셀러, 기술 컨설턴트, 애플리케이션 서비스 제공업체 또는 기타 이와 유사한 조직 등과 같이 다른 웹 사이트를 운영하는 조직입니다.
웹 호스트 프로그램	웹 호스트가 웹 호스트의 고객인 최종 사용 가입자를 대신하여 시큐어 서버 ID 와 글로벌 서버 ID 를 등록할 수 있도록 하는 프로그램입니다.
웹 사이트(웹 사이트 서비스 센터의 경우)	인증 신청자에게 시큐어 서버 ID 와 글로벌 서버 ID 리테일 인증서를 하나씩 제공하는 회원사의 업종입니다.
WAP(Wireless Application Protocol)	휴대폰 및 기타 무선 터미널에서 무선 정보와 전화 서비스를 제공하기 위한 표준입니다.
WTLS(Wireless Transport Layer Security)	무선 핸드셋과 서버 간의 통신과 같이 WAP(Wireless Application Protocol)를 사용하여 작동하는 애플리케이션 통신을 보호하는 프로토콜입니다.

용어	*정의*
Wireless Transport Layer Security 인증서(WTLS 인증서)	WAP(Wireless Application Protocol)의 일부로 정의된 형식을 갖춘 클래스 3 단체 인증서로서 WTLS 클라이언트에 대해 WTLS(Wireless Transport Layer Security) 서버를 인증하고 WTLS 서버와 WTLS 클라이언트 간의 암호화된 통신을 용이하게 합니다.