CrossCert
인증업무준칙

버전 3.8.8

발효일: 2012 년 7 월 29 일

(모든 인증기관(CA) 및 브라우저 포럼 특정 요건들(Browser Forum-specific requirements)은 2012 년 7 월 1 일자로 유효함)

(우)137-725
서울시 서초구 서초대로 320(서초동 1674-4) 하림빌딩 7 층
한국전자인증㈜
전화: +82-2-3019-5500
홈페이지: *www.crosscert.com*

CrossCert 인증업무준칙

인쇄일자: 2012 년 7 월 29 일

중요사항 – 인수 합병 공고

시만텍 주식회사(Symantec Corporation)는 베리사인 주식회사(VeriSign Inc)의 인증 사업 부문을 2010 년 8 월 9 일자로 인수하였습니다. 이에, 본 서류에 설명된 공개키 기반 구조(PKI) 서비스와 본 인증업무준칙의 모든 등재 소유자는 이제 시만텍입니다.
그러나, 인증 및 관련 서비스에 관한 신규 브랜드화를 완료하기까지는 “VeriSign”과 “Symantec” 양사의 혼용 표기가 있을 것입니다. VeriSign 에 대한 일체의 표기는 본 소유권상의 유래를 반영, 설명하는 용어로만 엄격히 간주됩니다.

상표 관련 공지

본 CrossCert 인증업무준칙(및 시만텍에게 사본을 요청하는 경우)을 복제하기 위한 승인을 요청하는 경우에는 다음의 연락처로 문의바랍니다. 한국전자인증㈜ (우)137-725 서울시 서초구 서초대로 320(서초동 1674-4) 하림빌딩 7 층, 참조: 인증개발부서. 전화: +82-2-3019-5500 Fax: +82-2-3019-5656 이메일: practices@crosscert.com.

목차:

4.6.6 CA에 의한 인증서 갱신의 게재(Publication of the Renewal Certificate by the CA)

4.6.7 CA에 의한 인증서 발행에 관한 타인 통지(Notification of Certificate Issuance by the CA to Other Entities)

4.7 인증서 키교체(Certificate Re-Key)

4.7.1 인증서 키교체 환경(Circumstances for Certificate Re-Key)

4.7.2 신규 공동키 인증을 요청할 수 있는 사람(Who May Request Certification of a New Public Key)

4.7.3 인증서 키교체 요청 처리(Processing Certificate Re-Keying Requests)

4.7.4 가입자에 대한 신규 인증서 통지(Notification of New Certificate Issuance to Subscriber)

4.7.5 키교체된 인증서에 대한 수락 행위(Conduct Constituting Acceptance of a Re-Keyed Certificate)

4.7.6 CA에 의한 키교체된 인증서의 게재(Publication of the Re-Keyed Certificate by the CA)

4.7.7 CA에 의한 인증서 발행에 관한 타인 통지(Notification of Certificate Issuance by the CA to Other Entities)

4.8 인증서 수정(Certificate Modification)

4.8.1 인증서 수정 배경(Circumstances for Certificate Modification)

4.8.2 인증서 수정을 요청할 수 있는 사람(Who May Request Certificate Modification)

4.8.3 인증서 수정 요청 처리(Processing Certificate Modification Requests)

4.8.4 가입자에 대한 신규 인증서 발행 통지(Notification of New Certificate Issuance to Subscriber)

4.8.5 수정된 인증서에 대한 수락 행위(Conduct Constituting Acceptance of Modified Certificate)

4.8.6 CA에 의한 수정된 인증서의 게재(Publication of the Modified Certificate by the CA)

4.8.7 CA에 의한 인증서 발행에 관한 타인 통지(Notification of Certificate Issuance by the CA to Other Entities)

4.9 인증서 폐지 및 정지(Certificate Revocation and Suspension)

4.9.1 폐지 환경(Circumstances for Revocation)

4.9.1.1 폐지 사유에 관한 CABF 요건(CABF Requirements for Reasons for Revocation)

4.9.2 폐지를 요청할 수 있는 자(Who Can Request Revocation)

4.9.3 폐지 요청 절차(Procedure for Revocation Request)

4.9.3.1 최종 사용자 가입자 인증서의 폐지를 요청하는 절차(Procedure for Requesting the Revocation of an End-User Subscriber Certificate)

4.9.3.2 인증서 폐지 절차에 대한 CABF 요건(CABF Requirements for Certificate Revocation Process)

4.9.3.3 CA 혹은 RA 인증서 폐지 요청 절차(Procedure for Requesting the Revocation of a CA or RA Certificate)

4.9.4 폐지 요청 유예 기간(Revocation Request Grace Period)

4.9.5 CA가 폐지 요청을 처리해야 하는 시간(Time within Which CA Must Process the Revocation Request)

4.9.6 신뢰자들에 대한 폐지 확인 요건(Revocation Checking Requirements for Relying Parties)

4.9.7 CRL 발행 빈도(CRL Issuance Frequency)

4.9.7.1 CRL 발행에 관한 CABF 요건(CABF Requirements for CRL Issuance)

4.9.8 CRL에 대한 최대 잠재기(Maximum Latency for CRLs)

4.9.9 온라인 폐지/상태 확인 가용도(On-Line Revocation/Status Checking Availability)

4.9.9.1 OCSP 가용도에 대한 CABF 요건(CABF

소개(INTRODUCTION)

본 문서는 CrossCert 인증업무준칙(“CPS”)입니다. 이는, ‘시만텍 네트워크 인증정책(Symantec Trust Network Certificate Policies; “CP”)’의 특정 요건에 따라 인증서를 발급, 관리, 폐지 및 갱신하는 사항을 포함한, 인증 서비스 제공에 관하여 CrossCert 인증기관(“CAs”)이 수행하는 업무 사항을 규정하고 있습니다.

CP 는 STN 을 지배하는 원칙적인 정책 규정입니다. 이는 STN 과 신뢰인증 서비스 제공업무 내에서 전자 인증서를 승인, 발급, 사용, 폐지하고 갱신하는 것과 관련된 사업, 법률 및 기술적인 요건들을 규정합니다. 이러한 요건들은 “STN 표준(STN Standards)”이라고 언급되며, STN 의 보안과 무결성을 보호하고, 모든 “STN 참여자들(STN Participants)”에게 적용되고, STN 전반에 걸친 통일적인 신뢰도를 보장합니다. STN 및 STN 표준에 관한 더 자세한 정보는 CP 에서 확인하실 수 있습니다.

CrossCert 는 STN 의 “서브 도메인(Sub-domain)”이라고 불리우는 STN 의 일부분에 대한 권한을 보유합니다. CrossCert 의 서브 도메인은 고객들(Customers), 가입자들(Subscribers), 그리고 신뢰자들(Relying Parties)과 같은 존재들이 포함합니다.

CP 가 ‘STN 참여자들이 충족하여야 하는 요건들’을 규정하고 있지만, 본 CPS 는 ‘CrossCert 가 이러한 요건들을 STN 의 CrossCert 서브 도메인 내에서 어떻게 충족하여야 하는가’에 대한 사항을 규정합니다. 더 상세히 말하자면, 본 CPS 는 ‘CrossCert 가 STN 의 CrossCert 서브 도메인 내에서 CP 와 STN 표준 요건들에 따라 다음의 업무들을 하는 것과 관련된 사항’을 설명합니다:

- STN 을 지원하는 핵심 기반을 안전하게 관리하는 것, 그리고
- “STN 인증서(STN Certificates)”를 발급, 관리, 폐기 및 갱신하는 것

본 CPS 는 인증서 정책(Certificate Policy)과 인증업무준칙 해석에 대하여 Internet Engineering Task Force (IETF) RFC 3647 를 준수합니다. 시만텍 신뢰 네트워크(Symantec Trust Network) 계층 내 CAs 들은 www.cabforum.org 에 개시된 ‘공개 인증서의 발급과 관리에 대한 기준(CA/Browser Forum (CABF) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates)’의 현행 버전을 준수합니다. 본 문서의 내용과 요건들이 ‘앞서 언급된 문서들’의 내용들과 일관되지 않는 경우에는, ‘앞서 언급된 문서들’의 내용이 본 문서의 내용보다 우선합니다.

현재, 본 CP 에 따라 CrossCert CAs 들에 의하여 발급된 ‘도메인 유효 및 기관 유효 SSL 인증서(domain-validated and organization-validated SSL Certificates)’는 CABF 요건(CABF Requirements)에 따라야 합니다. 해당 인증서들은, 본 규정 요건들에 대한 준수 여부를 표시하는 CP 제 1 조 2 항에 규정된 정책 표기자들과 부합하는 사항을 포함하여

발급되었습니다. CrossCert 인증기관들(CAs)은, '모든 인증서들이 CABF 요건들(CABF Requirements)을 따라 정책 표기자들이 발급되고 관리됨을 포함하여 발급되었음'을 확인합니다.

STN 의 CrossCert 서브 도메인은 한국 행정안전부와 CA 간 상호 인증되었으며 CrossCert 인증업무준칙의 요건들을 준수하며 운영되고 있습니다.

1.1 개요(Overview)

CrossCert 는 CP 제 1 조 1 항에 설명된 바와 같이 "프로세싱 센터(Processing Center)"이며, 이는 'CrossCert 가 인증서 발급에 사용되는 개인키(private keys)를 보유하는 암호화 모듈을 포함한 CA 시스템, 안전한 설비 보유 시스템을 설치하였음'을 의미합니다. CrossCert 는 STN 내에서 인증기관(CA)으로 업무를 수행하며, 인증서 발급, 관리, 폐기 및 갱신과 관련된 모든 인증서 생애(lifecycle) 서비스를 수행합니다. 또한, 기업 고객들이나 CrossCert 에 종속된 서비스 센터의 기업 고객들을 위하여 '인증기관 키 관리(CA key management)' 및 인증서 생애(lifecycle) 서비스도 제공합니다. CrossCert 는 비즈니스, 고객(클래스 1 및 클래스 2 고객 리테일 인증서), 웹싸이트(Secure Server IDs 및 Global Server IDs), 그리고 기업(Managed PKI 서비스 제공)을 위한 세가지 분야에 인증서들을 제공합니다. 계열회사들에 의하여 제공되는 서비스 또는 시만텍이 계열회사들에게 제공하는 서비스들과 관련된 업무에는 본 CPS 는 적용되지 아니합니다.

본 CPS 는 명시적으로 다음 사항에 적용됩니다:

- Symantec 의 '공인 인증기관(Public Primary Certification Authorities; PCAs)',
- CrossCert 기반 인증기관들(CAs), 그리고 '시만텍 신뢰 네트워크(Symantec Trust Network)'를 지원하는 CrossCert 행정 인증기관들(CrossCert Administrative CAs)
- CrossCert 의 공식 인증기관들(Public CAs) 그리고 STN 의 CrossCert 서브 도메인 내 인증서를 발급하는 기업 고객들의 인증기관들.

보다 일반적으로는, 본 CPS 는 CrossCert 서브 도메인 내의 개인이나 개체들(총칭하여, "CrossCert 서브 도메인 참여자들(CrossCert Sub-domain Participants)"이라 함)이 CrossCert 서브 도메인 내에서 STN 서비스를 이용하는 사안들도 관장합니다. 사설 인증기관들(CAs)과 CrossCert 에 의해 관리되는 하위 계층들은 본 CPS 적용 범위가 아닙니다.

STN 은 클래스 1 부터 4 에 이르는, 네 가지 클래스들의 인증서들을 포함합니다. CP 는 각각의 클래스별 인증서에 대한 정책들을 정의하고, 각 클래스에 대한 STN 표준을 설정하는 단일 문서입니다.

CrossCert 는 STN 의 서브 도메인 내에서 세 가지 클래스별 인증서들을 제공합니다. 본 CPS 는 'CrossCert 가 자신의 서브 도메인 내에서 각각의 클래스에 대한 CP 요건들을 어떻게 충족하는 지'를 설명합니다. 그러므로, 본 CPS 는, 단일한 문서로서, 세가지 인증서들 모두에 대한 발급과 관리에 관한 업무와 절차를 다룹니다.

CrossCert 는, 정부의 특정 정책상의 요건들 또는 기타 산업계 표준과 요건들을 충족하기 위하여 본 CPS 를 보완하는 인증업무준칙을 공표할 수 있습니다.

그러한 '보충적인' 인증서 정책들은 해당 보충 정책들에 따라 발급된 인증서들의 가입자들과 이를 신뢰하는 자들에게 공개되어야 합니다.

본 CPS 는, STN 의 CrossCeert 서브 도메인과 관련된 일련의 문서들 중에 하나 일뿐입니다. 다른 문서들은 아래 사항들을 포함합니다:

- 상세한 요건들을 제시함으로써 CP 와 CPS 를보완하는 부가적인 기밀 안전 및 운영상의 문서[1], 예를 들어:
  - STN 기반을 규율하는 보안 원칙을 규정한 '시만텍의 물리적 보안 정책(Symantec Physical Security Policy)',
  - 인력, 물리적, 의사소통, 논리적이고 암호화 키 관리 보안에 관한 시만텍과 계열사들의 상세한 요건들을 규정한 '시만텍 보안 및 감사 요건 가이드(Symantec Security and Audit Requirements (SAR) Guide), 그리고,
  - 상세한 키 관리 운영 요건들을 표시하는 '키 양식 레퍼런스 가이드(Key Ceremony Reference Guide)'.
- CrossCert 에 의해 부과되는 기타 부속 합의서들. 그러한 합의서들은 CrossCert 의 고객들, 가입자들 및 신뢰자들을 구속합니다. 다른 사항들과 더불어, 그러한 합의서들은 STN 참여자들에게까지 STN 표준을 준수하게 만들며, 어떤 경우에는, 'STN 표준을 어떻게 준수하여야 하는가'에 대한 특정 업무사항들을 규정합니다.

여러 경우에, 본 CPS 는, STN 중 CrossCert 서브 도메인의 보안을 양허할 수 있는 CPS 에서의 사양들을 포함하는 STN 표준 이행에 관한 상세사항에 대한 부속 문서들을 언급하기도 합니다.

1.2 문서 이름 및 식별(Document name and Identification)

[1] 비록 이러한 서류들이 공개되지 않으나, 해당 사양들은 시만텍의 인증기관에 대한 연간 WebTrust에 포함되어 있으며, 특정 계약서 체결 하에 고객들에게도 공개될 수 있음.

본 문서는 ‘CrossCert 인증업무준칙’입니다. STN 인증서들(STN Certificates)은 인증서의 STN 클래스에 대응하는 ‘대상 식별 값(object identifier values)’을 포함합니다. 그러므로, CrossCert 는 본 CPS 에 ‘대상 식별 값(object identifier values)’을 부여하지 않았습니다. ‘인증서 정책 대상 식별자(Certificate Policy Object Identifiers)’는 제 7 조 1 항 6 호에 따라 사용되었습니다.

‘도메인 유효 및 기관 유효 SSL 인증서들(Domain validated and organization validated SSL Certificates)’은, ‘인증기관/브라우저 포럼 요건들(CA / Browser Forum Baseline Requirements)’에 따르는, STN CP 의 제 1 조 2 항에 대응하는 OID 값을 포함합니다.

1.3 PKI 참여자들(PKI Participants)

1.3.1 인증기관(Certification Authorities)

‘인증기관(CA)’이라는 용어는, STN 내에서 공개키 인증서를 발급할 수 있는 권한을 가진 모든 개체들을 일컫는 포괄적인 용어입니다. ‘CA’라는 용어는 ‘기본적 인증기관(Primary Certification Authorities, “PCA”)’이라고 불리는 하위카테고리의 발급자들을 포함합니다. PCA들은 인증서의 각각의 클래스, 네 개의 도메인들[2]에 대한 루트(roots)로서 활동합니다. 각각의 PCA는 시만텍의 개체입니다. CrossCert 인증기관들은 PCA들에 종속하여, 최종 사용자 가입자나 다른 CA들에게 인증서들을 발급합니다.

시만텍은 “시만텍 통합 루트 인증기관(Symantec Universal Root Certification Authority)” 과 “시만텍 ECC 통합 루트 인증기관(“Symantec ECC Universal Root Certification Authority)”도 운영합니다. 통합 루트 인증기관들은 클래스 3 및 일부 선정된 클래스 2 하위 CA들을 발행합니다.

CrossCert의 기업 고객들은 자신들의 CA들을, CrossCert PCA에 대한 하위 CA로서, 운영할 수 있습니다. CrossCert와 계약관계를 가지는 고객은 STN CP와 CrossCert의 CPS 상의 모든 내용을 준수하여야 합니다. 그러나, 이러한 하위 CA들은, 내부 요건들에 근거하여 더욱 제한적인 업무를 수행할 수 있습니다.

STN CA 하나는, 기술상으로는, ‘PCA들 각자가 보안 서버 인증기관(Secure Server Certification Authority)’인 세 개의 지배계층들 밖에 존재합니다. 이러한 CA는, PCA나 루트와 같은, 상위 CA를 가지지 않습니다. 오히려, 보안 서버 인증기관은 자신의 루트로서 행동하며, 스스로 서명한 루트 인증서를 발행합니다. 또한, 최종 사용자 가입자들에게 인증서들을 발행하기도 합니다. 그러므로, 보안 서버 계층(Secure Server Hierarchy)은 보안 서버 인증기관(Secure

[2] 클래스 4 인증서는 현재 STN 에 의하여 발행되지 않음

Server CA)으로만 구성됩니다. 보안 서버 인증기관(Secure Server CA)은 보안서버 ID들을 발행하며, 이는 '클래스 3 기관용 인증서(Organizational Certificates)'로 간주됩니다.

보안 서버 인증기관(Secure Server CA)은 STN 내에서 다른 클래스 3 CA들과 상당히 유사한 생애주기 업무를 채택합니다. 즉, 시만텍은 보안 서버 인증기관(Secure Server Certification Authority)을 STN 내 클래스 3 CA로 지정하고 승인하였습니다. 그가 발행하는 인증서들은 다른 클래스 3 기관용 인증서들에 비교할 수 있는 신뢰도를 보장한다고 간주됩니다.

1.3.2 등록기관(Registration Authorities)

등록기관(Registration Authority; "RA")은, STN CA 를 대신하여 인증서 키 교체나 갱신 신청자를 승인하는 것, 그리고 최종 사용자 인증서에 대한 발급이나 유지, 폐기를 신청하는 인증서 신청자들의 신원을 확인하고 인증하는 업무를 담당하는 개체입니다. CrossCert 는 EV 와 '코드 서명 인증서(Code-Signing Certificates)' 이외의 인증서들을 발행하는 인증서 RA 로 역할을 수행할 수 있습니다. 시만텍 주식회사는, CrossCert 에 의해 제기된 'EV 와 코드 서명 인증서 관련 모든 인증서 요청들(Certificate Requests)'에 대한 RA 로서의 역할을 하여야 합니다.

CrossCert 와 계약관계를 체결한 제 3 자들은 자신들의 RA 를 직접 운영할 수 있으며 CrossCert CA 에 의한 인증서 발급을 인증할 수 있습니다. 제 3 자의 RA 들은 STN CP, CrossCert CPS 및 CrossCert 와 체결한 기업 서비스 계약상의 모든 규정과 조건을 준수하여야 합니다. 그러나, RA 들은 그들 내부 요건들에 근거하여 더욱 제한적인 업무를 수행하여야 할 수 있습니다[3]. ,

1.3.3 가입자(Subscribers)

STN 내의 가입자들은, STN CA 에 의해 발행되는 인증서의 모든 최종 사용자 (개체들 포함)을 포함합니다. 가입자는 인증서의 최종 사용자 가입자로 명명된 개체입니다. 최종 사용자 가입자는 개인이거나, 기관(organization)일 수도 있고, 보안벽, 라우터(routers), 신뢰 서버 혹은 기관(Organization) 내에서 사용되는 기타 장치들과 같이 기반 설비의 일부분도 될 수 있습니다.

어떤 경우에는, 인증서들은 개인이나 개체들에게 그들 자신들을 위한 사용 목적으로 직접 발행됩니다. 그러나, 일반적으로는, 인증서를 요구하는 자는 암호 정보가 적용되는 대상과 다른 경우가 보편적입니다. 예를 들어, 한 기관은 자신의 직원들이 전자거래/비즈니스에서 자기 조직을 대표할 수 있도록 하기 위하여 인증서를 필요로 할 수 있습니다. 그러한

[3] 제 3 자 RA 의 예를 들면, Managed PKI 서비스 고객의 고객임.

경우에, 인증서 발행을 위해 가입(즉, 특정 서비스를 가입하거나, 발행자로서 수수료 지급을 하는 것)하는 주체는, 인증서의 대상인 개체(일반적으로, 암호화된 정보의 보유자)와 다릅니다. 본 CPS 에서 사용되는 두 가지 용어들은 이러한 두 가지 역할들을 구분하기 위하여 사용됩니다: “가입자(Subscriber)"란, 암호 정보의 발급을 위하여 CrossCert 와 계약을 체결한 개체이며; “대상(Subject)”이란, 해당 암호 정보가 구속되는 사람을 의미합니다. 가입자는 암호 정보 사용에 대한 궁극적인 책임을 부담하지만, 대상은 암호 정보가 제출될 경우에 인증을 받는 개인입니다.

‘대상(Subject)’이 언급되는 경우에는, ‘가입자(Subscriber)’와 구분되는 것을 표시합니다. ‘가입자(Subscriber)’가 언급되는 경우에는 단순히 개별 개체로서의 가입자를 의미할 수도 있지만, 두 가지 의미를 모두 포함할 수도 있습니다. 본 CPS 에서 해당 용어들의 사용은 올바른 이해를 도울 것입니다.

인증기관들(CAs)은 기술적으로는, 자기 서명 인증서를 자신에게 발행하는 PCA 이거나 상위 CA 에 의해 인증서를 발행하는 CA 로서, STN 내의 인증서 가입자들이기도 합니다. 그러나, 본 CPS 에서 “최종 개체들(end entities)”과 “가입자들(subscribers)”에 대한 언급은 오직 최종 사용자 가입자들만 해당됩니다.

1.3.4 신뢰자(Relying Parties)

신뢰자(Relying Party)는, STN 하에서 발행된 전자서명 및/혹은 인증서에 의존하여 행동한 개인이나 개체입니다. 신뢰자는 STN 내에서의 가입자일 수도 있고, 가입자가 아닐 수도 있습니다.

1.3.5 인증서 수혜자(Certificate Beneficiaries)

인증서 수혜자(Certificate Beneficiaries)는 ‘인증기관 브라우저 포럼 가이드라인(CA / Browser Forum Guidelines)’에 따라 표시됩니다. 인증서 수혜자는, 다음을 포함하며, 이에 제한되지 않습니다:

1. 인증서 관련 ‘가입자 계약서(Subscriber Agreement)’의 당사자인 가입자;
2. 루트(Root) CA 와 계약을 체결하여 배포 대상 소프트웨어에 루트 인증서(Root Certificate)를 포함하고자 하는 해당 에플리케이션 소프트웨어 공급자들 모두; 그리고
3. 유효한 인증서(Valid Certificate)에 합리적으로 의존하는 모든 신뢰자들.

1.3.6 기타 참여자들(Other Participants)

적용사항 없음

1.4 *인증서의 용도(Certificate Usage)*

1.4.1 적정한 인증서 사용(Appropriate Certificate Usages)

1.4.1.1 개인용 인증서(Certificates Issued to Individuals)

개인용 인증서(Individual Certificates)는 일반적으로 개인들이 서명하고 이메일을 암호화하고 애플리캐이션에 인증(고객 인증)을 하기 위하여 사용됩니다. 개인용 인증서의 가장 보편적인 용도는 다음 [표 1]에 포함되어 있기는 하지만, 개인용 인증서는 다른 목적으로도 이용될 수 있습니다. 단, 신뢰자는 합리적으로 '인증서 및 그 용도는 인증서가 발급된 STN CP 와 CPS 규정과 법규상 제한 받지 않는 것이어야 하고, 가입자들과 체결한 계약조건에도 위반되지 않는 것'이라는 신뢰를 할 수 있는 것이어야 합니다.

인증서 클래스	보장 수준			용도		
	낮은 보장 수준	중간 보장 수준	높은 보장 수준	서명	암호화	고객 인증
클래스 1 인증서	✓			✓	✓	✓
클래스 2 인증서		✓		✓	✓	✓
클래스 3 인증서			✓	✓	✓	✓

[표 1] 개인용 인증서 용도

1.4.1.2 기관용 인증서(Certificates issued to Organizations)

기관용 인증서(Organizational Certificates)는, '해당 기관이 법적으로 존재하며 해당 인증서에 다른 기관 속성들이 포함된 것(미확인 가입자 정보 제외), 예를 들어, 인터넷 또는 이메일 도메인에 대한 소유권'을 인증한 후 기관에게 발행됩니다. 기관용 인증서에 대한 용도 유형을 제한하는 것은 본 CPS 의 의도가 아닙니다. 기관용 인증서의 가장 보편적인 용도는 다음 [표 2]에 포함되어 있기는 하지만, 기관용 인증서는 다른 목적으로도 이용될 수 있습니다. 단, 신뢰자는 합리적으로 '인증서 및 그 용도는 인증서가 발급된 STN CP 와 CPS 규정과 법규상 제한 받지 않는 것이어야 하고, 가입자들과 체결한 계약조건에도 위반되지 않는 것'이라는 신뢰를 할 수 있는 것이어야 합니다.

인증서 클래스	보장 수준		용도			
	높은 보장 수준	중간 보장 수준	코드/콘텐츠 서명	보안 SSL/TLS-세션	인증	서명 및 암호화
클래스 3 인증서	✓		✓	✓	✓	✓

[표 2] 기관용 인증서 용도[4]

1.4.1.3 보장 수준(Assurance levels)

낮은 보장 수준의 인증서(Low assurance certificates)는, 부인 방지(Non-repudiation)를 지원하거나 인증 목적을 위하여 사용되어서는 안 되는 인증서들입니다. 전자 서명은 '특정 이메일 주소에서 송신자로부터 발생된 이메일임'을 보장합니다. 그러나, 해당 인증서는, 가입자의 정체에 대한 증거를 제공하지 않습니다. 암호화 애플리캐이션은, 신뢰자가 가입자에 대한 메시지를 암호화하기 위하여 가입자의 인증서를 사용할 수 있게 합니다만, 메시지를 송신하는 신뢰자는 '수신자가 사실상 인증서에 명기된 사람임'을 확신할 수는 없습니다.

중간 보장 수준의 인증서(Medium assurance certificates)는, 클래스 1 과 클래스 3 인증서와 관련하여, 가입자의 정체에 대한 중간 수준의 보장을 필요로 하는 몇몇 기관 간 및 기관 내, 상업적 및 개인별 이메일을 안전하게 하는 데 적합한 인증서들입니다.

높은 보장 수준의 인증서(High assurance Certificates)는, 클래스 1 및 클래스 2 인증서들과 비교할 때 가입자의 정체에 대한 높은 수준의 보장을 제공하는 개인용 및 기관용 클래스 3 인증서들입니다.

1.4.2 인증서 사용 제한(Prohibited Certificate Uses)

인증서는 적용 법규에 일치하는 범위에서만 이용되어야 하며, 특히 적용 수출입 법규에서 허용하는 범위 내에서만 이용되어야 합니다.

시만텍과 CrossCert 인증서들은, 핵 시설 운영, 비행기 항로 추적이나 통신 시스템, 항로 통제 시스템, 또는 무기 통제 시스템 등과 같이 위험한 환경이나 잘못 사용될 경우 사망, 부상이나 환경 손실을 초래할 수 있는 데에는 사용되거나 재판매 될 수 없도록 설계되고, 의도되었으며 권한을 부여 받았습니다. 또한, 클래스 1 인증서는, 정체나 권한에 대한 부인방지(non-repudiation)를 지원하거나 정체 입증자료로 사용되어서는 아니 됩니다. 고객

[4] "한정적인 환경에서 클래스 2 인증서는 Managed MPKI 고객에 의하여 관계사(조직 내 개인은 아님)에게 발행될 수 있음. 그러한 인증서는 기관 인증과 애플리케이션 서명에만 사용될 수 있음. 시만텍에 의해 기업 서비스 계약서의 내용에 따라 명시적으로 허용되지 않은 한, 가입자들은 본 인증서를 코드와 컨텐츠 서명, SSL 암호 및 S/mime 서명에 사용할 수 없으며, 그러한 키 사용은 인증서들을 사용할 수 없게 함.

인증서(Client Certificates)는, 고객 애플리케이션을 위해 마련된 것이며, 서버 혹은 기관용 인증서로 사용되어서는 아니 됩니다.

CA 인증서는 CA 기능 이외에는 모든 기능을 위해 사용될 수 있습니다. 또한, 최종 사용자 가입자 인증서는 CA 인증서로 사용되어서는 아니 됩니다.

시만텍과 CrossCert 는 정기적으로 중계 CA 들의 키를 교체(rekey)합니다. 루트 인증서로서 포함된 중계 CA 를 가지는 제 3 자 애플리케이션 또는 플랫폼은 중계 CA 가 키를 교체한 후에는 원래 설계된대로 운영될 수 없습니다. 그러므로, CrossCert 는 중계 CA 가 루트 인증서로 사용되고 있음을 보증하지 않으며, 중계 CA 들이 루트 인증서로 애플리케이션이나 플랫폼에 포함되지 않도록 권장합니다. CrossCert 는 PCA 루트(Roots)를 루트 인증서로 사용할 것을 권장합니다.

1.5 정책 행정(Policy Administration)

1.5.1 정책 수행 기관(Organization Administering the Document)

한국전자인증㈜(“CrossCert”)
(우) 137-725 한국 서울시 서초구 서초대로 320(서초동 1674-4)
하림빌딩 7 층
참조: 인증업무 개발부서– 인증업무준칙
CrossCert 전화: +82-2-3019-5500
CrossCert 팩스: +82-2-3019-5656
sm@crosscert.com

1.5.2 연락 담당자(Contact Person)

CrossCert
Symantec Trust Network Policy Management Authority
인증 정책 관리자/ 보안 과장

CrossCert
(우) 137-725 한국 서울시 서초구 서초대로 320(서초동 1674-4)
하림빌딩 7 층
참조: 인증업무 개발부서– 인증업무준칙
CrossCert 전화: +82-2-3019-5500
CrossCert 팩스: +82-2-3019-5656
sm@crosscert.com

1.5.3 정책에 대한 CP 적정성을 판단하는 자(Person Determining CP Suitability for the Policy)

제 1 조 5 항 2 호에 규정된 기관은, '본 CPS 와 본 CPS 에 종속되거나 보완된 인증업무준칙의 성격상 기타 문서들이 CP 및 본 CPS 에 적합한 것인지'를 판단할 책임을 부담합니다.

1.5.4 CPS 승인 절차(CPS Approval Procedure)

본 CPS 및 후속 개정본들에 대한 승인은 PMA 에 의하여 이루어 집니다. 개정안들은 CPS 의 개정본 양식을 포함한 형식이거나 업데이트 통지 방식으로 작성됩니다. 개정된 버전이나 업데이트 내용은 인터넷 페이지 https://www.crosscert.com/repository/updates 에 위치한 CrossCert 저장소(Repository)의 '인증 업무 업데이트 및 통지(Practices Updates and Notices)' 항목에 링크되어야 합니다. 업데이트 내용은 CPS 의 참조 버전상의 모순 또는 지정된 규정들을 대체합니다.

1.6 정의 및 약어(Definitions and Acronyms)

약어 및 정의에 관한 표와 관련하여 첨부 A 를 참조하시기 바랍니다.

2. 게재 및 저장에 관한 책임 (Publication and Repository Responsibilities)

2.1 저장소(Repositories)

CrossCert 는 자신의 CA 들과 기업 고객들(Managed PKI 또는 ASB 고객들)의 CA 들을 위한 저장소 기능에 대한 책임을 부담합니다. CrossCert 가 최종 사용자 가입자들에게 발급하는 인증서는 CPS 제 2 조 6 항에 따라 저장소에 해당 인증서를 게재합니다.

최종 사용자 가입자의 인증서가 폐기되면, CrossCert 는 저장소에 해당 폐기사항을 게재합니다. CrossCert 는, 본 CPS 규정에 따라 자신의 CA 들 및 서비스 센터 및 기업 고객들의 CA 들을 위하여 자신의 서브 도메인 내에서 CRL 들을 발행합니다. 그리고, CrossCert 는 "온라인 인증서 현황 프로토콜(Online Certificate Status Protocol, "OCSP")" 서비스 계약을 체결한 기업 고객들에게 본 CPS 규정에 따라 OCSP 서비스를 제공합니다.

2.2 인증서 정보의 게재(Publication of Certificate Information)

CrossCert 는 신뢰자들이 인증서 폐기 및 기타 다른 인증서의 현황에 관한 질의를 온라인상에서 할 수 있게 하는 웹 기반 저장소를 유지합니다. CrossCert 는 신뢰자들에게

‘인증서의 현황을 확인할 수 있는 적정한 저장소를 찾는 법과 OCSP 가 가능하다면, 적정한 OCSP 수신자를 찾는 법’에 관한 정보를 제공합니다.

CrossCert 는, 자신의 CA 들과 고객 서비스 센터의 CA 들을 대신하여 그들의 서브 도메인 내에서 발행하는 인증서들을 게재합니다. 최종 사용자 가입자들의 인증서가 폐기되면, CrossCert 는 저장소에 해당 폐기와 관련된 통지를 게재합니다. 그리고, CrossCert 는, 가능하다면, ‘인증서 폐기 목록( )’을 발행하며, 자신의 서브 도메인 내의 자기 CA 들과 서비스 센터의 CA 들에게 OCSP 서비스를 제공합니다.

CrossCert 는 항시 하기 사항의 최신 버전을 게재합니다:

- STN 의 CP
- CrossCert 의 CPS,
- 가입자 계약서(Subscriber Agreements),
- 신뢰자 계약서(Relying Party Agreements)

CrossCert 는, STN 의 서브 도메인 내에서 CrossCert 의 CA 등과 기업 고객의 CA 들이 발행하는 인증서들에 대한 저장소 기능에 대하여 책임을 부담합니다.

CrossCert 는 아래에 설명한 바와 같이 http://www.crosscert.com/repository/의 CrossCert 웹싸이트 저장소 부문에 특정 CA 정보를 게재합니다.

CrossCert 는 CrossCert 의 웹사이트 중 저장소 항목에 STN 의 CP, 본 CPS, 가입자 계약서, 및 신뢰자 계약서를 게재합니다.

CrossCert 는 다음 [표 3]에 따라 인증서를 게재합니다.

인증서 종류(Certificate Type)	***게재 요건(Publication Requirements)***
STN PCA 와 STN 발급 Root CA 인증서	이하에서 설명하는 질의 기능을 통해 최종 사용자 가입자로부터 확보될 수 있는 인증서 체인의 일부분으로서 현행 브라우저 소프트웨어에 포함되어 신뢰자들에게 가용함.
CrossCert 발급 CA 인증서	이하에서 설명하는 질의 기능을 통해 최종 사용자 가입자로부터 확보될 수 있는 인증서 체인의 일부분으로서 신뢰자들에게 가용함.
Managed PKI Lite Certificates 을 지원하는 CrossCert CA 의 인증서와 Managed PKI 고객들의 CA 인증서	*directory.Crosscert.com* 에서 CrossCert LDAP 디렉토리 서버의 질의를 통해 가용함.
시만텍 OCSP 대응자 인증서	*directory.Crosscert.com* 에서 CrossCert LDAP 디렉토리 서버의 질의를 통해 가용함.

인증서 종류(Certificate Type)	*게재 요건(Publication Requirements)*
용도에 따른 클레스 3 인증서에 대한 예외가 있는 최종 사용자 가입자 인증서	선택적으로 https://www.crosscert.com/repository 에 소재한 CrossCert 저장소에 질의 기능을 통해 신뢰자들에게 게재되고 가용하며, directory.verisign.com 에 소재한 CrossCert 저장소에 질의 기능을 통해 가용한 클래스 3 SSL 과 코드 서명 인증서를 제외한 시만텍 LDAP 디렉토리 서버에서의 질의.
Managed PKI 고객들을 통하여 발행된 최종 사용자 가입자 인증서	상기에 나열된 질의 기능을 통하여 가용함, Managed PKI 고객들의 판단에 따라 다르기는 하지만, 인증서는 오직 인증서의 일련 번호를 사용한 검색을 통해서만 접근할 수 있음.

[표 3] – 인증서 게재 요건

2.3 게재 시기 또는 빈도(Time or Frequency of Publication)

본 CPS 에 대한 업데이트는 제 9 조 12 항에 따라 게재됩니다. 가입자 계약서들과 신뢰자 계약서들에 대한 업데이트 사항들은 필요에 따라 이루어 집니다. 인증서는 발행 시마다 게재됩니다. 인증서 현황 정보는 본 CPS 의 규정에 따라 게재됩니다.

2.4 저장소에 대한 접근 통제(Access Controls on Repositories)

CrossCert 웹싸이트의 저장소 부문에 게재된 정보는 일반 공중이 접근할 수 있는 정보입니다. 해당 정보에 대한 열람은 제한이 없습니다. CrossCert 는, 인증서, 인증서 현황 정보, 또는 CRL 들을 접근하기 위한 조건으로서 해당 당사자가 신뢰자 계약서 또는 CRL 사용 계약서에 동의할 것을 필요로 합니다. CrossCert 는, 권한 없는 자들이 저장소 항목을 추가, 삭제 또는 수정하는 것을 예방하기 위한 논리적이고 물리적인 보안 조치를 수행합니다.

3. 식별 및 인증(Identification and Authentication)

3.1 이름(Naming)

STN 의 CP, 본 CPS 또는 전자 서명의 내용에 달리 기재되지 않은 한, 본 CPS 혹은 전자 서명의 내용, STN 하에서 발행된 인증서에 표기된 이름은 인증된 것입니다.

3.1.1 이름의 종류(Type of Names)

STN 이 현재는 시만텍 주식회사 소유입니다만, 기존의 인증서들은 예전 소유자의 명의로 발행이 되었습니다. 기관(O)을 "베리사인 주식회사" 그리고 기관 단위(OU)을 "베리사인 신뢰 네트워크(VeriSign Trust Network)"라고 표기한 기존 인증서들은 각각 "시만텍 주식회사"와 "시만텍 신뢰 네트워크(Symantec Trust Network)"를 의미합니다.

CrossCert CA 인증서는 발행자와 대상 영역에서 X.501 식별명(Distinguished Names)을 포함합니다. CrossCert CA 식별명(Distinguished Names)는 다음 [표 4]에서 특정된 바와 같이 구성되어 있습니다.

속성(Attribute)	***값(Value)***
국가 (C) =	"KR", "US" 또는 사용하지 않음.
기관 (O) =	" 시만텍 주식회사" 또는 CrossCert [5] 또는 <기관명>[6]
기관 단위 (OU) =	CrossCert CA 인증서는 다수의 OU 속성을 포함할 수 있음. 해당 속성은 다음 중 하나 이상을 포함할 수 있음: • 인증기관 이름(CA Name) • 시만텍 신뢰 네트워크(Symantec Trust Network) • 인증서 사용 조건을 규정한 '신뢰자 계약서' 참조를 인용하는 문구 • 저작권 통지 • 인증서 종류를 설명하는 내용.
주 혹은 도 (S) =	사용되지 않음.
지역 (L) =	"인터넷"을 사용하는 '시만텍 상용 소프트웨어 발급 인증기관 (Symantec Commercial Software Publishers CA)'을 제외하면, 사용되지 않음
공통명 (CN) =	본 속성은 인증기관 이름을 포함(인증기관 이름이 OU 속성에 특정되어 있지 않은 경우)되거나, 사용되지 않음.

[표 4]– CA 인증서 상의 식별명 속성(Distinguished Name Attributes in CA Certificates)

최종 사용자 가입자 인증서(End-user Subscriber Certificates)는 대상 이름 영역에서 X.501 식별명을 포함하며 다음 [표 5]에 특정된 바와 같이 구성되어 있습니다.

속성(Attribute)	***값(Value)***
국가 (C) =	"KR" 또는 사용하지 않음.
기관 (O) =	기관 속성은 아래와 같음: • CrossCert OCSP Responder 의 경우, 그리고 기관 연계 (organization affiliation)가 없는 경우 개인용 인증서에 대하여는 선택적으로 "CrossCert". • Subscriber organizational name for 웹 서버 인증서의 경우,

[5] 본 내용에 대한 예외는"RSA Data Security, Inc.,"라고 표시되는 he Secure Server CA 이지만, 현재는 시만텍 CA 임.
[6] CA 고객 조직에 관하여, 구성물 (o=)는 조직의 법적 명칭이어야 함.

속성(Attribute)	*값(Value)*
	그리고 기관 연계(organization affiliation)를 가진 개인용 인증서에 대하여는 가입자 기관의 이름
기관 단위 (OU) =	CrossCert 최종 사용자 가입자 인증서는 다수의 OU 속성을 포함할 수 있음. 해당 속성은 다음 중 하나 이상을 포함할 수 있음:: • (기관용 인증서 및 기관 연계를 가지는 개인용 인증서에 대하여) 가입자 기관의 단위 • 시만텍 신뢰 네트워크(Symantec Trust Network) • 인증서 사용 조건을 규정한 '신뢰자 계약서' 참조를 인용하는 문구 • 저작권 통지 • 에플리캐이션이 시만텍에 의해 인증된 인증서에 "CrossCert 에 의해 인증됨" 그리고 "시만텍 신뢰 네트워크의 구성원" • 클래스 1 개인용 인증서에 대한 "외적 모습(persona)은 유효하지 않음" • 인증서 종류를 설명하는 내용. • (개인에게 발행된 코드 서명 인증서의 경우) "기관 연계되지 않음(No organization affiliation)"
주 혹은 도 (S) =	가입자의 주나 도를 표기함(개인들에게 발행된 인증서 내 영역에는 주(State)는 필요하지 않음).
지역 (L) =	가입자의 지역을 표기함(개인들에게 발행된 인증서 내 영역에는 지역(Locality)은 필요하지 않음)
공통명 (CN) =	본 속성은 다음 사항을 포함함: • (OCSP Responder 인증서의 경우) OCSP Responder 이름 • (웹 서버 인증서의 경우) 도메인 이름 • (code/object 서명 인증서의 경우) 기관 이름 • (개인용 인증서 또는 개인에게 발행된 코드 서명 인증서의 경우) 사람의 이름.
E-Mail 주소 (E) =	클래스 1 개인용 인증서와 일반적으로 MPKI 가입자 인증서의 경우, 이메일(E-mail) 주소

[표 5] – 최종 사용자 가입자 인증서의 식별명 속성(Distinguished Name Attributes in End User Subscriber Certificates)

최종 사용자 가입자 인증서의 식별면 대상의 공통명(Common Name; CN=) 구성은 클래스 2 와 클래스 3 인증서의 경우에 인증 받습니다.

- 기관용 인증서의 대상 식별명에 포함된 '인증된' 공통명 값은 도메인 이름(Secure Server IDs 와 Global Server IDs 의 경우)이거나 기관 또는 기관 내 단위의 법적 이름임.

- 그러나, 클래스 3 기관용 ASB 인증서의 대상 식별명에 포함된 '인증된' 공통명 값은 일반적으로, 기관의 비밀키를 사용할 수 있도록 승인된 기관의 대표자의 개인 명의로 수락되며, 기관(O=)의 구성은 기관의 법적 이름임.
- 개인용 인증서의 대상 식별명에 포함된 공통명 값은, 개인에 대하여 일반적으로 사용되는 사람의 이름으로 표시됨.

3.1.1.1 CABF 명명 요건(CABF Naming Requirements)

도메인 유효 및 기관 유효 SSL 인증서(Domain validated and organization validated SSL Certificates)는 CA / Browser Forum Baseline 요건을 준수합니다.

다음과 같은 명명 속성은 본 CP에 따라 발행된 인증서에 발행자를 포함하기 위하여 사용됩니다:

발행자 *국가이름* (필수)

국가이름(C=) 구성은 필수이며, 발행자의 사업지가 소재한 국가에 대한 ISO 316-1 국가코드 두 글자를 포함합니다.

발행자 *기관이름* (필수)

기관이름(O=) 영역은 필수이며, 발행자 기관이름 (혹은 해당 약어), 상표, 또는 CA 를 정확하게 표기한, CA 에 대한 기타 유의미한 식별자를 포함합니다. 해당 영역(field)은, "루트(Root)"나 "CA1"와 같은 포괄적인 칭호를 포함하지 않아야 합니다.

발행자 *공통명* (선택)

발행자 공통명(CN=) 영역(field)이 있는 경우에는, 반드시 발행하는 CA를 정확하게 특정하는 이름을 포함하여야 합니다.

다음과 같은 명명 속성은 본 CP에 따라 발행되는 인증서에 대상을 포함하기 위하여 사용됩니다:

***대상 대체이름* (필수)**

대상 대체이름 확장자는 필수이며, 최소한 1개의 엔트리를 포함하여야 합니다. 각 엔트리는 '완전히 적정한 도메인 이름(Fully-Qualified Domain Name)'을 포함한 DNS명 또는 서버의 IP주소를 포함한 IP 주소이어야 합니다. CrossCert CA는, '신청자가 완전히 적정한 도메인 이름("FQDN")' 또는 IP 주소를 소유하거나, 도메인 이름 등록기관이나 IP 주소 할당자로부터 해당 사용 권한을 부여받은 자임'을 확인합니다. FQDN들의 와일드 카드(Wildcard)는 허용됩니다.

예약된 IP 주소나 내부 서버 이름을 포함한 대상 대체이름 확장자 또는 대상 공통명 영역을 포함한 인증서 발행 전에, CrossCert CA 는 신청자에게 '인증서 사용은 CA / Browser Forum 에 의하여 만료될 것이고, 해당 업무는 2016 년 10 월까지 사라질 것'이라는 사항을 통지합니다. 또한, 2012 년 7 월 1 일 현재, CrossCert CA 는 IP 주소나 내부 서버 이름을 포함한 *대상 대체이름* 확장자 또는 대상 *공통명* 영역을 포함하는, 유효 만기일이 2015 년 11 월 1 일 이후가 되는, 인증서를 발행하지 않습니다. CrossCert CA 들은, 2016 년 10 월 1 일부터, *대상 대체이름* 확장자 또는 대상 *공통명* 영역이 예약된 IP 주소 또는 내부 서버 이름을 포함하는 '기간이 만료되지 않은' 인증서들 모두를 폐기하여야 합니다.

***국가이름* (선택)**

만약 존재하면, *국가이름*(C=)은 ISO 3166-1 국가 코드의 두 글자로 구성되어야 합니다. 제공되는 경우에는, CrossCert CA 들은, 제 3 조 2 항 2 호에 따라 대상과 관련된 국가를 확인하여야 합니다.

***기관이름* (선택)**

만약 *기관이름*(O=) 영역이 존재하면, 대상의 이름이나 DBA 를 포함하며, 필요한 주소 영역은 제 3 조 2 항 2 호에 따라 확인된 대상의 위치를 포함합니다.

만일 대상이 자연인인 경우에는, 개인에 대한 대상 이름(예를 들어, 성과 이름) 속성이 애플리케이션 소프트웨어에 광범위하게 지원되지 않으므로, 인증기관(CA)은 *기관이름* 영역을 대상의 이름이나 DBA(제 3 조 2 항 2 호 1 목 *개인 신청자에 대한 확인*. 참조)를 포함하기 위하여 사용할 수 있습니다.

CA가, 공통변수나 약어들과 같이, 영역(fields)에 사소한 차이가 있다고 간주하는 경우에는, CA는 해당 차이를 문서화하고 기관 이름(예를 들어, 공식 기록이 "회사명칭 incorporated"라고 표기되었으면, CA는 "회사 명칭 Inc."로 포함할 수 있음)을 약칭할 때에는 현지에서 수용될 수 있는 약어들을 사용하여야 합니다. *기관이름* 영역은 확인된 DBA나 대상의 상호명을 포함할 수 있습니다.

만일 *기관이름*이 존재하면, *지역이름*, *주혹은도이름* (필요시), 그리고 *국가이름*도 필요로 하며, *국가이름*에는 *거리주소*과 *우편번호*도 선택사항입니다. 만일 *기관이름*이 없는 경우에는, 인증서에는 *거리주소*, *지역이름*, *주혹은도이름*, 또는 *우편번호* 속성은 포함하지 않습니다. CA 는 상기의 *국가이름* 요건에 따라 다른 대상 정체 정보를 포함하지 않고 대상의 *국가이름* 영역을 포함할 수 있습니다.

***기관단위이름* (선택)**

기관단위(OU=) 구성이 제시될 때에는, CA 에 의하여 확인되지 않은 정보를 포함할 수 있습니다. '.', '-', 와 ' ' (즉, 빈 공간 표식) 문자 및/또는 기타 가치가 없거나 미완성 또는 적용불가의 표시로 된 것과 같은, 일체의 메타데이터(metadata)는 사용되지 않습니다.

CrossCert 는, 자신이 '해당 정보가 제 3 조 2 항 2 호에 따른 것임'을 확인하고 '해당 인증서가 제 3 조 2 항 2 호에 따라 대상:*기관이름*, 대상:*지역이름*, 대상:*지역이름* 및 대상: *국가이름* 속성도 포함함'을 확인하지 않은 한, OU 속성이 이름, DBA, 상호, 상표, 주소, 위치, 혹은 특정의 자연인이나 법적 개체를 언급하는 기타 내용(text)을 포함하지 못하게 하는 절차를 수행합니다.

OU 값이 요청서에 제출된 경우에는, 해당 값은 제 3 조 2 항 2 호 1 목 *고위험 요청* 조항에 나열된 다양한 고위험 목록의 확인 대상입니다. 만일 해당항목이 발견되면, 해당 값은 '정확하고 오해를 일으키는 것이 아닌지'를 RA 에 의하여 검토 받습니다. 만일 OU 값이 법적 개체의 이름을 표시하면, 해당 값은 제 3 조 2 항 2 호 1 목 *국가이름 및 기타 개체 정보를 구성하는 대상 개체의 확인* 조항에 따라 확인됩니다.

***공통명* (선택)**

공통명(CN=) 구성은 없어지게 됩니다 (사용이 권고되지 않는다는 것이며, 금지되는 것을 의미하는 건 아닙니다). 만일 제시되는 경우에는, *공통명*에는 인증서의 *대상대체이름* 확장자에 포함된 값 중의 하나인 FQDN 또는 단일 IP 주소를 포함합니다.

***도메인구성* (선택)**

도메인구성(dc=) 포함은 선택입니다. 만일 제시되는 경우에는, *도메인구성*은 대상의 등록된 도메인 이름의 모든 구성을 포함하며, 가장 중요한 구성과, 기본 이름에 가장 근접한 순서대로 끝까지 포함합니다.

기타 대상 속성(Other Subject Attributes)

선택 속성이 대상영역에 존재하는 경우에는, CA 에 의하여 확인된 정보를 포함하여야 합니다. '.', '-', 와 ' ' (즉, 빈 공간 표식) 문자 및/또는 기타 가치가 없거나 미완성 또는 적용불가의 표시로 된 것과 같은, 일체의 메타데이터(metadata)는 사용되지 않습니다.

CrossCert는, 상기와 같이 *대상대체이름* 및 *공통명*에 특정된 바를 제외하고, 대상 속성에 FQDN을 포함하지 않습니다.

3.1.2 유의미한 이름의 필요성(Need for Names to be Meaningful)

클래스 2와 클래스 3 최종 사용자 인증서는, '인증서의 대상이 개인인지 기관인지'에 대한 개체 판단을 허용하는 (일반적으로 이해되는) 의미를 가진 이름들을 포함합니다.

CrossCert CA 인증서는, '인증서의 대상인 CA의 개체 판단을 허용하는 (일반적으로 이해되는) 의미를 가진 이름들을 포함합니다.

3.1.3 가입자의 익명성(Anonymity or Pseudonymity of Subscribers)

클래스 1 개인 가입자의 신원은 인증 받지 않습니다. 클래스 1 가입자는 필명을 사용할 수도 있습니다. 특정한 최종 사용자 가입자들(예를 들어, 미성년자, 혹은 민감한 정부 공무원 관련 정보)의 신원을 보호하기 위한 정부나 국가기관의 요구가 있거나 법규에서 요구하지 않는 한, 클래스 2 및 클래스 3 가입자는 필명(가입자의 진정한 개인 이름이나 기관의 실명 이외의 이름)을 사용할 수 없습니다. 인증서에 익명을 요청하는 사안은 PMA 에 의하여 사안별로 심사될 것이며, 만일 허용된다면, 해당 인증서는 '신원은 인증되었으나, 보호받지는 않는다'는 것을 표기할 것입니다.

3.1.4 다양한 이름 양식 해석 규칙(Rules for Interpreting Various Name Forms)

해당 규정 없습니다.

3.1.5 이름의 유일성(Uniqueness of Names)

CrossCert 는, '가입자의 대상 식별이름(DN)이 가입자 등록 절차에서 자동화된 구성을 통해 특정 CA 의 도메인 내에서 유일한 것임'을 확실히 하여야 합니다. 가입자가 동일한 대상 식별이름을 가지는 두 개 혹은 그 이상의 인증서들을 가지는 것은 가능합니다.

3.1.6 인식, 인증, 및 상표의 역할(Recognition, Authentication, and Role of Trademarks)

인증서 신청자는, 자신들의 인증서 신청 중인 이름들을 '타인의 지적재산권을 위반하는 데' 사용하여서는 아니 됩니다. 그러나, CrossCert 는, '인증서 신청자가 인증서 신청에 표시된 이름에 대한 지적재산권을 가지고 있는지' 또는 '도메인 이름, 상호, 상표나 서비스표의 소유권과 관련된 일체의 분쟁을 해결, 중재, 또는 화해했는지'에 관하여 확인하지는 않습니다. CrossCert 는, 인증서 신청자에 대한 어떠한 책임도 부담하지 않은 채, 앞서 언급한 (지적재산권) 분쟁을 이유로 해당 인증서 신청을 거절 혹은 중단을 할 수 있습니다.

3.2 최초의 신원 확인(Initial Identity Validation)

3.2.1 개인키 보유 증명 방법(Method to Prove Possession of Private Key)

인증서 신청자는, '인증서에 나열된 공동키에 대응하는 개인키를 정당하게 보유하고 있음'을 설명하여야 합니다. 개인키 보유 입증 방법은 PKCS 10 호, 기타 암호학적으로 이와 동등한 설명, 또는 CrossCert 이 승인하고 시만텍이 승인한 방법에 따라야 합니다. 본 요건은 가입자를 위하여 CA 에 의하여 키 쌍이 발행된 경우에는, 예를 들어, 스마트 카드에 미리 발행된 키들이 배치되어 있는 경우, 적용되지 않습니다.

3.2.2 기관 정체의 인증(Authentication of Organization identity)

인증서가 기관의 이름을 포함하는 경우에는 항상, CrossCert 의 문서화된 유효 절차(Validation Procedures)에 규정된 절차에 따라 기관의 정체 및 인증서 신청자가 제공한 기타 등록정보(확인되지 않은 가입자 정보는 제외)가 확인됩니다.

최소한, CrossCert 는 다음사항을 이행하여야 합니다:

- '최소한 한 곳의 제 3 자 신원 확인 서비스 혹은 데이터베이스를 활용하여 해당 기관이 존재하는 지'를 판단하거나, 이를 대체하는 방안으로, '해당 기관의 존재를 확인하는 관련 정부기관이나 관할 기관에 의해 발급되거나 등재된 기관의 자료를 확인'함,
- 전화, 확인 우편이나 이와 유사한 절차로, 인증서 신청자에게 기관에 대한 특정 정보를 확인하고, 해당 기관이 인증서 신청 권한을 부여했는지도 확인하며, 인증서 신청자를 대신하여 신청서를 제출한 사람이 해당 권한을 부여받았는 지도 확인함. 인증서가 기관의 권한있는 대표로서 개인 이름을 포함하고 있는 경우에는, 해당 사람의 고용 여부와 해당 기관을 대신한 권한의 유무도 확인되어야 함.

인증서에 도메인 이름이나 e-mail 주소가 포함된 경우에는, CrossCert는 '도메인 이름을 전체를 사용할 권한이 있는 도메인 이름인지 혹은 e-mail 도메인으로만 사용할 수 있는 것인지'에 대한 기관의 권리를 인증합니다.

필요한 경우에는, CrossCert는 미국 산업과학부(United States Department of Commerce Bureau of Industry and Science: "BIS")에 의해 발효된 수출입규제 관련 법규를 충족하는 지 여부를 추가로 확인할 수 있습니다.

다음 [표 6]에서 특정 인증서에 대하여 추가적으로 필요한 절차를 설명합니다.

인증서 종류(Certificate Type)	***추가 절차(Additional Procedures)***
하드웨어 보호 SSL 인증서	시만텍은 '키 쌍이 FIPS 140 인증 하드웨어에서 생성 되었는지'를 확인함.
인트라넷 SSL 인증서를 위한 Managed PKI	시만텍은 '장치에 할당된 호스트 이름 혹은 IP 주소가 (공개적)인터넷에서 접근할 수 없으며 인증서 가입자의

인증서 종류(Certificate Type)	*추가 절차(Additional Procedures)*
	소유임'을 확인함.
인증된 컨텐츠 서명 인증서	시만텍이 전자적으로 ACS 를 사용하여 컨텐츠에 서명을 하기 전에, '해당 컨텐츠가 원래 코드 서명 인증서에 의해 서명된 컨텐츠임'을 확인함.

[표 6] 특정 인증 절차(Specific Authentication Procedures)

3.2.2.1 기관 신청자들에 대한 CABF 인증 요건(CABF Verification Requirements for Organization Applicants)

도메인 유효 및 기관 유효 SSL 인증서(Domain validated and organization validated SSL Certificates)는 CA / Browser Forum Baseline 요건을 준수합니다.

도메인 이름 등록자 인증(Authorization of Domain Name Registrant)

CrossCert CA들은, '인증서가 발행되는 날 현재, 신청자는 인증서에 기재된 IP 주소와 도메인 이름 전체에 유효한(FQDN) 사용권 내지 통제권한을 가지고 있거나, 해당 권리자로부터 완전 유효한 도메인 이름(FQDN)과 IP 주소를 포함한 인증서를 확보할 해당 권한을 (예를 들어, 대리권자 혹은 라이선스 권한 관계) 부여 받은 자임'을 확인하여야 합니다.

만일 CA가 '도메인 이름 등록기관(Domain Name Registrar)'으로부터 해당 등록 도메인 이름의 사용 통제 권한을 확인한 바에 의존하였고, 최상위 단계 도메인이 2 문자 국가코드(ccTLD)이면, 해당 CA는 '도메인 이름 등록기관(Domain Name Registrar)'으로부터 직접 ccTLD 규정이 적용되는 도메인 이름 단계에 대한 확인을 받아야 합니다. 예를 들어, 요청 받은 FQDN이 www.mysite.users.example.co.uk이라면, 해당 CA는 도메인 이름 ".co.uk"의 등록기관으로부터 확인을 받아야 합니다. 왜냐하면, 도메인 이름의 신청은 .uk 등록기관의 규정에 따라 ".co.uk"가 바로 종속되기 때문입니다.

만일 CA가 '신청자가 요청한 FQDN에 대한 인증서를 수령하기 위하여 도메인 이름 등록기관으로부터 승인을 받았는지'를 확인하기 위하여 인터넷 메일 시스템을 이용한 경우에는, 해당 CA는 아래와 같은 방식들 중 하나로 구성된 메일 시스템 주소를 이용하여야 합니다:

1. 도메인 이름 등록기관에 의해 제공받은 것;
2. 도메인의 WHOIS 기록에 나타난 대로, 도메인 이름 등록기관의 "등록자", "기술" 또는 "행정" 연락 정보; 또는;
3. 다음과 같이 도메인 이름에 대하여 미리 정지된 로컬 파트에 의함:

a. 로컬 파트(Local part) – 다음 중 하나: ‘행정’, ‘행정담당자’, ‘웹마스터’, ‘호스트마스터’, 또는 ‘포스트마스터’; 그리고
b. 도메인 이름 – 등록된 도메인 이름이나 신청된 ‘완전 유효한 도메인 이름(FQDN)’에서 영(0) 이나 이상의 구성을 정리함으로써 형성됨

만일 도메인 이름 등록기관이 개별적, 익명의, 대리 등록 서비스를 활용하였고, 해당 CA가 ‘전술한 바의 대체방안으로 수행한 도메인 인증(Domain Authorization)에 의존하였다면, 해당 도메인 인증은 반드시 등록 도메인 이름에 관한 WHOIS 기록에 명시된 ‘개별적, 익명의, 또는 대리 등록 서비스’로부터 직접 받아야 합니다. 해당 서류는 반드시 ‘개별적, 익명의, 혹은 대리 등록 서비스 공급자’의 서신 문두 표식(letterhead)이 있어야 하며, 총괄 관리자 또는 이와 동등한 권한자 임원의 서명, 인증서 신청일자, 그리고 인증서에 포함된 ‘완전히 유효한 도메인 이름(FQDN)’이 포함되어야 합니다.

WHOIS 기록이 도메인 이름 등록기관으로 ‘개별적, 익명의 혹은 대리 등록 서비스 공급자’를 특정한 경우에는, 도메인 인증(Domain Authorization)에는 반드시 “신청자에게 ‘인증서에 완전히 유효한 도메인 이름(FQDN)’을 사용할 권리를 부여한다”는 문구를 포함하여야 합니다. 해당 CA는 믿을 수 있는 제3자 독립기관의 정보원으로부터 수령한 연락 정보를 이용하여, 직접 ‘개별적, 익명의 혹은 대리 등록 서비스 공급자’에게 연락하여, ‘도메인 인증이 진정함’을 도메인 이름 등록기관으로부터 확인 받아야 합니다.

국가이름으로만 구성된 대상자 신원 인증(Verification of Subject Identity comprised of only Country Name)

신청자가, ‘오직 *국가이름* 영역으로만 구성된 대상자 신원 정보를 포함할 인증서를 요청하는 경우에는, 해당 CA는 다음 사항들 중 하나를 이용하여 대상자와 관련된 국가를 확인하여야 합니다:

a) 아래 둘 중 하나로 국가별로 할당된 IP 주소
   (i) 해당 웹싸이트에 대한 DNS 기록에 표기된 해당 웹싸이트의 IP 주소, 또는
   (ii) 신청자의 IP 주소;
b) 요청된 도메인 이름의 2 문자 국가 코드(ccTLD);
c) 도메인 이름 등록기관에 의해 제공된 정보; 또는
d) *“국가이름 및 기타 신원 정보로 구성된 대상자 신원 인증*(*Verification of Subject Identity comprised of Country Name and other Identity Information)”* 부문에 표기된 방법.

해당 CA는, 신청자가 실제로 소재하는 곳 이외의 나라들에 할당된 IP 주소에 의존하는 것을 예방하기 위하여 대리 서버들을 선별하는 절차를 수행하여야 합니다.

국가이름 및 기타 신원 정보로 구성된 대상자 신원 인증(Verification of Subject Identity comprised of Country Name and other Identity information)

신청자가 국가이름 영역과 기타 대상자 신원 정보를 포함할 인증서를 요청하면, 해당 CA는 해당 신청자의 신원을 인증하여야 하며, 다음과 같은 요건들을 충족하는 인증 절차를 활용하여 신청자 대표의 인증서 신청의 진정성을 확인하여야 합니다. 해당 CA는 본 조항에 근거하여 서류상의 변조 혹은 위조사항을 검사하여야 합니다.

A. 이름 혹은 주소 정체 확인 옵션(Name or Address Identity Verification Option)

만일 대상자의 신원정보가 기관의 주소 혹은 이름에 포함되는 경우에는, 해당 CA는 기관의 정체와 주소를 확인하고, 해당 주소가 신청자가 존속하거나 운영중인 곳인지 확인하여야 합니다. 해당 CA는 다음 사항 중 하나에 대한 의사소통을 통하거나, 서면 제공을 받아서 신청자의 신원과 주소를 확인하여야 합니다:

1) 신청자의 법적 설립지, 소재지 혹은 인지된 법정 관할지의 정부기관(예를 들어, 국무부);
2). 정기적으로 업데이트되는 외부 제3자의 데이터베이스(예를 들어, Dun & Bradstreet 데이터베이스)로, CrossCert가 (이하) 데이터 소스 정확성에 따라 평가한 곳;
3). CrossCert CA나 해당 CA를 위해 활동하는 대리인 제3자가 현장 방문; 또는
4) 공증서.

해당 CA는 신청자의 신원과 주소를 확인하기 위하여 상기 1항부터 4항까지 설명된 서면이나 의사소통을 활용할 수 있습니다.

해당 CA는 상기를 대체하는 방안으로, 가스, 전기 등 이용료 청구서, 은행 잔고증명서, 신용카드 청구서, 정부 발행 세금 청구서, 기타 데이터 소스 정확도(Data Source Accuracy)의 요건을 충족하는 양식의 신원확인 서면을 이용하여 신청자의 주소(신청자의 신원 제외)를 확인할 수 있습니다.

B. DBA/상표 정체 확인 옵션(DBA/Tradename Identity Verification Option)

대상자 신원 정보가 DBA나 상표를 포함하는 경우에는, 해당 CA는 최소한 다음 사항들 중 하나를 이용하여 신청자의 DBA/상표 사용 권한을 확인하여야 합니다:

1. 신청자의 법적 설립지, 소재지 혹은 인지된 법정 관할지의 정부기관과의 의사소통이나 제공받은 서면;
2. '데이터 소스 정확도(Data Source Accuracy)'의 요건을 충족하는, 제3자 정보원으로부터 제공받은 의사소통이나 서면;
3. 해당 DBA들이나 상표들을 관리하는 책임이 있는 정부기관과의 의사소통;
4. '데이터 소스 정확도(Data Source Accuracy)'의 요건을 충족함을 증명하는 서류를 동반한 공증서류; 또는,
5. 가스, 전기 등 이용료 청구서, 은행 잔고증명서, 신용카드 청구서, 정부 발행 세금 청구서, 기타 데이터 소스 정확도(Data Source Accuracy)의 요건을 충족하는 양식의 서류.

신뢰할 수 있는 의사소통 수단(Reliable Method of Communication)

대상자 신원 정보가 포함된 인증서 신청자가 기관(organization)인 경우, CrossCert는 신청자의 대표자의 인증서 요청에 대한 진정성을 확인하기 위하여 '신뢰할 수 있는 의사소통 수단(Reliable Method of Communication)'을 활용합니다: email, 우편 서비스 및 전화 포함.

해당 CA는 신뢰할 수 있는 의사소통 수단을 확인하기 위하여 이름 또는 주소 정체 확인을 위해 (상기) 나열된 정보원(source)들을 활용할 수 있습니다. 단, 해당 CA는 신뢰할 수 있는 의사소통 수단을 사용하여, 신청자 대표자 또는 신청자 기관의 권한 있는 자로부터 직접, 예를 들어, 신청자의 사무소, 기업 사무소, 인사과 사무소, 정보기술 사무소 또는 CA가 적정하다고 판단하는 해당 부서를 통하여, 인증서 신청의 진정성을 확인할 수 있습니다.

또한, 해당 CA는 신청자가 인증서를 요구하는 개인들을 특정할 수 있도록 허용하는 절차를 보유합니다. 신청자가 서면으로 '인증서를 요청하는 개인들'을 특정하면, 해당 CA는 해당 특정된 자들 이외에는 인증서 요청을 수락하지 않아야 합니다. 해당 CA는, 신청자의 인증된 서면 요청에 따라 신청자에게 공인된 '인증서 요청자들 목록'을 제공하여야 합니다.

개인 신청자 확인(Verification of Individual Applicant)

신청자가 자연인이면, CrossCert CA는 신청자의 이름, 신청자의 주소, 및 인증서 신청의 진정성(제3조1항1호1목 기관명 또한 참조)을 확인하여야 합니다.

해당 CA는, 또렷한 사본을 이용하여 신청자의 이름을 확인하여야 하고, 정부 발행 ID들(여권, 운전면허증, 군인신분증, 주민등록증, 기타 동등한 증명서) 중에 하나에서 신청자의 얼굴이 확연히 보여져야 합니다. 해당 CA는 해당 사본들의 위변조 여부를 검사하여야 합니다.

해당 CA는, 정부 신분증, 각종 사용료 청구서, 혹은 은행 잔고증명서나 신용카드 청구서 등, 데이터 소스 정확도(Data Source Accuracy)의 요건을 충족하는 양식의 신원확인 양식을 이용하여 신청자의 주소를 확인하여야 합니다. 해당 CA는 신청자의 이름을 확인하기 위하여 사용된 동일한 '정부 발행 신분증'에 의존할 수 있습니다.

해당 CA는 '신뢰할 수 있는 의사소통 수단'을 활용하여 신청자의 인증서 신청을 확인하여야 합니다.

인증서 데이터의 연령(Age of Certificate Data)

CA는, 인증서 발행 전 39 개월 이상 된 데이터나 서류인 경우에는, 인증서 요청을 유효하게 하는 데이터나 서류로 활용하지 말아야 합니다.

거부 목록(Denied List)

해당 CA는 (본 CPS 제5조2항2호) 서류 보유 요건에 따라, 피싱 혐의를 받았거나 기타 다른 사위적 이용 등의 이유로 인하여 예전에 폐기된 인증서들과 예전에 거부된 인증서 요청들에 관한 모든 내부 데이터베이스를, 최소 7 년간 보유하고 있어야 합니다.

CA는 본 정보를 추후의 의심스러운 인증서 요청들을 확인하기 위하여 사용하여야 합니다.

고위험 요청(High Risk Requests)

CrossCert는 고위험 인증서 요청들을 확인하여야 하며, 그에 대한 추가적인 확인활동을 하여야 하고, 해당 요청이 본 요건들에 적정하게 확인이 될 수 있도록 합리적으로 필요한 범위에서 추가적인 주의를 하여야 합니다.

CA는, 피싱에서 일반적으로 대상이 되는 적정 목록을 확인하고, 기타 사기적인 행태들에 대한 확인을 하고, 발행 전 검토하여야 하는 목록을 인증서 요청 사항에 자동적으로 확임함으로써 고위험 요청을 확인할 수 있습니다. 앞서 언급한 목록은, 예전에 폐기된 인증서를 포함한 CA에 의해 보유된 내부 데이터베이스 목록과 피싱 혐의를 받거나 사기적 사용을 이유로 예전에 거절되었던 인증서 요청들을 포함합니다.

CA는, CA의 고위험 분류에 의하여 확인된 정보를 '의심스러운 인증서 요청들'을 표시하는데 사용하여야 합니다. CA는, 의심스럽거나 고위험으로 표시된 인증서 요청사항들에 대하여 추가적인 확인을 위하여 문서화된 절차를 준수하여야 합니다.

데이터 소스 정확도(Data Source Accuracy)

대상자 신원 정보를 확인하기 위한 데이터 소스에 의존하기 전에, 해당 CA는 데이터 소스의 정확도와 신뢰도를 평가하여야 합니다. CA는, '데이터 소스가 합리적으로 정확하거나 믿을만하다'고 판단하지 않는 경우에는, 대상자 신원 정보를 확인하기 위하여 데이터 소스를 활용하지 말아야 합니다.

3.2.3 개인 신원의 인증(Authentication of Individual Identity)

개인 신원의 인증은 인증서의 클래스에 따라 다릅니다. STN 인증서의 각 클래스별 최소한의 인증기준은 아래 [표 7]에서 설명합니다.

인증서 클래스 (Certificate Class)	신원 인증(Authentication of Identity)
클래스 1	신원 인증 없음. 가입자에게 이메일을 보내서 가입자로 하여금 답변을 하게 하는, 제한적인 이메일 확인을 받음.
클래스 2	가입자로부터 제공받은 신원과 다음 정보를 대응하여 신원을 인증함: ○ 주요 신용기관이나 기타 신뢰할만한 정보 제공자들과 같이, CrossCert 가 인정하는 신원 확인 서비스의 데이터베이스에 보관된 정보, 또는 ○ 연계된 개인들에게 등록기관이 승인하는 인증서에 포함된 사업 정보(직원이나 고객 디렉토리)의 사업 기록이나 데이터베이스에 포함된 정보
클래스 3	클래스 3 개인용 인증서의 신원 확인은 인증서 신청자의 CA 나 RA 의 에이전트에

인증서 클래스 (Certificate Class)	신원 인증(Authentication of Identity)
	직접 출석하거나, 공증인 앞에 출석하거나, 인증서 신청자의 법적 관할지에서 이와 유사한 권한을 가진 공무원 앞으로 출석함을 기반으로 합니다. 에이전트, 공증인 또는 기타 공무원은 인증서 신청자의 신원을 '인지도가 높은 정부 발행 사진이 포함된 신분증', 예를 들어, 여권, 운전면허증, 및 기타 신뢰할만한 신분증,을 통하여 확인하여야 합니다. 클래스 3 행정 담당자 인증서의 인증은 기관에 대한 인증과 행정 담당자로 활동하는 자의 인증에 대한 기관의 확인을 근거로 이루어 집니다. CrossCert는 그들 자신의 행정 담당자들에 대한 인증서 신청을 승인할 수 있습니다. 행정 담당자들은 기관 내에서 "신뢰받는 사람들"입니다. 이러한 경우, 그들의 인증서 신청에 대한 인증은 그들의 고용관계 또는 계약관계 및 배경을 확인하는 절차에 근거하여 이루어 져야 합니다[7].

[표 7] 개인 신원의 인증(Authentication of individual identity)

3.2.4 미확인 가입자 정보(Non-Verified Subscriber information)

미확인 가입자 정보는 아래 사항을 포함한다:

- 몇 가지 예외[8]를 포함한 기관 단위(OU)
- 클래스 1 인증서 내 가입자의 이름
- 인증서에 미확인된 것으로 지정된 기타 다른 정보.

3.2.5 권한의 발효(Validation of Authority)

개인의 이름이 기관의 이름과 '개인적 연계나 기관을 대신하여 활동할 수 있는 권한을 표시한 방식으로 인증서에 포함되는 경우에는 언제나, CrossCert나 RA는:

---

7 CrossCert는 행정 담당 인증서를 사람이 아닌 수령자에게 승인할 수 있으며, 이에는 장치, 서버 인증 클래스 3 행정 담당자 인증서 신청과 관련되어 있으며, 다음을 포함함:

• 인증서 신청에 행정 담당자로 서비스 명칭이 명명되고 존재가 인증됨

• 행정 기능 수행에 일관된 방식으로 서비스가 안전하게 실행되는 인증

• 행정 담당자 인증서 등록자의 신원과 권한이 확인됨

8 도메인 유효화되고 기관 유효화된 인증서는 유효한 기관 단위 값을 가질 수 있음

- ‘기관이 존재하는 지’를 최소한 하나의 제 3 자 신원 확인 서비스 또는 데이터베이스, 혹은 대체방안으로, 해당 기관이 존재함을 확인하는 관련 정부기관이 발행하거나 등재된 기관 서류를 통하여 판단하며, 그리고
- RA 가 승인하는 인증서의 사업 정보(직원 또는 고객 디렉토리)의 데이터베이스나 사업 기록에 포함된 정보를 이용하거나, 전화, 수신확인 우편, 또는 이와 비교되는 절차로 기관에 해당 개인이 고용되어 있는지, 해당 신청자가 기관을 대신하여 신청할 권한이 있는 지를 확인함.

3.2.6 상호 운영 기준(Criteria for Interoperation)

CrossCert 는, STN CA 가 아닌 자가 일방적으로 해당 CA 를 인증함으로써 STN 과 상호 운영할 수 있도록 하는 상호운영 서비스를 제공할 수 있습니다. 이러한 방식으로 상호 운영될 수 있는 CA 들은, 필요 시마다 추가적으로 개정, 보완되는 STN CP 를 준수하여야 합니다.

CrossCert 는, 최소한 CA 가 다음 사항을 이행하는 경우에만 STN CA 가 아닌 자가 STN 과 상호 운영을 할 수 있도록 허락하여야 합니다:

- CrossCert 와 별도의 계약을 체결함
- 발행될 인증서에 대한 STN 요건들을 충족하는 CPS 하에서 운영됨
- 상호 운영되기 전에 준수 심사를 통과함
- 상호 운영에 대한 계속적인 자격에 대한 연례 심사를 통과함.

3.3 *키 교체 요청에 대한 신원확인과 인증(Identification and Authentication for Re-key Requests)*

가입자의 현재 인증서가 만료되기 전에, 가입자는 인증서의 계속 사용을 위하여 새로운 인증서를 확보할 필요가 있습니다. CrossCert 는 일반적으로, ‘가입자가 유효기간이 만료되는 키 쌍을 대체하기 이한 새로운 키 쌍을 생성할 것(기술상으로 “키교체”로 정의함)’을 요구합니다. 그러나, 어떤 경우에는(즉, 웹서버 인증서), 가입자들은 현존하는 키 쌍에 대하여 새로운 인증서를 요청(기술상으로 “갱신”이라 정의함)할 수도 있습니다.

일반적으로는, “키교체(Rekey)” 와 “갱신(Renewal)”은 모두 ‘예전 인증서는 새로운 인증서로 교체된다’ 사실에 초점을 두며, 새로운 키 쌍이 생성되었는지 아닌지에 대한 강조는 하지 않은 채, “인증서 갱신”이라고 일반적으로 설명됩니다. CrossCert 인증서들은 클래스 3 서버 인증서를 제외하면, 모든 클래스와 종류의 인증서에 CrossCert 의 최종 사용자 가입자 인증서 교체 절차의 일부분으로서 새로운 키 쌍이 항상 생성되므로, 이러한 구분은 중요하지 않습니다. 그러나, 클래스 3 서버 인증서에 대하여는, 가입자 키 쌍이 웹서버에서 생성되고

대부분의 웹서버 키 생성 도구가 현존하는 키 쌍에 대하여 새로운 인증서 요청을 하도록 허용하므로, “키교체(Rekey)” 와 “갱신(Renewal)” 사이의 구분이 있습니다.

3.3.1 통상적인 키교체에 대한 신원 확인과 인증(Identification and Authentication for Routine Re-key)

키교체 절차는, 최종 사용자 가입자 인증서의 키교체를 하고자 하는 사람 혹은 기관이 ‘사실상 인증서의 가입자인가’를 확실히 하는 것입니다.

수용 가능한 절차 하나는, 챌린지 문구를 이용하거나, ‘개인키를 보유하고 있음’을 증명하는 것을 통하여 이루어 집니다. 인증서의 갱신에 대하여는, ‘가입자가 올바르게 가입자의 재등록 정보와 함께 챌린지 문구(Challenge Phrase)(또는 이와 동등한 것)를 제출한 경우’이고, 등록정보(기업 및 기술 연락처 정보 포함)가 변경되지 않은 경우라면, 갱신된 인증서는 자동적으로 발행됩니다. 챌린지 문구(Challenge Phrase)(또는 이와 동등한 것)를 이용하는 것에 대한 대체방안으로, 시만텍은 인증서갱신을 위한 연락처로 확인된 연락처로 e-mail 을 송부하여 ‘인증서 갱신 주문과 인증서 발행 권한을 요구하는 지’를 확인할 수 있습니다. 인증서 발행을 승인하는 확인을 수령하면, 시만텍은 등록 정보(기업 및 기술 연락처 정보[9] 포함)가 변경되지 않았다면, 인증서를 발행합니다.

이러한 방식의 키교체나 갱신이 있은 후, 그리고 이후의 키교체와 갱신의 대체가 있은 후에는, CrossCert 나 RA 는 ‘원래의 인증서 신청상의 인증 요건들[10]과 신원확인 요건에 따라’ 가입자의 신원을 재확인합니다.

특히, 리테일 클래스 3 기관용 인증서에 대하여는 www.crosscert.com 을 통해서 CrossCert 는 제 6 조 3 항 2 호에 규정된 간격으로 인증서에 포함된 기관의 이름 및 도메인 이름을 다시 인증합니다. 만일, 다음과 같은 상황이라면:

- 챌린지 문구가 후속 인증서 갱신에 올바르게 사용되며:
- 인증서 식별이름이 변경되지 않았고.
- 기업 및 기술 연락처 정보가 예전에 인증된 내용과 변함이 없으면,

CrossCert 는 전화, 수신 확인 우편이나 이와 비교되는 절차로, 인증서 신청자에게 기관에 관한 일정한 정보, 기관이 인증서 신청을 위임했는지, 인증서 신청을 제출한 자가 인증서 신청을 할 수 있는 권한을 위임 받았는지를 재확인할 필요가 없습니다.

---

[9] 연락처 정보가 공식적인 변경절차에 따라 승인되어 변경된 경우에는, 인증서는 여전히 자동 갱신될 수 있음

[10] 그러나, 클래스 3 기관용 ASB 인증서에 대한 인증 요청은, 챌린지 문구 사용과 원 인증서 신청을 위하여 사용한 동일한 신원과 인증 확인이 필요함.

인증서 만료일로부터 30 일 후의 키교체는 원래의 인증서 신청으로 재인증되며, 자동적으로 발행되지는 않습니다.

3.3.2 폐지 후 키교체를 위한 신원확인과 인증(Identification and Authentication for Re-key After Revocation)

다음 이유로 폐지되었으면, 폐지 후 키교체/갱신은 허용되지 않습니다:

- (클래스 1 인증서 이외의) 인증서가 인증서의 대상으로 명명된 자 이외의 사람에게 발행되었음, 또는
- (클래스 1 인증서 이외의) 인증서가 해당 인증서의 대상자로 명명된 사람이나 개체의 권한 위임 없이 발행되었음, 또는
- 가입자의 인증서 신청을 승인하는 개체가 '인증서 신청 중의 중대한 사실이 거짓임'을 발견하거나, 이를 믿을만한 이유가 있음.
- STN 을 보호하기 위하여 시만텍이나 CrossCert 가 필요하다고 판단하는 기타 이유가 있음.

상기 문단의 내용에 따라, 인증서의 폐지 후에 CA 인증서 또는 기관용 인증서의 갱신은 '기관 혹은 CA 가 요구하는 갱신이 사실상 인증서의 가입자임'을 확실히 하는 갱신 절차임을 확인하는 한, 허용됩니다. 갱신된 기관용 인증서는 갱신된 기관용 인증서의 식별 이름 대상자의 이름과 동일한 대상자 식별이름을 포함합니다.

폐지 후의 개인용 인증서에 대한 갱신은, '갱신을 요구하는 자가, 사실상, 가입자임'을 확실히 하여야 합니다. 수용 가능한 한 절차로는, 챌린지 문구(Challenge Phrase)(또는 이와 동등한 것)을 이용하는 것입니다. 이러한 절차 또는 CrossCert 가 승인한 절차 이외에는, 원래의 인증서 신청에 대한 신원확인과 인증 요건은 폐지 후의 인증서 갱신에 활용되어야 합니다.

3.4 폐지 요청에 대한 신원확인과 인증(Identification and Authentication for Revocation Request)

인증서의 폐지 전에, CrossCert 는 '인증서의 가입자에 의하여 폐지가 요청되었으며, 해당 개체는 인증서 신청을 승인하였다'는 것을 확인합니다.

가입자의 폐지 요청을 인증하기 위한 수용 가능한 절차로는 다음을 포함합니다:

- 특정 인증서 종류의 경우에는 가입자의 챌린지 문구(또는 이와 동등한 것)를 제출하도록 하고, 기록상 챌린지 문구(또는 이와 동등한 것)와 합치되는 경우에는 인증서를 자동적으로 폐지함. (본 옵션은 모든 고객들에게는 가용하지 않음을 유의바랍니다.)
- 가입자로부터 '폐지를 요청하고 폐지될 인증서에 참조되는 전자서명을 포함하는 메시지를 수령함,

○ 인증서의 클래스에 따라 폐지를 요청하는 사람이나 기관이 사실상 가입자임'을 합리적인 수준으로 확실히 하는 가입자와의 의사소통. 이러한 의사소통은, 상황에 따라 다르지만, 전화, 팩스, 이메일, 우편 혹은 택배 중 하나의 수단을 포함할 수 있습니다.

CrossCert 행정 담당자들은 CrossCeert 의 서브 도메인 내에서의 최종 사용자 가입자 인증서의 폐지를 요청할 권한이 있습니다. CrossCert 는, 폐지 기능 또는 기타 다른 STN 승인 절차를 수행하는 것을 허락하기 전에, 행정 담당자들의 신원을 SSL 및 고객 인증을 활용한 접근을 통하여 확인합니다.

'자동 행정 소프트웨어 모듈(Automated Administration Software Module)'을 활용하는 RA 들은 CrossCert 에게 폐지 요청을 대량으로 제출할 수 있습니다. 그러한 요청들은 RA 의 자동화된 행정 하드웨어 표식 내에 개인키로 서명된 전자서명에 의하여 인증되어야 합니다.

CA 인증서를 폐지하는 요청은 CrossCert 에 의하여 '폐지는 사실상 CA 에 의하여 요청되었음'을 확실히 하여 인증되어야 합니다.

4. 인증서 라이프 사이클 운영 요건(Certificate Life-Cycle Operational Requirements)

4.1 인증서 신청(Certificate Application)

4.1.1 인증서 신청은 누가 할 수 있는가?(Who Can Submit a Certificate Application?)

다음은 인증서 신청을 제출할 수 있는 사람 목록입니다:

- 인증서의 대상자인 개인,
- 기관이나 개체의 권한 있는 대표자,
- CA 의 권한 있는 대표자,
- RA 의 권한 있는 대표자.

4.1.2 등록 절차 및 책임(Enrollment Process and Responsibilities)

4.1.2.1 최종 사용자 인증서 가입자(End-User Certificate Subscribers)

모든 최종 사용자 인증서 가입자들은, 제 9 조 6 항 3 호에 규정된 보증 및 진술사항과 다음과 같은 등록절차 수행으로 구성된, 가입자 계약서(Subscriber Agreement)에 명시적으로 동의하여야 합니다:

- 인증서 신청을 완료하고 진정하고 올바른 정보를 제공함,
- 키 쌍을 생성, 또는 생성되도록 할당함,
- CrossCert 에게 직접 혹은 RA 를 통해서 그 자신의 공개키를 전달함,
- CrossCert 에게 전달된 공개키와 합치하는 개인키에 대한 독점적인 통제권과/혹은 보유를 설명함,

4.1.2.2 CABF 인증서 신청 요건(CABF Certificate Application Requirements)

도메인 유효 및 기관 유효 SSL 인증서(Domain validated and organization validated SSL Certificates)는 CA / Browser Forum Baseline 요건을 준수합니다.

인증서를 발행하기 전에, CA는 다음의 서류를 신청자로부터 수령하여야 합니다:

1. 전자적으로도 할 수 있는, 인증서 신청; 그리고
2. 전자적으로도 할 수 있는, 가입자 계약서(Subscriber Agreement) 체결본.

CA 는, 본 요건을 충족하기 위하여 필요하다고 판단하는 추가 서류를 수령하여야 합니다.

인증서 발행 전에, CA 는 CA 가 지정한 양식으로 신청자가 작성하고 본 요건을 충족하는 인증서 신청서를 수령하여야 합니다. 인증서 신청서 하나는 동일한 신청자에게 발행되는 다수의 인증서들을 위해 충분할 수 있으나, 제 3 조 2 항 2 호 1 목 인증서 데이터의 연령상의 요건에 따라야 합니다. 단, 각 인증서는 신청자를 대신한 신청자 대표에 의해 서명된 최신 인증서 신청서로 보완되어야 합니다. 인증서 신청은 전자적으로 작성, 제출 및/혹은 서명될 수 있습니다.

신청 및 인증(Request and Certification)

인증서 신청은, 인증서 발행에 대한 신청자의, 신청자를 대신한, 요청을 반드시 포함하여야 하며, '신청에 포함된 모든 정보는 정확한 것임'을 신청자에 의하거나 신청자를 대신하여 인증되어야 합니다.

정보 요건(Information Requirements)

인증서 신청은, 인증서에 포함되어야 하는 신청자에 관한 모든 사실 정보를 포함할 수 있으며, 추가 정보는 본 요건 및 CA의 인증서 정책과 인증업무준칙을 충족하기 위해 CA가 필요하다고 판단하는 경우에 신청자로부터 수령합니다. 인증서 신청서가 신청자에 대하여 필요한 모든 정보를 포함하고 있지 않은 경우에는, CrossCert CA는 신청자로부터 나머지

정보를 수령하거나 신뢰할 수 있는 독립 제3자 데이터 소스로부터 정보를 얻고 이를 신청자와 확인할 수 있습니다.

신청자 정보는, 최소한 하나의 '완전히 유효한 도메인 이름(FQDN)' 혹은 IP 주소를 *대상자이름* 확장자에 포함하여야 합니다.

가입자 개인키(Subscriber Private Key)

가입자 이외의 자들은 '가입자 개인키(Subscriber Private Key)'를 보관하지 말아야 합니다.

만일 CA나 지정된 RA들 중의 하나가 가입자를 위하여 개인키를 생성한 경우에는, CA는 해당 개인키를 가입자에게 이전하기 위하여 암호화하여야 합니다.

CA 나 지정된 RA 들 중 하나가 '가입자의 개인키가 권한 없는 자 또는 가입자와 무관한 기관과 소통되었음'을 알게 된 경우에는, 해당 CA 는 소통된 개인키에 대응하는 공개키를 포함하는 모든 인증서들을 폐지하여야 합니다.

가입자 및 계약서(Subscriber and Agreement)

인증서 발행 이전에, CA는 CA와 인증서 수혜자들의 명시적인 혜택을 위하여, 신청자의 가입자 계약서(Subscriber Agreement) 합의를 CA와 하여야 합니다.

CA 는 '각 가입자 계약서가 신청자를 상대로 법적으로 구속력이 있음'을 확실히 하는 절차를 이행하여야 합니다. 어떠한 경우에도, 계약서는 인증서 신청에 따라 발행되는 인증서에 대하여 적용되어야 합니다.

CA 는 전자적 형태 혹은 "클릭하여 통과"하는 계약서 형식을 이용하며, 해당 계약서들은 법적으로 집행력이 있습니다. CA 가 신청자에게 발급하는 각각의 인증서가 명확하게 해당 가입자 계약서에 의하여 규율 받는다면, 각 인증서 신청이나 미래의 다수 인증서 신청에 대한 별도의 계약서는 활용될 수 있습니다.

4.1.2.3 CA 및 RA 인증서(CA and RA Certificates)

CA 및 RA 인증서들의 가입자는 CrossCert 와 계약을 체결합니다. CA 와 RA 신청자들은 그들의 신원을 설명하기 위하여 자신들의 암호 정보를 제공하여야 하며 계약 체결 절차 동안 연락처 정보를 제공하여야 합니다. 이러한 계약 체결 절차 기간과 CA 또는 RA 키 쌍이 생성되는 키생성 세레모니(Key Generation Ceremony)전까지는, 신청자는 적절한 식별 이름을 결정하고 신청자에 의해 발행될 인증서의 내용을 결정하는 데 CrossCert 와 협력을 하여야 합니다.

4.2 인증서 신청 처리 (Certificate Application Processing)

4.2.1 신원 확인 및 인증 기능 수행(Performing Identification and Authentication Functions)

CrossCert 혹은 RA 는 제 3 조 2 항의 규정에 따라 요구되는 모든 가입자 정보에 대한 신원 확인과 인증절차를 수행하여야 합니다.

4.2.2 인증서 신청에 대한 승인 혹은 거절(Approval or Rejection of Certificate Applications)

CrossCert 혹은 RA 는 인증서신청서가 다음과 같은 기준을 충족하는 지를 승인합니다:

- 제 3 조 2 항의 규정에 따라 요구되는 모든 가입자 정보에 대한 성공적인 신원 확인과 인증
- 수수료 등 대급 수령을 하였음

CrossCert 혹은 RA 는 다음의 경우에는 인증서 신청을 거절합니다:

- 제 3 조 2 항의 규정에 따라 요구되는 모든 가입자 정보에 대한 신원 확인과 인증이 완료될 수 없음, 혹은
- 가입자가 요청 받은 증빙 서류를 제출하지 못함, 혹은
- 가입자가 정해진 시간 안에 통지에 대한 답변을 하지 못함, 혹은
- 수수료 등 대금 수령을 하지 못하였음, 혹은
- RA 가 '가입자에게 인증서를 발행하는 것은 STN 을 오명에 빠지게 할 수 있다'고 생각하는 경우.

4.2.3 인증서 신청 처리 시간(Time to Process Certificate Applications)

CrossCert 는 인증서 신청을 수령한 후 합리적인 시간 내에 처리 절차를 시작합니다. 해당 가입자 계약서, CPS 또는 STN 참여자들 사이에 다른 계약서에 달리 특정하지 않은 한, 신청을 처리 완료하는 데 정한 시간 제한은 없습니다. 인증서 신청은 거절될 때까지는 유효하게 존속합니다.

4.3 *인증서 발행(Certificate Issuance)*

4.3.1 인증서 발행 중 CA 의 활동(CA Actions during Certificate Issuance)

인증서는, CrossCert 의 인증서 신청서 승인 후 또는 RA 의 인증서 발행 요청을 받은 후에 생성되고 발급됩니다. CrossCert 는 해당 인증서 신청 승인 후에 인증서 신청에 포함된 정보에 근거하여 인증서를 인증서 신청자에게 생성하고 발행합니다.

4.3.2 CA 에 의한 인증서 발행 관련 가입자 통지(Notifications to Subscriber by the CA of Issuance of Certificate)

CrossCert 는, 직접 혹은 RA 를 통해서, 가입자에게 '해당 인증서가 생성되었음'을 통지하고, 가입자에게 가용한 인증서에 접근권한을 제공하여야 합니다. 인증서는 최종 사용자 가입자들에게, 웹싸이트에서 다운로드 받거나, 인증서를 포함하여 가입자에게 메시지로 송부되는 방식으로, 사용될 수 있도록 제공 되어야 합니다.

4.3.3 루트 CA 에 의한 인증서 발행을 위한 CABF 요건(CABF Requirement for Certificate Issuance by a Root CA)

도메인 유효 및 기관 유효 SSL 인증서(Domain validated and organization validated SSL Certificates)는 CA / Browser Forum Baseline 요건을 준수합니다.

CrossCert 의 루트(Root) CA 개인키(Private Keys)들은 가입자 인증서를 서명하는 데 사용되어서는 아니 됩니다. CrossCert 의 루트(Root) CA 개인키(Private Keys)들은 다음과 같은 경우들에만 인증서를 서명하는데 사용될 수 있습니다:

1. 루트 CA 자신을 대표하기 위해 인증서에 자기 서명함;
2. 하위 CA 들이나 Cross 인증서를 위한 인증서;
3. 기반 인프라 목적을 위한 인증서(예를 들어, 행정 역할의 인증서, 내부 CA 운영상 장치 인증서, 및 OCSP 대응 확인 인증서).

루트 CA 에 의한 인증서 발행은, CA 로부터(즉, CA 시스템 운영자, 시스템 임원, 혹은 PKI 행정 담당자) '루트 CA 가 인증서 서명 운영을 할 수 있도록 직접명령을 내리는' 권한을 개인이 위임 받는 것을 필요로 합니다. 루트 CA 에 의한 인증서 발행에 대한 추가적인 통제권한은 제 5 조 6 항 *키변경(Key Changeover)*과 제 6 조 1 항 *키 쌍 생성(Key Pair Generation)*에 규정되어 있습니다.

4.4 인증서 수락(Certificate Acceptance)

4.4.1 인증서 수락 행위(Conduct Constituting Certificate Acceptance)

다음의 행동은 인증서를 수락하는 행동으로 해석됩니다:

- 인증서를 다운로드하거나, 메시지에 첨부된 인증서를 설치하는 것은 가입자의 인증서 수락을 의미합니다.
- 가입자가 인증서 또는 인증서의 내용에 대하여 이의를 제기하지 않는 것은 인증서 수락을 의미합니다.

4.4.2 CA 에 의한 인증서의 게재(Publication of the Certificate by the CA)

CrossCert 는 자신이 발행하는 인증서들을 공개적으로 접근이 허용된 저장소에 게재합니다.

4.4.3 다른 개체들에 대한 CA 의 인증서 발행 통지(Notification of Certificate Issuance by the CA to Other Entities)

RA 들은, 그들이 승인한 인증서 발행 통지를 수령할 수도 있습니다.

4.5 키 쌍 및 인증서 용도(Key Pair and Certificate Usage)

4.5.1 가입자 개인키와 인증서 용도(Subscriber Private Key and Certificate Usage)

인증서에서 공동키와 대응하는 개인키의 사용은 오직 가입자가 '가입자 계약서'에 동의하고 인증서를 수락하는 때 한번만 허용됩니다. 인증서는 STN CP 및 본 CPS 의 조건과 CrossCert 의 가입자 계약서에 따라 합법적인 범위에서 사용되어야 합니다. 인증서의 이용은 인증서에 포함된 키사용 영역 확장자의 내용과 일관된 범위 내에서만 이용되어야 합니다(예를 들어, 만일 전자서명이 가능하지 않다면, 인증서는 서명 용도로는 사용되지 않아야 합니다).

가입자들은 그들의 개인키를 권한없는 사용들로부터 보호하여야 하며 인증서 만료나 폐지 후에는 개인키 사용을 중단하여야 합니다. 가입자 이외의 자들은 가입자 개인키를, 제 4 조 12 항에 규정된 바를 제외하고, 보관하여서는 아니 됩니다.

4.5.2 신뢰자 공동키와 인증서 용도(Relying Party Public Key and Certificate Usage)

신뢰자들은 인증서를 신뢰하는 조건으로써 적용 '신뢰자 계약서'의 조건에 동의하여야 합니다.

인증서에 대한 의존은 주변 정황을 고려할 때 반드시 합리적인 것이어야 합니다. 만일 '주변 정황이 추가적인 확실함이 필요함'을 나타낸다면, 해당 신뢰자는 합리적이라고 판단되는 의존을 하기 위한 '추가적인 보장상황'을 반드시 확보하여야만 합니다.

의존 행위 전에, 신뢰자는 독립적으로 다음 사항을 평가하여야 합니다:

- 주어진 목적에 대한 인증서 이용의 적정성 및 인증서의 해당 목적에 대한 사용이 금지된 것이거나 본 CPS 에 의하여 금지된 것이 아닌 지에 대한 판단. CrossCert 가 인증서 사용의 적정성에 대한 평가에 대하여 책임이 없는지.
- 인증서에 포함된 키사용 영역 확장자의 내용과 일관된 범위 내에서만 이용되는지(예를 들어, 만일 전자서명이 가능하지 않다면, 인증서는 서명 용도로는 사용되지 않아야 함)
- 인증서 및 인증서를 발행한 인증서 채인(chain) 내의 CA 들 모두에 대한 현재 지위. 만일 인증서 채인 내의 어떠한 인증서가 폐지된 경우라면, 신뢰자는 '인증서 채인 내에서 인증서 폐지 전의 최종 사용자 가입자 인증서에 의한 전자서명이 합리적인 것인가'에 대한 유일한 검사 책임을 부담함. 그러한 의존은 완전히 신뢰자의 전적인 책임하에 이루어 짐.

인증서의 사용이 적정한 것이라고 가정하면, 신뢰자는 적정한 소프트웨어 및 하드웨어를 사용하여 전자서명 확인과 기타 암호화 운영을 하여야 하며, 이는 해당 이용과 관련하여 '인증서에 의존하기 위한 조건'입니다. 그러한 운영은 인증서 채인을 확인하는 것과 해당 인증서 채인 내의 인증서들 모두에 대한 전자서명을 확인하는 것을 포함합니다.

4.6 인증서 갱신(Certificate Renewal)

인증서 갱신은 인증서 내의 공동키 혹은 기타 다른 정보의 변경 없이 가입자에게 새로운 인증서를 발행하는 것입니다. 인증서 갱신은, 대부분의 웹서버 키 생성 도구가 '현존하는 키 쌍에 대한 새로운 인증서 요청'을 허용하므로, 키 쌍이 웹서버에서 생성되는, 클래스 3 인증서를 지원하는 것입니다.

4.6.1 인증서 갱신 환경(Circumstances for Certificate Renewal)

가입자는, 현존하는 가입자 인증서의 만료 전에, 인증서 사용을 계속하기 위하여 새로운 인증서로 갱신할 필요가 있습니다. 인증서는 만료 후에도 갱신될 수는 있습니다.

4.6.2 갱신을 요청할 수 있는 사람(Who May Request Renewal)

개인용 인증서에 대하여는 가입자만, 또는 기관용 인증서에 대하여는 권한 있는 대표자만이 인증서의 갱신을 요청할 수 있습니다.

4.6.3 인증서 갱신 요청 처리(Processing Certificate Renewal Requests)

갱신 절차는, 최종 사용자 가입자 인증서의 갱신을 요청하는 사람이나 기관이 사실상 인증서의 가입자(또는 가입자의 권한을 위임 받은 자)인지를 확실히 하는 것입니다.

수용 가능한 절차 하나는, 챌린지 문구(또는 이와 동등한 것)를 이용하거나, '개인키를 보유하고 있음'을 증명하는 것을 통하여 이루어 집니다. 가입자들은 챌린지 문구(또는 이와 동등한 것)를 그들의 등록정보로 선택하고 제출합니다. 인증서의 갱신에 대하여는, '가입자가 올바르게 가입자의 재등록 정보와 함께 챌린지 문구(Challenge Phrase)(또는 이와 동등한 것)를 제출한 경우'이고, 등록정보(기업 및 기술 연락처 정보 포함[11])가 변경되지 않은 경우라면, 갱신된 인증서는 자동적으로 발행됩니다. 챌린지 문구(Challenge Phrase)(또는 이와 동등한 것)를 이용하는 것에 대한 대체방안으로, CrossCert 는 인증서 갱신을 위한 연락처로 확인된 연락처로 e-mail 을 송부하여 '인증서 갱신 주문과 인증서 발행 권한을 요구하는 지'를 확인할 수 있습니다. 인증서 발행을 승인하는 확인을 수령하면, CrossCert 는 등록 정보(기업 및 기술 연락처 정보[12] 포함)가 변경되지 않았다면, 인증서를 발행합니다.

이러한 방식의 갱신이 있은 후, 그리고 이후의 갱신의 대체가 있은 후에는, CrossCert 나 RA 는 '원래의 인증서 신청상의 인증 요건들과 신원확인 요건에 따라' 가입자의 신원을 재확인합니다.

특히, 리테일 클래스 3 기관용 인증서에 대하여는 www.crosscert.com 을 통해서 CrossCert 는 제 6 조 3 항 2 호에 규정된 간격으로 인증서에 포함된 기관의 이름 및 도메인 이름을 다시 인증합니다. 만일, 다음과 같은 상황이라면:

- 챌린지 문구가 후속 인증서 갱신에 올바르게 사용되며:
- 인증서 식별이름이 변경되지 않았고.
- 기업 및 기술 연락처 정보가 예전에 인증된 내용과 변함이 없으면,

CrossCert 는 전화, 수신 확인 우편이나 이와 비교되는 절차로, 인증서 신청자에게 기관에 관한 일정한 정보, 기관이 인증서 신청을 위임했는지, 인증서 신청을 제출한 자가 인증서 신청을 할 수 있는 권한을 위임 받았는지를 재확인할 필요가 없습니다.

이러한 절차 또는 CrossCert가 승인한 절차 이외에는, 원래의 인증서 신청에 대한 신원확인과 인증 요건은 폐지 후의 인증서 갱신에 활용되어야 합니다.

---

[11] 연락처 정보가 공식적인 변경절차에 따라 승인되어 변경된 경우에는, 인증서는 여전히 자동 갱신될 수 있음.
[12] 연락처 정보가 공식적인 변경절차에 따라 승인되어 변경된 경우에는, 인증서는 여전히 자동 갱신될 수 있음.

4.6.4 가입자에 대한 신규 인증서발행 통지(Notification of New Certificate Issuance to Subscriber)

가입자에 대한 인증서의 갱신 발행 통지는 제 4 조 3 항 2 호에 따르기로 합니다.

4.6.5 인증서 갱신에 대한 수락 행위(Conduct Constituting Acceptance of a Renewal Certificate)

갱신된 인증서를 수락하는 행위는 제 4 조 4 항 1 호에 따르기로 합니다.

4.6.6 CA 에 의한 인증서 갱신의 게재(Publication of the Renewal Certificate by the CA)

갱신된 인증서는 CrossCert 의 공개적인 저장소에 게재됩니다.

4.6.7 CA 에 의한 인증서 발행에 관한 타인 통지(Notification of Certificate Issuance by the CA to Other Entities)

RA 들은 그들이 승인한 인증서의 발행 통지를 수령할 수 있습니다.

4.7 인증서 키교체(Certificate Re-Key)

인증서 키교체는 신규 공동키를 인증하는 신규 인증서의 발행 신청입니다. 인증서 키교체는 모든 인증서 클래스들에 대하여 지원됩니다.

4.7.1 인증서 키교체 환경(Circumstances for Certificate Re-Key)

가입자가 인증서의 사용을 유지하기 위하여, 현존하는 인증서의 만기 전에, 인증서의 키교체를 하여야 합니다. 인증서는 만기 후에도 키교체 될 수 있습니다.

4.7.2 신규 공동키 인증을 요청할 수 있는 사람(Who May Request Certification of a New Public Key)

개인용 인증서에 대하여는 가입자만, 또는 기관용 인증서에 대하여는 권한 있는 대표자만이 인증서의 갱신을 요청할 수 있습니다.

4.7.3 인증서 키교체 요청 처리(Processing Certificate Re-Keying Requests)

키교체 절차는, 최종 사용자 가입자 인증서의 갱신을 요청하는 사람이나 기관이 사실상 인증서의 가입자(또는 가입자의 권한을 위임 받은 자)인지를 확실히 하는 것입니다.

수용 가능한 절차 하나는, 챌린지 문구(또는 이와 동등한 것)를 이용하거나, '개인키를 보유하고 있음'을 증명하는 것을 통하여 이루어 집니다. 가입자들은 챌린지 문구(또는 이와 동등한 것)를 그들의 등록정보로 선택하고 제출합니다. 인증서의 갱신에 대하여는, '가입자가 올바르게 가입자의 재등록 정보와 함께 챌린지 문구(Challenge Phrase)(또는 이와 동등한 것)를 제출한 경우'이고, 등록정보(기업 및 기술 연락처 정보 포함[13])가 변경되지 않은 경우라면, 갱신된 인증서는 자동적으로 발행됩니다.

제 3 조 3 항 1 호를 조건으로 하고, 이러한 방식의 키교체가 있은 후, 그리고 이후의 키교체의 대체가 있은 후에는, CrossCert 나 RA 는 '원래의 인증서 신청상의 인증 요건들과 본 CPS 에 규정된 신원확인 요건에 따라' 가입자의 신원을 재확인합니다.

이러한 절차 또는 시만텍이 승인한 절차 이외에는, 원래의 인증서 신청에 대한 인증 요건은 최종 사용자 가입자 인증서 키교체에 활용되어야 합니다.

4.7.4 가입자에 대한 신규 인증서 통지(Notification of New Certificate Issuance to Subscriber)

가입자에 대한 인증서의 키교체 통지는 제 4 조 3 항 2 호에 따르기로 합니다.

4.7.5 키교체된 인증서에 대한 수락 행위(Conduct Constituting Acceptance of a Re-Keyed Certificate)

키교체된 인증서를 수락하는 행위는 제 4 조 4 항 1 호에 따르기로 합니다.

4.7.6 CA 에 의한 키교체된 인증서의 게재(Publication of the Re-Keyed Certificate by the CA)

키교체된 인증서는 CrossCert 의 공개적인 저장소에 게재됩니다.

4.7.7 CA 에 의한 인증서 발행에 관한 타인 통지(Notification of Certificate Issuance by the CA to Other Entities)

RA 들은 그들이 승인한 인증서의 발행 통지를 수령할 수 있습니다.

4.8 *인증서 수정(Certificate Modification)*

4.8.1 인증서 수정 배경(Circumstances for Certificate Modification)

[13] 연락처 정보가 공식적인 변경절차에 따라 승인되어 변경된 경우에는, 인증서는 여전히 자동 갱신될 수 있음.

인증서 수정은, 현존하는 인증서의 (가입자의 공동키 이외의) 정보에 변경이 있는 경우에 새로운 인증서 신청을 하는 것을 의미합니다.

인증서 수정은 제 4 조 1 항에 따른 인증서 신청으로 고려됩니다.

4.8.2 인증서 수정을 요청할 수 있는 사람(Who May Request Certificate Modification)

제 4 조 1 항 1 호 참조 바랍니다.

4.8.3 인증서 수정 요청 처리(Processing Certificate Modification Requests)

CrossCert 혹은 RA 는 제 3 조 2 항에 따라 필요한 모든 가입자에 대한 신원확인과 인증을 이행하여야 합니다.

4.8.4 가입자에 대한 신규 인증서 발행 통지(Notification of New Certificate Issuance to Subscriber)

제 4 조 3 항 2 호 참조 바랍니다.

4.8.5 수정된 인증서에 대한 수락 행위(Conduct Constituting Acceptance of Modified Certificate)

제 4 조 4 항 1 호 참조 바랍니다.

4.8.6 CA 에 의한 수정된 인증서의 게재(Publication of the Modified Certificate by the CA)

제 4 조 4 항 2 호 참조 바랍니다.

4.8.7 CA 에 의한 인증서 발행에 관한 타인 통지(Notification of Certificate Issuance by the CA to Other Entities)

제 4 조 4 항 3 호 참조 바랍니다.

4.9 인증서 폐지 및 정지(Certificate Revocation and Suspension)

4.9.1 폐지 환경(Circumstances for Revocation)

최종 사용자 가입자 인증서는 오직 아래와 같은 환경 하에서만 시만텍(혹은 가입자)에 의하여만 폐지되고 CRL 에 게재될 것입니다. 하기 나열된 이유 이외의 사유로 인증서를

사용할 수 없는(혹은 더 이상 사용하고자 하지 않는) 가입자의 요청에 따라, 시만텍은 해당 인증서를 자신의 데이터베이스에 비가동(inactive)인 것으로 지정하되, CRL 에 해당 인증서를 게재하지는 않습니다.

최종 사용자 가입자 인증서는 다음의 경우에는 폐지됩니다:

- CrossCert, 고객, 또는 가입자가 '가입자 개인키의 절충이 있음'을 믿을만하거나 강한 의혹을 가질만한 이유가 있는 경우,
- CrossCert 나 고객이 '가입자가 해당 '가입자 계약서(Subscriber Agreement)'상의 자신의 중대한 의무, 진술 혹은 보증사항을 위반하였음'을 믿을만한 이유가 있는 경우,
- 가입자와의 가입자 계약서가 해지된 경우,
- 기업 고객과 가입자의 연계관계가 해지되었거나, 달리 종결된 경우,
- 클래스 3 기관용 ASB 인증서의 가입자인 기관과 가입자의 개인키를 관리하는 기관의 대표간 연계관계가 해지되었거나 달리 종결된 경우,
- CrossCert 나 고객이 '인증서가 관련 CPS 에서 요구되는 절차대로 발행되지 않았고, (클래스 1 인증서 이외의) 인증서가 인증서 대상에 기명된 자 이외에게 발행되었으며, 또는 해당 인증서의 대상에 기명된 자의 승인없이 (클래스 1 인증서 이외의) 인증서가 발행되었다'고 믿을만한 이유가 있는 경우,
- CrossCert 나 고객이 '인증서 신청서 상의 중대한 사실이 거짓'이라고 믿을만한 이유가 있는 경우,
- CrossCert 나 고객이 판단하기에 '인증서 발행에 대한 중대한 전제요건이 충족되지도 않았거나 면제되지 않은' 경우,
- 클래스 3 기관용 인증서의 경우, 가입자의 기관 이름이 변경된 경우,
- 인증서 내의 정보 중 미확인 가입자 정보 이외의 정보가 정확하지 않거나 변경된 경우,
- 가입자 정체가 제 6 조 3 항 2 호에 따라 성공적으로 재확인되지 않은 경우,
- 가입자가 지급기한까지 해당 지급을 이행하지 않은 경우, 또는
- 해당 인증서의 계속 사용은 STN 에 해로운 경우.

'인증서 사용이 STN 에 해로운 지'에 관한 고려를 함에 있어서 CrossCert 는 다른 사항과 더불어 다음 사항을 고려합니다:

- 수령한 불만사항의 성격과 횟수
- 불만사항 제기자의 신원
- 시행중인 관련 법규
- 가입자로부터의 해당 '해로운 사용'에 대한 반응

'코드 서명 인증서 사용이 STN 에 해로운 지'에 관한 고려를 함에 있어서 CrossCert 는 추가로 다른 사항과 더불어 다음 사항을 고려합니다:

- 서명된 코드의 이름

- 코드의 행태
- 코드 배포 방법
- 코드 수령자에게 공개되는 사항들
- 코드에 관하여 추가적으로 제시되는 사항들

CrossCert 는, '만일 행정 담당자의 행동 권한이 해지되었거나 달리 종결된 경우에는', 행정 담당자의 인증서를 폐지할 수 있습니다.

CrossCert 가입자 계약서는, '최종 사용자 가입자가 그들의 개인키에 대한 절충을 알거나 의심하는 경우에는 즉시 CrossCert 에게 통지하여야 함'을 규정합니다.

4.9.1.1 폐지 사유에 관한 CABF 요건(CABF Requirements for Reasons for Revocation)

도메인 유효 및 기관 유효 SSL 인증서(Domain validated and organization validated SSL Certificates)는 CA / Browser Forum Baseline 요건을 준수합니다.

CrossCert는 다음 사항 중 하나 이상의 사유가 발생하면 24시간 이내에 인증서를 폐지하여야 합니다:

1. 가입자가 서면으로 CA 에게 인증서 폐지를 요청한 경우;
2. 가입자가 CA 에게 '원래의 인증서 신청은 권한 위임이 없었던 것이고, 회귀하여 권한 위임을 받지 않았음'을 통지한 경우;
3. CA 가 '가입자의 (인증서의 공동키에 대응하는) 개인키가 키 위반으로부터 피해를 받았거나, 인증서가 기타 다른 방식으로 오용됨(예를 들어, 개인키가 기록됨)'에 대한 증거를 입수한 경우;
4. CA 가, '가입자가 가입자 계약서상의 중대한 의무를 위반하였음'을 알게 된 경우;
5. CA 가, '인증서에 완전한 자격이 있는 도메인 이름(FQDN)이나 IP 주소 사용이 더 이상 법적으로 허용되지 않는다'는 상황을 알게 된 경우(예를 들어, 법원이나 중재원에 의하여 도메인 이름 등록기관의 도메인 사용 권한, 관련 라이선스 또는 서비스 계약서상 해당 신청자가 계약해지 되었거나, 도메인 등록자가 도메인 이름 갱신에 실패한 경우);
6. CA 가, '와일드 카드 인증서(Wildcard Certificate)가 하위 FQDN 을 의도적으로 오인하도록 인증에 사용되었음'을 알게 된 경우;
7. CA 가 '인증서에 포함된 정보에 중대한 변경이 있음'을 알게 된 경우;
8. CA 가 '인증서가 CrossCert CPS 에 따라 발행되지 않았음'을 알게 된 경우;
9. CA 가 '인증서상에 나타난 정보가 부정확하거나 오해를 초래하는 것'이라고 판단하는 경우;
10. CA 가 어떠한 이유로건 운영을 중단하고 다른 CA 에게 인증서 폐지 지원을 위한 업무 이전을 하지 않은 경우;

11. CA 가 CRL/OCSP 저장소 유지를 계속하는 업무 이관을 하지 않은 한, 본 CPS 에 따른 CA 의 인증서 발행 권한이 만료 혹은 폐지되거나 종료되는 경우;
12. CA 가 '하위 CA 의 개인키의 위반이 인증서 발행에 사용될 가능성이 있음'을 알게 된 경우;
13. CA 혹은 그가 지정한 RA 들이 '가입자의 개인키가 가입자와 연계되지 않은 기관이나 권한을 위임 받지 않은 사람들과 소통되었음'을 알게 된 경우;
14. 기타 CrossCert 의 CPS 에 의하여 폐지가 요구되는 경우, 또는
15. 인증서의 기술 내역이나 형식이 애플리캐이션 소프트웨어 공급자나 신뢰자들에게 수용될 수 없는 위험을 표시하는 경우(예를 들어, CA/Browser Forum 에 의하여 판단되는 바에 의함).

4.9.2 폐지를 요청할 수 있는 자(Who Can Request Revocation)

개인 가입자들은, <관계사(Affiliate)>의 권한 있는 대표 또는 RA 를 통하여 자신들의 개인용 인증서의 폐지를 요청할 수 있습니다. 기관용 인증서의 경우에는, 기관의 적정 권한이 있는 대표는 해당 기관에 발행된 인증서의 폐지를 요청할 권한이 있습니다. CrossCert 나 RA 의 적정 권한이 있는 대표는 RA 행정 담당자의 인증서에 대한 폐지를 요청할 수 있습니다. 가입자의 인증서 신청을 승인한 당사자는 가입자의 인증서 폐지를 요청하거나 취소할 수도 있습니다.

오직 CrossCert 만이 자신의 CA 들에게 발행된 인증서의 폐지를 신청하거나 개시할 수 있는 권한이 있습니다. RA 들은, 적정 권한이 있는 대표자들과 상위 기관들로 하여금 그들의 인증서들을 폐지해 줄 것을 요청하거나 개시할 권한을 가집니다.

4.9.3 폐지 요청 절차(Procedure for Revocation Request)

4.9.3.1 최종 사용자 가입자 인증서의 폐지를 요청하는 절차(Procedure for Requesting the Revocation of an End-User Subscriber Certificate)

폐지를 요청하는 최종 사용자 가입자는, 인증서 폐지 요청을 적절하게 개시할, CrossCert 나 고객이 승인하는 가입자의 인증서 애플리캐이션에 요청을 하여야 합니다. 기업 고객에 대하여는, 가입자는 기업 행정 담당자로 하여금 CrossCert 에 소통하도록 하여야 합니다. 해당 폐지 요청은 CPS 제 3 조 4 항에 따라 소통됩니다.

기업 고객이 최종 사용자 가입자 인증서의 폐지를 개시하는 경우에는, Managed PKI 의 고객이나 ASB 고객은 CrossCert 로 하여금 해당 인증서를 폐지할 것을 지시합니다.

4.9.3.2 인증서 폐지 절차에 대한 CABF 요건(CABF Requirements for Certificate Revocation Process)

도메인 유효 및 기관 유효 SSL 인증서(Domain validated and organization validated SSL Certificates)는 CA / Browser Forum Baseline 요건을 준수합니다..

폐지 요청(Revocation Request)

CrossCert CA 들은 가입자들에게 인증서 폐지를 요청하는 절차를 본 CPS 제 4 조 9 항에 규정된 바와 같이 제공하여야 합니다.

CrossCert 는 폐지 요청과 관련 요청사항을 1 일 24 시간 주 7 일 동안 대응할 수 있는 상황을 유지하여야 합니다.

인증서 장애 신고(Certificate Problem Reporting)

CrossCert CA 들은 개인키 위반, 인증서 오용이나 기타 사기, 부적절한 사용 또는 기타 인증서와 관련된 사항에 대한 신고방법에 대하여 가입자, 신뢰자, 애플리케이션 소프트웨어 공급자 및 기타 제 3 자에게 공개적으로 개시하여야 합니다.

조사(Investigation)

CrossCert CA 들은 인증서 장애 접수 후 24 시간 내에 조사에 착수하여, 다음과 같은 기준에 근거하여 폐지 혹은 기타 적정한 조치를 취하여야 합니다:

1. 제기된 장애 성격;
2. 특정 인증서 또는 가입자의 인증서 장애 신고 접수 횟수;
3. 불만신고를 한 개체(예를 들어, '불법행위에 연루된 웹싸이트에 대한 법 집행관의 신고'는 '물건을 배달 받지 못했다고 신고하는 고객의 신고'보다는 비중 있게 다루어져야 함); 그리고
4. 관련된 법규

대응(Response)

CrossCert 는 일 24 시간 주 7 일 항시 접수와 대응이 가능한 체계로 높은 우선 순위를 가지는 인증서 장애 신고체계를 유지하여야 하며, 필요한 경우에는 해당 신고 사항을 법 집행기관에 전달하여야 하며, 해당 신고 대상이 된 인증서를 폐지하여야 합니다.

4.9.3.3 CA 혹은 RA 인증서 폐지 요청 절차(Procedure for Requesting the Revocation of a CA or RA Certificate)

자신의 인증서들의 폐지를 요청하는 CA 또는 RA 는 해당 요청사항에 대하여 CrossCert 와 소통하여야 합니다. 그리고 나서, CrossCert 는 해당 인증서를 폐지합니다. CrossCert 는 CA 또는 RA 의 인증서 폐지를 개시할 수 도 있습니다.

4.9.4 폐지 요청 유예 기간(Revocation Request Grace Period)

폐지 요청은 상업적으로 합리적인 시간 내에 적시에 제출되어야 합니다.

4.9.5 CA 가 폐지 요청을 처리해야 하는 시간(Time within Which CA Must Process the Revocation Request)

CrossCert 는 폐지 요청을 지체 없이 처리하기 위하여 상업적으로 합리적인 조치를 취해야 합니다.

4.9.6 신뢰자들에 대한 폐지 확인 요건(Revocation Checking Requirements for Relying Parties)

신뢰자들은 그들이 의존하고자 하는 인증서들의 상태를 확인하여야 합니다. 신뢰자들이 인증서 상태를 확인하기 위하여 취할 수 있는 한 가지 방법은 신뢰하고자 하는 해당 인증서를 발급한 CA 로부터 가장 최신본 CRL 을 보고 확인하는 것입니다. 이에 대한 대안으로, 신뢰자들은 웹 저장소를 활용하거나 (가능하다면) OCSP 를 활용하여 인증서의 상태를 확인함으로써 본 요건을 충족할 수 있습니다. CA 들은 신뢰자들에게 '폐지 상태에 대한 확인을 위하여 어떻게 적정한 CRL, 웹 저장소 또는 (필요하다면) OCSP 대응자를 찾아볼 수 있는 지'에 대하여 정보를 제공하여야 합니다.

4.9.7 CRL 발행 빈도(CRL Issuance Frequency)

최종 사용자 가입자 인증서에 대한 CRL 들은 최소한 1 일에 1 회는 발행됩니다. CA 인증서들에 대한 CRL 들은 최소한 1 년에 한번, 단, CA 인증서가 폐지되는 때마다 발행되어야 합니다.

루트 CA 는 인증 컨텐츠 서명 (Authenticated Content Signing; ACS)에 대한 CRL 들을 최소한 1 년에 한번, 그리고 CA 인증서가 폐지되는 때마다 발행합니다.

CRL 에 나열된 인증서가 만료되면, 인증서의 기간 만료 후 발행되는 CRL 로부터 삭제됩니다.

4.9.7.1 CRL 발행에 관한 CABF 요건(CABF Requirements for CRL Issuance)

도메인 유효 및 기관 유효 SSL 인증서(Domain validated and organization validated SSL Certificates)는 CA / Browser Forum Baseline 요건을 준수합니다.

가입자 인증서 상태 요건(Subscriber Certificate Status Requirements)

CA 가 CRL 을 게재하는 경우에, CA 는 매 7 일 마다 최소한 1 회 이상 CRL 을 업데이트하고 재발행하여야 하며, *다음업데이트* 영역 값은 *이번업데이트* 영역 값의 10 일 이상이 되어서는 안됩니다.

하위 CA 인증서 상태 요건(Subordinate CA Certificate Status Requirements)

CA 는 최소한 (i) 12 개월에 1 회, 그리고 (ii) 하위 CA 인증서 폐지 후 24 시간 이내에 CRL 들을 업데이트하고 재발행하여야 하며, *다음업데이트* 영역 값은 *이번업데이트* 영역 값의 12 개월 이상이 되어서는 안됩니다.

4.9.8 CRL 에 대한 최대 잠재기(Maximum Latency for CRLs)

CRL 들은 생성 후 상업적으로 합리적인 시간 내에 저장소에 게재됩니다. 이는 일반적으로 생성 후 수 분(minutes)내에 자동적으로 수행됩니다.

4.9.9 온라인 폐지/상태 확인 가용도(On-Line Revocation/Status Checking Availability)

온라인 폐지 및 기타 인증서 상태 정보는 웹 기반 저장소와, 가능한 경우에는, OCSP 를 통하여 사용될 수 있습니다. CRL 들을 게재하는 것에 추가로, CrossCert 는 자신의 저장소상의 질의기능을 통하여 인증서 상태 정보를 제공합니다.

인증서 상태 정보는 하기 주소에 소재한 CrossCert 저장소를 통해 질의기능을 활용하여 확인할 수 있습니다.

- (개인용 인증서)
  https://onsite.crosscert.com/services/KECAIncCrossCertClass1ConsumerIndividualSubscriberCA/client/search.htm 그리고
- (SSL 또는 코드 서명 인증서)
  https://digitalid.verisign.com/services/server/search.htm (for SSL and Code Signing Certificates)

또한, CrossCert 는 OCSP 인증서 상태 정보를 제공합니다. OCSP 관련 계약을 체결한 기업 고객은 OCSP 를 사용하여 인증서 상태를 확인할 수 있습니다. 해당 OCSP 대응자에 대한 URL 은 기업 고객에게 제공됩니다.

4.9.9.1 OCSP 가용도에 대한 CABF 요건(CABF Requirements for OCSP Availability)

도메인 유효 및 기관 유효 SSL 인증서(Domain validated and organization validated SSL Certificates)는 CA / Browser Forum Baseline 요건을 준수합니다.

CA 는 2013 년 1 월 1 일부터 본 요건에 따라 발행된 인증서에 대한 GET 방식을 활용하여 OCSP 성능을 지원하여야 합니다.

가입자 인증서에 관한 인증서 상태(Certificate Status for Subscriber Certificates)

CA는 최소한 매 4일마다 온라인 인증서 상태 프로토콜(Online Certificate Status Protocol)을 통하여 정보를 업데이트하여야 합니다. 이러한 서비스에 대한 OCSP 대응은 반드시 최대 10일의 만료기간을 보유하여야 합니다.

하위 CA 인증서에 관한 인증서 상태(Certificate Status for Subordinate CA Certificates)

CA는 최소한 (i) 매 12개월 및 (ii) 하위 CA 인증서 폐지 후 24시간 내에 온라인 인증서 상태 프로토콜(Online Certificate Status Protocol)을 통하여 정보를 업데이트하여야 합니다.

4.9.10 온라인 폐지 확인 요건(On-Line Revocation Checking Requirements)

신뢰자는 반드시 자신이 신뢰하고자 하는 인증서의 상태를 확인하여야 합니다. 만일 신뢰자가 신뢰하고자 하는 인증서의 상태를 최신 CRL 을 통하여 확인하지 않은 경우에는, 해당 신뢰자는 관련 저장소에 문의하여 인증서 상태를 확인하거나 (OCSP 서비스가 가능하면) OCSP 대응자를 활용하여 인증서 상태를 요청하여 확인하여야 합니다.

4.9.11 폐지 홍보 관련 기타 가능 형식(Other Forms of Revocation Advertisements Available)

적용 사항 없습니다.

4.9.12 키 위반 관련 특별 요건(Special Requirements regarding Key Compromise)

CrossCert 는, 그들의 CA 들 중 하나 혹은 그들의 서브 도메인들 이내의 CA 들 중 하나의 개인키 위반이 있거나, 있다고 믿을만한 이유가 있는 경우에는, 잠재적인 신뢰자들에게 이를 통지하기 위한 상업적으로 합리적인 범위의 노력을 하여야 합니다.

4.9.13 중단 환경(Circumstances for Suspension)

적용 사항 없습니다.

4.9.14 중단을 요청할 수 있는 사람(Who Can Request Suspension)

적용 사항 없습니다.

4.9.15 중단 요청 절차(Procedure for Suspension Request)

적용 사항 없습니다.

4.9.16 중단 기간에 대한 제한(Limits on Suspension Period)

적용 사항 없습니다.

4.10 인증서 상태 서비스(Certificate Status Services)

4.10.1 운영상 특성(Operational Characteristics)

공공 인증서의 상태는 CrossCert 의 웹싸이트상의 CRL, LDAP 디렉토리와 (가능한 경우) OCSP 대응자를 통하여 알 수 있습니다.

4.10.2 서비스 가용도(Service Availability)

인증서 상태 서비스(Certificate Status Services)는 일정에 대한 장애 없이 1 일 24 시간 주 7 일기준으로 이용할 수 있습니다.

기관 유효 및 도메인 유효 SSL 인증서에 대하여는, CRL 및 OCSP 성능은 일반적인 운영 조건에서 10 초 이하의 대응시간을 제공하여야 합니다.

4.10.3 운영상 특성(Optional Features)

OCSP 는, 모든 제품에 대하여 가용하지는 않는 선택적인 상태 서비스이며, 다른 제품들에 대하여 특정하여 제한적으로 가능한 것입니다.

4.11 가입기간 종료(End of Subscription)

가입자는 CrossCert 인증서에 대한 가입기간을 하기 사항에 의하여 종료할 수 있습니다:

- 자신의 인증서가 갱신 혹은 키교체 없이 기간이 만료하는 것을 허용함
- 자신의 인증서 만료 전에 인증서를 교체하지 않고 폐지함.

4.12 키 에스크로우 및 복구(Key Escrow and Recovery)

Managed PKI 키 관리 서비스에 배포되는 기업들을 제외하면, STN 참여자는 누구도 CA, RA 또는 최종 사용자 가입자의 개인키들을 에스크로우할 수 없습니다.

시만텍 Managed PKI 서비스(Symantec Managed PKI Service) 내에서 키 에스크로우 옵션을 사용하는 기업 고객들은 인증서 신청을 승인한 가입자들의 개인키들에 대한 복사본을 에스크로우 할 수 있습니다. 기업 고객은 기업의 장소 내에서 또는 CrossCert 의 안전한 데이터 센터 내에서 키들을 에스크로우 할 수 있습니다. 만일 기업의 장소 밖에서 운영되는 경우에는, CrossCert 는 가입자의 개인키들의 사본을 보관하지 않으나, 가입자의 키 복구 절차에서 중요한 역할을 수행합니다.

4.12.1 키 에스크로우 및 복구 정책과 업무 실제(Key Escrow and Recovery Policy and Practices)

시만텍 Managed PKI 서비스(Symantec Managed PKI Service) (혹은 시만텍에 의한 이와 유사한 서비스) 내에서 키 에스크로우 옵션을 사용하는 기업 고객들은 최종 사용자 가입자의 개인키 에스크로우를 허용합니다. 에스크로우된 개인키들은 Managed PKI Key Manager 소프트웨어를 활용하는 암호화된 양식으로 보관되어야 합니다. Managed PKI 키 매니저 서비스(Managed PKI Key Manager Service) (혹은 시만텍에 의해 승인된 동등한 서비스)를 사용하는 기업 고객들을 제외하고, CA 들이나 최종 사용자 가입자의 개인키들은 에스크로우되어서는 안됩니다.

최종 사용자 가입자 개인키들은 오직 Managed PKI Key Management Service Administrator's Guide 내에서 허용되는 다음과 같은 상황 하에서만 복구될 수 있습니다:

- Managed PKI Key Manager 을 사용하는 기업 고객들은, '가입자가 되고자 하는 자의 정체는 사기꾼이 아닌 사실상의 가입자로부터 가입자 요청이 있도록 함을 확인하여야 하고,
- 기업 고객들은, 불법적이거나 사기 또는 기타 악의 목적이 아닌, 오직 합법적인 목적으로만 가입자의 권한 위임 없이 가입자의 개인키를 복구할 수 있어야 하고,
- 해당 기업 고객들은 키관리 서비스 행정 담당자들 및 기타 다른 사람들이 개인키에 권한 없이 접근하는 것을 막을 수 잇는 인력을 배치하여야 합니다.

시만텍 Managed PKI Service내에서 키 에스크로우 옵션을 사용하는 기업 고객들에게는 아래 사항이 권고됩니다:

- 가입자들에게 '그들의 개인키들이 에스크로우 되었음'을 통지
- 가입자들의 에스크로우된 키들을 권한 없는 공개로부터 보호,

- 가입자의 에스크로우된 키들을 복구하는데 사용될 수 있는 행정 담당자의 키를 포함한 모든 정보를 보호.
- 가입자의 에스크로우된 키들을 오직 적정하게 인증되고 권한 위임된 키복구 요청을 위하여만 제공함.
- 분실된 인증서의 사용을 중단하는 등과 같은 특정 상황 하에서 키 암호화 복구 이전에 가입자의 키 쌍을 폐지함.
- 가입자 본인이 키복구를 요청하는 경우를 제외하고, 가입자에게 키복구와 관련된 일체의 정보를 소통하지 않도록 요구함.
- 법, 정부 규칙, 또는 규정, 기업 기관의 정책, 또는 관할 법원의 명령에 의하지 않는 한, 에스크로우 키 또는 에스크로우된 키와 관련된 정보를 일체의 제 3 자에게 공개하거나 공개되도록 허락하지 않음.

4.12.2 세션키 캡슐화 및 복구 정책 및 업무 실제(Session Key Encapsulation and Recovery Policy and Practices)

개인키는 암호화된 양식으로 키 관리자(Key Manager) 데이터베이스에 보관됩니다. 각 가입자의 개인키는 개별적으로 고유의 3중 DES 대칭형 키로 암호화됩니다. 키 에스크로우 기록(Key Escrow Record; KER)이 생성되고, 3중 DES 키는 세션키 마스크를 형성하기 위하여 무작위로 결합됩니다. 결과물인 '감추어진' 세션키(MSK)는 안전하게 송부되고 CrossCert의 Managed PKI 데이터베이스에 보관됩니다. (최종 사용자의 개인키를 포함한) KER와 무작위 세션키 마스크는 키 관리자(Key Manager) 데이터베이스에 보관되며 모든 잔존 키 자료는 파기됩니다.

The Managed PKI 데이터 베이스는 CrossCert의 안전한 데이터 센터 내에서 운영됩니다. 기업 고객은 기업의 장소 내에서 혹은 CrossCert의 안전한 데이터 센터 내에서 키관리자(Key Manager)를 운영하는 것을 선택할 수 있습니다.

개인키와 디지털 인증서를 복구하기 위하여는 Managed PKI 행정 담당자로 하여금 Managed PKI Control Center에 안전하게 로그온하게 하여야 하고, 복구하기에 적절한 키 쌍을 선택하여야 하며, "복구" 하이퍼링크를 클릭하여야 합니다. 승인된 행정 담당자가 클릭한 후에만 "복구" 링크는 Managed PKI 데이터베이스로부터 회신된 키 쌍에 대한 MSK입니다. 키 관리자(Key Manager)는 KMD로부터 세션키를 출력하고, 이를 MSK와 결합하여 개인키를 원래 암호화하는 데 사용했던 3중 DES를 재생성하는데 사용하여, 최종 사용자의 개인키를 복구할 수 있도록 합니다. 마지막 단계로, 암호화된 PKCS#12 파일은 행정 담당자에게 회신되고 궁극적으로는 최종 사용자에게 배포됩니다.

5. 시설, 관리, 및 운영 통제(Facility, Management, and Operational Controls)

5.1 물리적 통제(Physical Controls)

CrossCert는, 본 CPS의 안전 요건을 지원하기 위하여 ‘CrossCert 물리적 보안 정책(Physical Security Policy)’을 실행합니다. 이러한 정책의 준수는 제8조에 규정된 CrossCert의 독립 감사 요건에도 포함되어 있습니다. ‘CrossCert 물리적 보안 정책(Physical Security Policy)’에는 민감한 보안 정보를 포함하며, 오직 CrossCert와의 계약에 따라서만 공개됩니다. 해당 요건들의 개요는 다음에서 설명됩니다.

5.1.1 현장 위치 및 건설 공사(Site Location and Construction)

CrossCert CA와 RA 운영은, 권한 없는 사용, 접근을 탐지하고, 예방하며, 민감한 정보의 공개와 공식 혹은 비공식 시스템의 권한 없는 접근 등으로부터 물리적으로 보호하는 환경 내에서 수행되어야 합니다.

또한, CrossCert는 CA 운영에 있어서 재난 복구 시설을 유지합니다. CrossCert의 재난 복구 시설은 CrossCert의 기본 설비의 수준과 비교할 수 있는 정도의 다중 보호가 되어야 합니다.

5.1.2 물리적 접근(Physical Access)

CrossCert CA 시스템은 최소한 4겹의 물리적인 보안층으로 보호되며, 낮은 층의 접근 권한이 있어야 더 높은 층으로의 접근 권한을 얻을 수 있습니다..

점진적으로 제한적인 물리적 접근 쉰한 통제는 각 층별 접근 권한을 통제합니다. 민감한 CA 운영상 활동, 인증, 확인 및 발행 등과 같은 인증서 절차 라이프사이클과 관련된 일체의 활동은 아주 제한적인 물리적 단계들 내에서 발생됩니다. 각 층마다 접근 권한은 담당 직원의 적정한 카드 배지(badge)를 사용하여야 합니다. 물리적인 접근은 자동적으로 접속되고 영상 녹취됩니다. 추가적인 층은 생물학적인 두 개의 함수 인증을 통해 개인적인 접근권한을 실행합니다. 담당자와 동반되지 않은 직원, 미신뢰 직원이나 방문자들은 해당 보안 구역으로 진입이 허용되지 않습니다.

물리적인 보안 시스템은, 'CSU들과 키 관련 자료의 온라인 및 오프라인상의 보관 모두를 보호하기 위하여 제공되는 키 관리 보안을 위한 추가 층'을 포함합니다. 암호화 자료를 생성하고 보관하기 위하여 사용되는 지역은 각각 '생물학적 사항을 포함한 두 개의 함수 인증'을 활용하여 이중 통제를 실행합니다. 온라인 CSU들은 폐쇄된 캐비넷 사용을 통하여 보호됩니다. 오프라인 CSU들은 폐쇄된 금고, 캐비넷과 컨테이너를 사용하여 보호됩니다.

CSU들과 키 관련 자료에 대한 접근 권한은 CrossCert의 의무 요건들 구분에 따라 제한됩니다. 이러한 층들 내의 캐비넷 혹은 컨테이너의 개폐는 감사 목적으로 접속됩니다..

5.1.3 전기 및 공기 조절(Power and Air Conditioning)

CrossCert의 보안 설비는 기본(primary) 장비 및 보완(backup) 장비로 구성되어 있습니다:

- 전력이 장애 없이 항시 사용될 수 있는 전력 시스템, 그리고
- 온도와 관련 습도를 조절하기 위한 열/환기/공기조절 시스템..

5.1.4 물에 대한 노출(Water Exposures)

CrossCert는 CrossCert 시스템들이 물에 노출되는 영향을 최소화하기 위하여 합리적인 범위의 사전 주의를 기울여야 합니다.

5.1.5 화재 예방 및 보호(Fire Prevention and Protection)

CrossCert는 화재 예방 및 진화 또는 기타 화염이나 연기에의 노출로 인한 손해를 예방하기 위하여 합리적인 범위의 사전 주의를 기울여야 합니다. CrossCert의 화재 예방과 보호조치는 현지 화재 안전 규정을 준수하도록 합니다.

5.1.6 미디어 저장(Media Storage)

생산 소프트웨어 및 데이터, 감사자료, 기록 또는 보완(backup) 정보는 CrossCert 설비 내에 보관되거나, 적절한 물리적 논리적 접근 통제체계를 보유하여 적정 권한 위임자만이 접근을 할 수 있도록 설계된 현지 저장 설비에 보관되어, 해당 미디어를 사고 (예를 들어, 홍수, 화재 및 전자기적 사고) 손해로부터 보호하여야 합니다.

5.1.7 폐기물 처분(Waste Disposal)

민감한 서류와 자료는 처분 전에 조각으로 잘러야 합니다. 민감한 정보를 취합하고 송부하는데 사용된 미디어는 처분 전에 '읽을 수 없는 것으로' 되어야 합니다. 암호화 장치는 물리적으로 폐기되거나, 처분 전에 제조자의 안내에 따라 초기화됩니다. 기타 다른 폐기물은 CrossCert의 일반 폐기물 처분 요건에 따라 처분됩니다.

5.1.8 부지 외 보충(Off-Site Backup)

CrossCert는 중대한 시스템 데이터, 감사 로그 데이터, 및 기타 민감한 정보에 대한 일상적인 보충(backup)을 수행합니다. '부지 외(Offsite)' 보충 미디어는, 연계된 제3자 보관 설비와 CrossCert의 재난 복구 설비를 활용하여 물리적으로 안전한 방식으로 보관됩니다.

5.2 절차상 통제(Procedural Controls)

5.2.1 신뢰된 역할(Trusted Roles)

신뢰받는 자(Trusted Persons)들은, 하기 사항에 중대한 영향을 미치는 인증 혹은 암호 조작을 통제하거나 접근할 수 있는 모든 직원, 하청업체 및 컨설턴트를 포함합니다:

- 인증서 신청서 상의 정보의 유효성;
- 인증서 신청, 폐지 요청, 갱신 요청, 또는 등록 정보의 처리나 수락, 거절;
- 저장소의 제한 구역에 대한 접근 권한을 가진 직원을 포함한, 인증서의 발행, 또는 폐지;
- 가입자 정보나 요청에 대한 처리.

신뢰받는 자들은, 이에 한정되지 않고, 다음 사항을 포함합니다:

- 고객 서비스 직원,,
- 암호화 사업 운영 직원,
- 보안 직원,,
- 시스템 행정 직원,
- 지정된 엔지니어링 직원, 및
- 기반(infrastructural) 신뢰도를 관리하도록 지정된 집행관들.

CrossCert 는 본 조항에서 '신뢰받는 자들(Trusted Persons) '로 분류된 직원들은 '신뢰받는 지위(Trusted Position)'를 가지는 것으로 간주됩니다. '신뢰받는 지위'를 획득함으로써 '신뢰받는 자들'이 되고자 하는 사람은 반드시 본 CPS 에서 규정한 요건을 성공적으로 통과하여야 합니다.

5.2.2 개별 임무에 대한 필요 인원 수(Number of Persons Required per Task)

CrossCert 는, 직무 책임에 근거한 업무 책임 구분을 확실히 하고 다수의 신뢰받는 자들이 민감한 업무를 수행하는 것을 확실히 하기 위하여 적극적인 통제 절차를 수립, 유지하고 집행하여야 합니다.

직무 책임에 근거한 임무 구분을 확실히 하기 위하여 정책과 절차는 수립되어 있습니다. CA 암호화 하드웨어에 대한 접근 권한 및 관리(암호 서명 단위 또는 CSU)와 같은 가장 민감한 업무들과 키 자료와 관련된 업무들은 다중의 신뢰받는 사람들이 요구됩니다.

이와 같은 내부 통제 절차는, '장치에 물리적 혹은 논리적 접근 권한을 확보하기 위하여는 최소한, 둘 이상의 신뢰받는 직원들이 요구되는 것을 확실히 하도록' 설계되었습니다. CA 암호화 하드웨어에 대한 접근 권한은 엄격하게 다중의 신뢰받는 사람들에 의하여

라이프사이클의 접수부터 최종 논리적 및/혹은 물리적 파괴에 이르기까지 집행되어야 합니다. 일단 모듈이 운영 키로 가동되면, 더 나아가 접근 통제가 물리적이고 논리적인 장치 접근 권한들 모두에 대한 분할 통제를 유발합니다. 모듈에 대한 물리적인 접근 권한을 가진 사람들은 “비밀 지분(Secret Shares)”을 보유하지 않으며, 그 반대의 경우도 마찬가지 입니다.

자동 유효화 및 발행 시스템에 의하여 발행되지 않은, 클래스 3 인증서의 유효화 및 발행과 같은 기타 수동 운영에는, 최소한 2 이상의 신뢰받는 사람들의 참여, 혹은 최소한 한 명의 신뢰받는 사람과 자동 유효화 및 발행 절차의 결합이 요구됩니다. 키복구에 대한 수동 운영은 선택적으로 2 명의 권한 있는 행정 담당자들의 유효화가 필요합니다.

5.2.3 각 역할에 대한 신원 확인과 인증(Identification and Authentication for Each Role)

신뢰받는 사람들로 되고자 하는 모든 직원들은 시만텍 인사과 혹은 보안 기능 부서에 실제 참석하여 통상적으로 신분 확인 기능을 하는 양식(예를 들어, 운전 면허증이나 여권)을 통해 신원확인과 인증을 받아야 합니다. 신원은 CPS 제 5 조 3 항 1 호에서 정한 절차에 따라 추가적으로 확인됩니다.

CrossCert 는, ‘직원들이 신뢰받는 지위를 확보했으며 해당 직원은 다음과 같은 사항에 대해 부서별 승인이 부여되었음’을 확실히 합니다:

- 접근 장치를 발급하였고 필요한 설비에 대한 접근 권한을 부여했음;
- STN CA, RA, 또는 IT 시스템에 대한 접근 권한을 가지고 특정 업무를 수행할 수 있는 전자적 암호를 발행함.

5.2.4 직무 구분이 요구되는 역할(Roles Requiring Separation of Duties)

직무 구분이 요구되는 역할들은 다음 사항을 (이에 한정하지 않고) 포함합니다

- 인증서 신청 상의 정보의 유효화;
- 인증서 신청의 수락, 거절, 혹은 기타 처리, 폐지 요청, 회복 요청, 또는 등록 정보;
- 인증서의 발행 혹은 폐지, 저장소의 제한 부분에 대한 접근 권한을 가진 직원 포함;
- 가입자 정보나 요청사항의 처리
- CA 인증서의 생성, 발행이나 폐기
- CA 를 생산 환경으로 끌어 올리는 것

5.3 직원 통제(Personnel Controls)

‘신뢰받는 사람’이 되고자 하는 직원들은, 각자의 직무 책임 수행에 필수적인 배경 증명서나 자격, 경력 증명서를 제출하여야 하며, 정부와의 계약상 인증업무를 위하여 필요한 경우에는 정부 발급 신원확인서도 제출하여야 합니다. 신뢰받는 지위를 보유하는 직원에 대한 배경 확인서는 최소한 5 년마다 반복되어야 합니다.

5.3.1 자격, 경력 및 신원 확인 요건(Qualifications, Experience, and Clearance Requirements)

CrossCert 는, 신뢰받는 사람이 되고자 하는 직원으로 하여금 배경, 자격, 및 각자의 직무 책임을 완전하고 만족스럽게 수행하기 위하여 필요한 경력을 증명하는 서류를 제출하여야 하며, 정부와의 계약상 인증업무를 위하여 필요한 경우에는 정부 발급 신원확인서도 제출하여야 합니다.

5.3.2 배경 확인 절차(Background Check Procedures)

CrossCert 는 ‘신뢰받는 역할’에 대한 고용을 시작하기 전에 다음 사항을 포함한 배경 확인을 수행하여야 합니다:

- 예전의 고용관계 확인,
- 직업적인 참조 추천 사항 확인,
- 최상위 혹은 가장 관련이 높은 학위 수령사항,
- 운전면허증 검색, 및
- 주민등록번호 검색

본 조항에 의하여 부과되는 요건이 현지 법규나 기타 환경상 금지된 경우에는, 해당 범위 내에서, CrossCert 는 적정한 정부 기관으로부터 배경 확인을 하는 것을 포함하여, 법률상 허용하는 범위 내에서 이를 대체할 만한 조사 기법을 사용할 수 있습니다.

배경 확인에서 드러난 사실들은 ‘신뢰받는 지위’ 후보를 거절하기 위한 근거로 간주될 수 있으며, 일반적으로 다음 사항을 범하는 신뢰받는 사람들에 대한 거절 근거로 간주할 수 있습니다:

- 후보 또는 신뢰받은 사람에 의한 오진술,
- 아주 좋지 않거나 믿을 수 없는 전문가 추천,
- 특정 범죄 범행, 그리고
- 재정 책임 부족에 대한 표시.

그러한 정보를 포함하는 기록은 인사과와 보안 직원들에 의해서 평가되며, 배경 확인을 통해 드러난 행동, 유형, 태도를 판단합니다. 그러한 행동은 해당 후보에 대한 고용 취소 혹은 현행 신뢰받은 사람들의 계약 해지 조치를 포함합니다.

해당 조치를 취하기 위해 배경 확인에서 드러난 정보의 사용은 관련 적용 법규에 따라야 합니다.

5.3.3 교육 요건(Training Requirements)

CrossCert 는 자신의 직원들이 해당 직무를 능숙하고 만족스럽게 수행할 수 있도록 직원들에 대한 고용 시부터 교육과 실무 수습을 제공하여야 합니다. CrossCert 는 해당 교육에 대한 기록을 유지하여야 합니다. CrossCert 는 해당 교육 프로그램을 정기적으로 평가하고 필요 시에는 강화하여야 합니다.

CrossCert 의 교육 프로그램들은 개별적인 책임과 다음 사항을 포함합니다:

- 기본 PKI 개념들,
- 직무 책임,
- CrossCert 보안 및 운영 정책과 절차,
- 배치된 소프트웨어 및 하드웨어의 사용과 운영,
- 사고 및 위반 신고 및 처리, 그리고
- 재난 복구 및 사업 계속 절차.

5.3.3.1 교육 및 기술 수준에 대한 CABF 요건(CABF Requirements for Training and Skill Level)

도메인 유효 및 기관 유효 SSL 인증서(Domain validated and organization validated SSL Certificates)는 CA / Browser Forum Baseline 요건을 준수합니다.

CrossCert는, 인증 업무를 수행하는 모든 직원들에게 기본 PKI 지식을 포괄하는 기술 교육, 인증 및 배팅 정책과 절차 (본 CPS 포함), 정보 인증 절차에 대한 일반적인 위협 (피싱 및 기타 소셜 엔지니어링 기법들) 및 상시적인 CABF 요건들에 대한 교육을 제공하여야 합니다.

CrossCert 는, 그러한 교육 기록을 유지하고, '유효화 전문가(Validation Specialists)' 업무에 신뢰되는 직원이 해당 업무를 만족스럽게 수행할 수 있도록 하여야 합니다. 인증서 발행에 간여하는 '유효화 전문가'는 CA 의 교육 및 수행 프로그램에 일치하는 기술 수준을 유지하여야 합니다.

CrossCert 는, 각 '유효화 전문가'가 업무 수행 이전에, 해당 업무 수행을 위하여 보유한 기술이 무엇인지를 기록하여 문서화합니다. CrossCert 는, 모든 '유효화 전문가'들이 CA 가 제공하는 'CABF 요건에 규정된 정보 인증 요건'에 관한 시험에 통과할 것을 필요로 합니다.

5.3.4 재교육 빈도 및 요건(Retraining Frequency and Requirements)

CrossCert 는, '해당 직원이 업무 책임을 능숙하고 만족스럽게 수행할 수 있는 숙련도를 유지할 수 있도록'하기 위하여 필요한 정도의 재교육과 업데이트를 제공합니다.

5.3.5 업무 순환 빈도 및 순서(Job Rotation Frequency and Sequence)

적용 사항 없습니다.

5.3.6 권한 없는 행동에 대한 처벌(Sanctions for Unauthorized Actions)

CrossCert 정책과 절차에 대한 '권한 없는 행위'나 기타 위반행위에 대하여는 적절한 징벌조치가 취해집니다. 징벌 조치에는 '권한 없는 행위'의 빈도와 구분에 따라 계약 해지 조치까지를 포함할 수 있습니다.

5.3.7 독립한 계약 당사자 요건(Independent Contractor Requirements)

제한적인 상황에서, 독립한 계약 당사자 또는 커널턴트는 '신뢰받는 지위'에 채워질 수 있습니다. 그러한 계약 당사자 혹은 컨설턴트는 해당 지위와 관련하여는 CrossCert 의 직원들과 동일한 기능과 보안 기준을 가지는 것으로 간주됩니다.

CPS 제 5 조 3 항 2 호에 따른 배경 확인을 완료하거나 통과하지 못한 독립 계약 당사자 혹은 컨설턴트는, 오직 신뢰받는 사람들에 의해 동반되거나 직접 감독되는 경우에만, CrossCert 의 보안 시설을 접근할 수 있습니다.

5.3.8 직원에 대하여 제공되는 서류(Documentation Supplied to Personnel)

CrossCert 는, 자신의 직원들에게 필요한 교육과 그들이 업무를 능숙하고 만족스럽게 수행하는 데 필요한 기타 서류를 제공합니다.

5.4 감사 개입 절차(Audit Logging Procedures)

5.4.1 기록된 사안의 유형(Types of Events Recorded)

CrossCert 는 다음과 같은 중대한 사안에 대하여 수동적으로건 자동적으로건 개입합니다:

- CA 키 라이프사이클 관리 사안, 이하 포함:

  - 키 생성, 보완, 저장, 복구, 기록, 및 파기
  - 암호화 장치 라이프사이클 관리 사안.
- CA 및 가입자 인증서 라이프사이클 관리 사안, 이하 포함:
  - 인증서 신청, 갱신, 키교체, 및 폐지
  - 요청에 대한 성공적이거나 실패적인 처리
  - 인증서 및 CRL 의 생성과 발행.
- 보안 관련 사안, 이하 포함:
  - 성공적이거나 실패적인 PKI 시스템 접근 시도
  - CrossCert 직원에 의한 PKI 및 보안 시스템 관련 행위
  - 보안에 민감한 파일이나 기록 열람, 작성이나 삭제
  - 보안 프로파일 변경
  - 시스템 충돌, 하드웨어 실패와 기타 비정상 현상들
  - 보안벽과 라우터 활동
  - CA 설비 방문자 출입.

로그 엔트리(Log entries)에는 다음과 같은 구성요소들을 포함합니다:

- 엔트리 일시
- 자동 저널 엔트리에 대한, 시리얼 혹은 순서 번호
- 저널 엔트리를 만드는 개체 신원
- 엔트리에 대한 설명/종류.

CrossCert RA 들과 기업 행정 담당자들은 다음 사항을 포함한 인증서 신청 정보에 접속합니다:

- 인증서 신청에 의하여 제출된 식별 서류의 종류
- 신분 서류의 고유 신원 데이터, 번호, 또는 그들의 조합(예를 들어, 인증서 신청자의 운전면허증 번호)
- 신청 및 식별 서류 사본의 저장 위치
- 신청을 수락하는 개체의 신원
- 신원 확인 서류를 유효화하기 위해 사용되는 방법
- 가능한 경우, 접수 CA 나 제출 RA 의 이름.

5.4.2 처리 접속 빈도(Frequency of Processing Log)

CA 시스템과 감사 접속(logs)은 중대한 보안 및 운영상의 사건에 대한 실시간 경보를 제공하기 위해 항시 감시됩니다. 그리고, CrossCert 는 CrossCert CA 와 RA 시스템에 발생하는 불규칙한 사건에 근거하여 발생되는 경보에 대한 의심스럽거나 비정상적인 활동에 대하여 자신의 감사 접속 상황을 평가합니다..

감사 접속 처리는 감사 접속과 감사 접속 요약본 내 중대한 사건 모두를 기록하는 것으로 구성됩니다. 감사 접속 평가는 '접속이 불규칙해지지는 않았는지에 대하여 모든 접속 엔트리를 확인하고, 접속상태마다 불규칙한 상황이나 경보가 있었는지를 조사하는' 확인절차를 포함합니다. 감사 접속 평가에 취해진 조치들도 기록됩니다.

5.4.3 감사 접속에 대한 보유 기간(Retention Period for Audit Log)

감사 접속 사항들은 처리된 후 최소한 2 개월 동안 현장에서 보유되며, 그 후에 제 5 조 5 항 2 호에 따라 기록됩니다.

5.4.4 감사 접속사항에 대한 보호(Protection of Audit Log)

감사 접속사항들은, 로그 파일(log files)을 권한 없는 열람, 변경, 삭제 혹은 기타 시도로부터 보호하기 위한 메카니즘을 포함한 '전자적 감사 로그 시스템(electronic audit log system)'으로 보호됩니다.

5.4.5 감사 접속사항 보완 절차(Audit Log Backup Procedures)

감사 접속사항들에 대한 점증적인 보완(backup)은 매일 생성되며, 완전한 보완은 1 주 단위로 수행됩니다.

5.4.6 (내부 對 외부) 감사 취합 시스템(Audit Collection System (Internal vs. External))

자동화된 감사 데이터는, 신청, 네트워크 및 운영 시스템 단계에서 생성되고 기록됩니다. 수동적으로 생성된 감사 데이터는 CrossCert 직원에 의해 기록됩니다.

5.4.7 사건 초래 대상에 대한 통지(Notification to Event-Causing Subject)

감사 취합 시스템에 의해 접속된 사건이 있는 경우에는, 해당 사건을 초래한 애플리캐이션이나 기관, 개인, 장치에 통보될 필요는 없습니다.

5.4.8 취약성 측정(Vulnerability Assessments)

감사 절차는, 부분적으로, 감시 시스템의 취약성에 접속됩니다. "논리적인 보안 취약성 측정(LSVAs)"은 이와 같은 감시 평가 후에 수행되고, 검토되며 수정됩니다. LSVAs 는 실시간 자동화된 접속 데이터에 근거하여 산출되고, 일, 월 및 연간 단위로 수행됩니다. 연간 LSVA 는 개체의 연간 '감사 준수(Compliance Audit)' 사항에 입력될 것입니다.

5.5 기록 보관(Records Archival)

5.5.1 보관 기록 유형(Types of Records Archived)

CrossCert 는 다음 사항을 보관합니다:

- 제 5 조 4 항에 따라 취합된 모든 감사 데이터
- 인증서 신청 정보
- 인증서 신청을 지원하는 서류화 정보
- 인증서 라이프사이클 정보, 예를 들어, 폐지, 키교체 및 갱신 신청 정보

5.5.2 기록 보관 기간(Retention Period for Archive)

인증서가 만료되거나 폐지되는 날로부터, 최소한, 하기에 규정된 기간 동안은 기록이 보관되어야 합니다.

- 클래스 1 인증서에 관하여는 5 년,
- 클래스 2 및 클래스 3 인증서에 대하여는 10 년 6 개월

5.5.3 기록의 보호(Protection of Archive)

CrossCert 는 기록을 보호하여, 오직 신뢰받는 사란들만이 해당 기록에 접근할 수 있도록 하여야 합니다. 기록은 '신뢰할만한 시스템(Trustworthy System)' 내에서 보관됨으로써 '권한 없는' 열람, 변경, 삭제 혹은 기타 시도로부터 보호됩니다. 기록 데이터와 기록 데이터 처리에 필요한 신청사항을 보유하는 미디어는, ' 기록 데이터가 본 CPS 에 규정된 기간 동안 접근될 수 있도록' 하여야 합니다.

5.5.4 기록 보완 절차(Archive Backup Procedures)

CrossCert 는 점진적으로 1 일 단위로 발행된 인증서 정보 전자 기록을 보완(back up)하여야 하고 1 주 단위로 완전 보완(full back up)을 실시합니다. 종이 기반 사본 기록들은 외부 안전 시설에서 보관되어야 합니다.

5.5.5 시점 인식 기록의 요건(Requirements for Time-Stamping of Records)

인증서, CRL 들, 및 기타 폐지 관련 데이터베이스 엔트리들은 시간과 날짜 정보를 포함하여야 합니다. 해당 시간 정보는 암호화 기반으로 되어야 할 필요가 없습니다.

5.5.6 (내부 혹은 외부) 기록 취합 시스템(Archive Collection System (Internal or External))

CrossCert 기록 취합 시스템들은, 기업 RA 고객들을 제외하면, 내부적입니다. CrossCert 는 자신의 기업 RA 들이 감사 자취를 보존하도록 지원합니다. 그러한 기록 취합 시스템은 그러므로 해당 기업 RA 에게는 외부적입니다.

5.5.7 기록 정보의 확보와 인증을 위한 절차(Procedures to Obtain and Verify Archive Information)

오직 권한 있는 '신뢰받은 직원들'만이 기록에 접근할 수 있습니다. 정보의 무결성은 저장되는 시점에서 인증됩니다.

5.6 키 변경(Key Changeover)

CrossCert CA 키 쌍들은 각자 CPS 에 규정된 최대 라이프타임 만료시에 서비스를 종료합니다. CrossCert CA 인증서는 CA 키 쌍의 축적된 인증 라이프타임이 CA 키 쌍의 최대 라이프타임을 초과하지 않았다면, 갱신될 수 있습니다. 신규 CA 키 쌍은필요한 경우에, 예를 들어, 종료된 CA 키 쌍을 대체하거나, 현존하는 가동중인 키 쌍들을 대체하고, 새로운 서비스를 지원하기 위한 경우에 생성될 것입니다.

상위 CA 에 대한 인증서 만료료 이전에, 키 교체 절차는, 오래전의 상위 CA 키 쌍에서부터 신규 CA 키 쌍까지의 상위 CA 의 수직계층 안의 개체들에 대한 완만한 변경을 활성화하기 위하여 집행됩니다. CrossCert 의 CA 키 변경 절차는 다음 사항을 요구합니다:

- 상위 CA 는, 상위 CA 의 지배 구조에서 상위 CA 키 쌍이 '하위 CA 들에 의하여 발행된 특정 유형의 '승인된 인증서 발효 기간'이 상위 CA 키 쌍의 잔존 생애기간과 동일한 경우에, 해당 시점 전 60 일 전("중단 발행 일자")보다 늦지 않게, 새로운 하위 CA 인증서 발행을 중단합니다.
- 하위 CA 인증서(또는 최종 사용자 가입자)의 성공적인 유효화 요청이 "발행 중단일자" 후에 수령된 경우에는, 인증서는 새로운 CA 키 쌍으로 서명될 것입니다.

상위 CA 는, 원래의 키 쌍을 사용하여 발행된 인증서의 마지막 만료일까지 원래의 상위 CA 개인키를 가지고 서명한 CRL 들을 계속하여 발행합니다.

5.7 위반과 재난 복구(Compromise and Disaster Recovery)

5.7.1 절차를 취급하는 사건과 위반(Incident and Compromise Handling Procedures)

CA 정보에 대한 보완(backup)은 외부 보관소에 보유되어야 하며, 위반 혹은 재난의 경우에 가용하여야 합니다: 발행된 모든 인증서에 대한 인증서 신청 데이터, 감사 데이터, 그리고 데이터베이스 기록들. CA 개인키들의 보완(backup)은 CP 제 6 조 2 항 4 호에 따라 생성되고 관리됩니다. CrossCert 는 자신의 CA 들에 대한 전술한 CA 정보에 대한 보완(backup)과 서브도메인 내 기업 고객들의 CA 들에 대한 보완사항도 유지합니다.

5.7.2 컴퓨팅 자원, 소프트웨어, 그리고/혹은 데이터가 변질된 경우(Computing Resources, Software, and/or Data Are Corrupted)

만일 컴퓨팅 자원, 소프트웨어, 그리고/혹은 데이터의 변질이 있는 경우, 해당 사항 발생이 CrossCert 보안실에 신고되고 CrossCert 의 사건 처리 절차는 수행됩니다. 그러한 절차들은 적정한 사고 조사, 그리고 사고 대응이 필요합니다. 만일 필요한 경우에는, CrossCert 의 키 위반 혹은 재난 복구 절차는 실행될 것입니다.

5.7.3 개체의 개인키 위반 절차(Entity Private Key Compromise Procedures)

CrossCert CA 의 의심스럽거나 알려진 위반이 있는 경우, STN 인프라 또는 고객 CA 개인키, CrossCert 의 키 위반 대응 절차는 'CrossCert 보안시고 대응팀(CSIRT)'에 의하여 집행됩니다. 해당 팀은, 보안, 암호화 사업 운영, 생산 서비스 직원, 그리고 기타 시만텍 관리 대표, 상황 분석, 실행 계획의 개발, 그리고 CrossCert 집행 관리 위원들의 승인사항을 실행합니다.

CA 인증서 폐지가 요구된 경우에는, 아래와 같은 절차는 수행되어야 합니다:

- 인증서의 폐지 상태는 CPS 제 4 조 9 항 7 호에 따라 CrossCert 저장소를 통해 신뢰받는 사람들에게 소통됩니다.
- STN 참여자들 모두에게 추가적인 폐지 통지를 제공하기 위하여 상업적으로 합리적인 노력을 기울여야 합니다. 그리고
- CA 는, CA 가 CPS 제 5 조 8 항에 따라 계약 해지되는 경우를 제외하면, CPS 제 5 조 6 항에 따라 신규 키 쌍을 생성하기로 합니다.

5.7.4 재난 후 사업 계속 능력(Business Continuity Capabilities after a Disaster)

시만텍은 사업 계속 계획(plan)을 창출하고 보유하여, 사업 곤란 사유 발생 시에도 주요 사업 기능들은 새로운 재개될 수 있습니다. 시만텍은 재난복구시설(Disaster Recovery Facility:

DRF)을 기본 생산 설비로부터 지역적으로 별도 소재한 '시만텍-소유' 설비에 유지합니다. DRF는 국가와 군사적 사양에 적정하게 설계된 설비이며, 시만텍의 보안 기준을 충족하도록 설계되었습니다.

시만텍의 기본 설비 운영의 영구적인 중단을 요구하는 자연적 혹은 인위적 재난이 발생한 경우에는,' 시만텍 사업 계속 팀(Corporate Symantec Business Continuity Team) '과 '시만텍 인증 운영 사건관리 팀(Symantec Authentication Operations Incident Management Team)'은 상호 협의하여 공식적으로 재난 상황과 사건 처리에 관한 판단을 하여야 합니다. 일단 재난 상황이 선언되면, DRF에서의 시만텍의 생산 서비스 기능은 개시됩니다.

시만텍은 managed PKI 서비스에 대한 '재난복구 계획(Disaster Recovery Plan; DRP)'을 개발해 왔습니다. DRP는 사건 발생과 회복시간 내에 필요한 적정한 시스템이 무엇이고 해당 계획을 실행하기 위한 조건들은 무엇인지 규정합니다. DRP는, 'STN 키들 사본의 보완(backup)과 보완 데이터를 사용한 시만텍 STN 운영을 재개하기 위한 팀 절차'를 규정합니다. 또한, 시만텍의 DRP는 다음사항들을 포함합니다:

- 필수 사업정보와 소프트웨어 보완(backup) 사본 확보에 관한 빈도,
- 대체 장소에서 암호화 자료를 저장하는 요건들(즉, 안전한 암호화 장치 및 가동 자료),
- CA 의 주요 소재지에서 재난 복구 장소와의 분리 거리,
- 원래 장소 또는 원격 장소에서 재난 발생 후부터 복구될 때까지 재난 설비를 안전하게 하기 위한 절차,

시만텍의 DRP 는 다음 사항을 포함한 행정 요건들을 표시합니다:

- 계획에 대한 유지 보수 일정;
- 인지 및 교육 요건들;
- R 개인들의 책임; 그리고
- 비상 계획에 대한 정기적인 테스트.

중요 생산 서비스 기능에 대한 목표 복구 시간은 24시간이 넘지 않습니다.

시만텍은, DRF 에서 서비스 기능성을 확실히 하기 위하여, 매년 최소한 1 회이상의 재난 복구 테스트를 실시합니다. 공식적인 사업 계속 훈련(Formal Business Continuity Exercises)도 해마다 시만텍 사업 계속성 팀(Corporate Symantec Business Continuity Team)의 지휘 하에 추가 시나리오(예를 들어, 지진, 홍수, 정전 등)에 대하여 실시되고 평가됩니다.

시만텍은 안정적인 사업 복구 계획을 개발, 유지하고 테스트하기 위한 중대한 조치를 취해야 하며, 재난 상황이나 심각한 사업 장애상황에 대한 시만텍의 계획은 동종 업계에 형성된 최고 업무 관행에 부합하여야 합니다.

시만텍은 재난 복구 시설에 하드웨어를 감축하고 CA 의 보완(backup) 및 기반 시스템 소프트웨어를 유지합니다. 또한, CA 개인키들은 CPS 제 6 조 2 항 4 호에 따라 재난 복구 목적을 위하여 보완(back up)되고 유지됩니다.

시만텍은 시만텍 CA 들과 시만텍의 서브 도메인 내 서비스 센터와 기업 고객의 CA 들을 위하여 중요한 CA 정보의 원격지 보완(backup)을 유지합니다. 그러한 정보는 다음을, 이에 한정하지 않고, 포함합니다: 인증서 신청 데이터, 감사 데이터(제 4 조 5 항 기준), 그리고 발행된 모든 인증서에 대한 데이터베이스 기록들.

인증서를 발행하는 주체가 CrossCert (CPS 제 1 조 1 항 참조)인 경우의 서비스에 대하여는, CrossCert 본사의 안전한 시설로부터 23km 이상 떨어진 곳에 재난 복구 장소를 설정합니다. CrossCert 는 모든 종류의 자연적 혹은 인위적 재난의 영향을 줄이기 위한 재난 복구 계획을 개발, 실행 및 테스트해 왔습니다. 이러한 계획은 정기적으로 테스트되며, 확인되고, 재난 시에 운영될 수 있게 업데이트됩니다.

상세한 재난 복구 계획은 정보 시스템 서비스의 복구와 주요 사업 기능을 설명하기 위해 편성됩니다. CrossCert 의 재난 복구 장소는 물리적인 보안 보호 및 안전하고 안정적인 보완 운영 체계를 제공하기 위하여 시만텍 보안 감사 요건들(Symantec Security and Audit Requirements; SAR) 을 실행합니다.

CrossCert 의 기본 설비에서 임시 혹은 영구적인 운영 중단이 필요한 자연 또는 인위적인 재난이 발생하는 경우, CrossCert 의 재난 복구 절차는 CrossCert 의 '긴급상황 대응팀(CrossCert Emergency Response Team; CERT)'에 의하여 시작됩니다.

CrossCert 는 재난 발생 1 주일 이내에 최소한 다음 기능들에 대한 지원이나, 운영 복구를 위한 능력을 갖출 것입니다:

- 인증서 발행,
- 인증서 폐지,
- 폐지 정보의 게재, 그리고
- Managed PKI Key Manager 를 사용하는 Managed PKI 고객들을 위한 키복구 정보 제공.

CrossCert 의 재난 복구 데이터베이스는 정기적으로 SAR 가이드에 규정된 시간 내에 동시 생성되어야 합니다. CrossCert 의 재난 복구 장치는 CPS 제 5 조 1 항 1 호에 규정된 보안층들에 비교할만한 물리적 보안 보호체계로 보호될 것입니다.

CrossCert 의 재난 복구 계획은 CrossCert 의 주 소재지에서 재난이 발생한 지 1 주 이내에 완전 복구를 할 수 있도록 설계되었습니다. CrossCert 는 자신의 주 소재지에서, 전체 설비를 운영할 수 없게 하는 재난을 제외하고, 대부분의 재난 발생 시 CA/RA 기능을 지원하기

위하여 설비를 테스트합니다. 그러한 테스트 결과는 감사 및 계획 목적으로 검토되고 보관됩니다. 가능한 경우, 주요 재난 후에 가능한한 빨리 운영은 재개되도록 합니다.

CrossCert 는 재난 복구 시설에 하드웨어를 감축하고 CA 의 보완(backup) 및 기반 시스템 소프트웨어를 유지할 것입니다. 또한, CA 개인키들은 CPS 제 6 조 2 항 4 호에 따라 재난 복구 목적을 위하여 보완(back up)되고 유지됩니다.

CrossCert 는 CrossCert CA 들과 CrossCert 의 서브 도메인 내 서비스 센터와 Managed PKI 고객들을 위하여 중요한 CA 정보의 원격지 보완(backup)을 유지합니다. 그러한 정보는 다음을, 이에 한정하지 않고, 포함합니다: 신청 로그, 인증서 신청 데이터, 감사 데이터(제 4 조 5 항 기준), 그리고 발행된 모든 인증서에 대한 데이터베이스 기록들.

DRP는 사건 발생과 회복시간 내에 필요한 적정한 시스템이 무엇이고 해당 계획을 실행하기 위한 조건들은 무엇인지 규정합니다. 또한, CrossCert 의 DRP는 다음사항들을 포함합니다:

- 필수 사업정보와 소프트웨어 보완(backup) 사본 확보에 관한 빈도,
- 대체 장소에서 암호화 자료를 저장하는 요건들(즉, 안전한 암호화 장치 및 가동 자료),
- CA 의 주요 소재지에서 재난 복구 장소와의 분리 거리,
- 원래 장소 또는 원격 장소에서 재난 발생 후부터 복구될 때까지 재난 설비를 안전하게 하기 위한 절차,

CrossCert 의 DRP 는 다음 사항을 포함한 행정 요건들을 표시합니다:

- 계획에 대한 유지 보수 일정;
- 인지 및 교육 요건들;
- 개인들의 책임; 그리고
- 비상 계획에 대한 정기적인 테스트.

5.8 CA 또는 RA 계약의 종료(CA or RA Termination)

CrossCert 혹은 기업고객 CA 가 운영을 중단할 필요가 있는 경우에는, CrossCert 는 그러한 CA 계약 종료 이전에 해당 종료로 인해 영향을 받을 수 있는 사람들과 가입자, 신뢰자들에게 상업적으로 합리적인 범위 내에서 통지하는 노력을 기울여야 합니다. CA 계약 종료가 필요한 경우에는, CrossCert 와, 고객 CA 의 경우에는 해당 고객은, 고객들, 가입자들 및 신뢰자들에게 불폄을 최소화하기 위한 계약 종료 계획을 개발해야 합니다. 해당 계약 종료 계획은, 필요한 경우, 다음 사항을 표시할 수 있습니다:

- 계약 종료에 영향을 받는 사람들인, 가입자, 신뢰자들, 및 고객들과 같은 사람들에게 통지하여 CA 의 상태를 알림,
- 해당 통지의 비용 처리,

- CrossCert 에 의해 CA 에게 발행된 인증서의 폐지,
- 본 CPS 에서 필요한 기간에 대한 CA 의 기록 보존,
- 가입자 및 고객 지원 서비스의 계속,
- CRL 들이나 온라인 상태 확인 서비스 유지보수와 같은 폐지 서비스의 계속,
- 필요한 경우, 최종 사용자 가입자와 하위 CA 들의 '만료되지 않고 폐지되지 않은' 인증서의 폐지,
- 계약 종료 계획에 따라 폐지되는 유효한 인증서들의 가입자들에게 (필요한 경우) 환불하거나, 이에 대한 대체안으로, CA 승계자로 하여금 대체 인증서를 발행하여 제공함,
- CA 의 개인키 및 해당 개인키를 포함하는 하드웨어 표식의 처분, 그리고
- CA 의 서비스를 CA 승계자에게 이전하는 데 필요로 하는 사항을 제공함.

5.9 데이터 보안(Data Security)

5.9.1 목적(Objectives)

CrossCert는 하기 사항을 위하여 종합적인 보안 프로그램을 개발, 이행하고 유지합니다:

1. 인증서 데이터 및 인증서 관리 절차의 기밀성, 통합 무결성, 및 가용성을 보호;
2. 인증서 데이터 및 인증서 관리 절차의 기밀성, 통합 무결성, 및 가용성에 위협이나 위험요소가 되는 것으로부터 보호;
3. 인증서 데이터 혹은 인증서 관리 절차에 대한 '권한 없는' 혹은 '불법적인' 접근, 사용, 공개, 변경이나 파괴로부터 보호;
4. 인증서 데이터 혹은 인증서 관리 절차에 대한 사고 손실 혹은 파괴, 혹은 손해로부터 보호; 그리고
5. 법규상 CA 에 대하여 적용되는 기타 모든 요건들을 준수.

5.9.2 위험 측정(Risk Assessment)

CrossCert는 아래와 같은 위험 측정을 매년 실시합니다:

1. 인증서 데이터나 인증서 관리 절차에 권한 없는 접근이나 공개, 오사용, 변경이나 파괴를 초래할 수 있는 내외부적으로 예측이 가능한 위협요소를 표시함;
2. 인증서 데이터나 인증서 관리 절차의 민감도를 고려하여 위협에 대한 잠재적 손해 발생 가능성과 규모에 대하여 측정함; 그리고
3. 해당 위협에 직면한 CA 의 정책, 절차, 정보 시스템, 기술 및 다른 사항들에 대한 충분성에 대한 측정함.

5.9.3 보안 계획(Security Plan)

연간 위험 측정 결과에 근거하여, CrossCert 는 보안 절차, 조치, 및 인증서 데이터와 인증서 관리 절차를 고려하여 해당 목적을 달성하기 위한 제품과 위험 측정 시에 나타난 위험사항들을 관리하고 통제하기 위한 사항들을 포함한 보안 계획을 개발, 이행하고 유지합니다.

보안 계획에는, 인증서 데이터와 인증서 관리 절차의 민감도에 적정한 행정적, 조직적, 기술적, 및 물리적인 안전장치를 포함합니다. 보안 계획은 해당 시점에 가용한 기술과 특정 조치에 소요되는 비용 및 보안 규정 위반 시 초래될 손해와 보호 특성에 합리적으로 적합한 수준으로 고려됩니다.

6. 기술적 보안 통제(Technical Security Controls)

6.1 키 쌍 생성 및 설치(Key Pair Generation and Installation)

6.1.1 키 쌍 생성(Key Pair Generation)

CA 키 쌍 생성은, 사전에 선정된 교육받은 신뢰받는 다수의 개인들에 의하여 신뢰 시스템과 생성된 키에 필요한 암호 강도와 보안 절차를 통하여 생성됩니다. PCA 와 발행 루트 CA 들, 키 생성을 위한 암호화 모듈은, FIPS 140-1, 3 단계 요건을 충족합니다. (CrossCert CA 들과 Managed PKI Customer CA 들을 포함한) 다른 CA 들, 암호화 모듈들은 FIPS 140-1, 2 단계 요건을 충족합니다.

모든 키 쌍들은 키 세레모니 참조 가이드 요건(Key Ceremony Reference Guide), CA 키 관리 도구 이용자 가이드(CA Key Management Tool User's Guide), 및 시만텍 SAR 가이드에 따라 사전에 계획된 키 생성 세레모니에 생성됩니다. 각 키 생성 세레모니에서 수행된 활동들은 모든 관여자들에 의하여 기록되며, 일자와 서명됩니다. 이러한 기록들은 CrossCert 경영진이 적정하다고 판단하는 기간 동안 감사와 추적 목적으로 보유됩니다.

RA 키 쌍의 생성은 일반적으로 브라우저 소프트웨어에서 공급받은 FIPS 140-1, 1 단계 암호화 모듈을 사용하여 RA 에 의해서 수행됩니다.

기업 고객들은 자동화된 행정 서버들(Automated Administration servers)에 의해 사용되는 키 쌍을 생성합니다. CrossCert 는, 자동화된 행정 서버 키 쌍 생성이 FIPS 140-1, 2 단계 인증 암호화 모듈을 사용하여 수행될 것을 권장합니다.

최종 사용자 가입자 키 쌍은 일반적으로 가입자에 의하여 생성됩니다. 클래스 1, 클래스 2 인증서 및 클래스 3 code/object 서명 인증서에 대하여는, 가입자는, 키 생성을 위해 브라우저 소프트웨어로부터 제공받은 FIPS 140-1, 1 단계 인증된 암호화 모듈을 일반적으로 이용합니다. 서버 인증서에 대하여는, 가입자는 전형적으로 웹서버 소프트웨어에 제공된 키 생성 유틸리티를 사용합니다.

ACS Application ID 들에 대하여는, CrossCert 는, 최소한 3 단계 요건을 충족하는, 암호화 모듈에서 무작위로 생성된 숫자를 사용하여 가입자를 대신하여 키 쌍을 생성합니다.

6.1.2 가입자에 대한 개인키 전달(Private Key Delivery to Subscriber)

최종 사용자 키 쌍이 최종사용자 가입자에 의하여 생성된 경우, 가입자에 대한 개인키 전달은 적용되지 아니합니다. ACS Application ID 들에 관해서도, 가입자에 대한 개인키 전달도 적용사항이 없습니다.

RA 혹은 최종 사용자 가입자 키 쌍이 CrossCert 에 의하여 사전에 하드웨어 표식이나 스마트 카드에 생성되어 있는 경우에는, 해당 장치들은 RA 나 최종 사용자 가입자에게 상업적 배송 서비스를 활용하여 배포됩니다. 해당 장치를 가동하기 위하여 필요한 데이터는 밴드 절차를 활용하여 RA 나 최종 사용자 가입자에게 소통 됩니다. 해당 장치의 배포는 CrossCert 에 의하여 접속됩니다.

최종 사용자 가입자 키 쌍이 기업 고객들에 의하여 사전에 하드웨어 표식이나 스마트 카드에 생성되어 있는 경우에는, 해당 장치들은 최종 사용자 가입자에게 상업적 배송 서비스를 활용하여 배포됩니다. 해당 장치를 가동하기 위하여 필요한 데이터는 밴드 절차를 활용하여 RA 나 최종 사용자 가입자에게 소통 됩니다. 해당 장치의 배포는 기업 고객에 의하여 접속됩니다.

키 복구 서비스를 위하여 Managed PKI Key Manager 를 사용하는 기업 고객에 관하여는, 고객은 (인증서 신청이 승인된 가입자들을 대신하여) 암호 키 쌍을 생성하고 해당 키 쌍을 가입자에게 암호로 보호된 PKCS # 12 파일을 통해 전달할 수 있습니다.

6.1.3 인증서 발행자에 대한 공개키 전달(Public Key Delivery to Certificate Issuer)

최종 사용자 가입자들과 RA 들은 PKCS#10 인증서 서명 요청(Certificate Signing Request; CSR)이나 Secure Sockets Layer (SSL)로 보호되는 세션의 디지털 서명 패키지를 통하여 시만텍에게 인증을 위한 공동키를 제출합니다 CA, RA, 또는 최종 사용자 가입자 키 쌍이 시만텍에 의하여 생성되는 경우에는, 이러한 요건은 적용되지 않습니다.

6.1.4 신뢰자에 대한 CA 공개키 전달(CA Public Key Delivery to Relying Parties)

CrossCert 는, 시만텍 PCA 들과 루트 CA 들을 위한 CA 인증서를 그들의 웹 브라우저 소프트웨어에 포함시켜 가입자들과 신뢰자들이 이용할 수 있게 합니다. 새로운 PCA 와 루트 CA 인증서가 생성되면 CrossCert 는 브라우저 개발업체에 새로운 인증서를 제공하여 신규 브라우저 출시와 업데이트에 포함되도록 합니다.

CrossCert 는 인증서 발행 시 최종 사용자 가입자에게 (발행 CA 및 체인 내 모든 CA 들을 포함) 모든 인증 체인을 제공합니다. CrossCert CA 인증서는 CrossCert LDAP 디렉토리인 *directory. Crosscert.com* 에서도 다운로드할 수 있습니다.

6.1.5 키 크기(Key Sizes)

키 쌍은 타인들이 해당 키의 개인키를 판별하지 못하도록 키 쌍의 사용기간 동안 암호분석을 사용하여 충분한 길이로 구성되어야 합니다. 최소 키 크기에 대한 CrossCert 기준은 강도 상 PCA 들 및 CA 들에 대하여 2048 비트 RSA 키 쌍의 사용입니다[14].

시만텍의 제 3 및 제 5 세대(G3 및 G5) PCA 들은 2048 비트 RSA 키 쌍을 가집니다.

시만텍은 RA 들과 최종 개체 인증서 키 쌍에 대하여 최소한 2048 비트 RSA 와 같은 강도의 키 크기로 발행합니다.

시만텍의 제 4 세대(G4) 클래스 3 PCA(ECC 총괄 루트 CA)는 384 비트 ECC 키를 포함합니다.

STN 의 모든 클래스들과 CrossCert PCA 들 및 CA 들과 RA 들 및 인증서 최종 개체는 디지털 서명 해쉬 알고리즘으로 SHA-1 이나 SHA-2 를 사용하고 시만텍 처리 센터의 특정 버전들은 최종 개체 가입자 인증서에 SHA-256 과 SHA-384 해쉬 알고리즘의 사용을 지원합니다.

6.1.5.1 키 크기에 대한 CABF 요건(CABF Requirements for Key Sizes)

도메인 유효 및 기관 유효 SSL 인증서는 CA /Browser Forum Baseline 요건들을 준수합니다.

---

[14] CA 신뢰는 시만텍의 1 세대 및 2 세대 Trusted Roots 1024 비트 키 쌍으로 연장되며, 기존 고객 플랫폼과 1024 비트 RSA 최종 개체 인증서는 2011 년 12 월 31 일 전까지의 유효기간으로 발행될 수 있음. 2011 년을 초과하는 기존 애플리케이션의 사업 계속성을 보전하기 위해 사전 승인 하에 제 6 조 3 항 2 호에 따라 시만텍의 계열사가 운영하는 프로세싱 센터 소프트웨어에 대하여는 추가로 개별적인 예외는 허용될 수 있음.

루트 CA 인증서들은 알고리즘 유형과 키 크기에 대하여 다음 요건들을 충족하여야 합니다:

	2010년 12월 31일 전에 개시된 유효 기간	2010년 12월 31일 이후부터 개시된 유효기간
축소 알고리즘	MD5는 권고되지 않음, SHA-1, SHA-256, SHA-384 또는 SHA-512	SHA-1*, SHA-256, SHA-384 또는 SHA-512
최소 RSA 모듈 크기(비트)	2048**	2048
ECC 커브	NIST P-256, P-384 또는 P-521	NIST P-256, P-384 또는 P-521

표 4A – 루트 CA 인증서에 대한 CA / Browser Forum 알고리즘 및 키 크기

하위 CA 인증서들은 알고리즘의 유형과 키 크기에 대하여 다음 요건들을 충족해야 합니다:

	2010년 12월 31일 전에 개시되고 2013년 12월 31일 이전에 종료되는 유효 기간	2010년 12월 31일 전에 개시되거나 2013년 12월 31일 이후에 종료되는 유효 기간
축소 알고리즘	SHA-1, SHA-256, SHA-384 또는 SHA-512	SHA-1*, SHA-256, SHA-384 또는 SHA-512
최소 RSA 모듈 크기(비트)	1024	2048
ECC 커브	NIST P-256, P-384 또는 P-521	NIST P-256, P-384 또는 P-521

[표 4B]– 하위 CA 인증서에 대한 CA / Browser Forum 알고리즘 및 키 크기

CA 들은 오직 다음 유형의 알고리즘과 키 크기를 가지는 키들을 가지는 가입자 인증서만을 발행하여야 합니다.

	2013년 12월 31일 이전에 종료되는 유효 기간	2013년 12월 31일 이후에 종료되는 유효 기간
축소 알고리즘	SHA-1*, SHA-256, SHA-384 또는 SHA-512	SHA-1*, SHA-256, SHA-384 또는 SHA-512
최소 RSA 모듈 크기(비트)	1024	2048
ECC 커브	NIST P-256, P-384 또는 P-521	NIST P-256, P-384 또는 P-521

[표 4C] – 가입자 인증서에 대한 CA / Browser Forum 알고리즘 및 키 크기

* SHA-1 는 세계의 신뢰자들에 의해 상당히 많은 비율로 사용되는 브라우저에 의해 SHA-256 이 지원되는 때까지 사용될 수 있습니다

** 2010 년 12 월 31 일 전에 RSA 키 크기로 2048 비트 미만인 루트 CA 인증서는 본 요건에 따라 트러스트 앵커 가입자 인증서들이 발행되는 데 사용될 수 있습니다..

CrossCert CA 들은, 필요한 공개키가 본 조항에서 규정된 최소 알고리즘 키 크기를 충족하지 못하면, 인증서 요청을 거절하여야 합니다.

6.1.6 공개키 매개변수 생성 및 품질 확인(Public Key Parameters Generation and Quality Checking)

해당 사항 없습니다.

6.1.7 (X.509 v3 키 사용 영역에 대한) 키 사용 목적(Key Usage Purposes (as per X.509 v3 Key Usage Field)

제 7 조 1 항 2 호 1 목 참조 바랍니다.

6.2 개인키 보호 및 암호화 모듈 엔지니어링 통제(Private Key Protection and Cryptographic Module Engineering Controls)

CrossCert 는 자신과 기업 고객 CA 개인키들의 안전을 확실히 하기 위하여 물리적, 논리적이고 절차적인 통제 결합을 수행합니다. 가입자들은 개인키의 권한 없는 사용과 변경, 공개Ⅱ, 혹은 손실을 막기 위하여 필요한 사전 주의 조치를 취하기 위한 계약이 필요합니다.

6.2.1 암호화 모듈 기준과 통제(Cryptographic Module Standards and Controls)

PCA 및 발행 루트 CA 키 쌍 생성과 CA 개인키 저장에 대해서는, CrossCert 는 'FIPS 140-1, 3 단계 요건을 충족하는' 인증된 하드웨어 암호화 모듈을 사용합니다.

6.2.2 개인키 (m/n) 다중인 통제(Private Key (m out of n) Multi-Person Control)

CrossCert 는 다중의 신뢰받는 사람들이 민감한 CA 암호화 조작을 수행하기 위하여 필요한 기술적 절차적 메카니즘을 실행합니다. CrossCert 는, 분리된 부분으로 CA 개인키를 사용하기 위한 가동 데이터를 분산하기 위해 "비밀 공유(Secret Sharing)"라고 불리우는 업무를 수행하고, "지분보유자(Shareholders)"라고 불리우는 신뢰받는 자들에 의해 교육됩니다. 비밀 공유의 핵심 수는 (m) 특정 하드웨어 암호화 모듈에 대하여 생성되고 배포된 비밀 공유 전체의 수 중에서, (n) 모듈에 저장된 CA 개인키를 가동하는데 필요합니다.

CA 인증서를 서명하기 위하여 요구된 지분 핵심 수는 3 입니다. 재난 복구 표식으로 배포된 지분의 수는, 요구되는 핵심 필요 지분이 동일하게 유지되기는 하지만, 운영상의 표식에

대하여 배포된 수보다 적을 수 있음을 유의하여야 합니다. 비밀 지분은 본 CPS 에 따라 보호됩니다.

6.2.3 개인키 에스크로우(Private Key Escrow)

CA 개인키는 에스크로우 되지 않습니다. 최종 사용자 가입자를 위한 개인키 에스크로우는 제 4 조 12 항에 더 상세히 설명됩니다.

6.2.4 개인키 보완(Private Key Backup)

CrossCert 는 일상적인 복구와 재난 복구 목적으로 CA 개인키의 보완(backup) 사본을 생성합니다. 그러한 키들은 하드웨어 암호화 모듈 내에서 암호화된 양식으로 저장되며, 키 저장 장치에 연계됩니다. CA 개인키 저장에 사용되는 암호화 모듈은 본 CPS 의 요건을 충족합니다. CA 개인키는 본 CPS 에 따라 '보완(backup) 하드웨어 암호화 모듈'로 복사됩니다.

CA 개인키들의 보완 사본을 포함하는 모듈은 본 CPS 상의 요건을 따릅니다. CA 개인키들의 재난 복구 사본을 포함한 모듈은 본 CPS 의 요건을 따릅니다.

CrossCert 는 RA 개인키의 사본을 보관하지 않습니다. 최종 사용자 가입자 개인키들에 대한 보완(backup)에 관하여는, 제 6 조 2 항 3 호 및 제 4 조 12 항을 참조하시기 바랍니다. ACS 애플리케이션 ID 들에 관하여는, CrossCert 는 가입자 개인키들의 사본을 보관하지 않습니다.

6.2.5 개인키 기록 보관(Private Key Archival)

CrossCert CA 인증서 만료 시, 인증서와 관련된 키 쌍은, 본 CPS 요건을 충족하는 하드웨어 암호화 모듈을 사용하여 최소한 5 년 기간 동안 안전하게 보관됩니다. 이러한 CA 키 쌍들은, CA 인증서가 본 CPS 에 따라 갱신되지 않은 한, CA 인증서에 부합하는 유효기간 후에 일체의 서명을 위해 사용되어서는 아니됩니다.

CrossCert 는 RA 와 가입자 개인키들의 사본을 기록 보관하지 않습니다.

6.2.6 암호화 모듈에서의 개인키 전달(Private Key Transfer Into or From a Cryptographic Module)

CrossCert 는 CA 키 쌍을 하드웨어 암호화 모듈에 생성하고, 해당 키들은 생성 과정에 사용됩니다. 추가로, CrossCert 는 해당 CA 키 쌍들의 사본을 일상적인 복구와 재난 복구 목적으로 만듭니다. CA 키 쌍들이 다른 하드웨어 암호화 모듈로 보완되면, 해당 키 쌍들은 암호화된 양식으로 모듈 간에 이전됩니다.

6.2.7 암호화 모듈에 대한 개인키 저장(Private Key Storage on Cryptographic Module)

하드웨어 암호화 모듈들에 보유된 CA 나 RA 개인키들은 암호화된 형식으로 저장되어야 합니다.

6.2.8 개인키 가동 방법(Method of Activating Private Key)

모든 CrossCert 서브 도메인 참여자들은, 개인키들에 대한 가동 데이터를 분실, 도난, 변조, 권한 없는 공개, 혹은 권한 없는 사용으로부터 보호해야 합니다.

6.2.8.1 클래스 1 인증서(Class 1 Certificates)

클래스 1 개인키 보호 기준은, 가입자들이 워크 스테이션에서 가입자의 워크 스테이션을 물리적으로 보호하고, 가입자의 권한 위임 없이 관련된 개인키들이 사용되지 않도록 상업적으로 합리적인 조치를 취하는 것입니다. 그리고, CrossCert 는, '가입자들이 제 6 조 4 항 1 호 또는 개인키 가동 전에 가입자를 인증하는 것과 동등한 강도의 보안기준에 따라 암호를 사용할 것'을 권고하며, 이는, 예를 들어, 개인키, 윈도우 로그온 혹은 화면 보호기 암호나 네트워크 로그온 암호를 포함합니다.

6.2.8.2 클래스 2 인증서(Class 2 Certificates)

클래스 2 개인키 보호 기준은, 가입자들이 아래의 사항을 하도록 하는 것입니다:

- 제 6 조 4 항 1 호 또는 개인키 가동 전에 가입자를 인증하는 것과 동등한 강도의 보안기준에 따라 암호를 사용할 것'을 권고하며, 이는, 예를 들어, 개인키, 윈도우 로그온 혹은 화면 보호기 암호나 네트워크 로그온 암호를 포함; 그리고
- 워크 스테이션에서 가입자의 워크 스테이션을 물리적으로 보호하고, 가입자의 권한 위임 없이 관련된 개인키들이 사용되지 않도록 상업적으로 합리적인 조치를 취하는 것입니다.

가동되지 않게 되었을 경우에는, 개인키들은 암호화된 양식으로만 보관되어야 합니다.

6.2.8.3 행정 담당자 인증서 이외의 클래스 3 인증서(Class 3 Certificates other than Administrator Certificates)

(행정 담당자들 이외의) 클래스 3 개인키 보호 기준은 가입자가 다음 사항을 하는 것입니다:

- 개인키 가동 전에 가입자를 인증하기 위한 강도와 동등한 수준의 보안이나 생체 인식 접근 장치, 또는 스마트 카드를 사용; 그리고
- 워크 스테이션에서 가입자의 워크 스테이션을 물리적으로 보호하고, 가입자의 권한 위임 없이 관련된 개인키들이 사용되지 않도록 상업적으로 합리적인 조치를 취하는 것입니다.

제 6 조 4 항 1 호에 따른 스마트 카드 또는 생체 인식 접근 장치와 함께 암호를 사용할 것을 권고합니다. 가동되지 않게 되었을 경우에는, 개인키들은 암호화된 양식으로만 보관되어야 합니다.

6.2.8.4 행정 담당자의 개인키 (클래스 3)(Administrators' Private Keys (Class 3))

행정 담당자의 개인키 보호 기준은 다음 사항을 이행할 것을 필요로 합니다:

- 개인키 가동 전에 가입자를 인증하기 위한 강도와 동등한 수준의 보안이나 생체 인식 접근 장치, 스마트 카드, 또는 제 6 조 4 항 1 호에 따른 암호를 사용하며, 이에는, 예를 들어, 개인키, 윈도우 로그온 혹은 화면 보호기 암호나 네트워크 로그온 암호를 포함; 그리고
- 워크 스테이션에서 행정 담당자의 워크 스테이션을 물리적으로 보호하고, 행정 담당자의 권한 위임 없이 관련된 개인키들이 사용되지 않도록 상업적으로 합리적인 조치를 취하는 것입니다.

CrossCert 는, '행정 담당자들이 스마트 카드 또는 생체 인식 접근 장치 혹은 제 6 조 4 항 1 호에 따른 동등한 수준의 보안과 암호를 개인키 가동 전에 행정 담당자를 인증하기 위해 사용할 것'을 권고합니다.

가동되지 않게 되었을 경우에는, 개인키들은 암호화된 양식으로만 보관되어야 합니다.

6.2.8.5 (자동화된 행정 혹은 Managed PKI Key Manager 서비스와) 암호화 모듈을 사용하는 기업 RA 들(Enterprise RAs using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service))

암호화 모듈을 사용하는 행정 담당자들에 대한 개인키 보호 기준은 다음 사항을 이행할 것을 필요로 합니다:

- 개인키 가동 전에 행정 담당자를 인증하기 위해 제 6 조 4 항 1 호에 따른 암호와 암호화 모듈을 사용; 그리고
- 행정 담당자의 권한 위임 없이 암호화 모듈과 관련된 개인키와 워크 스테이션을 사용하는 것을 방지하기 위하여 암호화 모듈 리더를 포함하는 워크 스테이션에 대한 물리적인 보호를 위한 상업적으로 합리적인 조치를 취함.

6.2.8.6 처리 센터에 의해 보유되는 개인키들(클래스 1~3)(Private Keys Held by Processing Centers (Class 1-3))

제 6 조 2 항 2 호에 정의된 바와 같이, (안전한 미디어에 보관된) 가동 데이터를 제공하는 핵심 주주들에 의하여 온라인 CA 의 개인키들은 가동되어야 합니다. 일단, 개인키들이 가동되면, 개인키는 CA 가 오프라인이 되어 가동되지 않게 될 때까지 계속 가동될 수

있습니다. 이와 유사하게, 대다수 주주들은 오프라인 CA 의 개인키를 가동하기 위하여 가동 데이터를 제공하여야 합니다. 일단, 개인키가 가동되면, 오직 한 번만 가동됩니다.

6.2.9 개인키 비가동 방법(Method of Deactivating Private Key)

표식 리더로부터 제거되면 CrossCert CA 개인키들은 가동되지 않게 됩니다. (RA 애플리케이션에 인증용으로 사용된) CrossCert RA 개인키들은 시스템 접속이 끊기면 가동되지 않게 됩니다. CrossCert RA 들은, 그들의 업무 영역을 떠나게 되면, 그들의 워크스테이션으로부터 접속을 끊어야 합니다.

고객 행정 담당자들, RA 및 최종 사용자 가입자 개인키들은, 사용자가 활용하는 인증 메카니즘에 따라, 스마트 카드 리더기로부터 스마트 카드를 제거하는 때, 또는 시스템에서 접속을 끊은 때에 각각 가동이 되지 않게 될 수 있습니다. 이러한 모든 경우에, 최종 사용자 가입자들은 본 CPS 에 따라 그들의 개인키들을 충분히 보호하기 위한 의무를 부담합니다. ACS Application ID 와 관련된 개인키는, 코드 서명을 위해 사용된 경우에는 사용 즉시 제거됩니다.

6.2.10 개인키 폐기 방법(Method of Destroying Private Key)

필요한 경우, CrossCert 는 CA 개인키들을, 키의 재구축을 초래하는 키 부산물들이 남지 않도록 합리적 범위 내에서 확실히 하는 방식으로, 폐기합니다. CrossCert 는, 하드웨어 암호화 모듈의 기능을 무력화하고 CA 개인키들을 완전하게 폐기하는 것을 확실히 하는 적정한 수단을 사용합니다. 이러한 수행이 있는 경우, CA 키 폐기 활동은 접속됩니다. ACS Application ID 와 관련된 개인키는, 코드 서명을 위해 사용된 후에는 즉시 삭제됩니다.

6.2.11 암호화 모듈 등급(Cryptographic Module Rating)

제 6 조 2 항 1 호를 참조 바랍니다.

6.3 키 쌍 관리의 다른 측면(Other Aspects of Key Pair Management)

6.3.1 공동키 기록 보관(Public Key Archival)

CrossCert CA, RA 및 최종 사용자 가입자 인증서들은, CrossCert 의 일상적인 보완(backup) 절차의 일부분으로 보완되고 기록 보관됩니다.

6.3.2 인증서 운영 기간 및 키 쌍 사용 기간들(Certificate Operational Periods and Key Pair Usage Periods)

인증서의 운영 기간은 해당 유효기간의 만기 혹은 폐기 시점에 종료됩니다. 키 쌍들에 대한 운영 기간은, 복호화 및 서명 인증을 위해 계속 사용되는 경우를 제외하면, 관련된 인증서들에 대한 운영 기간과 동일합니다. 본 CPS 유효일로부터 발행된 인증서에 대한 CrossCert 인증서의 최대 운영 기간들은 다음 [표 8]에 규정되어 있습니다. 현존하는 가입자 인증서들의 갱신본인 최종 사용자 가입자 인증서들은 (3 개월 까지) 유효 기간이 더 길어질 수 있습니다.

또한, CrossCert CA 들은, CA 의 인증서 만료 전에 적정한 시점에서 신규 인증서들을 발행하는 것을 중단해서, 상위 CA 인증서들의 유효기간이 만료된 후에는 하위 CA 에 의하여 인증서가 발행되지 않도록 하여야 합니다.

발행되는 인증서:	***유효 기간***
자기 서명 PCA (1024 bit RSA)	30 년까지
자기 서명 PCA (2048 bit RSA)	50 년까지
자기 서명 PCA (256 bit ECC)	30 년까지
자기 서명 PCA (384 bit ECC)	30 년까지
오프라인 중계 CA 에 대한 PCA	일반적으로 10 년이지만 갱신 후 15 년까지
온라인 CA 에 대한 PCA	일반적으로 5 년이지만 갱신 후 10 년까지[15]
오프라인 중계 CA 에 대한 온라인 CA	일반적으로 5 년이지만 갱신 후 10 년까지 [16]

[15] The Symantec Onsite Administrator CA-Class 3 은 기존 시스템을 지원하기 위해 10 년 이상의 유효기간을 가지며, 적정 시점에서 폐지될 것임

[16] 만일 6 년짜리 최종사용자 인증서가 발행되면, 온라인 CA 인증서의 운영기간은 갱신 옵션 없이 10 년임. CA 키 교체는 5 년 후에는 필요함. .

발행되는 인증서:	*유효 기간*
최종 사용자 개인 가입자에 대한 온라인 CA	보통 3 년까지이지만, 하기와 같은 상황에서는 6 년까지[17], 하기 조건에서 갱신이나 키 교체 옵션 없음. 6 년후 신규 등록이 필요함.
최종 개체 기관 가입자에 대한 온라인 CA	하기와 같은 상황에서는 6 년까지[18][19], 하기 조건에서 갱신이나 키 교체 옵션 없음. 6 년후 신규 등록이 필요함.

[표 8] – 인증서 운영 기간(Certificate Operational Periods)

STN CP 의 제 6 조 3 항 2 호의 조건 상, 시만텍 PMA 는 해당 제한을 초과하는 제한적인 수의 CA 들을 예외적으로 승인하였으며, 이는 CA 키 쌍 이전 기간 동안 PKI 서비스가 방해 받지 않게 하기 위함입니다. 이러한 예외는, 오직 SSL 인증서를 발행하는 CA 들과 관련 없는 기반과 행정 CA 들을 위한 프로세싱 센터를 운영하는 CrossCert 에 적용될 수 있습니다. 이러한 예외는 CA 의 유효기간이 2014 년 8 월 31 일까지 총 14 년을 초과하여 사용될 수 없으며, 2011 년 12 월 31 일 후에는 가용하지 않아야 합니다.

본 조항에서 규정되지 않은 한, CrossCert 서브 도메인 참여자들은 해당 이용기간이 만료된 후에는 키 쌍들의 사용을 중단해야 합니다.

다음의 경우에는, CA 들에 의해 발행된 인증서들은 3 년 이상, 6 년까지의 운영 기간을 보유할 수 있습니다:

- 기관용 인증서에 대한 운영 환경과 관련된 가입자 키 쌍 보호, 강화된 데이터 센터의 보호 및 개인용 인증서, 가입자의 키 쌍들은, 스마트 카드와 같은, 하드웨어 표식에 상존함,
- 가입자들은 최소한 매 3 년마다 제 3 조 2 항 3 호에 따라 재인증을 실행하여야 함,
- 가입자들은 최소한 매 25 개월마다 제 3 조 2 항 3 호에 따라 인증서 내에서 공개키에 합치하는 개인키의 보유를 입증하여야 함,
- 만일 가입자가 성공적으로 재인증을 완료할 수 없거나 앞서 언급한 대로의 개인키를 보유하고 있음을 증명하지 못하면, CA 는 가입자 인증서를 폐지하여야 합니다.

[17].6 년짜리 최종 사용자 가입자 인증서가 발행되면, 온라인 CA 인증서 운영기간은 갱신 옵션 없이 10 년임, CA 키 교체는 5 년 후부터 필요함.

[19] 최소한 인증서의 식별명은 인증서 발행일로부터 3 년 후 재인증하여 3 년이상 유효기간을 가짐. 시만텍 자동 행정인증서는 예외이나, 기관용 최종 사용자 인증서는 5 년 유효기간으로 발행되며 갱신후 최대 10 년간 유효 가능함.

또한, CrossCert 는 Secure Server CA 를 레가시 자기 서명 발행 루트 CA 로서 운영하며, 이는 시만텍 신뢰 네트워크의 일부이며 15 년까지의 운영 기간을 보유합니다. 본 CA 에 의하여 발행되는 최종 사용자 가입자 인증서는 CA 가 상기 [표 8]에 규정된 최종 사용자 가입자 인증서에 대한 요건을 충족합니다.

시만텍 클래스 3 국제 서버 CA 는 PCA 에 의하여 서명된 온라인 CA 입니다. 본 CA 의 유효성은, SGC/step up 기술 사용과 관련하여 브라우저 판매자들과의 계약 의무를 준수하기 위하여 상기 표 8 에 명기된 유효 기간을 초과할 수 없으며, 이러한 성능을 제안하는 인증서의 계속적인 상호 호환성을 확실히 합니다.

6.3.2.1 CABF 유효 기간 요건들(CABF Validity Period Requirements)

도메인 유효 및 기관 유효 SSL 인증서는 CA /Browser Forum Baseline 요건을 준수합니다. 유효기간 후에 발행된 해당 인증서는 48 개월 (4 년)보다 길지 않은 유효기간을 가져야 합니다.

이하에서 설명된 사항을 제외하고, 2015년 4월 1일 이후에 발행된 인증서는 반드시 36개월 (3년)을 넘지 않는 유효 기간을 가져야 합니다. 2015년 4월 1일을 지나면, CA들은 다음의 경우를 위한 인증서인 경우에만 36개월 이상 48개월 미만의 유효기간을 가지는 인증서를 계속해서 발행할 수 있습니다:

a) 유효일자 이전에 사용 중임;
b) 신청자 혹은 신뢰자들 중 상당한 수가 최근 사용 중임;
c) 유효 기간이 48개월보다 짧은 경우에 운영하지 못함;
d) 신뢰자들에게 알려진 보안 위험을 포함하지 않음; 그리고
e) 중대한 경제적 경비 없이 배치나 대체가 힘든 경우임.

6.4 가동 데이터(Activation Data)

6.4.1 가동 데이터 생성 및 설치(Activation Data Generation and Installation)

시만텍 CA 개인키들을 보호하기 위하여 사용되는 가동 데이터(비밀 비율)는 CPS 제 6 조 2 항 2 호와 카 세레모니 참조 가이드(Key Ceremony Reference Guide)에 따라서 생성됩니다. 비밀 비율(Secret Shares)의 생성과 배포는 접속됩니다.

시만텍 RA 들은 그들의 개인키들을 보호하기 위해서 강한 수준의 암호들을 선택하도록 요구됩니다. 시만텍의 암호 선정 가이드라인은 아래와 같은 암호를 선택할 것을 요구합니다:

- 사용자에 의하여 생성됨;

- 최소한 15 자를 가짐;
- 최소한 1 자의 알파벳과 1 자의 숫자를 가짐;
- 최소한 1 자의 소문자를 가짐;
- 같은 문자를 많이 가지지 않음;
- 운영자의 프로파일 이름과 같지 않음; 그리고
- 이용자의 프로파일 이름의 긴 부속 문자열을 가지지 않음.

CrossCert 는, 기업 행정 담당자, RA 들 및 최종 사용자 가입자들이 동일한 요건들을 충족할 것을, 강력하게 권고합니다. 또한, CrossCert 는 두 가지 함수의 인증 메커니즘들(예를 들면, 표식 및 통과구절, 생체인식 및 표식, 혹은 생체인식 및 통과구절)을 개인키 가동을 위해 사용할 것을 권고합니다.

6.4.2 가동 데이터 보호(Activation Data Protection)

CrossCert 의 지분 보유자들은 비밀 지분을 안전하게 보호해야 하고 자신들의 책임에 대한 부분을 인지하는 계약서를 체결합니다.

CrossCert RA 들은 그들의 행정담당자/RA 개인키들을 암호를 사용해 암호화하여야 하며 브라우저에 “높은 수준의 보안” 옵션을 사용하여야 합니다.

CrossCert 는, 고객 행정 담당자들, RA 들 및 최종 사용자 가입자들이 개인키들을 암호화한 방식으로 저장하고 하드웨어 표식이나 높은 수준의 통과구절을 사용하여 보호할 것을, 강력하게 권고합니다. 두 가지 함수의 인증 메커니즘들(예를 들면, 표식 및 통과구절, 생체인식 및 표식, 혹은 생체인식 및 통과구절)을 사용할 것을 권장합니다.

6.4.3 가동 데이터의 다른 측면(Other Aspects of Activation Data)

6.4.3.1 가동 데이터 전송(Activation Data Transmission)

개인키들을 위한 가동 데이터가 전송되는 범위에서, STN 참여자들은 해당 개인키들의 분실, 도난, 변조, 권한 없는 공개, 혹은 권한 없는 사용으로부터 보호하는 방식을 채용하여 전송을 보호하여야 합니다. 최종 사용자 가입자 용 가동 데이터로는 윈도우, 네트워크 로그온 사용자 이름/암호 결합이며, 네트워크를 사용하는 암호는 권한 없는 사용자들의 접근으로부터 보호되어야 합니다.

6.4.3.2 가동 데이터 폐기(Activation Data Destruction)

CA 개인키에 대한 가동 데이터는 해당 개인키들의 분실, 도난, 변조, 권한 없는 공개, 혹은 권한 없는 사용으로부터 보호하는 방식을 채용하여 해체되어야 합니다. 제 5 조 5 항 2 호에

규정된 기록 보존 기간이 지난 후에는, CrossCert 는 덧붙여 쓰거나(overwriting) 물리적인 파기를 통하여 가동 데이터를 해체하여야 합니다.

6.5 컴퓨터 보안 통제(Computer Security Controls)

CrossCert 는, 시만텍의 SAR 가이드 요건을 충족하는 신뢰할 수 있는 시스템들(Trustworthy Systems)을 활용하여 모든 CA 와 RA 기능들을 수행합니다. 기업 고객들은 반드시 신뢰할 수 있는 시스템들(Trustworthy Systems)을 사용하여야 합니다.

6.5.1 특정 컴퓨터 보안 기술 요건(Specific Computer Security Technical Requirements)

CrossCert 는, CA 소프트웨어와 데이터 파일들이 권한 없는 접근으로부터 보호되는 신뢰할 수 있는 시스템들(Trustworthy Systems)임을 확실히 합니다. 그리고, CrossCert 는 생산 서버들에게 접근하고자 하는 개인들의 해당 접근에 대하여 적정한 사업상의 목적으로 제한합니다. 일반적인 애플리케이션 사용자들은 생산 서버들에 계정을 가지지 않습니다.

CrossCert 의 생산 네트워크는 다른 구성물들과는 논리적으로 분리되어 있습니다. 이러한 분리는, 정의된 애플리캐이션 절차를 통하는 경우를 제외하고, 네트워크 접근을 예방합니다. CrossCert 는 내외부적 침투로부터 생산 네트워크를 보호하기 위해 보안벽을 사용하며, 생산 시스템에 접근할 수 있는 네트워크 성격과 소스를 제한합니다.

CrossCert 는, 최소한의 문자 길이와 알파 숫자와 특수문자의 결합을 필요로 하는 암호 사용을 요구합니다. CrossCert 는, 암호들이 정기적으로 변경되는 것을 요구합니다.

CrossCert 의 CA 운영을 지원하는 CrossCert 데이터베이스에 직접 접근하는 것은, 해당 접근에 대한 유효한 사업 이유를 가지는 CrossCert 의 생산 운영 그룹 내 신뢰받는 사람들에 한정합니다.

6.5.1.1 시스템 보안에 대한 CABF 요건(CABF Requirements for System Security)

도메인 유효 및 기관 유효 SSL 인증서는 CA /Browser Forum Baseline 요건을 준수합니다. 이러한 인증서에 대하여는, 인증서 관리 절차 (Certificate Management Process)는 다음 사항을 포함하여야 합니다:

- 물리적 보안 및 환경 통제;
- 시스템 통합 통제, configuration 관리, 신뢰 코드의 통합 관리, 및 잘못된 설비 예방/감지 포함;

- 네트워크 보안 및 보안벽 관리, 포트 제한 및 IP 주소 필터링 포함;
- 사용자 관리, 분리된 신뢰 역할 배정, 교육, 인지, 및 훈련; 그리고
- 개별적인 신뢰도를 제공하기 위한 논리적 접근 통제, 활동 접속, 그리고 비활동 타임아웃.

CA 는 인증서 발행을 직접 초래하는 가능한 모든 계정들에 대한 다중 요소 인증을 집행하여야 합니다.

6.5.2 컴퓨터 보안 등급(Computer Security Rating)

해당 규정 없습니다.

6.6 라이프 싸이클 기술 통제(Life Cycle Technical Controls)

6.6.1 시스템 개발 통제(System Development Controls)

애플리케이션은 CrossCert 시스템 개발 및 변경 관리 기준에 따라 CrossCert 에 의해 개발되고 실행됩니다. 또한, CrossCert 는 RA 와 특정 CA 기능을 수행하기 위하여 기업 고객들에게 소프트웨어를 제공합니다. 그러한 소프트웨어는 CrossCert 시스템 개발 기준에 따라 개발됩니다.

처음 장착되면, 시만텍 개발 소프트웨어는, 시만텍이나 CrossCert 로부터 생성된 시스템에서 소프트웨어를 인증하기 위한 도구를 제공하며, 이는 설치 전에 수정되지 않은 채로 사용 목적의 버전입니다.

6.6.2 보안 관리 통제(Security Management Controls)

CrossCert 는 CA 시스템의 configuration 을 감시하고 통제하기 위하여 마련된 매카니즘과 정책을 가집니다. CrossCert 는 모든 소프트웨어 패키지와 CrossCert 소프트웨어 업데이트의 해쉬 함수를 생성합니다. 이러한 해쉬 함수는 해당 소프트웨어의 무결성을 수동으로 인증하는데 사용됩니다. 설치 시와 그 후에 정기적으로, CrossCert 는 CA 시스템의 무결성을 유효화합니다.

6.6.3 라이프 싸이클 보안 통제(Life Cycle Security Controls)

해당 규정 없습니다.

6.7 네트워크 보안 통제(Network Security Controls)

CrossCert 는, 권한 없는 접근과 기타 악의적인 활동을 예방하기 위해 시만텍 SAR 가이드에 따라 보안된 네트워크를 사용하여 모든 CA 및 RA 기능을 수행합니다. CrossCert 는, 암호와 전자서명의 이용을 통하여 민감한 정보의 소통을 보호합니다.

6.8 시점 인식(Time-Stamping)

인증서, CRL, 및 기타 폐지 데이터베이스 엔트리는 시간 및 날짜 정보를 포함하여야 합니다. 그러한 시간 정보는 암호화 기반일 필요는 없습니다.

7. 인증서, 인증서 폐지목록 및 OCSP 프로파일(Certificate, CRL, and OCSP Profiles)

7.1 인증서 프로파일(Certificate Profile)

CrossCert 인증서는 일반적으로 (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 과 (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280")[20]을 준수합니다. 인증서 유형에 따라, STN 인증서는 공개적으로 신뢰받는 인증서의 발행과 관리에 대한 최신본 CA/Browser Forum Baseline Requirements 를 준수합니다.

X.509 인증서는 최소한 다음 [표 9]에 규정된 기본 영역과 값을 가집니다:

영역(Field)	*값 혹은 값 한계(Value or Value constraint)*
일련 번호	최소 20 비트의 엔트로피를 가지는 발행자 DN 별 고유 값
서명 알고리즘	인증서 서명에 사용되는 알고리즘 객관 표기자 (CP 7 조 1 항 3 호 참조)
발행자 식별명(DN)	제 7 조 1 항 4 호 참조
유효기간(시작)	통합 조정 시간 기준. U.S. Naval Observatory 의 Master Clock 에 동시화. RFC5280 에 따라 코드화됨.
유효기간(끝)	통합 조정 시간 기준. U.S. Naval Observatory 의 Master Clock 에 동시화. RFC5280 에 따라 코드화됨.
대상자 식별명	제 7 조 1 항 4 호 참조
대상자 공동키	RFC5280 에 따라 코드화됨
서명	RFC5280 에 따라 생성되고 코드화됨

[20] STN 인증서가 일반적으로 RFC 5280 을 준수하기는 하지만, 일정한 조항은 지원되지 않기도 함.

[표 9] – 인증서 프로파일 기본 영역(Certificate Profile Basic Fields)

7.1.1 버전 수(Version Number(s))

CrossCert 인증서는, 특정 루트 인증서가 기존의 시스템을 지원하는 X.509 버전 1 인증서에게 허용되기는 하지만, X.509 버전 3 인증서입니다. CA 인증서는 X.509 버전 1 이거나 X.509 버전 3 인증서이어야 합니다. 최종 사용자 인증서는 X.509 버전 3 인증서이어야 합니다

7.1.2 인증서 확장(Certificate Extensions)

CrossCert 는 X.509 버전 3 STN 인증서를 제 7 조 1 항 2 호 1 목부터 동 조항 8 목까지에 따라 요구되는 확장자들로 채웁니다. 개별적인 확장이 허용되지만 본 CP 와 적용 CPS 에 따라 허락되지 않으면 개별적 확장은 특별히 규정된 경우가 아니면 사용될 수 없습니다.

7.1.2.1 키 용도(Key Usage)

X.509 버전 3 인증서는 일반적으로 “RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002”에 따라서 이식됩니다: 키용도 영역의 확장자는 일반적으로 CA 인증서에 대하여는 TRUE 로 설정되어 있으며, 최종 개체 가입자 인증서에는 TRUE 혹은 FALSE 로 설정될 수 있습니다.

주의: 부인방지 비트[21]는 이러한 인증서에 설정되어 있을 필요는 없으며, 이는 PKI 업계가 아직 비부인방지 비트가 의미하는 공통 기준에 대하여 합의한 바가 없기 때문입니다. 그러한 합의가 이루어질 때까지는, 비부인방지 비트는 잠재적인 신뢰자들에게 의미가 없을 것입니다. 더 나아가, 가장 일반적으로 사용되는 애플리캐이션들이 항상 비부인방지 비트를 존중하지는 않습니다. 그러므로, 비트를 설정하는 것이 신뢰자들이 어떤 결정을 내릴 때 도움을 주지 못할 수 있습니다. 결과적으로, 본 CPS 는 비부인방지 비트 설정을 요구하지 않습니다. Managed PKI Key Manager 를 통하여, 혹은 달리 요구되는 바대로듀얼 키 서명 인증서가 발행된 경우에는 설정될 수도 있습니다. 전자 인증서 사용으로 인하여 발생된 비부인방지와 관련된 일체의 분쟁은 전적으로 가입자와 신뢰자들 간의 문제입니다. 시만텍과 CrossCert 는 해당 분쟁과 관련하여 일체의 책임을 부담하지 않습니다.

[21] 비부인방지 비트는 X.509 표준에 따라 전자서명 내용약정으로 언급될 수도 있슴.

7.1.2.2 인증서 정책 확장(Certificate Policies Extension)

X.509 버전 3 인증서의 "*인증서 정책*" 확장자에는 CP 제 7 조 1 항 6 호와 CP 제 7 조 1 항 8 호에 규정된 정책 조건들에 따른 STN CP 에 대한 객체 식별자로 채워집니다. 본 확장자의 중요 영역은 FALSE 로 설정됩니다.

7.1.2.2.1 인증서 정책 확장에 대한 CABF 요건(CABF Requirement for Certificate Policies Extension)

도메인 유효 및 기관 유효 SSL 인증서는 CA /Browser Forum Baseline 요건을 준수합니다. 루트 CA 인증서는 "*인증서 정책*" 확장자를 포함하지 않아야 합니다.

7.1.2.3 대상 대체 이름(Subject Alternative Names)

X.509 버전 3 인증서의 "*대상대체이름*" 확장자에는, Public Lite 계정에 대해서는 선택적으로 이메일 주소를 "*대상대체이름*"에서 제외한 채, RFC 5280 에 따릅니다. 본 확장자의 중요 영역은 FALSE 로 설정됩니다.

7.1.2.4 기본 제한(Basic Constraints)

CrossCert X.509 버전 3 CA 인증서의 *"기본제한*" 확장자는 CA 영역에 TRUE 로 설정되어 있어야 합니다. 최종 사용자 인증서는 *"기본제한*" 확장자는 CA 영역에 FALSE 로 설정되어 있어야 합니다. 본 확장자의 중요도 영역에는 CA 인증서에 대하여는 TRUE 로 설정되어 있으며, 최종 사용자 가입자 인증서에는 TRUE 혹은 FALSE 로 설정될 수 있습니다.

CrossCert X.509 버전 3 CA 인증서는 해당 인증서가 인증 통로에 따를 수 있는 CA 인증서의 최대 숫자에 *"기본제한"* 확장자의 "*통로제한"* 영역을 보유하여야 합니다. 온라인 기업 고객에게 발행된 CA 인증서가 발행하는 최종 사용자 가입자 인증서에는 "*통로제한"* 영역이 "0" 값으로 설정되어, 오직 최종 사용자 가입자 인증서가 인증서 통로 내에 따를 수 있음을 표시합니다.

7.1.2.5 확장된 키 용도(Extended Key Usage)

기본적으로, *"확장된 키 용도"*는 비중요 확장자로 설정됩니다. STN CA 인증서는 *"확장된 키 용도"* 확장자를 포함하지 않습니다.

7.1.2.6 CRL 배포 지점(CRL Distribution Points)

대부분의 CrossCert X.509 버전 3 최종 사용자 가입자 인증서와 중간 CA 인증서는, 신뢰자가 CA 인증서의 상태를 확인할 수 있는 CRL 을 확보할 수 있는 장소의 URL 을 포함하는 *"cRL 배포지점"* 확장자를 포함합니다.

7.1.2.7 권한자 키 표시자(Authority Key Identifier)

CrossCert 는 일반적으로 X.509 버전 3 최종 사용자 가입자 인증서와 중간 CA 인증서의 확장자에 권한자 키 표시자(Authority Key Identifier)를 채워 넣습니다. 인증서 발행자가 대상 키 표시자 확장자를 포함하는 때에는, 권한자 키 표시자는 CA 발행 인증서의 공동키의 160 비트 SHA-1 해쉬함수로 구성됩니다. 그렇지 않으면, 권한자 키 표시자 확장자는 발행 CA 의 대상 식별명과 일련 번호를 포함합니다. 본 확장자의 중요도 영역은 FALSE 로 설정됩니다.

7.1.2.8 대상 키 표시자(Subject Key Identifier)

CrossCert 가 X.509 버전 3 STN 인증서를 *"대상키표시자"* 확장자로 채우는 경우에는, 인증서의 대상자의 공동키에 근거한 "*키표시자*"가 RFC5280 에 규정된 방식 중 하나에 따라 생성되어야 합니다. 본 확장자의 중요도 영역은 FALSE 로 설정됩니다.

7.1.3 알고리즘 객체 표시자(Algorithm Object Identifiers)

CrossCert 인증서는 다음 알고리즘들 중 하나를 이용하여 서명됩니다.

- ***sha256withRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- ***ecdsa-with-Sha384*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}
- **sha-*1WithRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
- ***md5WithRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}

이와 같은 알고리즘들을 이용하여 생성된 인증서 서명은 RFC 3279 를 준수하여야 합니다. ***sha-1WithRSAEncryption*** 와 ***sha256WithRSAEncryption***, 둘 중 하나는 ***md5WithRSAEncryption***[22]에 사용됩니다.

[22] ***md5WithRSAEncryption*** 은 오직 사업 계속성을 보전하기 위하여 사전에 승인하기 위하여만 사용됨.

7.1.4 이름 양식(Name Forms)

CrossCert 는 STN 인증서에 발행자 이름과 대상 식별명을 제 3 조 1 항 1 호에 따라 채워 넣습니다. 발행자 이름은 각각의 발행된 인증서에 국가, 조직명과 발행자 CA 의 공통이름을 포함합니다.

또한, CrossCert 는, 관련 신뢰자 계약서에 지명된 URL 에 규정된 인증서의 사용조건을 표시하는 통지를 포함한 추가적인 기관 단위를 최종 사용자 가입자 인증서 내에 포함할 수 있습니다. 전술한 요건에 대한 예외는, 오직 인증서 내의 공란, 포맷팅 혹은 상호운용 제한이 해당 기관 단위로 하여금 인증서가 원래 목적대로 사용할 수 없게 되었거나, 적용 신뢰자 계약서에 지정된 바가 인증서의 정책 확장자에 포함된 경우에만 허용됩니다.

7.1.5 이름 제한(Name Constraints)

해당 사항 없습니다.

7.1.6 인증서 정책 객체 표시자(Certificate Policy Object Identifier)

인증서 정책 확장자가 사용된 경우에는, 인증서는 STN CP 제 1 조 2 항에 규정된 적정 인증서 클래스에 합치하는 인증서 정책에 대한 객체 표시자를 포함합니다. 인증서 정책 확장자를 포함한 STN CP 의 게재 전에 발행된 기존 인증서에 대하여는, 해당 인증서에 관한 STN CPS 를 참조하십시오.

7.1.6.1 인증서 정책 객체 표시자에 대한 CABF 요건(CABF Requirements for Certificate Policy Object Identifier)

도메인 유효 및 기관 유효 SSL 인증서는 CA /Browser Forum Baseline 요건을 준수합니다. STN CP 제 1 조 2 항에 규정된 정책 표시자에 합치하는 인증서들은 해당 인증서가 이러한 요건들에 따라 발행되었고 관리됨을 표시합니다.

발행 CA 의 관계사가 아닌 하위 CA 에게 발행된 인증서는, 2012 년 7 월 1 일부터 다음과 같습니다:

- 하위 CA 의 CABF 요건 준수를 표시하는, 제 1 조 2 항에 규정된 정책 부합 표시자를 포함하여야 함; 그리고
- *"정책"* 표시자(2.5.29.32.0)를 포함하지 않아야 함.

발행 CA 의 관계사인 하위 CA 에게 발행된 인증서는, 2012 년 7 월 1 일부터 다음과 같습니다:

- 하위 CA 의 CABF 요건 준수를 표시하는, 제 1 조 2 항에 규정된 정책 부합 표시자를 포함할 수 있음; 그리고

- *"정책"* 표시자(2.5.29.32.0)를 명시적인 정책 표시자에 포함할 수 있음.

7.1.7 정책 제한 확장자의 사용(Usage of Policy Constraints Extension)

해당 사항 없습니다.

7.1.8 정책 수식 의미론과 구문론(Policy Qualifiers Syntax and Semantics)

CrossCert 는 일반적으로 X.509 버전 3 STN 인증서에 '인증서 정책 확장자' 내에 정책 수식 내역을 채워 넣습니다. 일반적으로, 그러한 인증서는, 적용 신뢰자 계약서 또는 CrossCert CPS 를 적시하는, CPS 지정 수식어를 포함합니다. 이에 추가로, 일부 인증서들은, 적용 신뢰자 계약서를 지정하는 사용자 통지 수식어(User Notice Qualifier)를 포함하기도 합니다.

7.1.9 중요 인증서 정책에 대한 구문론 처리(Processing Semantics for the Critical Certificate Policies Extension)

해당 사항 없습니다.

7.2 인증서 폐지 목록 프로파일(CRL Profile)

인증서 유형에 맞추어, 이에 부합하는 CRL 은 공개적으로 신뢰받는 인증서의 발행과 관리를 위한 최신본 CA/Browser Forum Baseline Requirements 을 준수합니다.

버전 2 CRL 들은 RFC 5280 을 준수하며 아래 [표 13]에 규정된 사항들과 기본 영역들을 포함합니다:

영역(Field)	값 혹은 값 제한(Value or Value constraint)
버전	제 7 조 2 항 1 호 참조.
서명 알고리즘	RFC 3279 에 따라 CRL 서명하는데 사용되는 알고리즘.
발행자	CRL 을 서명하고 발행하는 존재.
유효일자	CRL 발행일자. CRL 들은 발행 시 유효함.
차기 업데이트	차기 CRL 이 발행될 날짜. CRL 발행 빈도는 제 4 조 4 항 7 호 요건에 따름.
폐지된 인증서	폐지된 인증서와 폐지 일자의 일련 번호를 포함한, 폐지된 인증서 목록.

[표 13] – CRL 프로파일 기본 영역(CRL Profile Basic Fields)

7.2.1 버전 수(Version Number(s))

CrossCert 인증서는 X.509 버전 1 과 버전 2 CRL 들 모두를 지원합니다. 버전 2 CRL 들은 RFC 5280 요건들을 준수합니다.

7.2.2 CRL 과 CRL 엔트리 확장(CRL and CRL Entry Extensions)

해당 규정이 없습니다.

7.3 온라인 인증서 상태 프로토콜 프로파일(OCSP Profile)

OCSP (온라인 인증서 상태 프로토콜; Online Certificate Status Protocol)은, 특정 인증서의 폐지 상태에 관한 시간적 정보를 수령하는 방법입니다. CrossCert 는 다음을 유효화합니다:

- RFC 2560 을 준수하는 클래스 2 기업 인증서들의 기업 OCSP, 그리고
- RFC 5019 를 준수하는 시만텍 신뢰 글로벌 유효화 프로토콜 (TGV)를 사용한 클래스 2 기업 인증서와 클래스 3 기관 인증서.

OCSP 서명을 위한 CABF 요건(CABF Requirement for OCSP Signing)

도메인 유효 및 기관 유효 SSL 인증서는 CA /Browser Forum Baseline 요건을 준수합니다.

OCSP 대응들은 RFC 5019 를 준수해야 하며, 다음 사항들 중 하나를 준수하여야 합니다:

- 폐지 상태가 확인된 인증서를 발행한 CA 에 의해 서명됨, 혹은
- 폐지 상태가 확인된 인증서를 발행한 CA 에 의하여 서명된 인증서의 OCSP 대응자에 의하여 서명됨. 그러한 OCSP 대응자가 서명한 인증서는 RFC2560 에 규정된 *id-pkix-ocsp-nocheck* 확장자를 포함하고 있어야 함.

7.3.1 버전 수(Version Number(s))

RFC 2560 에 규정된 OCSP 사양의 버전 1 과 RFC 5019 에 규정된 OCSP 사양의 버전 1 은 지원됩니다.

7.3.2 OCSP 확장(OCSP Extensions)

TGV 서비스는, 각 OCSP 대응의 최신성을 수립하기 위하여 안전한 시점 인식과 유효기간을 활용합니다. CrossCert 는 각 OCSP 대응의 최신성을 수립하기 위하여 임시적인 사항을 이용하지 않으며, 고객들도 임시 사항이 포함된 요청에 임시적인 사항을 기대하지 않습니다. 대신, 고객들은 대응의 최신성을 확인하기 위해 현지 시각을 적용하여야 합니다.

8. 준법 감사 및 기타 측정(Compliance Audit and Other Assessments)

인증기관 v2.0 또는 그 후속 버전에 대한 연간 웹트러스트(WebTrust) 검사는, CrossCert 의 데이터 센터 및 STN 루트 CA 들, 클래스 3 기관용 CA 들, 클래스 2 기관용 및 개인용 CA 들, 그리고 제 1 조 3 항 1 호에 규정된 클래스 1 개인용 CA 들을 포함한 Managed PKI CA

서비스에 대하여 시행됩니다. 고객 특정의 CA 들은, 해당 고객에 의하여 요구되지 않는 한, CrossCert 의 운영에 대한 감사의 일부분으로 특정되어 감사 받지는 않습니다. CrossCert 는, 기업 고객들에게 본 CPS 와 해당 유형의 고객들에 대한 감사 프로그램에 따라 감사를 받을 것을 요구할 권한을 가집니다. An annual for Certification Authorities v2.0 or later (or equivalent) 준법 감사와 더불어, CrossCert 는 STN 내 자신의 서브 도메인의 신뢰도를 확실히 하기 위한 검사와 조사를 실행할 권한을 가지며, 다음을, 이에 한정하지 않고, 포함합니다:

- CrossCert 는 자신의 독자적인 판단으로, 자신이 판단하기에 피감사 개체가 STN 기준을 충족하지 못하였거나, STN 의 무결성이나 보안성에 실제 혹은 잠재적인 위협을 가하는 작위 혹은 부작위 상황을 초래하거나 경험하였다고 믿는 경우에는, 언제든지 해당 고객에 대하여 “긴급 감사/조사”를 실행할 수 있습니다.
- CrossCert 는, 준법 감사 혹은 통상의 사업 과정에서 전반적인 위험 관리 절차의 일부분에서 불완전하거나 이상 징후가 보인 경우에는, 고객에 대하여 “보충적 위험 관리 검토”를 실행할 수 있습니다.

CrossCert 는, 이러한 감사, 검토, 및 조사를 수행할 권한을 제 3 자 감사 회사에게 위임할 수 있습니다. 피감사 대상은 CrossCet 와 해당 감사, 검토 혹은 조사를 실행하는 직원들에게 합리적인 범위의 협력을 제공하여야 합니다.

자기 감사를 위한 CABF 요건(CABF Requirement for Self-Audits)

도메인 유효 및 기관 유효 SSL 인증서는 CA /Browser Forum Baseline 요건을 준수합니다.

CrossCert 는 자신의 정책 및 CPS 요건들에 대한 준수 여부를 감시하기 위해 자기 감사를 실시하여야 하며 최소한 1 분기마다 무작위로 추출한 1 개 이상의 인증서 혹은 이전 자기 감사에서 샘플을 추출한 후부터 인증서의 최소한 3%를 선정하여 서비스 품질을 엄격하게 통제하여야 합니다.

8.1 평가 빈도 및 환경(Frequency and Circumstances of Assessment)

준법 감사는 피감사 개체의 비용만으로 최소한 연간 1 회이상 실시됩니다. 감사는 1 년 기간보다 길지 않은 기간에 중단 없이 실시되어야 합니다.

8.2 평가 주체/자격(Identity/Qualifications of Assessor)

CrossCert 의 CA 준법 감사는 회계법인에 의하여 다음을 감사합니다:

- 인증기관 v2.0 혹은 그 이후버전에 대한 WebTrust 수행의 능숙도 설명,
- 공동키 인프라 기술, 정보 보안 툴 및 기술, 보안 감사 및 제 3 자 공증 기능의 능숙도 설명, 그리고

- 적정 인력의 배치와 전문 교육 훈련 요건에 관한 동료 검사, 능숙도 테스팅, 기준과 같은 특정 기술 수준, 품질 보증 조치미국 회계사 협회에 의해 승인되었는지.
- 법규, 정부 규정, 혹은 전문가 윤리규정에 구속되는 지; 그리고
- 최소한 US 1 백만 달러를 보상하는 '전문가 책임 보험'을 유지하는 지.

8.3 피감사 대상에 대한 평가자의 관계(Assessor's Relationship to Assessed Entity)

CrossCert 의 운영에 대한 준법 감사는 CrossCert 에 독립한 회계법인에 의하여 수행됩니다.

8.4 평가 주제(Topics Covered by Assessment)

인증기관(혹은 그와 동등)에 대한 CrossCert 의 연간 WebTrust 감사에는 CA 환경 통제, 키 관리 운영 및 인프라/행정적 CA 통제, 인증서 라이프 싸이클 관리 및 CA 업무 준칙 공개에 관한 사항을 포함합니다.

8.5 부족한 결과에 대한 조치(Actions Taken as a Result of Deficiency)

CrossCert 의 운영에 대한 감사와 관련하여, 준법 감사 기간 중에 나타난 중대한 예외사항이나 부족한 사항에 대하여는 조치가 취해집니다. 이러한 조치는 감사의 의견과 CrossCert 경영진에 의하여 결정됩니다. CrossCert 경영진은 교정 활동 계획을 수립하고 실행할 책임을 가집니다. 만일 CrossCert 가 판단하기에, 해당 부족한 사항이나 예외 사항이 STN 의 보안에 즉시적인 위협을 가할 수 있는 것이라고 판단하는 경우에는, 교정 활동 계획은 30 일 이내에 수립되어야 하고 상업적으로 합리적인 기간 내에 실행되어야 합니다. 중대하지 않은 예외사항이나 부족한 사항들에 관하여는, CrossCert 경영진은 해당 이슈의 심각성을 평가하고 적정한 조치를 취할 것을 판단하여야 합니다.

8.6 결과 공유(Communications of Results)

CrossCert 는 연간 감사 보고서를 각 감사 기간 종료 후 3 개월 이내에 공개하여야 합니다. 3 개월 이상 지연하는 경우에는, CrossCert 는 공인 감사의 서명이 된 해명서를 제공하여야 합니다. CA (혹은 이와 동등) 감사 보고서에 대한 CrossCert 의 WebTrust 사본은 http://www.crosscert.com/repository 에서 확인하실 수 있습니다.

9. 기타 사업 및 법적 사항(Other Business and Legal Matters)

9.1 수수료(Fees)

9.1.1 인증서 발행 혹은 갱신 수수료(Certificate Issuance or Renewal Fees)

CrossCert 는, 인증서의 발행, 관리, 및 갱신에 대하여 최종 사용자 가입자에게 수수료를 청구할 권한이 있습니다.

9.1.2 인증서 접근 수수료(Certificate Access Fees)

CrossCert 는, 인증서를 저장소 혹은 기타의 방법으로 신뢰자들이 인증서를 볼 수 있도록 하는 것에 관하여 수수료를 부과하지 않습니다.

9.1.3 폐지 혹은 상태 정보 접근 수수료(Revocation or Status Information Access Fees)

CrossCert 는, 본 CP 에서 요구되는 CRL 들을 저장소 혹은 기타의 방법으로 신뢰자들이 볼 수 있도록 하는 것에 관하여 수수료를 부과하지 않습니다. 그러나, CrossCert 는 고객 맞춤형 CRL 들, OCSP 서비스, 혹은 기타 가치 부가형 폐지 및 상태 정보 서비스를 제공하는 것과 관련하여는 수수료를 부과할 수 있습니다. CrossCert 는 폐지 정보, 인증서 상태 정보 혹은 CrossCert 의 사전 서면 동의 없이 해당 인증서의 상태 정보를 사용하는 서비스를 제공하는 제 3 자에 의한 저장소 시점 인식에 대한 접근을 허락하지 않습니다.

9.1.4 기타 서비스 수수료(Fees for Other Services)

CrossCert 는 본 CPS 열람에 대한 수수료를 부과하지 않습니다. 단순히 서류를 열람하는 목적 이외의 사용은, 예를 들어 복제, 재배포, 변조, 혹은 파생물 작성 등은, 해당 서류의 저작권을 보유한 자와의 라이선스 계약서에 따르기로 합니다.

9.1.5 환불 정책(Refund Policy)

CrossCert 의 서브 도메인 내에, 다음과 같은 환불 정책(http://www.crosscert.com/repository/refund/ 참조)이 유효합니다:

CrossCert 는, 인증 업무와 인증서 발행에 관한 업무를 수행함에 있어서 업무 준칙과 정책을 준수합니다. 그럼에도 불구하고, 가입자가 완전히 만족하지 못하는 경우에는, 가입자는 CrossCert 에게 인증서를 발행 30 일 이전에 폐지하고 환불을 해 줄 것을 요구하실 수 있습니다. 최초 30 일 기간이 지나면, CrossCert 가 보증사항을 위반하였거나 가입자 혹은

가입자의 인증서와 관련하여 CPS 상의 중대한 의무를 위반한 경우에는 가입자는 인증서를 폐지하고 환불해 줄 것을 요구하실 수 있습니다. CrossCert 가 가입자의 인증서를 폐지한 후에는, CrossCert 는 (인증서 수수료가 신용카드로 납부된 경우) 가입자의 신용카드 계정에 크레디트를 추가하거나, 가입자에게 수표로 해당 인증서 관련 수수료 전액을 상환하여야 합니다. 환불 요청은 고객 서비스 센터인 *+82-2-3019-5500* 로 연락하시기 바랍니다. 이러한 환불 정책은 유일한 구제책이 아니며, 가입자에게 주어지는 기타 다른 구제책을 제한하지 않습니다.

9.2 재정적인 책임(Financial Responsibility)

9.2.1 보험 보상 범위(Insurance Coverage)

기업 고객들은, 실수나 부작위로 인하여 발생할 수 있는 손해에 대하여, 자기 보유이건 보험회사를 통해서건 상업적으로 합리적인 수준의 보험을 유지하는 것이 권고됩니다. CrossCert 는 그러한 실수나 부작위에 대한 보험 보상을 유지합니다.

9.2.2 기타 자산(Other Assets)

기업 고객은 운영과 임무 수행을 위하여 충분한 재정 자원을 유지하여야 하며, 가입자와 신뢰자들에 대한 책임을 부담할 수 있어야 합니다. CrossCert 의 재정적 자원에 관한 사항은 *http://www.crosscert.com/service_company/Main.jsp?_action=SHOW&_param=WELCOME_IR_PAGE* 에서 공개되어 있습니다.

9.2.3 추가 보장 보상 범위(Extended Warranty Coverage)

[CrossCert PKI Warranty Program Protection Plan 은 추가 보장 프로그램이며, STN 의 시만텍의 서브도메인 내에서 적용됩니다. 이 프로그램이 적용되는 경우에는, CrossCert PKI Warranty Program Protection 은 CrossCert SSL 과 코드 서면 인증서 가입자들을 CrossCert 의 인증서 발행 결함이나 기타 CrossCert 의 과실 혹은 의무 위반(단, 가입자는 해당 서비스 계약 상의 의무를 준수하여야 함)으로 인한 손실이나 손해로부터 보호합니다. CrossCert PKI Warranty Program 에 관한 일반적인 사항과 인증서와 관련하여 보상받는 범위에 관하여는 http://www.crosscert.com/pkiwarrantyprogram 을 참조하시기 바랍니다.

9.3 사업 정보의 기밀유지(Confidentiality of Business Information)

9.3.1 기밀정보의 범위(Scope of Confidential Information)

제 9 조 3 항 2 호를 조건으로 하여, 가입자에 대한 다음 기록들은 기밀("기밀정보")로 유지되어야 합니다:

- 승인되었건 승인되지 않았건, CA 신청 기록,
- 인증서 신청 기록,
- Managed PKI Key Manager 를 사용하여 기업 고객들이 보유하게 된 개인키들과 해당 개인키들을 복구하기 위해 필요한 정보,
- 거래 기록(거래 관련 모든 기록 및 감사 자취 기록),
- 시만텍 혹은 고객이 생성하거나 보유한 감사 자취 기록들,
- CrossCert 혹은 고객(해당 보고서가 보유되는 한) 혹은 그들의 감사들(내부 혹은 공개 감사)에 의해 생성된 감사 기록,
- 비상 계획과 재난 복구 계획; 그리고
- CrossCert 의 소프트웨어와 하드웨어 및 인증서 서비스 행정과 지정된 등록 서비스 운영을 통제하는 보안 조치.

9.3.2 기밀정보에 포함되지 않는 정보(Information Not Within the Scope of Confidential Information)

인증서, 인증서 폐지 및 기타 상태 정보, CrossCert 의 저장소 및 해당 저장소에 포함된 정보는 기밀정보로 간주되지 않습니다. 제 9 조 3 항 1 호에서 기밀정보로 명시적으로 간주되지 않은 정보는 기밀인 것도 아니며 개인적인 것도 아닌 것으로 간주됩니다. 본 조항은 관련 개인정보 보호 법규에 따라 변경될 수 있습니다.

9.3.3 기밀정보 보호 책임(Responsibility to Protect Confidential Information)

CrossCert 는 제 3 자에 대한 공개와 위반으로부터 개인 정보를 보호합니다.

9.4 개인정보의 프라이버시(Privacy of Personal Information)

9.4.1 개인정보 보호 계획(Privacy Plan)

CrossCert 는 개인 정보 보호 정책을 수립하여 시행 중이며, 이는 http://www.crosscert.com/service_gcca/library/Main.jsp?action=SHOW&_param=GCCA_LIBRARY_CPS08_PAGE 에 공개되어 있고 CP 제 9 조 4 항을 준수하고 있습니다.

9.4.2 개인정보로 취급되는 정보(Information Treated as Private)

발행된 인증서, 인증서 디렉토리 및 온라인 CRL 들에서 공개적으로 볼 수 없는 가입자에 관한 일체의 정보는 개인적인 것으로 취급됩니다.

9.4.3 개인적인 것으로 간주되지 않는 정보(Information Not Deemed Private)

인증서에서 공개된 모든 정보는, 현지 법규를 조건으로 하여, 개인적이지 않은 것으로 간주됩니다.

9.4.4 개인정보 보호 책임(Responsibility to Protect Private Information)

개인정보를 수령하는 STN 참여자들은 제 3 자에 대한 공개로부터 안전하게 하여야 하고, 해당 법정지의 개인정보보호 법규 전체를 준수하여야 합니다.

9.4.5 개인정보 사용 통지와 동의(Notice and Consent to Use Private Information)

본 CPS, 관련 개인정보보호 정책, 혹은 계약서에 달리 규정되지 않은 한, 개인정보는 해당 정보가 적용되는 당사자의 동의 없이는 사용되지 않아야 합니다. 본 조항은 관련 개인정보 보호 법규에 따라 변경될 수 있습니다.

9.4.6 사법 행정 절차에 따른 공개(Disclosure Pursuant to Judicial or Administrative Process)

CrossCert 는, 선의로 다음과 같이 믿는 경우에는, 기밀정보를 공개할 수 있습니다:

- 검찰의 소환장이나 수색 영장에 대응하여 공개가 필요한 경우.
- 소환장, 사전조사, 인정 요청 및 서류 제출 요구를 받는 등, 민사 혹은 행정 절차상 사실 확인 기간에 사법, 행정 혹은 기타 법적 절차에 대응하여 공개가 필요한 경우.

본 조항은 관련 개인정보 보호 법규에 따라 변경될 수 있습니다.

9.4.7 기타 정보 공개 상황(Other Information Disclosure Circumstances)

해당 규정 없습니다.

9.5 지적재산권(Intellectual Property rights)

가입자들과 신뢰자들 이외의 CrossCert 서브 도메인 참여자들 사이의 지적재산권 배정은 해당 CrossCert 서브 도메인 참여자들 사이의 관련 계약서에 정한 바를 따릅니다. 가입자와 신뢰자들과 관련된 지적재산권은 제 9 조 5 항의 다음과 같은 조건을 적용합니다.

9.5.1 인증서와 폐지 정보의 재산권(Property Rights in Certificates and Revocation Information)

CA 들은 자신이 발행하는 인증서와 폐지 정보에 관한 일체의 지적재산권을 보유합니다. CrossCert 와 고객들은 비독점 무상조건으로 인증서를 재생산하고 배포할 수 있는 권한을 부여합니다. 단, 해당 인증서의 사용은 완전한 형태로 재생산되어야 하고 해당 인증서에 참조된 신뢰자 계약서에 따라야 합니다. CrossCert 와 고객들은, 관련된 CRL 사용 계약서, 신뢰자 계약서, 또는 기타 관련 계약서들을 조건으로 하여, 신뢰자 기능을 수행하기 위한 폐지정보의 사용을 허용합니다.

9.5.2 CPS 내 재산권(Property Rights in the CPS)

STN 참여자들은, CrossCert 가 본 CPS 에 관한 모든 지적재산권을 보유함을 인지합니다.

9.5.3 이름에 대한 재산권(Property Rights in Names)

인증서 신청자는 인증서 신청서에 (있는 경우) 포함된 자신의 상표, 서비스표, 혹은 상호와 해당 인증서 신청자에게 발행된 모든 인증서 내의 식별 이름에 대한 모든 권리를 보유합니다.

9.5.4 키와 키 자료에 대한 재산권(Property Rights in Keys and Key Material)

CA 들과 최종 사용자 가입자의 인증서에 합치하는 키 쌍들은, Managed PKI Key Manager 을 사용하는 기업 고객의 권리를 조건으로 하여, 해당 키들의 저장 장소나 해당 키들의 모든 지적재산권을 보유하는 자의 물리적 매체가 무엇이든 상관없이, CA 들과 이러한 인증서들의 각자의 대상들인 최종 사용자 가입자의 재산입니다. 전술한 바에 제한되지 않고, 시만텍의 루트 공개키와 PCA 공개키와 자기 서명 인증서를 포함한 루트 인증서는, 시만텍의 재산입니다. 시만텍은 소프트웨어 및 하드웨어 생산자에게 믿을 수 있는 하드웨어 장치와 소프트웨어에 해당 루트 인증서를 복제할 수 있도록 라이선스를 부여하였습니다. 마지막으로, CA 의 개인키의 비밀 지분(Secret Shares)은 CA 의 재산이며, CA 는 해당 비밀 지분(Secret Shares)에 대한 모든 지적재산권을, 그들이 시만텍으로부터 해당 지분이나 CA 의 물리적 소유를 확보할 수 없게 되더라도, 그러합니다.

9.6 진술과 보증(Representations and Warranties)

9.6.1 CA 의 진술과 보증(CA Representations and Warranties)

CrossCert 는 다음 사항을 보증합니다:

- 인증서 신청을 승인하거나 인증서를 발행하는 개체에게 알려지거나 연유된 사실 관계에서 중대한 잘못된 진술이 존재하지 않음,
- 인증서 신청이나 인증서 발행을 하는 과정에서 합리적인 범위의 주의의무 위반으로 인한, 인증서 신청이나 인증서 발행을 승인하는 개체에 의하여 소개된 인증서 정보에 착오가 존재하지 않음,
- 그들의 인증서들이 본 CPS 의 모든 중대한 요건들을 충족함, 그리고
- 폐지 서비스와 저장소 사용이 모든 중대한 측면에서의 CPS 적용사항을 준수함.

가입자 계약서는 추가적인 진술과 보증사항을 포함할 수 있습니다.

9.6.1.1 CABF 보증 및 의무(CABF Warranties and Obligations)

도메인 유효 및 기관 유효 SSL 인증서는 CA /Browser Forum Baseline 요건을 준수합니다.
CA 는 인증서를 발행함으로써, 본 조항에 나열된 인증서 보증을 제 1 조 3 항 5 호에 나열된 인증서 수혜자들에게 제공하여야 합니다.

CA는, 해당 인증서가 유효한 기간 동안, 'CA가 인증서를 발행 및 관리함에 있어서 본 요건들, 인증서 정책 및/혹은 인증업무준칙을 준수함'을 인증서 수혜자들에게 진술하고 보증합니다. 인증서 보증사항으로는 특히, 이에 한정하지 않고, 다음 사항을 포함합니다:

1. 도메인 이름이나 IP 주소 사용권: 발행 시점에, CA 는, (i) 신청자는 인증서의 대상 영역과 *대상대체이름* 확장자에 나열한 도메인 이름(혹은, 도메인 이름과 관련하여는, 사용 통제권한을 가진 자로부터 권한을 위임 받았음)과 IP 주소에 대한 이용권한이나 통제권한을 확인하기 위한 절차를 수행하였고; (ii) 인증서 발행 절차에 따랐으며, 그리고 (iii) CA 의 인증서 정책과 /혹은 인증업무준칙상의 절차에 정확하게 설명하였음;
2. 인증서에 대한 권한 위임: 발행시점에서, CA 는 (i) 대상을 대신하여 인증서를 신청하도록 권한을 위임 받은 신청 대표와 대상이 권한을 위임한 인증서 발행사항에 대한 확인 절차를 수행하였고; (ii) 인증서 발행 절차에 따랐으며, 그리고 (iii) CA 의 인증서 정책과 /혹은 인증업무준칙상의 절차에 정확하게 설명하였음;
3. 정보의 정확도: 발행시점에서, CA 는 (i) 인증서에 포함된 모든 정보(*대상.기관.단위명* 부분에 대하여는 예외)의 정확성을 확인하는 절차를 수행했으며; (ii) 인증서 발행 절차에 따랐으며, 그리고 (iii) CA 의 인증서 정책과 /혹은 인증업무준칙상의 절차에 정확하게 설명하였음;

4. 오인을 유도하는 정보 없음: 발행시점에서, CA 는 (i) 인증서의 *대상.기관.단위명* 부분에 포함된 정보가 오인을 초래할 확률을 줄이기 위한 절차를 수행하였으며; (ii) 인증서 발행 절차에 따랐으며, 그리고 (iii) CA 의 인증서 정책과 /혹은 인증업무준칙상의 절차에 정확하게 설명하였음;
5. 신청자의 신분: 인증서가 대상자 신분 정보를 포함하는 경우에는, CA 는 (i) 제 3 조 1 항 1 호 1 목 및 제 3 조 2 항 2 호 1 목에 따른 신청자 신원을 확인하는 절차를 수행하였으며; (ii) 인증서 발행 절차에 따랐으며, 그리고 (iii) CA 의 인증서 정책과 /혹은 인증업무준칙상의 절차에 정확하게 설명하였음;
6. 가입자 계약서: CA 와 가입자가 계열사 관계가 아닌 경우에는, 가입자와 CA 는 본 요건들을 충족하는 법적 구속력이 있고 집행 가능한 가입자 계약서의 당사자임. 한편, CA 와 가입자가 계열사 관계에 있는 경우라면, 신청 대표는 이용약관을 인지하고 수락함;
7. 상태: CA 는 만료되지 않은 인증서들의 (유효 혹은 폐지) 상태와 관련된 최신 정보로 제공되는 24 시간 주 7 일에 일반에게 접근 가능한 저장소를 유지함; 그리고
8. 폐지: CA 는 본 요건에 규정된 일체의 이유에 근거하여 인증서를 폐지할 것임.

루트 CA의 의무(Root CA Obligations)

루트 CA 는 하위 CA 의 요건 준수 및 본 요건에 따른 책임 및 면책의무 이행에 관하여 업무수행과 보증사항에 대하여, 루트 CA 가 인증서를 발행하는 하위 CA 인 것처럼, 책임을 집니다.

9.6.2 RA 의 진술과 보증(RA Representations and Warranties)

RA 들은 다음사항을 보증합니다:

- 인증서 신청을 승인하거나 인증서를 발행하는 개체로부터 혹은 이에 알려진 인증서에 사실상 중대한 오진술 사항이 존재하지 않음,
- 인증서 신청을 관리함에 있어서 합리적인 주의의무를 기울이지 않은 이유로, 인증서 신청을 승인한 개체에 의하여 소개된 인증서에 착오가 존재하지 않음,
- 그들의 인증서들이 본 CPS 의 모든 중요 요건들을 충족함, 그리고
- (적용 가능한 경우) 폐지 서비스와 모든 중대한 측면에서 적용 가능한 CPS 를 준수하는 저장소의 사용.

가입자 계약서는 추가적인 진술과 보증사항을 포함할 수 있습니다.

9.6.3 가입자의 진술과 보증(Subscriber Representations and Warranties)

가입자들은 다음사항을 보증합니다::

- 인증서에 나열된 공동키에 합치하는 개인키를 사용하여 생성된 각 전자 서명은 가입자의 전자서명이며 인증서는 전자서명이 생성될 때에 (만료 혹은 폐지되지 않은) 수락되고 운영되었음,
- 그들의 개인키는 보호되며, 권한 없는 자가 가입자의 개인키에 접근한 적이 없었음,
- 가입자가 제출한 인증서 신청에 가입자가 진술한 모든 사항이 진실임,
- 가입자에 의하여 제공되고 인증서에 포함된 된 모든 정보가 진실임,
- 인증서는 본 CPS 에 부합하는 권한과 법적인 목적을 위하여만 사용됨, 그리고
- 가입자는 최종 사용자 가입자이며 CA 가 아니고, CA 혹은 다른 자격으로 인증서 (또는 인증된 공동키의 다른 양식), 혹은 CRL 에 전자 서명할 목적으로 인증서에 나열된 공동키에 부합하는 개인키를 사용하지 않음.

가입자 계약서는 추가적인 진술과 보증사항을 포함할 수 있습니다.

9.6.4 신뢰자의 진술과 보증(Relying Party Representations and Warranties)

신뢰자 계약서(Relying Party Agreements)는, 신뢰자가 '인증서에 의존하고자 하는 범위에 대하여 충분히 정보를 제공받았음'을 인식하게 하여야 하며, 그들이 해당 정보에 의존할 지 여부에 대한 판단에 대하여 전적인 책임이 있으며, 본 CPS 상의 신뢰자의 의무 미이행에 따른 법적 결과를 부담해야 함을 인식시켜야 합니다.

신뢰자 계약서(Relying Party Agreements)는 추가적인 진술과 보증사항을 포함할 수 있습니다.

9.6.5 다른 참여자들의 진술과 보증(Representations and Warranties of Other Participants)

해당 규정 없습니다.

9.7 보증 부인(Disclaimers of Warranties)

적용 법규가 허용하는 범위 내에서, 가입자 계약서와 신뢰자 계약서는, 상업성 보증이나 특정 목적에의 적합성 보증을 포함한, CrossCert 의 일부 보증들을 부인합니다.

9.8 책임의 한계(Limitations of Liability)

CrossCert 가 STN 인증서 정책과 CrossCert 인증업무준칙을 준수하여 발행하고 관리하는 인증서에 대하여는, CrossCert 는 해당 인증서의 사용이나 의존으로 인하여 발생된 일체의 손해에 대하여 가입자, 일체의 신뢰자, 혹은 기타 제 3 자에 대하여 일체의 책임을 지지 않습니다. 관련 법규가 허용하는 범위 내에서는, 가입자 계약서와 신뢰자 계약서는

CrossCert 의 책임을 제한합니다. 책임의 제한은, 간접적인, 특별한, 부수적이고 결과적인 손해배상 책임을 배제할 것을 포함합니다. 이에는 특정 인증서에 관한 CrossCert 의 손해배상 책임의 상한선을 아래와 같이 포함할 수 있습니다:

클래스(Class)	책임 상한선(Liability Caps)
클래스 1	120,000 원
클래스 2	6,000,000 원
클래스 3	120,000,000 원

[표 14] – 책임의 상한선(Liability Caps)

주의: [표 14]에 규정된 책임 상한선은 'CrossCert 보호 계획(CrossCert Protection Plan)'의 내용 이외에서 회복할 수 있는 손해배상액을 제한하는 것입니다. 'CrossCert 보호 계획(CrossCert Protection Plan)' 내에서의 지급 금액은 자신의 책임 상한선에 따라 변경 가능합니다. 상이한 종류별 인증서들에 대한 'CrossCert 보호 계획(CrossCert Protection Plan)'에 따른 책임 상한선은 120,000 원에서 120,000,000 원 사이입니다.

가입자의 책임(및/혹은 책임의 상한)은 해당 가입자 계약서에 규정됩니다.

기업 RA 들과 관련 CA 의 책임(및/혹은 책임의 상한)은 해당 계약서들에 규정됩니다.

신뢰자들의 책임(및/혹은 책임의 상한)은 해당 신뢰자 계약서들에 규정됩니다.

9.9 면책사항(Indemnities)

9.9.1 가입자들에 의한 면책(Indemnification by Subscribers)

관련 법규에서 허용하는 한, 가입자들은 다음 사항과 관련하여 CrossCert 를 면책하여야 합니다:

- 가입자의 인증서 신청에 가입자에 의해 제공된 거짓 사실이나 오진술 사실,
- 오진술이나 부작위가 과실 혹은 타인을 기망하고자 하는 고의로 이루어 진 경우, 인증서 신청에 있어서 가입자가 중요 사실 공개를 하지 않은 경우,
- 가입자가, 가입자의 개인키 보호를 하지 못하였거나, Trustworthy System 을 이용하지 않은 경우, 혹은 가입자의 개인키에 대한 손실, 공개, 변조 혹은 권한 없는 사용에 대한 필요한 주의조치를 취하지 않은 경우, 혹은
- 가입자가 제 3 자의 지적재산권을 침해하는 (도메인 이름 혹은 이메일 주소, 공통명 등을 포함) 이름을 사용하는 경우.

관련 가입자 계약서는 추가적인 면책사항을 포함할 수 있습니다.

9.9.2 신뢰자들에 의한 면책(Indemnification by Relying Parties)

관련 법규에서 허용하는 한, 신뢰자 계약서는 신뢰자들로 하여금 다음 사항과 관련하여 CrossCert 를 면책하도록 하여야 합니다:
:

- 신뢰자가 자신의 의무를 이행하지 않은 경우,
- 신뢰자의 인증서에 대한 의존이 주변 상황상 합리적이지 못한 경우, 혹은
- 신뢰자가, 해당 인증서가 만료된 것인지 폐지된 것인지에 대한 인증서 상태 확인을 하지 않은 경우.

관련 신뢰자 계약서는 추가적인 면책사항을 포함할 수 있습니다.

9.9.3 애플리케이션 소프트웨어 공급자의 면책(Indemnification of Application Software Suppliers)

가입자들과 신뢰자들에 대한 책임 상한선 규정에도 불구하고, CA 는, CrossCert 루트 CA 의 입장에 놓인 인증서 배포 계약서 당사자인 애플리케이션 소프트웨어 공급자들은 본 요건상의 CA 로서의 책임과 의무 혹은 신뢰자나 기타 다른 사람들에 의한 신뢰나 인증서 발행 혹은 유지로 인하여 발생할 수 있는 요건 일체를 부담하지 않음을, 인식하고 인지합니다.

그러므로, CA 는, 소송 제기 이유 혹은 법 이론과 상관없이, CA 에 의해 발행된 인증서와 관련된 애플리캐이션 소프트웨어 공급자에게 발생되는 일체의 손실, 클레임, 손해들로부터 손해를 보지 않도록 각각의 애플리케이션 소프트웨어 공급자를 면책하여야 합니다. 그러나, 이러한 사항은, (1) 기간이 만료된 인증서, 혹은 (2) 폐지된 인증서 (그러나, CA 로부터 온라인으로 폐지 상태가 공개되는 경우이며, 해당 애플리케이션 소프트웨어 공급자가 해당 상태의 확인을 하지 않았거나 폐지 상태 표시를 무시한 경우에만 해당)와 같이, '유효하거나 믿을 수 있는 것으로 표시되지 않은' 인증서로 인하여 애플리케이션 소프트웨어 공급자에게 직접적으로 초래된 손해, 클레임이나 손실이 해당 CA 가 발행한 인증서로 인하여 애플리케이션 소프트웨어 공급자가 겪는 클레임, 손해 혹은 손실에는 적용되지 않습니다.

9.10 계약 기간 및 계약 종료(Term and Termination)

9.10.1 계약기간(Term)

CPS 는 CrossCert 저장소에 게재 시부터 효력이 발생합니다. 본 CPS 의 개정본은 CrossCert 저장소에 게재 시부터 효력이 발생합니다.

9.10.2 계약 종료(Termination)

본 CPS 는, 새로운 버전으로 대체될 때까지, 수시로 개정되는 대로, 유효하게 존속하기로 합니다.

9.10.3 계약 종료와 존속 효과(Effect of Termination and Survival)

그럼에도 불구하고, 본 CPS 의 종료 시에, CrossCert 의 서브 도메인 참여자들은 모든 인증서들의 잔여 유효기간 동안의 계약조건에 구속됩니다.

9.11 참여자들과의 의사소통 및 개별적 통지(Individual Notices and Communications with Participants)

양 당사자들 간 계약서에 달리 규정하지 않은 한, CrossCert 서브 도메인 참여자들은 문제의 중요성과 소통의 주제에 대한 고려를 한 후, 서로 소통하기 위하여 상업적으로 합리적인 범위의 방법을 강구하여야 합니다.

9.12 개정(Amendments)

9.12.1 개정 절차(Procedure for Amendment)

본 CPS 의 개정본은 CrossCert Policy Management Authority(PMA)에 따라 작성됩니다.
개정본은 CPS 의 개정양식이나 업데이트 양식 중 하나의 방식으로 이루어 집니다. 개정된 버전이나 업데이트는 https://www.crosscert.com/repository/updates 에 공개된 CrossCert 저장소의 '업무 준칙 업데이트와 통지(Practices Updates and Notices)'부문에 연결되어야 합니다. 업데이트는, 참조된 CPS 버전의 기지정 사항 혹은 모순되는 조항을 대체합니다. PMA 는, CPS 의 변경사항이 각 인증서 클래스에 합치하는 인증서 정책의 객체 표시자에 변경이 필요한 지를 판단하여야 합니다.

9.12.2 통지 메카니즘과 기간(Notification Mechanism and Period)

CrossCert 와 PMA 는, 입력 오류에 대한 교정, URL 에 대한 변경, 및 연락처 변경 등과 같이 중요하지 않은 사항에 개정에 대하여는, 통지 없이 CPS 를 개정할 권한을 가집니다. 개정사항이 중요한 사항인지 중대하지 않은 사항인지 결정하는 PMA 의 판단은, 전적으로 PMA 의 판단 권한 내의 사항입니다.

CPS 에 대한 개정안 제안은, https://www.crosscert.com/repository/updates 에 소재한 CrossCert 저장소의 '업무 준칙 업데이트와 통지(Practices Updates and Notices)'부문에 게재됩니다.

CPS 에 달리 규정되어 있다고 하더라도, PMA 가 'CPS 에 대한 중대한 개정사항이 STN 혹은 그 일부의 보안을 위반하는 것을 즉시 중단하거나 예방하기 위하여 필요하다'고 믿는 경우에는, CrossCert 와 PMA 는 CrossCert 저장소에 해당 개정사항을 게재할 수 있습니다. 그러한 개정사항들은 게재와 동시에 즉시 효력을 가집니다. 게재한 후, 합리적인 시간 내에,

CrossCert 는 해당 개정사항에 관하여 CrossCert 서브 도메인 참여자들에게 통지하여야 합니다.

9.12.2.1 의견 개진 기간(Comment Period)

달리 규정된 경우를 제외하고, CPS 개정안의 중요사항에 대한 의견 개진 기간은, 개정안이 CrossCert 저장소에 게시된 날로부터 15 일 동안입니다. CrossCert 의 서브도메인 참여자들은 의견 개진 기간 종료 시까지 의견을 등록할 수 있습니다.

9.12.2.2 의견 처리 메커니즘(Mechanism to Handle Comments)

PMA 는 제안된 개정사항들에 대한 모든 의견을 고려하여야 합니다. PMA 는, (a) 개정절차 이행 없이 개정 제안사항을 허용하거나, (b) 개정 제안사항을 개정하고 필요한 경우 신규 개정사항을 다시 게재하거나, (c) 개정 제안사항들을 철회하여야 합니다. PMA 는 관계사들에게 통지하고 CrossCert 저장소 '업무 준칙 업데이트와 통지(Practices Updates and Notices)'부문에 통지함으로써 개정 제안사항을 철회할 수 있습니다. 제안된 개정사항이 개정되거나 철회되지 않은 한, 의견 개진 기간이 만료되면 해당 사항들에 대한 효력이 개시됩니다.

9.12.3 OID 가 변경되어야 하는 상황(Circumstances under Which OID Must be Changed)

만일 PMA 가, '인증서 정책에 합치하는 객체 표시자가 변경될 필요가 있다'고 판단하는 경우에는, 개정 사항들은 각 인증서 클래스에 부합하는 인증서 정책에 대한 신규 객체 표시자를 포함하여야 합니다. 그렇지 않으면, 개정사항들은 인증서 정책 객체 표시자에 변경이 필요하지 않습니다.

9.13 분쟁 해결 조항(Dispute Resolution Provisions)

9.13.1 시만텍, CrossCert, 그리고 고객간 분쟁(Disputes among Symantec, CrossCert, and Customers)

CrossCert 서브 도메인 참여자들 사이의 분쟁은 당사자들 사이의 관련 계약서의 계약 조항에 따라 해결되어야 합니다.

9.13.2 최종 사용자 가입자 혹은 신뢰자간 분쟁(Disputes with End-User Subscribers or Relying Parties)

적용 법규가 허용하는 범위 내에서, 가입자 계약서와 신뢰자 계약서는 분쟁 해결 조항을 포함하여야 합니다. CrossCert 가 간여된 분쟁은 최초 60 일간의 협상기간을 두어야 하고, 그 후 CrossCert 법정 관할지의 법원에서 소송에 의하여 해결됩니다. 소 제기자 혹은 모든 소제기자가 한국 거주자인 경우에는, 국제상사중재원(ICC)의 해당 중재규칙에 따라 중재로 분쟁 해결을 하기로 합니다.

9.14 준거법(Governing Law)

관련 법규에서 규정된 제한사항을 조건으로 하여, 본 CPS 의 집행가능성, 해석, 및 유효성은, 한국의 상업적 접근성에 관한 요건 충족과 계약법 혹은 국제사법과 상관없이, 대한민국 법규에 따르기로 합니다. 이러한 준거법은, 그들이 소재한 장소와 상관없이, 모든 CrossCert 서브 도메인 참여자들에 대한 통합 절차와 해석을 확실히 하기 위하여, 선정되었습니다.

본 준거법 조항은 본 CPS 에만 적용됩니다. 본 CPS 에 참조된 계약서들은, 자신들만의 준거법 조항을 가지고 있으며, 다만, 본 제 9 조 14 항은, 해당 계약서들의 계약 조건들과는 별개로, 본 CPS 의 집행 가능성, 해석, 그리고 유효성을 관할합니다. 이는 적용 법규에 규정된 제한사항에 따라 변경이 가능합니다.

9.15 적용 법규 준수(Compliance with Applicable Law)

본 CPS 는, 소프트웨어, 하드웨어 혹은 기술 정보의 수출입에 관한 규제 등, 관련 국가, 지방정부, 해외법규, 규정, 명령, 규칙, 훈령 등을 포함한 일체의 규정에 따라 변경 가능합니다. CrossCert 는, '인증서 발행'과 관련하여 해당 법정지에서 라이센스가 필요한 경우에는, 각 법정지마다 CA 들에게 라이센스를 부여합니다.

9.16 기타 조항(Miscellaneous Provisions)

9.16.1 완전 합의(Entire Agreement)

해당 규정 없습니다.

9.16.2 양도(Assignment)

해당 규정 없습니다.

9.16.3 분리 조항(Severability)

본 CPS 의 규정이 법원 혹은 권한 있는 기관의 판결에 의해 집행 불가능한 것으로 판결된 경우에는, CPS 의 다른 잔존 조항들은 여전히 유효합니다.

9.16.4 집행 강제력(변호사 비용 및 권리 포기)(Enforcement (Attorney's Fees and Waiver of Rights))

해당 규정 없습니다.

9.16.5 불가항력(Force Majeure)

관련 법규가 허용하는 범위 내에서, 가입자 계약서와 신뢰자 계약서는 시만텍을 보호하는 불가항력 조항을 포함하여야 합니다.

9.17 기타 조항(Other Provisions)

해당 규정 없습니다.

첨부(Appendix) A. 약어표 및 용어 정의(Table of Acronyms and definitions)

약어표(Table of Acronyms)

용어(Term)	정의(Definition)
AICPA	American Institute of Certified Public Accountants.
ANSI	The American National Standards Institute.
ACS	Authenticated Content Signing.
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce.
CA	Certification Authority.
ccTLD	Country Code Top-Level Domain
CICA	Canadian Instituted of Chartered Accountants
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
DBA	Doing Business As
DNS	Domain Name System
FIPS	United State Federal Information Processing Standards.
FQDN	Fully Qualified Domain Name
ICC	International Chamber of Commerce.
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol.
OID	Object Identifier
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
RA	Registration Authority.
RFC	Request for comment.
SAR	Security and Audit Requirements
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
STN	Symantec Trust Network.
TLD	Top-Level Domain
TLS	Transport Layer Security
VOID	Voice Over Internet Protocol

정의(Definitions)

용어(Term)	정의(Definition)
행정 담당자(Administrator)	Processing Center, Service Center, Managed PKI Customer, or Gateway Customer 조직 내

용어(Term)	정의(Definition)
	'신뢰받는 자'로, 유효화 업무, CA 나 RA 기능을 수행함.
행정 담당자 인증서(Administrator Certificate)	행정 담당자에게 발행된 인증서이며, CA 나 RA 기능을 수행하는 데에만 사용됨.
관계사(Affiliate)	선도적인 신뢰받는 제 3 자, 예를 들면, 기술, 정보통신 혹은 재무 서비스 산업에서 시만텍과 계약 체결하여 STN 배포와 서비스 채널을 가지기로 한 자. CAB Forum 내용 내에서,"관계사(*Affiliate)*" 라는 용어는: 다른 개체와 공동의 통제나 경영 지배를 받는 기업, 파트너쉽, 합병회사, 기타 조직, 혹은 정부 개체로부터 직접 통제를 받는 정부 기관 내지 개체, 조직을 의미함.
관계사 업무 관련 법적 요건 안내서(Affiliate Practices Legal Requirements Guidebook)	시만텍 서류로써, 관계사 CPS, 계약서, 유효화 절차 및 개인정보보호정책, 그리고 관계사가 충족해야 하는 기타 요건들.
관계인(Affiliated Individual)	Managed PKI Customer, Managed PKI Lite Customer, or Gateway Customer 개체와 관계된 자연인으로, (i) 개체 내에서의 임원, 이사, 직원, 파트너, 계약자, 인턴 등의 사람들, (ii) 시만텍의 등재된 구성원, 또는 (iii) 개체가 해당 사람의 정체에 대한 적정한 보증을 제공하는 기타 기록 혹은 사업관계에 있는 개체와 관계를 유지하는 사람.
신청인(Applicant)	인증서 (갱신) 신청을 하는 자연인이나 법적 정체. 인증서가 일단 발행되면, 신청인은 가입자로 언급됨.장치에 발행된 인증서에 대하여는, 신청인은 인증서에 명명된 장치를 지배하고 운영하는 개체이며, 이는 해당 장치가 실제로 인증서 요청을 송신하더라도 그러함.
신청인 대표(Applicant Representative)	신청인, 신청인에 의해 고용되었거나, 신청인을 대표할 명시적인 권한을 가지는 권한 있는 에이전트인 자연인이나 자연인 스폰서로써: (i) 신청인을 대신하여 인증서 신청서를 서명, 제출하거나 승인하는 사람, 그리고/혹은 (ii) 신청인을 대신하여 가입자 계약서를 서명하고, 제출하는 사람, 그리고/혹은 (iii) 신청인이 CA 의 관계사인 경우, 신청인을 대신하여 인증서 이용약관을 인지하고 동의하는 사람.
애플리케이션 소프트웨어 공급자(Application Software Supplier)	인터넷 브라우저 소프트웨어나 인증서를 사용하거나 디스플레이하고 루트 인증서에 포함된 기타 신뢰자 애플리케이션 소프트웨어의 공급자.
공증 서한(Attestation Letter)	'해당 주제 정보가 회계사, 변호사, 정부 관료, 혹은 관례상 기타 신뢰받을 수 있는 자에 의하여 정확하게 쓰여짐'을 공증하는 서한.
감사 보고서(Audit Report)	적격 감사로부터의 보고서로, '개체의 절차와 통제가 본 요건들의 강제조항들을 준수했는지'에 관한 적격감사의 의견을 서술한 것.
신청인(Applicant)	인증서 (갱신) 신청을 하는 자연인이나 법적 정체. 인증서가 일단 발행되면, 신청인은 가입자로 언급됨.장치에 발행된 인증서에 대하여는, 신청인은 인증서에 명명된 장치를 지배하고 운영하는 개체이며, 이는 해당 장치가 실제로 인증서 요청을 송신하더라도 그러함.
자동화된 행정(Automated Administration)	'등록 정보가 데이터베이스에 포함된 정보와 일치하는 지', 인증서 신청이 자동으로 승인되는 절차.
자동화된 행정 소프트웨어 모듈(Automated Administration Software Module)	자동화된 행정을 수행하는 시만텍에 의하여 제공되는 소프트웨어.
인증서(Certificate)	최소한, 이름, CA, 가입자가 누군지를 언급하는 메세지로써, 가입자의 공동키를 포함하고, 인증서의 운영기간도 표기하고, 인증서 일련번호를 포함하며, CA 에 의하여 전자서명됨.
인증서 신청인(Certificate Applicant)	CA 에 의한 인증서 발급을 신청하는 개인이나 기관.
인증서 신청(Certificate Application)	인증서 신청인(혹은 신청인의 권한 있는 에이전트)이 CA 에게 인증서 발행을 요청하는 것.
인증서 체인(Certificate Chain)	루트 인증서에서 종료하는 최종 사용자 가입자 인증서와 CA 인증서를 포함한 인증서 주문 목록.
인증서 데이터(Certificate Data)	CA 가 보유 혹은 접근에 대한 통제권을 가지는 인증서 요청과 관련된 데이터(신청인으로부터 수령하는 가는 무관함).
인증서 관리 통제 목적(Certificate Management Control Objectives)	개체가 준법감사를 만족하기 위하여 반드시 충족해야 하는 기준들.

용어(Term)	정의(Definition)
인증서 관리 절차(Certificate Management Process)	CA 가 확인하는 인증서 데이터, 발급, 저장소 유지 및 인증서 폐지함에 있어서 키, 하드웨어 및 소프트웨어의 사용과 관련된 절차와 준칙.
인증서 정책(Certificate Policies (CP))	본 서류이며, "Symantec Trust Network Certificate Policies"로, STN 을 지배하는 원칙적인 서면상 원칙.
인증서 장애 보고서(Certificate Problem Report)	키 위반, 인증서 오남용 혹은 기타 유형의 사기, 위반, 혹은 인증서 관련하여 부적절한 행동에 대한 불평 불만사항.
인증서 폐지 목록(Certificate Revocation List (CRL))	정기적으로 (혹은 임시적으로) 발행된, CA 에 의해 전자서명된, CP 제 3 조 4 항에 따라 만기 전에 폐지된 인증서 목록. 해당 목록은 일반적으로 CRL 발행자 이름, 발행일자, 차기 CRL 발행 예정일자, 폐지된 인증서의 일련번호, 그리고 폐지 이유 및 특정 시간을 표시함.
인증서 서명 요청(Certificate Signing Request)	인증서가 발급되도록 요청하는 메세지.
인증기관(Certification Authority (CA))	STN 내에서 인증서를 발행, 관리, 폐지, 및 갱신하도록 권한을 위임받은 존재.
인증업무준칙(Certification Practice Statement (CPS))	시만텍 혹은 관계사가 인증서 신청을 수락 혹은 거절, 인증서의 발행, 관리 및 폐지를 함에 있어서 채용하며, Managed PKI 고객들과 Gateway 고객들이 채용해야 하는 업무 준칙.
챌린지 문구(Challenge Phrase)	인증서 등록하는 동안 인증서 신청인에 의해 선택된 비밀 문구. 인증서가 발행되면, 인증서 신청인은 가입자가 되며, CA 혹은 RA 는, 가입자가 가입자의 인증서를 폐지 혹은 갱신하고자 하는 경우, 가입자를 인증하기 위하여 챌린지 문구를 사용함.
클래스(Class)	CP 에 규정된 바 대로의 특정된 보장 수준. CP 제 1 조 1 항 1 호 참조.
고객 서비스 센터(Client Service Center)	고객에게 고객 혹은 기업의 사업 과정에서 관계사가 제공하는 서비스 센터.
준법 감사(Compliance Audit)	'Processing Center, Service Center, Managed PKI Customer, 혹은 Gateway Customer 가 관련 STN 기준들을 준수하는지'에 관하여 검사 받는 정기적인 감사.
위반(Compromise)	보안 규정의 위반(혹은 의심받는 위반)으로, 민감 정보에 대한 권한 없는 공개, 통제권한 상실의 발생. 개인키와 관련하여는, 위반은 손실, 도난, 공개, 변조, 권한 없는 사용, 혹은 해당 개인키에 대한 기타 다른 보안 위반.
기밀정보(Confidential/Private Information)	CP 제 2 조 8 항 1 호에 따라 기밀이 유지되어야 하는 정보.
상호 인증서(Cross Certificate)	두 곳의 루트 CA 들간의 신뢰관계 형성에 사용되는 인증서.
인증서 폐지 목록 사용 계약서(CRL Usage Agreement)	CRL 이나 해당 CRL 내 정보가 사용될 수 있는 조건을 규정한 계약서.
수임받은 제 3 자(Delegated Third Party)	CA 는 아니지만, CA 에 의해 권한을 위임받아 인증서 관리절차를 이행하거나 CA 요건을 충족시킴으로써 관리절차를 지원하는 자연인이나 법적 존재.
고객(Customer)	Managed PKI 고객, Gateway 고객, 또는 ASB 고객 중의 한 조직.
도메인 권한 위임(Domain Authorization)	특정 도메인 이름공간에 인증서 요청을 위한 신청인의 권한을 공증하는 도메인 이름 등록자에 의해 제공되는 서류나 기타 문서.
도메인 이름(Domain Name)	도메인 이름 시스템상의 노드(node)에 배정된 레벨(label).
도메인 이름공간(Domain Namespace)	도메인 이름 시스템상의 단일 노드에 종속한 가능한 모든 도메인 이름들의 세트.
도메인 이름 등록자(Domain Name Registrant)	도메인 이름의 "소유자"로 종종 언급되나, 더 정확하게는, 도메인 이름 등록기관에 등록한 사람이나 존재이며, 도메인 이름 사용 권한을 통제할 수 있는, WHOIS 나 도메인 이름 등록기관에 등재된 자연인 혹은 법적 정체를 의미함.
도메인 이름 등록기관(Domain Name Registrar)	(i)아이칸(ICANN), (ii) 국가 도메인 이름 등록기관, 또는 (iii) 네트워크 정보 센터(그들의 계열사, 계약사, 수임자들, 승계자들 혹은 양수인)들과 계약서나 상황에 따라 도메인 이름을 등록한 사람이나 기관.
기업 서비스 센터 내 기업(Enterprise, as in Enterprise Service Center)	관계사가 Managed PKI 서비스를 Managed PKI 고객들에게 제공하는 일련의 사업.
임시 감사/조사(Exigent Audit/Investigation)	시만텍이 '누군가가 STN 기준을 충족하지 못하였거나, STN 의 보안을 위반하거나 위협을 가하고 있다'고 믿을만한 이유가 있는 경우에, 시만텍에 의해 실시되는 감사나 조사.
유효기간 일자(Expiry Date)	인증서의 유효기간의 마지막 날로 정의된, 인증서에 "~이후에는 아님"로 표시된 날짜.
완전히 충족하는 도메인 이름(Fully-Qualified Domain Name)	인터넷 도메인 이름 시스템 내에 모든 상위 노드들의 라벨(label)을 포함한 도메인 이름.

용어(Term)	정의(Definition)
정부개체(Government Entity)	정부가 운영하는 법적 정체, 에이전시, 부서, 장관, 지사, 혹은 기타 유사한 지방 정부 및 그 하위 조직(예를 들어, 주, 도, 시, 구 등).
지적재산권(Intellectual Property Rights)	다음 사항들 중 하나 이상에 대한 권리: 저작권, 특허권, 영업비밀, 상표, 및 기타 지적재산권.
중간 인증기관(Intermediate Certification Authority (Intermediate CA))	자신의 인증서가, 최종 사용자 가입자의 인증서를 발행하는 인증기관의 인증서와 루트 CA 의 인증서 사이의, 인증서 체인에 소재하는 인증기관.
내부 서버 이름(Internal Server Name)	공공의 DNS 를 이용하여 풀 수 없는 서버 이름(미등록 도메인 이름에 포함되지 않을 수 있음).
국제기구(International Organization)	국제기구는, 둘 이상의 주권 국가들의 서명이 있는 정관, 조약, 협약, 혹은 유사한 서류들에 근거하여 설립된 조직임.
발행 CA(Issuing CA)	특정 인증서와 관련하여, 인증서를 발행하는 CA. 루트 CA 이거나 하위 CA 일 수 있음.
키 위반(Key Compromise)	권한 없는 사람들에게 공개된 값의 경우, 권한 없는 사람이 접근한 것, 혹은 권한 없는 자에 의해 발견된 값에 실무적으로 존재하는 기술은 위반된 것으로 언급됨.
키 생성 세레모니(Key Generation Ceremony)	CA 의 혹은 RA 의 키 쌍이 생성, 개인키가 암호화 모듈로 이전되거나, 개인키가 보완되거나, 공동키가 인증되는 절차.
키 생성 스크립트(Key Generation Script)	CA 키 쌍의 생성을 위한 절차에 관한 서류상의 계획.
키 관리자 행정 담당자(Key Manager Administrator)	Managed PKI Key Manager 를 사용하여 Managed PKI 고객을 위해 키 생성과 복구 기능을 수행하는 행정 담당자.
키 쌍(Key Pair)	개인키와 관련된 공동키.
키 복구 블록(Key Recovery Block (KRB))	암호화 키를 사용하여 암호화된 가입자의 개인키를 포함하는 데이터 구조. KRB 들은 Managed PKI Key Manager 소프트웨어를 사용하여 생성됨.
키 복구 서비스(Key Recovery Service)	'가입자의 개인키를 복구하기 위하여 Managed PKI 고객의 Managed PKI Key Manager 사용의 일부분으로 키 복구 블록을 복구하는데 필요한 암호 키를 제공하는' 시만텍의 서비스.
법적 정체(Legal Entity)	해당 국가의 법률 시스템상 법적 정체를 가지는 사단, 회사, 합자회사, 신탁, 정부기관, 혹은 기타 법적 조직체.
Managed PKI	시만텍의 기업 고객과 그 관계사가 인증서를, 직원, 파트너, 공급자, 및 고객, 그리고 서버, 라우터 및 보안벽과 같은 장치류와 개인들에게 배포할 수 있도록, 완전하게 통합된 '시만텍의 managed PKI 서비스'. Managed PKI 는, 기업이 메세징, 인트라네트, 엑스트라네트, 가상 개인 네트워크, 그리고 전자상거래 애플리케이션을 안전하게 할 수 있도록 허용함.
Managed PKI 행정 담당자(Managed PKI Administrator)	Managed PKI 고객을 위한 유효화 내지 RA 기능들을 수행하는 행정 담당자.
Managed PKI 통제 센터(Managed PKI Control Center)	Managed PKI 행정 담당자가 인증서 신청에 대한 메뉴얼 인증을 수행할 수 있게 허용하는 웹 기반 인터페이스.
Managed PKI 키 관리자(Managed PKI Key Manager)	특별한 Managed PKI 계약서에 따라 키 복구를 실행할 것을 선택한 Managed PKI 고객들을 위한 키 복구 솔루션.
Managed PKI 키 관리 서비스 행정 담당자의 가이드(Managed PKI Key Management Service Administrator's Guide)	Managed PKI Key Manager 를 사용하는 Managed PKI 에 대한 운영 요건과 업무 준칙을 규정한 서류.
메뉴얼 인증(Manual Authentication)	웹기반 인터페이스를 사용하여 행정 담당자에 의하여, 인증서 신청 사항이 하나씩 수동으로 승인되고 검토되는 절차.
넷슈어 보호 계획(NetSure Protection Plan)	CPS 제 9 조 2 항 3 호에 규정된 확대 보장 프로그램.
미확인 가입자 정보(Non-verified Subscriber Information)	인증서 신청인이 CA 나 RA 에게 제출되고 인증서에 포함된 정보이지만, CA 나 RA 에 의하여 확인되지 않아서,관련 CA 와 RA 가 인증서 신청인에 의해 제출된 정보 이외에 대하여 보장하지 않는 정보.
부인방지(Non-repudiation)	제출되거나 수령한 소통사항을 거짓으로 부인하는 것을 방지하는 소통 기술. 송신 부인은, 송신자가 누구인지 알려지지 않았더라도, 동일한 자원으로부터 하나 이상의 예전 메세지에 대한 후행 결과로 초래된 소통사항을 부인하는 것을 포함. 주의: 오직 법원, 중재원, 혹은

용어(Term)	정의(Definition)
	위원회만이 궁극적으로 부인을 방지할 수 있음. 예를 들어, STN 인증서에 대하여 인증된 전자서명은 위원회에 의하여 부인방지 결정을 지지하는 증거를 제공할 수 있으나, 그 자체만으로는 부인방지를 구성하지는 않음.
객체 표시자(Object Identifier)	특정 객체나 객체 클래스에 대한 국제기구의 표준에 따라 등록된 고유의 알파수 혹은 수치 표시자.
OCSP (온라인 인증서 상태 프로토콜; Online Certificate Status Protocol)	신뢰자들에게 실시간 인증서 상태 정보를 제공하는 온라인 인증서 확인 프로토콜.
OCSP 대응자(OCSP Responder)	인증서 상태 요청을 진행하기 위하여 CA 의 권한 하에서 운영되고 저장소에 연결된 온라인 서버. 온라인 인증서 상태 프로토콜 참조.
오프라인 CA(Offline CA)	네트워크 침입자의 공격으로부터 보호하기 위한 보안을 이유로 오프라인 현장에서 유지 운영되는 STN PCA 들, 발행 루트 CA 들 및 기타 지정된 중간 CA 들. 이러한 CA 들은 직접 최종 사용자 가입자 인증서를 서명하지 않음.
온라인 CA(Online CA)	최종 사용자 가입자 인증서를 서명하는 CA 들은, 계속적인 서명 서비스를 제공하기 위하여 온라인에서 유지됨.
온라인 인증서 상태 프로토콜(Online Certificate Status Protocol (OCSP))	신뢰자들에게 실시간 인증서 상태 정보를 제공하는 온라인 인증서 확인 프로토콜.
운영 기간(Operational Period)	인증서가 발행된 일시부터(혹은, 인증서에서 정해진 바가 있으면 해당 일시) 인증서가 만료되는 일시 혹은 만료 전에 폐지되는 일시.
PKCS #10	RSA Security Inc.에 의하여 개발된, 공동키 암호 기준(Public-Key Cryptography Standard #10)으로, 인증서 서명 요청에 대한 구조를 정의함.
PKCS #12	RSA Security Inc.에 의하여 개발된, 공동키 암호 기준(Public-Key Cryptography Standard #12)으로, 개인키 이전에 대한 안전한 수단을 정의함.
정책 관리 권한자(Policy Management Authority (PMA))	STN 내 전반에 걸쳐 본 정책을 공표하는 책임을 지는 시만텍 내의 기관.
기본 인증 기관(Primary Certification Authority)(PCA)	인증서 특정 클래스에 대한 루트 CA 로 활동하며 하위 CA 들에게 인증서를 발행하는 CA.
개인키(Private Key)	키 쌍의 보유자에 의하여 비밀리에 보관되는 키 쌍의 키이며, 전자서명을 생성하기 위하여 사용되고, 합치하는 공동키로 암호화된 전자 기록이나 파일을 복호화 하는 데 사용됨.
처리 센터 (Processing Center)	인증서 발행에 사용되는 암호화 모듈과 같은 안전 설비 하우징을 생성하는 기관(시만텍 혹은 특정 관계사). 고객 및 웹싸이트 사업분야에서, 처리센터는 STN 내에서 CA 들로서의 역할을 수행하며, 인증서의 발행, 관리, 폐지, 및 갱신의 모든 라이프 사이클을 수행함. 기업 사업 분야에서, 처리센터는 하위 서비스 센터의 Managed PKI 고객을 대신하여 라이프 사이클 서비스를 제공함.
공동키(Public Key)	합치하는 개인키의 소유자에 의하여 공공연히 공개되는 키 쌍의 키이며, 신뢰자가 소유자의 개인키로 생성한 전자서명을 인증하고 암호화하기 위하여 사용되므로, 오직 소유자의 개인키로만 복호화됨.
공동키기반구조(Public Key Infrastructure (PKI))	인증서 기반공동키 암호화 시스템의 운영과 실행을 종합적으로 지원하는 설계, 기관, 기술, 업무 준칙. STN PKI 는 STN 을 공급하고 실행하는데 상호 협력하는 시스템으로 구성됨.
공개적으로 신뢰받는 인증서(Publicly-Trusted Certificate)	합치하는 루트 인증서가 널리 통용되는 애플리케이션 소프트웨어에 신뢰자로 배포됨으로써 신뢰받음.
유자격 감사(Qualified Auditor)	제 17 조 6 항(감사의 자격)을 충족하는 자연인이나 법적 정체.
등록된 도메인 이름(Registered Domain Name)	도메인 이름 등록기관에 등록된 도메인 이름.
등록 기관(Registration Authority (RA))	인증서 신청, 신청 거절이나 승인, 인증서 폐지나 갱신과 관련하여 인증서 신청인을지원할 수 있도록 CA 로부터 승인 받은 개체.
믿을 수 있는 통신 수단(Reliable Method of Communication)	우편, 특송, 전화번호, 이메일 주소와 같이 신청인 대표 이외의 정보원을 사용하여 인증된 의사소통 수단.
신뢰자(Relying Party)	인증서 및/혹은 전자서명을 신뢰하여 활동하는 개인이나 기관.
신뢰자 계약서 (Relying Party Agreement)	신뢰자로 활동하는 개인이나 기관의 조건을 CA 에 의하여 규정한 계약서..

용어(Term)	정의(Definition)
저장소(Repository)	CRL 이나 OCSP 대응 양식으로 공개적인 PKI 지배 서류(인증서 정책 및 인증업무준칙)와 인증서 상태 정보를 포함한 온라인 데이터베이스.
재판매자(Reseller)	특정 마켓에서 시만텍이나 관계사를 대신하여 서비스를 마케팅하는 개체.
예약된 IP 주소 (Reserved IP Address)	IANA 가 예약된 것으로 표시한 IPv4 나 IPv6 주소: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
리테일 인증서 (Retail Certificate)	시만텍이나 관계사의 웹싸이트에 각자신청하는 개인이나 기관들에게, CA 로서, 시만텍이나 관계사가 발행하는 인증서.
루트 CA(Root CA)	애플리케이션 소프트웨어 공급자를 통해 루트 인증서를 배포하고 하위 CA 인증서를 발행하는 가장 높은 단계의 인증기관.
루트 인증서 (Root Certificate)	자신을 확인하기 위해 루트 CA 에 의해 자기 서명 발행된 인증서와 인증서 인증을 하기 위해 하위 CA 들에게 발행된 인증서.
RSA	Rivest, Shamir, 그리고 Adelman 에 의해 발명된 공동키 암호화 시스템.
RSA Secure Server CA	Secure Server ID 들을 발행하는 인증기관.
RSA Secure Server 지배구조	RSA Secure Server 인증기관으로 구성된 PKI 지배구조.
비밀 비중(Secret Share)	비밀 공유 배정에 따라 CA 개인키를 운영하는데 필요한 데이터 비중과 CA 개인키의 비중.
비밀 공유(Secret Sharing)	CP wp6wh2 항 2 호에 따라 CA 개인키 운영에 대한 다중인 통제를 위해 운영되는 CA 개인키 데이터나 개인키의 분산 업무.
Secure Server ID	웹브라우저와 웹싸이트 사이의 SSL 세션을 지원하기 위하여 사용되는 클래스 3 기관용 인증서.
Secure Sockets Layer (SSL)	업계 표준인, '넷스케이프사가 개발한' 웹 커뮤니케이션 보호 도구. SSL 보안 프로토콜은, 데이터 암호화, 서버 인증, 메시지 무결성, 및 전송 제어 프로토콜에 대한 고객 인증을 제공함.
보안 및 감사 요건 가이드(Security and Audit Requirements (SAR) Guide)	절차센터와 서비스센터에 대한 보안 및 감사 요건과 업무준칙을 규정한 시만텍 서류.
보안 및 업무 검토(Security and Practices Review)	관계사가 운영을 개시하기 전에 시만텍이 관계사를 심사하는 것.
서비스 센터 (Service Center)	특정 클래스의 인증서 발행을 목적으로 서명단위를 가지지 않는 관계사, 그러나 해당 인증서의 발행, 관리, 폐지 및 갱신을 수행하기 위하여 절차 센터에 의존함.
서브 도메인(Sub-domain)	STN 지배계층 내에서 한 개체의 지배를 받는 SN 내의 일정 부분.
대상(Subject)	인증서에 대상자로 표시된 자연인, 장치, 시스템, 단위, 혹은 법적 정체이며 공동키에 부합하는 개인키의 소유자. 대상자는 가입자이거나 가입자의 지배 하에 있는 장치임. "대상"이라는 용어는, 기관용 인증서에서는 개인키를 보유한 장치나 장비를 언급함. 대상의 인증서에 포함된 공개키에 귀속되는 모호하지 않은 이름으로 배정됨. .
대상자 신원 정보(Subject Identity Information)	인증서 대상을 표시하는 정보. 대상 신원 정보는 *subjectAltName* 나 *commonName* 확장자에 나열된 도메인 이름을 포함하지 않음.
하위 CA(Subordinate CA)	자신의 인증서가 루트 CA 나 다른 하위 CA 에 의하여 서명되는 인증기관.
가입자(Subscriber)	개인용 인증서의 경우, 인증서의 대상이며 인증서를 발행 받은 사람. 기관용 인증서의 경우, 인증서의 대상이거나 발행된 인증서를 다루는 장치를 소유한 기관. 가입자는 인증서에 나열된 공동키에 합치하는 개인키를 사용하거나 사용할 수 있는 권한이 있음.
가입자 계약서 (Subscriber Agreement)	개인이나 기관이 가입자로서 활동해야 하는 조건이 CA 나 RA 에 의해 규정된 계약서.
우월한 개체 (Superior Entity)	STN 지배 계층(클래스 1,2, 혹은 3 지배) 내에 상위에 존재하는 개체.
보충적 위험 관리 검토(Supplemental Risk Management Review)	통상의 사업 과정에서 전체 위험관리절차로서 혹은 준법감사에서 불완전하거나 예외사항이 발견된 경우에 시만텍이 후속 검사 조치를 하는 것.
재판매자(Reseller)	특정 마켓에서 시만텍이나 관계사를 대신하여 서비스를 마케팅하는 개체.
시만텍(Symantec)	시만텍 주식회사 및/혹은 본 CPS 규정의 각 운영상의 이슈에 책임을 부담하는 시만텍의 자회사를 의미함.
시만텍 전자 공증 서비스(Symantec Digital Notarization Service)	Managed PKI 고객들에게 제공되는 서비스로, 특정 시간에 특정 데이터나 서류가 전자적으로 서명 동의되었음(전자적 수령자) 확인하는 서비스.
이용약관(Terms of Use)	신청인/가입자가 CA 의 관계사인 때, 본 요건에 따라 발행된 인증서를 이용하는데 필요한 통상의 사용 관련 규정.

용어(Term)	정의(Definition)
신뢰받는 자 (Trusted Person)	개체의 기반 신뢰구조, 제품, 서비스, 시설 및/혹은 인증업무, 그리고 CP 제 5 조 2 항 1 호에 규정된 업무준칙에 대하여 책임지는 STN 내의 개체의 직원, 계약자, 컨설턴트.
신뢰받는 직위 (Trusted Position)	신뢰받는 사람에 의해 운영되는 STN 개체 내 지위.
믿을 수 있는 시스템 (Trustworthy System)	침입이나 오용으로부터 합리적으로 보안을 실행할 수 있는 컴퓨터 하드웨어, 소프트웨어 및 절차; 합리적인 수준의 신뢰도, 정확한 운영; 의도한 대로의 기능 수행; 적정 보안 정책의 집행력을 제공함. 믿을 수 있는 시스템은 "신뢰받는 시스템"일 필요는 없음.
시만텍 저장소 (Symantec Repository)	온라인으로 접근할 수 있는, Symantec 의 인증서 데이터 베이스와 기타 Symantec Trust Network 관련 정보.
시만텍 신뢰 네트워크(Symantec Trust Network (STN))	Symantec Trust Network 인증서 정책에 의해 지배되는 인증서 기반 공동키 기반 구조이며, 시만텍, 관계사, 및 각 고객들, 가입자들 및 신뢰자들에 의한 인증서 사용과 세계적인 배포를 가능하게 함.
STN 참여자 (STN Participant)	STN 내에서 다음 중 하나인 개인이나 기관: 시만텍, 관계사, 고객, 통합 서비스 센터, 재판매자, 가입자, 혹은 신뢰자.
STN 기준 (STN Standards)	STN 내에서 인증서의 발행, 관리, 폐지, 갱신 및 사용을 위한 사업, 법적, 및 기술적 요건들.
미등록 도메인 이름(Unregistered Domain Name)	등록된 도메인 이름이 아닌 도메인 이름.
유효한 인증서 (Valid Certificate)	RFC 5280 에 규정된 유효화 절차를 통과한 인증서.
유효화 전문가 (Validation Specialists)	본 요건에 규정된 정보 인증 업무를 수행하는 자.
유효 기간 (Validity Period)	인증서가 발행될 때부터 유효기간이 만료될 때까지의 기간.
와일드카드 인증서 (Wildcard Certificate)	인증서에 포함된 대상의 완전한 조건을 충족하는 도메인 이름의 왼쪽 끝에 (*)을 표시한 인증서.