한국전자인증㈜ 전자서명인증사업자

공동인증서

전자서명 인증 업 무 준 칙

- Certification Practice Statement -

Version 5.0

한 국 전 자 인 증 주 식 회 사

Copyright© 2007, CROSSCERT : Korea Electronic Certification Authority, Inc. All Rights Reserved.

본 전자서명인증업무준칙에 대한 지적재산권은 한국전자인증㈜에 있습니다. 한국전자인증㈜의 사전허가 없이 이 자료를 복제하거나 컴퓨터 시스템에 저장 또는 삽입할 수 없으며, 어떤 형태나 방법(전자, 기계, 복사, 기록 등)으로도 배포할 수 없습니다. 위와 같은 제한에도 불구하고 (i) 상기 저작권 조항과 첫 단락을 각 사본의 처음에 명시하고, (ii) 문서에 대한 권한을 한국전자인증㈜에 귀속한 상태에서 완전 복제한다는 조건으로 비독점적인 무료 복제와 배포가 허용됩니다.

본 전자서명인증업무준칙은 전자서명법에 의한 전자서명인증사업자인 한국전자인증㈜에서 제공하는 공동인증서 인증서비스의 이용 및 운영에 관한 포괄적인 절차를 정하고 있습니다. 본 전자서명인증업무준칙은 전자서명법, 동법 시행령, 동법 시행규칙 을 준수합니다.

목 차

제1장 소 개 8

1.1 개요 8

1.1.1 준칙의 배경 및 목적 8

1.1.2 전자서명인증체계 소개 8

1.2 인증업무준칙의 명칭 8

1.3 전자서명인증체계 관련자 8

1.3.1 과학기술정보통신부 8

1.3.2 한국인터넷진흥원 9

1.3.3 한국전자인증 9

1.3.3.1 역할 9

1.3.3.2 책임과 의무 9

1.3.4 등록대행기관 11

1.3.4.1 역할 11

1.3.4.2 책임과 의무 12

1.3.5 중계서비스기관 12

1.3.5.1 역할 12

1.3.5.2 책임과 의무 13

1.3.6 가입자 14

1.3.6.1 역할 14

1.3.6.2 책임과 의무 14

1.3.7 이용자 15

1.3.7.1 역할 15

1.3.7.2 책임과 의무 15

1.4 공동인증서 종류 15

1.5 인증업무준칙의 관리 16

1.5.1 인증업무준칙의 관리부서 및 연락처 16

1.5.2 인증업무준칙의 개정 사유 16

1.5.3 인증업무준칙의 제·개정 절차 16

1.5.3.1 인증업무준칙의 공고 16

1.5.3.2 인증업무준칙 개정에 대한 가입자 동의 방법 17
1.6 정의 및 약어 17
제2장 전자서명인증업무 관련 정보의 공고 18
2.1 공고설비 18
2.2 공고방법 19
2.3 공고 주기 19
2.4 공고된 정보에 대한 책임 19
제3장 신원확인 20
3.1 가입자 이름(DISTINGUISHED NAME)의 표시 방법 20
3.2 공동인증서 신규 발급 시 신원확인 20
3.2.1 신원확인 방법 20
3.2.1.1 개인용 인증서 21
3.2.1.2 법인용 인증서 22
3.2.1.3 서버 인증서 23
3.2.1.4 대리인이 신청하는 경우 24
3.2.1.5 대면에 준하는 비대면 신원확인 방법 24
3.2.2 가입자의 전자서명생성정보 소유증명 방법 25
3.2.3 가입자가 인증서 발급 신청서에 기재한 사항 중 전자서명인증사업자가 해당 내용의 정확성을 확인하는 사항 26
3.3 공동인증서 갱신 발급, 재발급 및 변경 시, 신원확인 26
3.3.1 갱신발급 신원확인 방법 및 절차 26
3.3.2 재발급 신원확인 방법 및 절차 26
3.3.3 변경 신원확인 방법 및 절차 26
3.3.4 갱신발급, 재발급 및 변경 시 가입자의 전자서명생성정보 소유증명 방법 27
3.4 공동인증서 효력정지·효력회복·폐지 시, 신원확인 27
3.4.1 효력정지 신원확인 방법 및 절차 27
3.4.2 효력회복 신원확인 방법 및 절차 27
3.4.3 폐지 신원확인 방법 및 절차 28
제4장 인증서 관리 28
4.1 공동인증서 발급 신청 28

4.1.1 공동인증서 발급 신청 주체 및 신청 절차 28
4.1.1.1 개인에 대한 신원확인 29
4.1.1.2 법인에 대한 신원확인 29
4.1.1.3 찾아가는 서비스 29
4.1.1.4 방문발급 서비스 30
4.1.1.5 온라인 신원확인 30
4.2 공동인증서 발급 신청 처리 30
4.2.1 인증서 발급 신청 접수 및 처리 절차 30
4.2.2 인증서 발급 신청에 대한 거절 기준 31
4.2.3 인증서 발급 신청 접수에 대한 처리 기간 31
4.3 공동인증서 발급 절차 및 보호 조치 31
4.3.1 인증서 발급 절차 31
4.3.2 가입자 정보의 전송방법 및 가입자 정보의 기밀성, 무결성 등에 대한 정보보안 방법 32
4.4 공동인증서 수령 32
4.5 공동인증서 이용 33
4.6 공동인증서 갱신발급 33
4.6.1 갱신발급 요건, 신청주체 및 신청절차 33
4.6.2 가입자가 갱신 발급된 공동인증서를 수령하는 방법 33
4.7 공동인증서 재발급 34
4.7.1 재발급 요건, 신청주체 및 발급절차 34
4.7.2 가입자가 재발급된 공동인증서를 수령하는 방법 34
4.8 공동인증서 변경 34
4.8.1 가입자 정보가 변경된 인증서 발급 요건, 신청주체 및 신청절차 34
4.8.2 가입자가 정보가 변경된 공동인증서를 수령하는 방법 35
4.9 공동인증서 효력정지·효력회복·폐지 35
4.9.1 신청요건, 신청주체 및 신청절차 35
4.9.1.1 공동인증서 효력정지 요건 및 신청주체 35
4.9.1.2 공동인증서 효력정지 신청절차 35
4.9.1.3 공동인증서 효력회복 요건, 신청주체 및 신청절차 36
4.9.1.4 공동인증서 폐지 요건 및 신청주체 36
4.9.1.5 공동인증서 폐지 신청절차 37
4.9.2 가입자 정보의 전송방법 및 가입자 정보의 기밀성, 무결성 등에 대한 정보보안 방법 37

4.9.3 신청접수부터 해당 인증서 효력정지·효력회복 또는 폐지까지 소요되는 처리시간 37
4.9.4 공동인증서 효력정지 및 폐지목록(CRL) 발행 주기 37
4.9.5 공동인증서 효력정지 및 폐지목록(CRL) 발행 시점부터 해당 인증서 효력정지 및 폐지목록을 공고하는데 까지 소요 시간 38
4.9.6 공동인증서 효력정지 상태 유지 가능 기간 38
4.10 공동인증서 유효성 확인 서비스(OCSP) 38
4.10.1 공동인증서 유효성 확인 서비스 이용 방법, 이용 조건 38
4.10.2 공동인증서 유효성 확인 서비스 이용계약 해지 39
4.11 서비스 가입 철회 39
4.12 기타 부가 서비스 39
4.12.1 시점 확인 서비스 이용 방법 39
4.12.2 시점 확인 서비스 이용계약 해지 40
제5장 시설 및 운영 관리 40
5.1 물리적 보호조치 41
5.1.1 시설 위치와 구조에 관한 사항 41
5.1.2 물리적 보호조치에 관한 사항 41
5.1.3 물리적 잠금장치에 관한 사항 41
5.1.4 화재, 수재, 정전 방지 및 방호에 관한 사항 42
5.1.5 항온·항습, 통풍 및 기타 보호설비에 관한 사항 42
5.1.6 시설 및 장비의 폐기처리 절차에 관한 사항 42
5.1.7 원격지 백업설비 안전운영에 관한 사항 42
5.2 절차적 보호조치 43
5.2.1 전자서명인증업무 수행을 위해 필요한 업무의 종류와 그 업무 분장에 관한 사항 43
5.2.2 동일인에 의해 동시 수행될 수 없는 전자서명인증업무 44
5.2.3 업무 담당자 현황 및 담당자 인증방법 45
5.3 인적 보안 45
5.3.1 전자서명인증업무 수행 인력의 자격, 경력 등 요구사항 및 요건 충족 여부 확인 등 신원확인 절차 45
5.3.2 업무 수행 인력의 교육 및 업무순환에 관한 사항 45
5.3.3 비인가된 행위에 대한 처벌에 관한 사항 45
5.4 감사 기록 46

5.4.1 감사기록의 유형 및 보존기간 46
5.4.2 감사기록 보호조치 및 감사기록 백업주기 및 절차 46
5.5 기록 보존 46
5.5.1 보존되는 기록의 유형 및 보존기간 46
5.5.2 보존기록의 보호조치 47
5.5.3 보존기록의 백업주기 및 백업절차 47
5.6 전자서명인증사업자의 전자서명생성정보 갱신 47
5.7 장애 및 재해 복구 47
5.7.1 전자서명인증업무 장애 및 재해 유형별 처리 및 복구 절차 48
5.7.2 전자서명인증업무 장애방지 등 연속성 보장 대책 48
5.8 업무 휴지, 폐지, 종료 48

제6장 기술적 보호 조치 48

6.1 전자서명생성정보 보호 49
6.2 전자서명생성정보 보호 조치 49
6.3 전자서명생성정보 및 전자서명검증정보의 관리 49
6.4 데이터 보호 조치 49
6.5 시스템 보안 통제 50
6.6 시스템 운영 관리 50
6.7 네트워크 보호조치 50
6.8 시점확인서비스 보호조치 51

제7장 인증서 형식 51

7.1 공동인증서 형식 51
7.2 공동인증서 유효성 확인 정보 형식 54
7.3 공동인증서 유효성 확인 서비스 형식 55

제8장 감사 및 평가 57

8.1 감사 및 평가 현황 57
8.2 평가자의 신원, 자격 57
8.3 평가 대상과 평가자의 관계 57
8.4 평가 목적 및 내용 58
8.5 부적합 사항에 대한 조치 58

8.6 결과 보고 58

제9장 전자서명인증업무 보증 등 기타사항 58

9.1 수수료 58

9.1.1 공동인증서 수수료 58

9.1.2 공동인증서비스 수수료 59

9.1.3 전자인증서비스에 대한 환불 정책 59

9.2 배상 60

9.2.1 전자서명인증서비스 관련 배상 내용 60

9.2.2 면책 60

9.3 영업비밀 61

9.4 개인정보보호 61

9.5 지식재산권 62

9.6 보증 62

9.7 보증 예외 사항 63

9.8 보험의 보상 범위 63

9.9 배상 한계 63

9.10 준칙의 효력 63

9.10.1 준칙 시행일 63

9.10.2 준칙의 효력이 종료되는 조건 64

9.11 통지 및 의사소통 64

9.12 이력 관리 64

9.13 분쟁 해결 64

9.13.1 관련자에게 전달되는 문서(또는 전자문서)가 법적 효력을 갖기 위한 요건 64

9.13.2 분쟁을 해결하는 절차 64

9.14 관할 법원 65

9.15 관련 법의 준수 65

9.16 기타 규정 65

제1장 소 개

1.1 개요

1.1.1 준칙의 배경 및 목적

전자서명인증사업자인 한국전자인증 주식회사(이하 "한국전자인증"이라 한다)는 공동인증서의 발급(신규/갱신/재발급), 효력정지, 효력회복, 폐지 등의 인증서 인증업무와 인증시스템의 운영 및 절차에 관하여 필요한 사항을 정하고 인증업무와 관련된 책임과 의무를 규정하기 위하여 본 전자서명인증업무준칙(이하 "인증업무준칙"이라 한다)을 제정합니다. 한국전자인증의 인증업무준칙은 인증센터의 구축과 개시, 저장소 운영부터 가입자 등록에 이르기까지의 전체 프로세스를 대상으로 하고 있습니다.

1.1.2 전자서명인증체계 소개

전자서명인증체계(이하 "인증체계"라 한다)라 함은 공동인증서의 발급 및 인증관련 기록의 관리, 공동인증서를 이용한 부가 업무 등을 제공하기 위한 체계를 말합니다.

1.2 인증업무준칙의 명칭

본 인증업무준칙은 한국전자인증 공동인증서 인증업무준칙 버전(version) 5.0입니다.

1.3 전자서명인증체계 관련자

1.3.1 과학기술정보통신부

과학기술정보통신부는 전자서명을 안전하고 신뢰성 있게 이용할 수 있는 환경을 조성하고 전자서명인증사업자를 행정적,재정적,기술적 지원할 수 있으며 다음과 같은 업무를 수행합니다.

- 법 제5조(전자서명의 이용 촉진을 위한 지원)
- 법 제7조(전자서명인증업무 운영기준 등)

- 법 제9조(인정기관) 규정에 따라 인정기관을 지정
- 법 제10조(평가기관) 규정에 따라 평가기관을 선정, 고시
- 법 제12조(평가기관 선정의 취소 등) 규정에 따라 평가기관을 선정 취소, 정지
- 법 제16조(검사 등) 규정에 따라 인정을 받은 전자서명인증사업자에 검사
- 법 제17조(시정명령) 규정에 따라 인정을 받은 전자서명인증사업자에 시정

1.3.2 한국인터넷진흥원

한국인터넷진흥원은 법 제9조(인정기관) 규정에 따라 인정기관 업무 수행 및 법 제21조(전자서명인증 정책의 지원 등) 규정에 따라 전자서명인증 정책 지원업무를 수행합니다.

1.3.3 한국전자인증

1.3.3.1 역할

한국전자인증은 전자서명법, 동법 시행령 및 시행규칙(이하 "전자서명관련법" 이라 한다)과 인증업무준칙에 의하여 다음의 업무를 수행합니다.

- 가입자의 신원확인
- 인증서비스 관련 제반 신청서 접수 및 처리
- 등록대행기관의 지정과 관리 및 운영
- 시점확인 서비스의 제공
- 공동인증서 발급(신규/재발급/갱신), 효력정지, 효력회복, 폐지 등의 인증서비스의 제공
- 공동인증서 목록, 공동인증서 효력정지 및 폐지목록 등 공동인증서 관련 정보 공고
- 인증업무준칙 공고
- 공동인증서 관련 정보 공고
- 기타 인증서비스와 관련된 업무

1.3.3.2 책임과 의무

① 관련 법규 및 인증업무준칙의 준수

한국전자인증은 인증서비스를 수행하는 동안 전자서명관련법 을 준수합니다.

한국전자인증은 가입자 및 이용자에게 공동인증서의 신뢰성이나 유효성에 영향을 미칠 수 있는 다음과 같은 정보를 인증체계에 의하여 누구든지 항상 확인할 수 있도록 지체 없이 공고할 책임과 의무가 있습니다.

- 전자서명인증사업자의 인증업무 휴지·정지 또는 폐지
- 전자서명인증사업자 양도·양수 또는 합병
- 공동인증서에 대한 정보
  - 가입자의 공동인증서
  - 가입자의 공동인증서 효력정지 및 폐지목록 등
- 기타 인증업무 수행관련 정보 등

한국전자인증은 전자인증사업자와 관련하여 제공되는 정보는 홈페이지를 통해 공고합니다. 또한 공동인증서, 공동인증서 효력정지 및 폐지목록 등의 공동인증서 상태 정보를 정보통신망을 통해 항상 검색할 수 있도록 디렉토리 서비스를 제공합니다.

② 인증서비스의 제공

한국전자인증은 정당한 사유 없이 인증서비스의 제공을 거부하지 않으며 가입자 또는 이용자를 부당하게 차별하지 않습니다. 한국전자인증은 가입자 및 이용자에게 다음과 같은 인증서비스를 제공합니다.

- 공동인증서 발급(신규/재등록/갱신)
- 공동인증서 효력정지, 효력회복 및 폐지
- 공동인증서 서비스 제공(발급, 효력정지, 효력회복, 폐지 등)과 관련한 신원확인 업무
- 공동인증서 관련 정보 공고
- 기타 공동인증서와 관련된 서비스 등

③ 인증서비스의 보장

한국전자인증은 한국인터넷진흥원이 한국전자인증을 위하여 발급한 전자서명인증사업자용 인증서에 포함된 전자서명검증정보에 합치하는 전자서명생성정보로 발급한 가입자 공동인증서에 대해 다음 사항을 보장합니다.

- 발급된 공동인증서에 포함된 내용이 신청·등록된 사실과 오차가 없다는 사실

- 공동인증서 효력정지 및 폐지목록에 대한 내용이 틀림없다는 사실
- 전자서명관련법 및 인증업무준칙의 규정을 준수하여 공동인증서가 발급되었다는 사실

하지만 공동인증서가 가입자 및 이용자의 신용등급, 가입자 관련정보의 불변성 등 상기 사항 이외의 것까지 보장한다는 것을 의미하지는 않습니다.

④ 가입자의 개인정보 보호 및 자료의 보안 유지

한국전자인증은 본 인증업무준칙 9.4에 규정된 개인정보보호정책을 준수함으로써 가입자의 개인정보를 보호하고 자료의 보안을 유지합니다.

⑤ 전자서명생성정보의 올바른 이용

한국전자인증은 이용목적에 따라 다음과 같은 여러 가지 전자서명생성정보를 생성할 수 있습니다. 그러나 전자서명생성정보는 원래 목적한 분야에만 이용할 수 있습니다.

- 공동인증서 발급용 전자서명생성정보: 공동인증서 발급에만 이용
- 시점 확인용 전자서명생성정보: 시점확인에만 이용
- OCSP(Online Certificate Status Protocol)용 전자서명생성정보: OCSP를 위해서만 이용
- 기타 전자서명생성정보: 해당 용도에만 이용

⑥ 전자서명생성정보의 보호

한국전자인증은 신뢰할 수 있는 소프트웨어나 하드웨어 등을 이용하여 안전한 방법으로 한국전자인증의 전자서명인증사업자용 전자서명생성정보를 생성하며, 생성된 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리합니다.

1.3.4 등록대행기관

1.3.4.1 역할

한국전자인증은 한국전자인증을 대신하여 가입자에 대한 신원확인을 수행하고 공동인증서 발급, 효력정지, 효력회복 또는 폐지 등의 신청을 접수·등록하는 자(이하 "등록대행기관"이라 한다)를 지정하여 운영할 수 있습니다. 등록대행기관의 업무는 다음과 같습니다.

- 공동인증서 발급(신규/재발급/갱신), 폐지, 효력정지 및 효력회복 신청 접수 및 등록
- 인증서비스 신청인의 신원확인 업무
- 기타 인증서비스와 관련하여 한국전자인증이 위임한 업무

1.3.4.2 책임과 의무

① 인증업무준칙의 이해

등록대행기관은 한국전자인증의 인증업무준칙과 한국전자인증과 체결한 계약서에 정한 사항을 준수하여야 하며 가입자 신원확인의 정확성에 대한 책임이 있습니다.

② 가입자의 신원확인

등록대행기관은 공동인증서를 발급받고자 하는 자에 대하여 전자서명관련법에서 정하는 신원확인의 기준 및 방법에 따라 신원을 확인하여야 하며 당해 신청내용의 무결성을 확인하여야 합니다.

③ 배상과 책임

등록대행기관은 본 인증업무준칙상 의무사항을 위반함으로써 한국전자인증, 가입자 또는 이용자에게 손해를 입힌 경우 그 손해에 대해 배상하여야 할 책임이 있습니다.

④ 인증업무준칙의 준수

등록대행기관은 인증서비스의 제공과 관련하여 본 인증업무준칙에서 정한 등록대행기관의 업무를 성실히 수행할 의무를 가집니다.

⑤ 가입자의 개인정보보호

등록대행기관은 등록대행업무 수행 중 취득한 가입자의 개인정보를 보호하고 자료에 대한 보안을 유지할 의무가 있습니다.

1.3.5 중계서비스기관

1.3.5.1 역할

중계서비스기관은 한국전자인증 및 등록대행기관간 약정을 체결하여 가입자 등록정보 등을 단순 전달하는 시스템(이하 "중계시스템"이라 한다)을 운영하는 자를 말합니다.

1.3.5.2 책임과 의무

① 인증업무준칙의 이해

중계서비스기관은 한국전자인증의 인증업무준칙을 숙지하고 있어야 하며 중계서비스를 위해 한국전자인증과 맺은 계약서에서 정한 사항을 준수할 책임을 가지며, 다음과 같은 정보에 대해서 한국전자인증 및 등록대행기관이 처음 전송한 상태대로 전달할 책임이 있습니다.

- 가입자 이름(성명 또는 법인명) · 식별번호(주민등록번호 또는 사업자등록번호 등) · 주소 · 전화번호 · 전자우편 주소 · DN(Distinguished Name) 등 가입자의 등록정보
- 한국전자인증기관이 생성한 참조번호 및 인가코드

② 중계서비스기관의 의무

중계서비스기관은 다음의 사항들에 대해서 중계시스템 및 보호설비를 갖추어야 합니다.

- 출입통제
- 물리적 침입 감시
- 시스템 및 네트워크 보호

③ 배상책임

중계서비스기관은 본 인증업무준칙상 의무사항을 위반함으로써 한국전자인증, 가입자 또는 이용자에게 손해를 입힌 경우 그 손해에 대해 배상하여야 할 책임이 있습니다.

④ 인증업무준칙의 준수

중계서비스기관은 인증서비스의 제공과 관련하여 본 인증업무준칙에서 정한 중계서비스기관의 업무를 성실히 수행할 의무를 가집니다.

⑤ 가입자의 개인정보보호

중계서비스기관은 중계되는 가입자의 개인정보를 보호하고 자료에 대한 보안을 유지할 의무가 있습니다.

1.3.6 가입자

1.3.6.1 역할

가입자는 전자서명생성정보에 대하여 한국전자인증으로부터 전자서명인증을 받은 자를 말합니다.

1.3.6.2 책임과 의무

① 정확한 정보의 제공

가입자는 가입자의 목적에 맞는 공동인증서를 선택해서 신청해야 하며, 다음과 같은 경우에 정확한 정보 및 사실만을 한국전자인증에 제공할 의무가 있습니다.

- 공동인증서 발급(신규/재발급/갱신)신청 시
- 공동인증서 효력정지 신청 시
- 공동인증서 효력정지 회복 신청 시
- 공동인증서 폐지 신청 시
- 가입자 신원정보 변경 시 변경된 정보 제공

② 전자서명생성정보의 관리

가입자는 자신의 전자서명생성정보를 안전하게 보관관리하고, 이를 분실훼손 또는 도난유출되거나 훼손될 수 있는 위험을 인지한 때에는 그 사실을 한국전자인증에게 통보하여야 합니다. 이 경우 가입자는 지체 없이 이용자에게 한국전자인증에 통보한 내용을 고지하여야 합니다.

③ 공동인증서의 관리

가입자는 공동인증서의 유효기간 이내에 당해 공동인증서의 기재사항 또는 공동인증서와 결부된 정보가 정확하고 완전하게 유지되도록 상당한 주의를 기울여야 합니다. 또한 가입자는 공동인증서를 이용범위 또는 용도에서 벗어나 부정하게 사용하여서는 아니되며, 행사하게 할 목적으로 다른 사람에게 공동인증서를 양도 또는 대여하거나 행사할 목적으로 다른 사람의 공동인증서를 양도 또는 대여 받아서는 아니됩니다.

④ 가입자의 배상책임

가입자는 본 인증업무준칙상 가입자 의무사항을 위반함으로써 한국전자인증과 이용자에게 손해를 입힌

경우에는 그 손해를 배상하여야 합니다.

1.3.7 이용자

1.3.7.1 역할

이용자는 한국전자인증이 제공하는 전자서명인증서비스를 이용하는 자를 말합니다.

1.3.7.2 책임과 의무

① 이용자의 준수사항

이용자는 (1)가입자의 이름 (2)전자서명검증정보 (3)한국전자인증이 이용하는 전자서명방식 (4)공동인증서의 일련번호 (5)공동인증서의 유효기간 (6)한국전자인증이 전자서명인증사업자임을 확인할 수 있는 정보에 의하여 전자서명의 진위여부를 확인하기 위하여 다음 각 조치를 취하여야 합니다.

- 공동인증서의 유효 여부의 확인
- 공동인증서의 정지 또는 폐지 여부의 확인
- 공동인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항 확인
- 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격 등의 표시를 요청한 경우 이에 관한 사항 확인

② 이용자의 배상책임

이용자가 고의 또는 과실로 인한 위법행위로 한국전자인증 또는 가입자에게 손해를 입힌 경우에 그 손해를 배상할 책임이 있습니다.

1.4 공동인증서 종류

한국전자인증은 개인과 법인/단체/개인사업자에 대하여 공동인증서를 발행하며 발행되는 공동인증서의 종류, 발급대상, 용도 및 유효기간은 다음과 같습니다.

발급대상	공동인증서 종류	용도(이용범위)	유효 기간

법인/단체/개인사업자	범용	-일반 전자상거래 -금융기관 업무 -정부 전자 조달/민원업무 -국세청 전자 세금계산서/민원업무	3년 이내
	용도제한용	-전자세금계산서 업무 -은행, 보험 및 신용카드 업무 -기타 별도 계약에 따름	
개인	범용	-일반 전자상거래 -금융기관 업무 -정부 민원업무	
	용도제한용	-은행, 보험 및 신용카드 업무 -정부 민원업무 -기타 별도 계약에 따름	
서버	범용	-온라인상 서버를 통해 인증서비스를 이용하는 업무	3년 이내

[표1] 공동인증서의 종류 및 용도 등

1.5 인증업무준칙의 관리

1.5.1 인증업무준칙의 관리부서 및 연락처

본 인증업무준칙의 관리는 한국전자인증 공동인증사업본부에서 담당하며 연락처는 다음과 같습니다.
(전화: 02-3019-5686 팩스: 02-3019-5656 전자우편:gca@crosscert.com)

1.5.2 인증업무준칙의 개정 사유

한국전자인증은 다음의 사유가 발생한 경우에 인증업무준칙을 개정합니다.

- 한국전자인증에서 제공하는 인증서비스의 내용이나 절차가 변경되었거나 신규로 제공하는 인증관련 서비스로 인해 인증업무준칙의 변경이 필요하다고 판단된 경우 인증업무준칙을 개정할 수 있습니다.

1.5.3 인증업무준칙의 제·개정 절차

1.5.3.1 인증업무준칙의 공고

한국전자인증은 제정, 개정된 인증업무준칙을 공동인증서 관련 정보저장 위치에 규정된 URL에 적용하기 2주 전에 공고합니다. 공고는 한국전자인증의 웹사이트(https://www.crosscert.com)에 게시하는 방법으로 합니다.

한국전자인증은 필요하다고 인정되는 경우에 본 인증업무준칙의 일부 또는 전부를 변경할 수 있으며, 이 경우에는 적용 일자 2주 전에 변경된 인증업무준칙을 공고하고 인증업무준칙의 변경사실을 가입자에게 고지합니다.

1.5.3.2 인증업무준칙 개정에 대한 가입자 동의 방법

가입자가 변경된 인증업무준칙이 공고된 후 2주 이내에 서면 또는 전화, 전자메일의 수단을 통하여 이의를 제기하지 아니한 때에는 변경된 인증업무준칙에 동의하는 것으로 간주하며, 한국전자인증은 이러한 동의간주의 내용 또한 변경된 업무준칙과 동시에 공고하거나 고지하여야 합니다. 고지는 공고와 동일한 방법 또는 전자우편의 수단을 통하여 할 수 있습니다.

1.6 정의 및 약어

DN(Distinguished Name): 공동인증서 발급자 및 공동인증서 소유자를 확인하기 위해 사용되는 X.500 표준을 준수하는 이름 형식을 말합니다.

디렉토리: 공동인증서, 공동인증서 효력정지 및 폐지목록을 보관하고 신뢰당사자에게 공고 및 검색 서비스를 제공하기 위한 것으로 X.500 표준을 준수하는 시스템을 말합니다.

서비스 방해 공격: 시스템의 정상적인 기능 수행을 방해하는 공격 행위를 말합니다.

실명: 실명이란 주민등록표상의 명의, 사업자등록증상의 명의, 기타 금융실명거래및비밀보장에관한법률 및 동 시행령에서 정하는 실지명의를 말합니다.

서명자 : 전자서명생성정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말합니다.

인증: 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말합니다.

전자문서: 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말합

니다.

전자서명: 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말합니다.

전자서명검증정보: 전자서명을 검증하기 위하여 이용하는 전자적 정보를 말합니다.

전자서명생성정보: 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말합니다.

전자서명키: 전자서명생성정보와 이에 합치하는 전자서명검증정보를 말합니다.

핵심인증시스템: 키 생성시스템, 공동인증서 생성 관리시스템, 디렉토리 시스템 및 시점확인 시스템을 말합니다.

단말기 지정: 인증서 신청시 가입신청자의 단말기(PC, 스마트폰 등)의 기기정보(IP, MAC, HDD Serial 등)를 수집하여 등록대행기관에 등록하고, 인증서 발급 시 가입신청자가 등록한 단말기인지 여부를 확인하여 가입신청자의 신원을 확인하는 방법을 말합니다.

추가인증: 휴대폰 SMS인증, 다채널 인증 등과 같이 단말기 지정 이외의 수단으로 가입신청자의 신원을 확인하는 방법을 말합니다.

다채널 인증: 서로 다른 두 가지 이상의 통신경로를 이용하여 가입신청자의 신원을 확인하는 방법을 말합니다.

보안토큰: 전자서명 생성키 등 비밀정보를 안전하게 저장·보관하기 위하여 키 생성·전자서명 생성 등이 기기 내부에서 처리되도록 구현된 하드웨어 기기(일반 보안토큰, 지문보안토큰, USIM 포함)를 말합니다.

사고정보: 전자금융사고 또는 공동인증서 유출 등 사고가 발생한 가입자의 기기정보 및 개인정보(성명, 주민등록번호, 전화번호, 휴대전화번호, 이메일)를 말합니다.

다년형 인증서: 유효기간 2년 이상의 인증서를 말합니다.

기타 용어의 정의는 전자서명법에 따릅니다.

제2장 전자서명인증업무 관련 정보의 공고

2.1 공고설비

한국전자인증은 인증업무준칙, 공동인증서, 공동인증서 효력정지목록 및 공동인증서 폐지목록 등 공동인증서 발급 및 관리 등에 관련된 정보("전자서명인증업무관련정보"라 한다)를 누구든지 항상 확인할 수 있도록 전자서명인증업무관련정보를 공고하는 설비를 운영하여야 하고 전자서명인증업무관련정보의 내용이 변경되는 때에는 해당 변경사항을 지체없이 공고하여야 합니다

2.2 공고방법

한국전자인증은 전자서명인증업무관련정보를 본 인증업무준칙 2.1(공고설비)의 정보저장위치를 통하여 지체없이 공고하여야 합니다. 전자서명인증업무관련정보의 내용이 변경되는 경우에는 본 인증업무준칙 4.9.4(공동인증서 효력정지 및 폐지목록(CRL) 발행 주기)에 따라 해당 사안의 처리가 완료되는 즉시 공고하여야 하는 책임이 있습니다.

한국전자인증의 전자서명인증업무관련정보의 저장·공고위치는 다음과 같습니다.

한국전자인증 관련 정보

전자서명인증업무준칙	https://crosscert.com/glca/01_5_05_2.jsp
공동인증서 효력정지 및 폐지목록	ldap://dir.crosscert.com
등록대행기관 정보	https://www.crosscert.com/glca/01_4_01.jsp

2.3 공고 주기

공동인증서 발급 및 관리 등에 관련된 정보는 처리 후 즉시 공고하며, CRL은 최대 24시간을 주기로 갱신·공고합니다. 주기는 변경될 수 있으며, 변경이 발생하는 경우 당해 사실을 한국전자인증의 홈페이지(https://www.crosscert.com)에 공고합니다.

2.4 공고된 정보에 대한 책임

위에서 명시한 공고 위치, 공고방법, 공고 시점 및 공고주기를 준수하며, 해당 사항이 지켜지지 아니하여 발생하는 문제에 대한 책임이 있습니다.

제3장 신원확인

3.1 가입자 이름(Distinguished Name)의 표시 방법

공동인증서, 공동인증서 효력정지 및 폐지목록내의 기본영역에 사용되는 명칭은 X.500에서 정한 DN (Distinguished Name) 방식을 준용합니다.

① DN의 표현방법

한국전자인증은 공동인증서를 발급함에 있어 가입자의 이름에 대해 다음과 같은 것들을 허용합니다.

- 개인 실명, 법인명 등 법적 이름(영문)
- 인터넷 도메인명
  - 인터넷 IP 주소
  - 증명서가 수반된 특허청 또는 국제적으로 인정된 상표권 등
  - WWW용 URL
  - 전자우편 주소 등

단, 가입자가 별도의 명칭을 요청할 경우에는 협의절차를 거쳐 공동인증서에 가입자가 원하는 이름을 기재하도록 허용할 수 있습니다.

② DN의 유일성 보장방법

가입자가 제출한 정보를 이용하여 주어진 기준에 따라 DN을 구성하여 공동인증서에 저장하게 됩니다. 이때 DN은 이용자가 공동인증서를 확인하고자 할 때 사용될 수 있는 기준정보가 되므로 DN의 중복성 확인 절차를 거치게 되며 중복되지 않는 경우에만 공동인증서를 발급합니다. 만약 DN이 중복되는 경우에는 가입자에게 새로운 DN을 요청할 수 있으며 인증서비스를 이용하려면 반드시 이에 응해야만 합니다.

3.2 공동인증서 신규 발급 시 신원확인

3.2.1 신원확인 방법

한국전자인증은 공동인증서의 이용범위 및 용도 등을 고려하여 그 신원을 확인하며 기본원칙은 다음과

같습니다.

- 신규가입자는 직접 대면(운영기준에 적합한 것으로 인정받은 직접 대면에 준하는 비대면 방법을 포함)에 의한 신원확인을 실시하는 것을 원칙으로 합니다. 단, 금융기관 혹은 공공기관 등 신뢰할 수 있는 기관을 통해 직접 대면에 의한 신원확인을 거친 가입신청자에 대해서는 대면에 준하는 방식으로 신원확인을 할 수 있습니다.
- 한국전자인증 혹은 타 전자서명인증사업자에서 발급된 유효한 공동인증서를 이용하여 신원확인을 할 수 있습니다.
- 한국전자인증이 정한 신원확인 절차를 거친 가입자에게만 공동인증서를 발급합니다.
- 제출되는 서류는 최초 가입신청을 할 때와 비교하여 변경된 사항만을 통보하면 됩니다. 이 경우에도 가입신청자의 정보통신망상의 주요 연락처는 반드시 통보해야만 합니다.

3.2.1.1 개인용 인증서

- 일반인 (성년)
  - 인증서비스 신청서
  - 주민등록증 발급대상자는 주민등록증
  - 다만, 주민등록증에 의하는 것이 곤란할 경우에는 국가기관 또는 지방자치단체 및 교육기본법에 의한 학교의 장이 발급한 것으로서 성명, 주민등록번호가 기재되어 있고 부착된 사진에 의하여 본인임을 확인할 수 있는 증표 사본 (원본 지참)
- 미성년자
  - 인증서비스 신청서
  - 미성년자와 법정대리인의 주민등록증 (주민등록증 발급 대상자)
  - 다만, 주민등록증에 의하는 것이 곤란할 경우에는 국가기관 또는 지방자치단체 및 교육기본법에 의한 학교의 장이 발급한 것으로 성명, 주민등록번호가 기재되어 있고, 부작된 사진에 의하여 본인임을 확인할 수 있는 증표 사본 (원본지참) 또는
  - 주민등록증 발급대상자가 아닌 자는 주민등록번호를 포함한 주민등록표 초본과 법정대리인의 신분증 증표 또는 실지명의의 확인이 가능한 증표·서류
  - 법정대리인의 동의서
  - 미성년자와 법정대리인의 관계를 증명할 수 있는 증명 서류
- 재외국민
  - 인증서비스 신청서

- □ 주민등록표(주민등록법 제6조에 따라 주민등록이 된 재외국민의 경우, 원본지참) 또는
- □ 여권 사본 (원본지참) 또는
- □ 재외국민등록증 사본 (원본지참)

❑ 외국인

- □ 인증서비스 신청서
- □ 출입국관리법에 의한 외국인등록증, 선원수첩, 국제운전면허증, 여권 중 사본 (원본지참)
- □ 외국인등록증이 발급되지 아니하고 위 증표가 없는 경우 해당국가의 관할 관청이 발급한 신원확인증표 사본 (원본지참)

3.2.1.2 법인용 인증서

① 대표자 본인이 한국전자인증 또는 등록대행기관을 방문하여 공동인증서 발급신청을 할 경우

❑ 국내법인

- □ 인증서비스 신청서
- □ 법인의 신원확인 증표

  비송사건절차법에 의한 법인등기부등본, 상업등기법에 의한 상업등기부등본, 법인세법에 의한 사업자등록증, 소득세법에 의한 납세번호증, 부가가치세법에 의한 고유번호증, 사업자등록증명원 중 사본 (법인등기부등본, 상업등기부등본은 원본 제출)
- □ 대표자의 주민등록증, 운전면허증, 여권 또는 국가기관 또는 지방자치단체의 장이 발행한 사진을 부착한 증명서 중 사본 (원본 지참)

❑ 단체

- □ 인증서비스 신청서
- □ 단체의 신원확인증표

  납세번호 또는 고유번호가 있는 경우: 납세번호, 고유번호 부여사실 통보문서 사본(원본지참)

  납세번호 또는 고유번호가 없는 경우: 대표자의 주민등록증, 운전면허증, 여권 또는 국가기관 또는 지방자치단체의 장이 발행한 사진을 부착한 증명서 중 사본 (원본 지참)

❑ 외국법인 또는 외국단체

- □ 인증서비스 신청서
- □ 법인/단체의 신원확인 증표

  당해 국가의 관할관청이 발급한 법인등기부등본(또는 상업등기부 등본)이나 당해 국가의 관할관청 또는 국내에 있는 그 외국영사가 인증한 것으로써 그 법인 또는 단체의 존재를 인정

할 수 있는 서면 등 신원확인 관련 증빙서류 사본 (원본 지참)

- □ 대표자의 신분증명서(사진 부착) 사본 (원본지참)

❑ 개인사업자의 경우

■ 국내인

- □ 인증서비스 신청서
- □ 사업자 등록증 사본
- □ 대표자의 주민등록증, 운전면허증, 여권, 국가기관 또는 지방자치단체의 장이 발행한 사진을 부착한 증명서 중 사본 (원본 지참)

■ 재외국민

- □ 인증서비스 신청서
- □ 사업자 등록증 사본
- □ 대표자의 여권, 재외국민등록증 중 1의 사본 (원본지참)

■ 외국인

- □ 인증서비스 신청서
- □ 사업자 등록증 사본
- □ 대표자의 신분증명서(사진 부착) 사본(원본지참)

② 대리인이 한국전자인증 또는 등록대행기관을 방문하여 공동인증서 발급신청을 하는 경우에는 본 인증업무준칙 3.2.1.4와 같습니다.

3.2.1.3 서버 인증서

① 대표자 본인이 한국전자인증 또는 등록대행기관을 방문하여 서버인증서 발급신청을 할 경우 서버인증서를 신청하는데 있어서 제출해야 할 문서 및 서류는 다음과 같습니다. 단, 외국법인 및 외국단체 사업자, 외국인 개인사업자의 경우 3.2.1.2(법인용 인증서)에서 명시된 바와 같이 서류를 제출하면 됩니다.

❑ 법인용 서버인증서

- □ 인증서 발급 신청서
- □ 법인의 신원확인 증표

  비송사건절차법에 의한 법인등기부등본, 상업등기부등본, 법인세법에 의한 사업자등록증, 소득세법에 의한 납세번호증, 부가가치세법에 의한 고유번호증, 사업자등록증명원 중 사본 (법인등기부등본 상업등기부등본은 원본 제출)

- □ 대표자의 주민등록증, 운전면허증, 여권, 국가기관 또는 지방자치단체의 장이 발행한 사진을 부착한 증명서 중 사본 (원본 지참)

- ◘ 개인사업자용 서버인증서
  - □ 인증서 발급 신청서
  - □ 사업자 등록증 사본
  - □ 대표자의 주민등록증, 운전면허증, 여권, 국가기관 또는 지방자치단체의 장이 발행한 사진을 부착한 증명서 중 사본 (원본 지참)

② 대리인이 한국전자인증 또는 등록대행기관을 방문하여 서버인증서 발급신청을 하는 경우에는 본 인증업무준칙 3.2.1.4와 같습니다.

3.2.1.4 대리인이 신청하는 경우

법인용 인증서 및 서버인증서의 신청 시 대표자에 대한 신원확인은 대표자의 위임을 받은 법인의 임•직원에 대한 신원확인으로 갈음 할 수 있으며, 이 경우 추가로 필요한 서류는 다음과 같습니다.

인증서비스 신청서
본 인증업무준칙 3.2.1.2에서 정한 법인/단체/외국법인 신원확인증표
위임장 (인감날인)
법인 인감증명서 (개인사업자는 대표자의 인감증명서)
대리인의 신분증명서 사본 (원본지참)

3.2.1.5 대면에 준하는 비대면 신원확인 방법

한국전자인증은 대면에 준하는 비대면의 방법으로 온라인으로 비대면 신원확인을 할 수 있으나, 이는 개인사업자와 법인사업자로 한정합니다. 가입신청자가 개인사업자인 경우 해당 개인 대표자의, 법인사업자인 경우 법인 및 법인 대표자의 신원을 확인합니다. 다만, 법인의 대표자는 해당 법인의 임•직원을 대리인으로 하여 가입신청할 수 있으며, 이 경우 법인 대표자 대신 그 대리인의 신원을 확인합니다. 개인사업자 또는 법인사업자의 대표자가 직접 가입신청을 한 경우는 물론, 법인 대표자가 대리인을 통해 가입신청을 한 경우에도 신원확인을 위하여 제출 받는 서류는 본 인증업무준칙 3.2.1에서 정한 서류와 동일합니다. 그러나 한국전자인증이 원본과의 동일성을 확인할 수 있을 정도의 스캔본 또는 촬영본(이하 '스캔본 등')을 제출 받은 경우, 해당 스캔본 등을 통해 신원을 확인할 수 있으며, 별도의 원본을 요구하지 않을 수 있습니다.

한국전자인증이 온라인으로 비대면 신원확인을 하는 경우 그 방법은 아래와 같습니다.

◘ 개인사업자의 대표자 또는 법인사업자의 대표자가 직접 가입 신청하는 경우의 신원확인

① 개인용 인증서를 통한 신원확인

- 가입신청자의 개인용 인증서 인증(가입신청자의 선택에 따라 본인 명의 휴대폰 인증으로 대체 가능)을 통해 인적사항을 확인합니다.
- 가입신청자가 제출한 본인확인수단 관련 정보를 해당 인증기관으로 전송한 뒤 해당 인증기관으로부터 본인확인정보 검증결과를 수신하고 그 결과에 따라 절차를 진행합니다.

② 신원확인증표 스캔본 등을 통한 신원확인

- 개인사업자에 대한 신원확인증표(3.2.1.2에서 정한 서류를 의미함, 이하 같음), 법인사업자에 대한 신원확인증표의 스캔본 등이 원본과 동일함을 확인합니다.
- 신원확인 절차 및 방법은 대면 방식과 동일하나, 스캔본 등을 토대로 진행합니다. 이 경우 한국전자인증은 신원확인증표의 진위여부를 확인하기 위해 신원확인증표의 직접 촬영본 등을 요구할 수 있습니다.- 사업자등록증명, 법인등기부등본, 상업등기부등본은 신청서 접수일 7일이내 발급분으로 제한합니다.

③ 계좌인증에 의한 신원확인

- 실명 확인된 가입신청자의 은행계좌를 통해 소액을 송금하거나 송금 받도록 하는 방식입니다.
- 해당 계좌가 가입신청자 명의의 계좌인지 여부, 가입신청자가 해당 계좌를 조회하거나 송금할 권한을 보유한 실제 권리자인지 여부를 확인합니다.

◘ 법인의 대표자가 대리인을 통해 신청하는 경우의 신원확인

① 법인의 대표자가 직접 신청하는 경우의 신원확인 방법에 따르되, 그 중 대표자 개인에 대한 신원확인 절차는 대리인에 대한 신원확인 절차로 대체합니다.

② 대리인의 자격을 확인하기 위하여 건강보험자격득실확인서(신청서 접수일 7일이내 발급분에 한함)를 추가로 제출 받으며, 법인 대표자의 위임장과 법인인감증명서은 원본과의 동일성을 확인할 수 있을 정도의 스캔본 등으로 대체할 수 있습니다.

③ 나머지 신원확인 절차 및 방법은 대면에 의한 대리인 신청의 경우와 동일합니다.

3.2.2 가입자의 전자서명생성정보 소유증명 방법

가입자는 자신의 전자서명생성정보로 전자서명 된 정보를 한국전자인증에 제출하고 한국전자인증은 그 전자서명 된 정보를 가입자의 전자서명검증정보로 검증하는 과정을 통해서 가입자의 전자서명생성정보와 가입자의 전자서명검증정보가 합치하는가를 확인함으로써 가입자가 전자서명생성정보를 소유한다는

사실을 확인하고 공동인증서를 발급합니다.

3.2.3 가입자가 인증서 발급 신청서에 기재한 사항 중 전자서명인증사업자가 해당 내용의 정확성을 확인하는 사항

한국전자인증 또는 등록대행기관은 가입자가 인증서비스 신청서에 기재한 사항과 신원확인증표 및 제출된 추가서류 등을 통해 신청내용의 정확성을 확인합니다.

3.3 공동인증서 갱신 발급, 재발급 및 변경 시, 신원확인

3.3.1 갱신발급 신원확인 방법 및 절차

① 신원확인 방법 및 절차

공동인증서의 갱신여부는 보안 및 기타 상황을 감안하여 처리해야 하므로 등록대행기관을 통하지 않고 한국전자인증의 공동인증서 갱신화면을 통해서만이 신청이 가능하며, 가입자의 전자서명으로 신원확인을 대신합니다.

3.3.2 재발급 신원확인 방법 및 절차

① 신원확인 방법 및 절차

한국전자인증으로부터 공동인증서를 기 발급받은 가입자가 공동인증서의 재발급을 위하여 가입자의 유효한 전자서명생성정보로 전자 서명된 신청서를 정보통신망을 이용하여 신청하는 경우에는 전자서명 및 공동인증서에 의하여 가입자의 신원을 확인할 수 있습니다. 등록된 정보 및 전자서명을 전자서명검증정보로 검증하여 신원을 확인합니다. 단, 가입자의 공동인증서가 효력정지 상태인 경우에 신청한 사실은 인정되지 않습니다. 그 밖의 신원확인의 방법 및 절차는 본 인증업무준칙 3.2.1을 따릅니다.

3.3.3 변경 신원확인 방법 및 절차

① 신원확인 방법 및 절차

한국전자인증으로부터 공동인증서를 기 발급받은 가입자가 공동인증서의 변경을 위하여 가입자의 유효한 전자서명생성정보로 전자 서명된 신청서를 정보통신망을 이용하여 신청하는 경우에는 전자서명 및

공동인증서에 의하여 가입자의 신원을 확인할 수 있습니다. 등록된 정보 및 전자서명을 전자서명검증정보로 검증하여 신원을 확인합니다. 단, 가입자의 공동인증서가 효력정지 상태인 경우에 신청한 사실은 인정되지 않습니다. 그 밖의 신원확인의 방법 및 절차는 본 인증업무준칙 3.2.1을 따릅니다.

3.3.4 갱신발급, 재발급 및 변경 시 가입자의 전자서명생성정보 소유증명 방법

본 인증업무준칙 3.2.2을 준용합니다.

3.4 공동인증서 효력정지·효력회복·폐지 시, 신원확인

3.4.1 효력정지 신원확인 방법 및 절차

① 직접 방문하는 경우

한국전자인증 및 등록대행기관을 직접 방문하여 효력정지를 신청할 수 있습니다. 효력정지 신청은 본 인증업무준칙 3.2.1에 따라 신원확인을 수행하고 효력정지를 합니다.

② 온라인 등을 이용하는 경우

□ 한국전자인증의 홈페이지를 이용하는 경우

효력정지를 신청하고자 하는 가입자는 한국전자인증의 효력정지 신청화면에 온라인상으로 접속하여 효력정지를 신청하고 신원확인은 가입자의 유효한 인증서를 이용하여 생성된 전자서명검증으로 신원확인 후 효력정지를 합니다.

□ 한국전자인증의 고객센터를 이용하는 경우

만약 시스템에 접속할 상황이 되지 않거나 등록대행기관에 방문이 불가능한 경우 한국전자인증의 고객센터(전화: 1566-0566)로 효력정지 신청을 할 수 있습니다. 한국전자인증에서는 주민등록번호를 제외한 사전에 등록된 두 가지 이상의 개인정보를 확인 등, 신뢰할 수 있는 방법을 통하여 당해 가입자의 본인여부를 확인한 시점으로부터 최대 24시간 이내 효력정지를 처리합니다.

3.4.2 효력회복 신원확인 방법 및 절차

효력정지를 신청할 때와는 달리 효력정지 된 공동인증서는 효력이 정지된 상태이므로 공동인증서의 효력회복은 온라인 또는 유선상으로는 신청할 수 없으며 반드시 한국전자인증 및 등록대행기관을 방문하여 공동인증서 효력회복을 신청해야 합니다.

가입자가 등록대행기관 또는 한국전자인증을 방문하여 공동인증서의 효력회복에 대한 절차에 따라 효력회복 신청서를 제출하면 한국전자인증 및 등록대행기관은 본 인증업무준칙 3.2.1에 따라 신원확인 수행 후에 한국전자인증에 가입자의 공동인증서에 대한 효력회복을 시킵니다.

3.4.3 폐지 신원확인 방법 및 절차

① 직접 방문하는 경우

한국전자인증 및 등록대행기관을 직접 방문하여 폐지를 신청할 수 있습니다. 폐지 신청은 본 인증업무준칙 3.2.1에 따라 신원확인을 수행하고 폐지를 합니다.

② 온라인 등을 이용하는 경우

□ 한국전자인증의 홈페이지를 이용하는 경우

폐지를 신청하고자 하는 가입자는 한국전자인증의 폐지 신청화면에 온라인상으로 접속하여 폐지를 신청하고 신원확인은 가입자의 유효한 인증서를 이용하여 생성된 전자서명검증으로 신원확인 후 폐지를 합니다.

□ 한국전자인증의 고객센터를 이용하는 경우

만약 시스템에 접속할 상황이 되지 않거나 등록대행기관에 방문이 불가능한 경우 한국전자인증의 고객센터(전화: 1566-0566)로 폐지 신청을 할 수 있습니다. 한국전자인증에서는 주민등록번호를 제외한 사전에 등록된 두 가지 이상의 개인정보를 확인 등, 신뢰할 수 있는 방법을 통하여 당해 가입자의 본인여부를 확인한 시점으로부터 최대 24시간 이내 폐지를 처리합니다.

한국전자인증은 인증서 폐지 처리에 대해 가입자에게 SMS 또는 유선으로 고지합니다.

제4장 인증서 관리

4.1 공동인증서 발급 신청

4.1.1 공동인증서 발급 신청 주체 및 신청 절차

① 공동인증서 신청 주체는 법인/단체/개인사업자 또는 개인이며, 이 신청 주체가 직접 혹은 대리인을 통

하여 한국전자인증 또는 등록대행기관에 본 조의 공동인증서 발급 신청서류를 제출하여 신청합니다.

② 한국전자인증이 대면에 준하는 비대면의 방법으로 가입자의 신원을 확인할 경우 발급신청에 필요한 신청서는 온라인에서 작성된 전자문서의 형태로, 신청서 이외의 신원확인에 관한 서류는 본 인증업무준칙 3.2.1.5에서 정하는 방식으로 제출 받을 수 있습니다.

4.1.1.1 개인에 대한 신원확인

개인에 대한 신원확인의 경우 본 인증업무준칙 3.2.1.1에 따른 공동인증서 발급 신청 서류에 의해 제출된 제반 서류상의 성명과 주민등록번호의 확인뿐만 아니라 개인의 신원확인증표에 첨부된 사진 등에 의하여 본인 여부를 확인합니다. 다만, 당해 신청인이 제시한 신원확인증표의 사진에 의하여 본인여부의 식별이 곤란한 경우에는 다른 신원확인증표를 대체적으로 사용할 수 있습니다.

4.1.1.2 법인에 대한 신원확인

법인에 대한 신원확인의 경우 본인증업무준칙 3.2.1.2에 따른 공동인증서 발급 신청 서류에 의해 제출된 서류상의 명칭, 대표자 성명, 사업자등록번호 등에 의하여 진위여부를 확인하며, 당해 법인 또는 임의단체의 대표자에 대하여도 신원을 확인합니다. 다만, 대리인이 신청하는 경우 그 대리인으로부터 대표자의 위임장을 제출 받고 당해 대리인의 신원을 확인합니다.

4.1.1.3 찾아가는 서비스

① 공동인증서 신청 시 한국전자인증에서 제공하는 찾아가는 서비스를 이용하실 수 있습니다. 이 때 수수료는 별도의 협약에 따라 본 인증업무준칙 9.1의 수수료 이외에 추가로 부과할 수 있습니다.

② 찾아가는 서비스는 한국전자인증의 신원확인 절차와 보안교육을 이수한 담당자가 신청자를 방문하여 신규발급 절차와 같이 신원확인을 수행합니다. 가입자 서류는 개인정보보호를 위해 별도 분리하여 한국전자인증으로 이관됩니다. 이 때 신청자는 신원확인 수행자의 신분을 확인하기 위해 한국전자인증이나 등록대행기관에 신원확인을 요청할 수 있습니다. 한국전자인증은 이관된 서류가 신청정보와 동일한지 확인합니다.

4.1.1.4 방문발급 서비스

① 공동인증서 신청 시 한국전자인증에서 제공하는 방문발급 서비스를 이용하실 수 있습니다. 이 때 수수료는 별도의 협약에 따라 본 인증업무준칙 9.1의 수수료 이외에 추가로 부과할 수 있습니다.

② 방문발급 서비스는 한국전자인증의 신원확인 절차와 보안교육을 이수한 담당자가 신청자를 방문하여 신규발급 절차와 같이 신원확인을 수행합니다. 가입자 서류는 개인정보보호를 위해 별도 분리하여 한국전자인증으로 이관됩니다. 이 때 신청자는 신원확인 수행자의 신분을 확인하기 위해 한국전자인증이나 등록대행기관에 신원확인을 요청할 수 있습니다

4.1.1.5 온라인 신원확인

한국전자인증은「금융실명거래 및 비밀보장에 관한 법률」제2조제1호 각 목에 따른 금융기관에서 실지명의가 확인된 전자금융거래 가입자가 공동인증서를 발급받으려는 경우에는 그의 사전 동의를 받아 정보통신망을 통하여 신원을 확인한 가입자를 대상으로 온라인으로 비대면 신원확인 할 수 있으며, 사전 동의 받는 대상 고객, 업무, 신청 및 변경 방법은 아래와 같습니다.

- 대상고객: 개인 및 법인 가입자
- 대상업무: 공동인증서 발급 및 재발급
- 사전동의 신청 및 변경 방법: 온라인 신원확인 (단, 미동의에서 동의로 변경은 대면확인을 통해서만 가능합니다.)

이 경우는 아래 사항을 확인합니다.

① 전자금융거래 가입자의 계정(ID)과 그 비밀번호 또는 계좌번호와 그 비밀번호

② 전자금융거래 가입자의 주민등록번호

③ 금융기관이 전자금융거래를 위하여 가입자에게 제공한 일회용비밀번호(보안카드의 비밀번호를 포함한다) 또는 가입자 본인만이 알 수 있는 두 가지 이상의 정보

④ 제①호부터 제③호까지에서 규정된 사항 외에 전자금융거래 가입자의 신용카드 정보 등 신원을 확인할 수 있는 정보. 다만, 전자금융거래 가입자가 해외체류자, 법인, 단체, 외국인 또는 점자보안카드 사용자(해당 정보 확인에 동의한 점자보안카드 사용자는 제외한다)인 경우는 제외합니다.

4.2 공동인증서 발급 신청 처리

4.2.1 인증서 발급 신청 접수 및 처리 절차

한국전자인증 또는 등록대행기관은 공동인증서 발급 신청 정보 및 신청서류를 확인하고 가입 신청자의

신원확인을 마친 후 참조번호와 인가코드를 가입 신청자에게 전달합니다.

4.2.2 인증서 발급 신청에 대한 거절 기준

한국전자인증은 다음 각 호에 해당하는 가입 신청자에게는 인증서비스를 제공하지 않으므로 공동인증서 발급신청을 거부할 수 있습니다.

- 타인명의의 신청
- 가입신청서의 내용을 허위로 기재하였거나 허위서류를 첨부하여 가입신청을 하였을 경우
- 납부할 인증수수료를 인증업무준칙에서 정한 기간 내 납부하지 아니한 경우
- 제출된 서류만으로 신원확인이 곤란하거나 불가능한 경우
- 사고정보를 이용하여 발급 신청하였거나 사고정보로 의심되는 경우
- 기타 법령에 위반하거나 부당한 목적으로 공동인증서 발급을 신청한 경우

한국전자인증은 가입신청 후 공동인증서를 발급하기 이전에 위 사유를 발견한 경우에도 공동인증서 발급을 거부할 수 있습니다.

4.2.3 인증서 발급 신청 접수에 대한 처리 기간

공동인증서 발급신청 접수에 대한 처리기간은 가입신청자가 해당 수수료를 지급하고 신청서 및 구비서류를 제출 한 날부터 3일 이내를 원칙으로 합니다. 단 아래의 경우 발급 지연 시 가입자에게 고지하고 신청처리 기간을 조정할 수 있습니다.

- 가입신청자의 신원확인정보가 일치하지 않은 경우
- 신청서류의 진위여부를 확인할 수 없거나 식별이 어려운 경우
- 천재지변/국가재난 등의 경우

4.3 공동인증서 발급 절차 및 보호 조치

4.3.1 인증서 발급 절차

한국전자인증은 가입자가 등록대행기관으로부터 받은 참조번호와 인가코드를 수령한 후에 한국전자인증의 공동인증서 발급시스템에 접속하여 참조번호와 인가코드를 입력한 후 공동인증서 생성을 요청한 경우에 공동인증서를 발급합니다

4.3.2 가입자 정보의 전송방법 및 가입자 정보의 기밀성, 무결성 등에 대한 정보보안 방법

가입신청자 또는 그 대리인은 가입신청과 신원확인이 끝나면 한국전자인증의 전자인증센터 웹사이트에 접속하여 "가입자 인증서 관리 프로그램"을 다운로드 받거나 등록대행기관에서 제공한 동 프로그램을 이용하여 전자서명키를 생성하고 공동인증서 등록확인서에 기재된 주소를 이용하여 통보된 참조번호/인가코드를 입력하여 공동인증서 발급을 신청합니다. 상기 발급신청 과정 중 특정부분은 가입자의 사용자 소프트웨어에 의해 자동으로 처리될 수 있습니다.
한국전자인증은 등록대행기관으로부터 공동인증서를 발급받고자 하는 자의 등록정보를 정보통신망을 통하여 받는 경우, 가입자의 등록정보에 대해 암호화를 적용하여 가입자 정보의 기밀성, 무결성 등을 보장합니다.

한국전자인증이 중계서비스기관을 이용하는 경우 한국전자인증은 다음 각 호의 정보에 대하여 중계서비스기관으로 하여금 한국전자인증 및 등록대행기관이 처음 전송한 상태대로 전달하도록 하여야 합니다. 또한 중계서비스기관이 다음 각 호의 정보를 복호화하거나 보유하지 못하도록 하여야 합니다.

1. 가입자 이름, 식별번호, 주소 등 가입자의 등록정보
2. 한국전자인증이 생성한 참조번호 및 인가코드

한국전자인증은 공동인증서 신규 발급 시 다음 사항을 확인한 후 공동인증서를 발급합니다.

본 인증업무준칙의 공동인증서 신규발급 신청 시 신원확인 절차에 따른 공동인증서 신청자의 신원확인
공동인증서 가입신청자가 제출한 전자서명검증정보의 유일성 확인
공동인증서 가입신청자가 제출한 전자서명검증정보의 합치하는 전자서명생성정보의 소유여부 확인
공동인증서 가입신청자가 제출한 가입자 식별명(DN)의 유일성 확인
공동인증서 가입신청자가 제출한 가입자 식별명(DN)와 ID의 일치성 확인

신규로 발급된 공동인증서는 발급과 동시에 한국전자인증의 디렉토리에 등재됩니다.

4.4 공동인증서 수령

한국전자인증은 본 인증업무준칙에 따라 신청자에 대한 신원확인과 신청서류의 진정성을 확인한 후, 신청자에게 공동인증서 발급코드를 제공하며, 신청자는 한국전자인증의 인증시스템에 접속, 인증서비스 이용약관에 동의하고 해당 발급코드를 입력하여 공동인증서를 다운로드 받음으로써 공동인증서를 수령합니다.

4.5 공동인증서 이용

한국전자인증이 발급한 인증서는 전자거래 등의 업무에 사용할 수 있습니다. 앞의 전자거래 등의 업무의 인증서 사용은 정당한 권한을 가진 가입자가 인증서의 이용범위, 발급 용도 및 유효기간에 맞게 인증서를 사용하는 것을 말합니다. 그러하지 아니한 경우 한국전자인증은 인증서의 사용을 제한할 수 있습니다.

4.6 공동인증서 갱신발급

4.6.1 갱신발급 요건, 신청주체 및 신청절차

① 요건

가입자는 기존에 사용하던 공동인증서의 유효기간이 만료되기 60일 전부터 기존 공동인증서의 전자서명키 쌍(생성키/검증키)과 동일한 종류의 새로운 공동인증서 갱신발급을 신청할 수 있습니다. 갱신 발급된 공동인증서는 갱신발급 시점부터 효력이 발생하여 기존 공동인증서 만료시각 이후로부터 1년 또는 공동인증서의 종류에 따라 3년이내 유효기간만큼 연장됩니다.. 기존 발급된 인증서는 갱신시점에 자동 폐지됩니다.

② 신청주체 및 신청절차

가입자가 온라인상으로 공동인증서 갱신신청을 하면 한국전자인증은 갱신여부를 검토한 후 갱신이 허용되면 새로운 유효기간의 공동인증서를 새로 발급합니다.

만약 가입자가 공동인증서에 포함된 내용을 변경하고자 하려면 공동인증서 갱신이 아닌 공동인증서 재발급 신청을 통하여 새로운 공동인증서를 발급 받아야 합니다.

4.6.2 가입자가 갱신 발급된 공동인증서를 수령하는 방법

가입자가 온라인상으로 공동인증서 갱신신청을 하면 한국전자인증은 갱신여부를 검토한 후 갱신이 허용

되면 새로운 유효기간의 공동인증서를 새로 발급함으로써 가입자는 갱신 발급된 공동인증서를 수령합니다. 이때 가입자의 신원확인은 가입자의 전자서명으로 대체할 수 있습니다.

4.7 공동인증서 재발급

4.7.1 재발급 요건, 신청주체 및 발급절차

① 요건

가입자가 현재 이용중인 공동인증서의 안전성 등의 문제로 새로운 공동인증서를 신청해야 할 필요가 있을 경우에 기존의 공동인증서를 폐지하고 새로운 공동인증서를 발급 신청할 수 있습니다.

② 신청주체 및 신청절차

가입자가 등록대행기관 또는 한국전자인증을 방문하거나 온라인 또는 비대면 방식을 통하여 공동인증서의 재발급에 대한 절차에 따라 재발급 신청서류를 제출하면 등록대행기관 및 한국전자인증은 신원확인 절차를 수행한 후에 공동인증서를 재발급합니다.

공동인증서가 재발급되면 기존의 공동인증서는 자동적으로 폐지되며 신규로 재발급된 공동인증서의 유효기간은 기존 공동인증서의 최초 발급 시 설정된 유효기간 중 사용기간일수를 공제한 잔여기간으로 설정되며 유효 만료 기일은 변동이 없습니다. 이때 새로운 전자서명검증정보를 이용하여 공동인증서를 생성하여 가입자에게 발급합니다.

4.7.2 가입자가 재발급된 공동인증서를 수령하는 방법

본 인증업무준칙 4.4를 준용합니다.

4.8 공동인증서 변경

4.8.1 가입자 정보가 변경된 인증서 발급 요건, 신청주체 및 신청절차

① 요건

한국전자인증은 가입자가 공동인증서의 상호 변경 등 공동인증서에 포함된 정보변경으로 새로운 공동인

증서를 신청해야 할 필요가 있을 경우에 기존의 공동인증서를 폐지하고 새로운 공동인증서를 발급 신청할 수 있습니다.

② 신청주체 및 신청절차

가입자가 등록대행기관 또는 한국전자인증을 방문하거나 온라인 또는 비대면 방식을 통하여 공동인증서의 정보변경에 대한 절차에 따라 정보변경 신청서류를 제출하면 등록대행기관 및 한국전자인증은 신원확인 절차를 수행한 후에 새로운 공동인증서를 발급합니다.

새로운 공동인증서가 발급되면 기존의 공동인증서는 자동적으로 폐지되며 새로운 공동인증서의 유효기간은 기존 공동인증서의 최초 발급 시 설정된 유효기간 중 사용기간일수를 공제한 잔여기간으로 설정되며 유효 만료 기일은 변동이 없습니다. 이때 새로운 전자서명검증정보를 이용하여 공동인증서를 생성하여 가입자에게 발급합니다.

4.8.2 가입자가 정보가 변경된 공동인증서를 수령하는 방법

본 인증업무준칙 4.4를 준용합니다.

4.9 공동인증서 효력정지·효력회복·폐지

4.9.1 신청요건, 신청주체 및 신청절차

4.9.1.1 공동인증서 효력정지 요건 및 신청주체

- 한국전자인증은 가입자가 공동인증서의 효력정지를 원하는 경우에 가입자 또는 대리인의 신청에 의해 공동인증서의 효력을 정지시킵니다.
- 한국전자인증은 가입자 공동인증서의 전자서명생성정보가 분실훼손 또는 도난·유출 등을 인지하여 공동인증서의 안전성과 신뢰성을 확보할 수 없고 가입자의 효력정지 신청이 불가능한 경우 해당 공동인증서의 효력을 정지할 수 있습니다.

4.9.1.2 공동인증서 효력정지 신청절차

① 직접 방문하는 경우

한국전자인증 및 등록대행기관을 직접 방문하여 효력정지를 신청할 수 있습니다.

② 온라인 등을 이용하는 경우

□ 한국전자인증의 홈페이지를 이용하는 경우

효력정지를 신청하고자 하는 가입자는 한국전자인증의 효력정지 신청화면에 온라인상으로 접속하여 효력정지를 신청할 수 있습니다.

□ 한국전자인증의 고객센터를 이용하는 경우

만약 시스템에 접속할 상황이 되지 않거나 등록대행기관에 방문이 불가능한 경우 한국전자인증의 고객센터(전화: 1566-0566)로 효력정지 신청을 할 수 있습니다.

4.9.1.3 공동인증서 효력회복 요건, 신청주체 및 신청절차

가입자가 공동인증서의 효력정지 신청을 하여 공동인증서의 효력이 정지된 날로부터 6개월 이내에 공동인증서의 효력을 회복하기 위해 효력회복을 할 경우 해당 공동인증서에 대한 효력을 회복합니다. 이때, 효력회복 공동인증서의 유효기간은 변하지 않습니다.

효력정지를 신청할 때와는 달리 효력정지 된 공동인증서는 효력이 정지된 상태이므로 공동인증서의 효력회복은 온라인 또는 유선상으로는 신청할 수 없으며 반드시 한국전자인증 및 등록대행기관을 방문하여 공동인증서 효력회복을 신청해야 합니다.

4.9.1.4 공동인증서 폐지 요건 및 신청주체

가입자는 공동인증서를 폐지할 권리가 있으며, 일단 폐지된 공동인증서는 다시 효력을 회복할 수 없습니다. 한국전자인증은 다음의 사유가 발생한 경우 해당 공동인증서를 폐지할 수 있습니다.

- 가입자 또는 그 대리인이 공동인증서 폐지를 신청한 경우
- 가입자가 사기 기타 부정한 방법으로 공동인증서를 발급받은 사실을 인지한 경우
- 가입자의 공동인증서가 사고정보를 이용하여 발급된 사실을 인지한 경우
- 가입자의 사망·실종선고 또는 해산사실을 인지한 경우
- 가입자의 전자서명생성정보가 분실훼손 또는 도난·유출된 사실을 인지한 경우
- 본 인증업무준칙 4.9.1의 규정에 따라 효력이 정지된 공동인증서에 대한 효력회복신청이 공동인증서의 효력이 정지된 날로부터 6개월 이내에 없는 경우

❑ 한국전자인증의 전자서명생성정보가 유출된 경우

4.9.1.5 공동인증서 폐지 신청절차

① 직접 방문하는 경우

한국전자인증 및 등록대행기관을 직접 방문하여 폐지를 신청할 수 있습니다.

② 온라인 등을 이용하는 경우

□ 한국전자인증의 홈페이지를 이용하는 경우

폐지를 신청하고자 하는 가입자는 한국전자인증의 폐지 신청화면에 온라인상으로 접속하여 폐지를 신청할 수 있습니다.

□ 한국전자인증의 고객센터를 이용하는 경우

만약 시스템에 접속할 상황이 되지 않거나 등록대행기관에 방문이 불가능한 경우 한국전자인증의 고객센터(전화: 1566-0566)로 폐지 신청을 할 수 있습니다.

4.9.2 가입자 정보의 전송방법 및 가입자 정보의 기밀성, 무결성 등에 대한 정보보안 방법

본 인증업무준칙 4.4를 준용합니다.

4.9.3 신청접수부터 해당 인증서 효력정지·효력회복 또는 폐지까지 소요되는 처리시간

공동인증서 효력정지, 효력회복, 폐지 신청 접수에 대한 처리는 최대 24시간 이내 처리 합니다. 단, 아래의 경우 가입자에게 고지하고 신청처리 기간을 조정할 수 있습니다.

- 가입자의 신원확인정보가 일치하지 않은 경우
- 천재지변/국가재난 등의 경우

4.9.4 공동인증서 효력정지 및 폐지목록(CRL) 발행 주기

한국전자인증은 공동인증서 효력정지, 공동인증서 폐지목록 등 인증서비스에 관련된 정보에 대한 변경이 생기는 경우에는 이를 신속하게 공고하여야 합니다. 공동인증서 효력정지, 공동인증서 폐지목록은 매일 1회 최대 24시간 단위로 정기적으로 갱신한 후 인증관리체계에 의하여 누구든지 그 사실을 항상 확인할 수

있도록 공고합니다.

4.9.5 공동인증서 효력정지 및 폐지목록(CRL) 발행 시점부터 해당 인증서 효력정지 및 폐지목록을 공고하는데 까지 소요 시간

한국전자인증은 공동인증서 효력정지 및 폐지목록(CRL) 발행 시점부터 해당 공동인증서 효력정지 및 폐지목록(CRL)을 1시간 이내 공고합니다.

4.9.6 공동인증서 효력정지 상태 유지 가능 기간

일단 효력정지 신청이 되어 효력정지가 된 공동인증서는 효력정지 후 6개월 까지만 유지할 수 있으며 6개월 이내에 효력회복 신청이 접수되지 않을 경우에는 효력정지된 해당 공동인증서는 자동으로 폐지가 됩니다. 단, 효력정지 기간 중에 유효기간이 만료되는 경우에는 일반 공동인증서의 유효기간 만료와 동일하게 간주됩니다.

4.10 공동인증서 유효성 확인 서비스(OCSP)

4.10.1 공동인증서 유효성 확인 서비스 이용 방법, 이용 조건

한국전자인증이 제공하는 공동인증서 유효성 확인 서비스는 이용자가 실시간으로 공동인증서 폐지 및 효력정지 상태를 검증할 수 있게 하는 서비스를 의미합니다.

한국전자인증의 유효성확인 서비스 신청자 또는 그 대리인은 전자서명사업자의 인증서비스에 가입하고 등록대행기관 또는 한국전자인증에 유효성 확인서비스 등록신청서를 제출하여야 합니다.

한국전자인증의 유효성확인 서비스 가입자는 등록대행기관 또는 한국전자인증에서 제공받은 유효성확인 소프트웨어 또는 자신이 보유하고 있는 소프트웨어를 이용하여 자신의 공동인증서에 대한 유효성확인을 요청합니다.

한국전자인증은 이용자가 원하는 공동인증서 상태 조회 요청이 있을 경우 해당 공동인증서의 상태 정보를 이용자에게 응답하여 줍니다.

4.10.2 공동인증서 유효성 확인 서비스 이용계약 해지

가입자가 유효성 확인 서비스를 해지하고자 하는 경우에는 한국전자인증에 해지신청서를 제출하고 해지를 신청합니다. 해지신청서를 접수한 후, 한국전자인증은 유효성 확인서비스 이용 계약에 따라 신속하게 해당 서비스 이용계약을 해지하고 신청자에게 통보 합니다. 단, 유효성 확인 서비스 계약의 해지는 해지 이전에 발생한 권리의무관계로 인해 발생한 손해배상의 청구에 영향을 미치지 아니합니다.

4.11 서비스 가입 철회

가입자는 서비스 철회를 원할 경우 인증서를 폐지함으로써 서비스 이용을 중단할 수 있습니다. 가입자 개인정보는 본 인증업무준칙의 "5.5 기록 보존"을 준용하며, 한국전자인증의 개인정보처리방침에 따라 파기합니다.

4.12 기타 부가 서비스

4.12.1 시점 확인 서비스 이용 방법

한국전자인증이 시점확인 서비스 이용자에게 제공하는 시점확인 토큰은 해당 데이터가 특정 시간에 존재했음을 증명하는데 사용됩니다.

한국전자인증의 시점확인 서비스 신청자 또는 그 대리인은 한국전자인증의 인증서비스에 가입하고 등록대행기관 또는 한국전자인증에 시점확인서비스 등록신청서를 제출하여야 합니다. 등록절차 후 등록대행기관 또는 한국전자인증은 시점 확인용 계정이 포함된 시점확인 서비스 등록확인서를 신청자 또는 그 대리인에게 교부합니다.

한국전자인증의 시점확인 서비스 가입자는 등록대행기관 또는 한국전자인증에서 제공받은 시점확인 소프트웨어 또는 자신이 보유하고 있는 소프트웨어를 이용하여 자신의 시점확인 계정을 확인 받은 후 해당 데이터에 대한 시점확인 토큰을 요청합니다.

한국전자인증은 시점확인토큰 요청이 접수되면 요청자를 확인하고 요청정보의 유효성을 확인한 후 해당 요청 데이터에 대한 시점확인 토큰을 발행합니다. 한국전자인증은 시점확인토큰 요청에 대하여 1분 이내 응답이 불가능할 경우 서비스 제공이 불가능하다는 오류메시지로 응답합니다.

한국전자인증은 시점확인토큰 요청에 대하여 다음의 사항을 포함한 시점확인 응답 정보를 요청자에게 제공합니다.

- 시점확인기관의 명칭
- 시점확인토큰의 일련번호
- 시점확인기관의 정책
- 시점확인토큰 발급시간
- 해시값
- 해시 알고리즘
- 시점확인기관의 공동인증서 정보
- 시점확인기관의 서명
- 기타 시점확인 서비스를 위하여 필요한 정보

시점확인 서비스 가입자는 시점확인토큰 요청 시 다음의 사항을 포함한 정보를 정보통신망을 통하여 한국전자인증에 제출하여야 합니다.

- 해시값
- 해시 알고리즘
- 기타 시점확인 서비스를 위하여 필요한 정보

4.12.2 시점 확인 서비스 이용계약 해지

가입자가 시점 확인 서비스를 해지하고자 하는 경우에는 한국전자인증에 해지신청서를 제출하고 해지를 신청합니다. 해지신청서를 접수한 후, 한국전자인증은 시점 확인서비스 이용 계약에 따라 신속하게 해당 서비스 이용계약을 해지하고 신청자에게 통보합니다. 단, 시점 확인 서비스 계약의 해지는 해지 이전에 발생한 권리의무관계로 인해 발생하는 손해배상의 청구에 영향을 미치지 아니합니다.

제5장 시설 및 운영 관리

한국전자인증은 인증업무에 관한 시설의 안전성 확보를 위하여 다음과 같은 보호조치를 준수합니다.

5.1 물리적 보호조치

5.1.1 시설 위치와 구조에 관한 사항

한국전자인증은 핵심인증시스템을 보호하기 위하여 핵심인증시스템 별로 분리된 별도의 통제구역 내에 핵심인증시스템을 설치 운영합니다.

5.1.2 물리적 보호조치에 관한 사항

한국전자인증은 외부로부터의 침입이나 불법적 접근시도 등의 물리적 위협으로부터 핵심인증시스템 등이 설치된 장소를 보호하기 위하여 다음과 같은 물리적 접근 통제를 수행합니다.

- 한국전자인증 인증센터는 권한 있는 자만이 출입이 허가됩니다.
- 한국전자인증의 출입통제 시스템은 소지기반/생체기반의 출입통제장치를 다중으로 결합하여 핵심인증시스템 및 통제구역에 대한 접근을 통제합니다.
- 한국전자인증은 특별한 경우(하드웨어 보수 등의 업무수행)를 제외하고는 외부인의 출입을 삼가며 하드웨어 보수 등의 이유로 통제구역 내에 외부인의 출입이 필요할 경우는 반드시 담당관리자가 동행하도록 합니다.
- 한국전자인증은 24시간 출입통제를 감시 및 통제하며 인증센터 내에 출입하는 모든 인원에 대하여 출입내역을 기록하고 주기적으로 출입기록을 백업장치에 저장하고 이를 안전한 장소에 보관합니다.
- 한국전자인증은 24시간 감지가 가능한 보안·감시 장치를 설치 운영하며, 침입감지 및 이상 상황 발생 시 경보 기능을 갖는 감시통제시스템을 설치·운영합니다.
  - 출입구 및 인증센터의 모든 주요 장소에 CCTV 카메라 설치
  - 24시간 감시가 가능한 관제시스템 설치·운영
  - 외부로부터의 불법적인 침입에 대비하여 인증센터 전체를 포함하는 침입감지 장치 설치
- 한국전자인증은 인가된 보안경비업체와 계약하여 24시간 보안체제를 운영합니다.

5.1.3 물리적 잠금장치에 관한 사항

한국전자인증은 시스템 보호 및 물리적 접근통제를 위하여 보안캐비닛 내에 핵심인증시스템을 설치 운영합니다.

5.1.4 화재, 수재, 정전 방지 및 방호에 관한 사항

한국전자인증은 수해발생 시 핵심인증시스템 및 중요장비가 물에 노출되지 않도록 지상으로부터 12㎝ 이상 높은 곳에 설치하였습니다.

한국전자인증은 핵심인증시스템실 및 인증센터 내에 연기감지장치, 온도감지장치 등의 화재경보장치를 설치하였으며 핵심인증시스템실 등에 휴대용 소화기 및 자동소화설비를 설치 운영합니다. 또한 소화 시에 시스템에 악영향을 미치지 않는 소화설비를 설치합니다.

한국전자인증은 정전 발생시 지속적인 인증업무의 수행이 가능하도록 일정시간 전원을 공급해줄 수 있는 무정전 전원공급장치 및 자가발전설비를 사용하며 무정전 전원장치의 사용시 예비전력이 모두 소모되어 더 이상 서비스가 불가능 할 경우 안전하게 시스템을 전원차단(shut-down)하여 시스템의 심각한 피해를 최소화 시킵니다.

5.1.5 항온·항습, 통풍 및 기타 보호설비에 관한 사항

한국전자인증 핵심인증시스템 및 중요 장비가 습기에 노출되지 않도록 하기 위하여 통풍, 항온·항습장치를 설치·운영합니다.

5.1.6 시설 및 장비의 폐기처리 절차에 관한 사항

한국전자인증은 인증서비스와 관련된 문서, 디스켓, 저장매체 등을 폐기하는 경우 3인 이상의 공동 참여하에 원상복구가 불가능하도록 물리적으로 이를 파기하며, 인증서비스와 관련된 시설 및 장비를 폐기하는 경우 그 내용을 관리 대장에 기록하고 관리자의 승인을 득하여 폐기합니다.

5.1.7 원격지 백업설비 안전운영에 관한 사항

한국전자인증은 전자서명인증사업자 인증서, 인증서비스를 제공하는데 사용되는 중요한 저장매체, 가입자 공동인증서, 공동인증서 효력정지 및 폐지목록 등을 화재, 홍수로부터 안전하게 보호하기 위하여 주기적으로 백업하여 원격지 저장 설비에 5년간 보관하며 공동인증서 효력정지 및 폐지목록 등은 공동인증서의 효력이 소멸된 날로부터 5년간 보관합니다.
원격지 저장 설비를 보호하기 위하여 다음과 같은 물리적 보호조치를 수행합니다.

- 소지기반/생체기반의 출입통제장치를 설치·운영합니다.
- 특별한 경우(하드웨어 보수 등의 업무수행)를 제외하고는 외부인의 출입을 삼가며 하드웨어 보수 등의 이유로 원격지 백업설비 구역 내에 외부인의 출입이 필요할 경우는 반드시 담당관리자가 동행하도록 합니다.
- 24시간 감지가 가능한 보안 감시 CCTV 카메라 설치를 설치 운영하며, 침입감지 및 이상 상황 발생시 경보 기능을 갖는 감시통제시스템을 설치·운영합니다
- 수해발생 시 백업 설비 및 중요장비가 물에 노출되지 않도록 지상으로부터 12㎝이상 높은 곳에 설치하고 습기에 노출되지 않도록 하기 위하여 통풍, 항온·항습 장치를 설치·운영합니다.
- 화재 방지 및 방호를 위해 원격지 백업설비 구역내에 연기감지장치, 온도감지장치 등의 화재경보장치와 휴대용 소화기 및 자동소화설비를 설치·운영합니다.
- 정전 발생시 지속적인 인증업무의 수행이 가능하도록 일정시간 전원을 공급해줄 수 있는 무정전 전원공급장치 및 자가발전설비를 사용하며 무정전 전원장치의 사용시 예비전력이 모두 소모되어 더 이상 서비스가 불가능 할 경우 안전하게 시스템을 전원차단(shut-down)하여 시스템의 심각한 피해를 최소화 시킵니다.

5.2 절차적 보호조치

5.2.1 전자서명인증업무 수행을 위해 필요한 업무의 종류와 그 업무 분장에 관한 사항

한국전자인증의 인증업무에 대한 업무분장과 담당자 배치 현황은 다음과 같습니다.

<전자서명인증업무에 대한 업무분장 및 담당자>

인증업무	소속 (담당자)	인원
전자서명인증업무 총괄	공동인증사업본부 (본부장)	1명
인증센터 운영관리	데이터센터 총괄팀 (팀장)	1명

전자서명인증사업자 전자서명키 생성 및 공동인증서 생성시스템 정책관리	전자인증사업팀 (팀장), ISLAB팀 (팀장) 글로벌마케팅팀 (팀장)	3명
인증센터 보안 및 감사관리 침입 차단/탐지 시스템 감사관리 출입통제 시스템 감사관리 인증센터 열쇠 관리 전자서명키 생성 감사관리 시점확인시스템 감사관리	SM본부 (관리자)	1명
공동인증서 생성시스템 운영관리 디렉토리 시스템 업무운영관리 OCSP 시스템 운영관리 시점확인시스템 업무운영관리 등록관리시스템 업무운영관리 웹서버 운영관리 침입 차단/탐지 시스템 운영관리 출입통제 시스템 운영관리 기타 인증서비스와 관련된 시스템운영관리	데이터센터 총괄팀 (운영관리자)	6명
인증센터 감사 관리 금고비밀번호 관리 금고키 관리	SM본부 (관리자)	1명
공동인증서 분실신고접수 고객지원	전자인증서비스팀 (팀장)	1명

5.2.2 동일인에 의해 동시 수행될 수 없는 전자서명인증업무

한국전자인증은 다음의 업무가 동일인에 의해 동시 수행되지 않도록 하여야 합니다.

- 한국전자인증이 자신의 전자서명키를 생성하는 경우 (3인 이상)

- 한국전자인증이 공동인증서를 발급받고자 하는 자의 전자서명키를 생성하는 경우 (2인 이상)
- 한국전자인증이 다음 각호의 시스템을 설치, 운영 및 유지, 보수하는 경우 (2인 이상)
- 가입자의 등록정보관리 기능을 지원하는 시스템
- 공동인증서 생성, 발급, 관리 기능을 지원하는 시스템
- 시점확인 기능을 지원하는 시스템

5.2.3 업무 담당자 현황 및 담당자 인증방법

한국전자인증은 내부의 전자서명인증업무 담당자들에 대하여 개인 ID 카드, 지문, 패스워드를 통한 인증방법으로 전자서명인증업무 담당자를 확인합니다.

5.3 인적 보안

5.3.1 전자서명인증업무 수행 인력의 자격, 경력 등 요구사항 및 요건 충족 여부 확인 등 신원확인 절차

한국전자인증은 인증센터의 출입 및 인증시스템의 접근, 인증서비스 관련 업무를 운영·취급하는 모든 임직원에 대하여 철저하게 신원을 조회하며 인가된 임직원만이 인증 및 보안 관련 업무를 수행할 수 있도록 합니다.

5.3.2 업무 수행 인력의 교육 및 업무순환에 관한 사항

한국전자인증은 인증서비스의 안전한 운영을 위하여 인증업무를 각 시스템 및 기능별로 서로 다른 직원이 수행하도록 역할을 본 인증업무준칙 5.2.1에 따라 분리하여 수행하고 있으며, 한 직원이 여러 가지 인증업무를 수행할 경우 인증서비스 보안상 문제가 없도록 업무순환 하고 있습니다.

한국전자인증은 업무 수행 인력에 대해 년 1회 이상 정보보호 교육을 이수하도록 하고 있습니다.

5.3.3 비인가된 행위에 대한 처벌에 관한 사항

한국전자인증은 내부 인증업무를 수행하는 자가 전자서명법규 및 본 인증업무준칙에 인가되지 아니한 행위를 한 경우에는 법 제24조(벌칙) 및 정보통신기반보호법의 벌칙규정에 따라 처벌되도록 합니다. 이와 별도로, 한국전자인증은 해당 위반자에 대하여 사규에 따라 처벌합니다.

5.4 감사 기록

5.4.1 감사기록의 유형 및 보존기간

한국전자인증은 핵심인증시스템에서 발생한 다음 종류의 사실(또는 사건)과 결부된 시각(時刻) 및 행위자들에 대한 내역 등 세부내용을 감사기록 파일에 기록, 저장하여 둡니다.

- 가입자 등록정보를 입력·접근·변경·삭제한 사실
- 가입자 공동인증서 등을 등록 및 관리한 사실
- 계정의 추가 및 삭제 사실
- 로그인(Log-in) 및 로그오프(Log-off) 한 사실
- 이용자 권한 변경 사실
- 공동인증서를 생성·발급·갱신·효력정지 또는 폐지한 사실
- 전자서명키를 생성·접근·파기한 사실
- 전자문서를 시점 확인한 사실
- 핵심인증시스템의 시동/정지한 사실
- 기타 핵심인증시스템 관리자의 주요 활동 사실

한국전자인증은 전자서명인증업무 운영과 관련된 기록 및 인증시스템에서 생성되는 기록의 이상유무를 확인합니다.

5.4.2 감사기록 보호조치 및 감사기록 백업주기 및 절차

한국전자인증의 감사관지라는 인증시스템의 감사기록을 검토하고 본 인증업무준칙 5.5상의 보존기록 조항에 의거하여 보존합니다.
각 시스템의 감사기록에 대한 총괄관리는 감사관리자가 실행하며 시스템의 각 업무관리자는 각자의 업무에 대한 감사기록만을 열람할 수 있습니다.

5.5 기록 보존

5.5.1 보존되는 기록의 유형 및 보존기간

한국전자인증은 핵심인증업무를 수행함에 있어 다음 사항을 준수합니다.

- 가입자 및 이용자가 공동인증서 취득 시 제출한 기본 정보
- 물리적 및 절차적 통제에 따른 통제 내역
- 공동인증서 발급부터 폐지 및 효력정지/회복에 이르기까지의 제반 인증업무에 관한 사항
- 핵심인증시스템 운영상의 각종 감사기록 및 운영자의 운영 내역
- 기타 한국전자인증이 기록할 필요성이 있다는 판단 하에 결정된 정책 사항

본 조의 기록보존 대상은 정기적 원본의 분류 및 복사본 보관 등 2중 보관을 통해 당해 공동인증서의 효력이 소멸한 날로부터 5년 동안 보존하는 것을 원칙으로 합니다.

5.5.2 보존기록의 보호조치

한국전자인증은 보존기록에 대해 물리적 및 절차적, 인적 통제를 통해 보안을 유지하고 조회가 필요할 경우 인적 통제를 통한 인가된 관리자 업무범위에 한정시키며 시건 장치가 구비된 캐비닛에 보관하여 보존기록의 위·변조 및 훼손을 방지하도록 보호합니다.

5.5.3 보존기록의 백업주기 및 백업절차

한국전자인증은 천재지변 및 기타 재난 발생시 보존기록의 손실 및 파괴에 대비하여 원격지 저장설비에 백업 저장 합니다.

5.6 전자서명인증사업자의 전자서명생성정보 갱신

한국전자인증은 새로운 한국전자인증의 공동인증서가 발급되면 새로 갱신된 전자서명생성정보는 공동인증서 공고 설비(LDAP: Lightweight Directory Access Protocol) 를 통해 게시하고 가입자와 이용자에게 이를 공지하여 필요한 조치를 취합니다. 가입자는 한국전자인증의 갱신된 전자서명생성정보를 발급/재발급/갱신 시 가입자 소프트웨어를 통해 자동으로 배포 받습니다. 이용자는 전자서명검증 요청 시 LDAP을 통해 받을 수 있습니다.

5.7 장애 및 재난 복구

5.7.1 전자서명인증업무 장애 및 재해 유형별 처리 및 복구 절차

한국전자인증은 시스템 자원 및 소프트웨어 등에 장애 및 손실이 발생한 경우에 2중으로 설치한 시스템 자원 및 소프트웨어를 이용하여 신속하게 복구합니다.

한국전자인증은 가입자 공동인증서 등의 주요 데이터에 훼손·멸실이 발생하였을 경우 백업 저장해둔 보존기록을 이용하여 신속히 복구합니다.

보안사고 발생시 인증업무 각 시스템 운영인력은 지체 없이 침입탐지시스템의 자동경보기능 등을 이용하여 담당업무 관리자에 통보해야만 합니다.

5.7.2 전자서명인증업무 장애방지 등 연속성 보장 대책

한국전자인증은 안정적인 인증서비스 제공에 노력합니다.

한국전자인증은 시스템운영 환경의 변화에 따라 효율적인 보안통제수단을 모색하기 위하여 년1회 외부기관을 통해 취약성 평가를 실시하며 매년 ISMS 인증심사 등을 통해 취약점을 개선하고 있습니다.

한국전자인증은 감사기록, 인증서비스 관련 자료, 가입자 공동인증서 등을 백업장치에 주기적으로 저장하며 물리적으로 접근통제가 가능한 금고에 보관합니다.

5.8 업무 휴지, 폐지, 종료

한국전자인증의 사정으로 인하여 인증서비스의 전부 또는 일부를 휴지 또는 폐지하고자 하는 경우에 한국전자인증은 휴지기간 및 휴지일과 폐지일을 정하고 휴지는 휴지하고자 하는 날 30일 전까지, 폐지는 폐지하고자 하는 날 60일 전까지 법 제15조(전자서명인증업무준칙의 준수 등) 규정에 따라 가입자에게 해당 사실을 통보합니다.

제6장 기술적 보호 조치

6.1 전자서명생성정보 보호

전자서명키 생성시스템은 내부 및 외부의 정보통신망과 연결되지 아니하며 독립적으로 운영됩니다. 전자서명키 생성시스템은 물리적 침해로부터 보호되며 권한 있는 자만이 전자서명키 생성시스템에 접근하여 전자서명키쌍 및 공동인증서 요청양식을 생성할 수 있도록 다중출입통제 장치를 설치하여 운영합니다.

한국전자인증은 안전성이 확인되고 신뢰성 있는 전자서명 알고리즘을 사용하기 위하여 2048비트 이상의 키 크기를 갖는 RSA 알고리즘을 이용하여 전자서명키를 생성하며, 해시값을 생성하기 위하여 SHA-256 해시 알고리즘을 사용합니다.

6.2 전자서명생성정보 보호 조치

한국전자인증은 전자서명키 생성시스템에서 생성된 전자서명 생성키를 안전하게 저장 및 관리하기 위하여 전자서명생성정보를 봉인, 접근권한 확인 및 전자서명생성정보 유출·변경 방지 기능을 갖춘 저장장치에 암호화하여 저장합니다.

전자서명키 생성시스템은 전자서명생성정보를 생성하여 전자서명생성정보 저장장치에 저장한 후 전자서명키를 시스템의 메모리로부터 즉시 삭제하며 시스템을 재부팅 합니다.

한국전자인증은 전자서명인증사업자용 전자서명생성정보를 해당 인증서가 유효한 동안에만 사용하며, 인증서의 유효기간이 만료되거나 전자서명생성정보가 훼손·유출되었을 경우에 해당 전자서명생성정보가 저장되어 있는 저장매체를 원상복구가 불가능하도록 3인 이상의 공동참여 하에 물리적, 논리적으로 완전히 파기합니다.

6.3 전자서명생성정보 및 전자서명검증정보의 관리

한국전자인증은 전자서명생성정보의 분실·훼손·도난·유출 방지를 위하여 내부 및 외부의 정보통신망과 연결되지 아니하고, 전자서명키 생성시스템은 물리적 침해로부터 보호되며 권한 있는 자만이 전자서명생성정보를 생성하여 보관할 수 있도록 합니다.

6.4 데이터 보호 조치

전자서명생성정보의 유출 방지를 위하여 전자서명키 생성시스템은 전자서명생성정보를 생성하여 전자서명생성정보 저장장치에 저장한 후 전자서명키를 시스템의 메모리로부터 즉시 삭제하며 시스템을 재부팅 합니다.

6.5 시스템 보안 통제

한국전자인증은 핵심인증시스템 및 인증서비스 운영과 관련된 주요 시스템을 이중 구성하였으며 주 시스템에 문제가 발생하여 인증서비스가 불가능할 경우에 보조 시스템을 이용하여 인증서비스가 가능하도록 이중화되어 있습니다.

6.6 시스템 운영 관리

한국전자인증은 다음 각호의 시설 및 장비에 대하여 형상관리를 하여야 합니다.

- 인증시스템 및 가입자 소프트웨어
- 네트워크 구성 및 장비
- 네트워크안전운영시스템 및 서버관리 시스템
- 출입통제 관련 시스템
- 기타 운영시스템

한국전자인증은 가입자 소프트웨어 배포 시 당해 소프트웨어에 대하여 무결성을 보장할 수 있는 전자서명 또는 해시값 등을 관리하여야 합니다.

6.7 네트워크 보호조치

한국전자인증은 내/외부의 네트워크를 통한 불법적인 침입 및 정보유출을 방지하기 위하여 한국인터넷진흥원으로부터 CC등급의 평가필증을 받은 침입차단시스템을 사용하며 서비스 방해 공격을 방지하고 인증서생성관리시스템, OCSP시스템, 디렉토리 시스템, 시점확인시스템 (이하 "핵심인증시스템"이라 한다) 등 모든 핵심인증시스템 및 인증운영관련시스템에 대한 침입을 탐지하기 위하여 침입탐지 시스템을 설치·운영합니다. 구성된 네트워크 회선은 서로 다른 ISP(Internet Service Provider)로부터 제공되도록 이중화하

여 구성하였으며 하나의 네트워크 회선에 문제가 발생할 경우 다른 회선으로 자동 전환되도록 구성합니다.

6.8 시점확인서비스 보호조치

① 시각(時刻)원천

한국전자인증은 시점확인 서비스를 위하여 원자시계와 위성수신장치 등을 이용한 안전하고 신뢰할 수 있는 시각원천을 이용하며 지속적인 시각보정 기능을 사용합니다.

② 시스템 이중화

한국전자인증은 지속적인 부가서비스를 제공하기 위하여 동일한 기능을 갖춘 부가서비스를 운영하기 위한 시스템을 이중으로 설치하여 운영합니다.

③ 시스템의 접근통제

한국전자인증은 부가서비스 제공을 위한 소프트웨어의 위·변조 및 시스템을 변조하려는 위협에 대처하기 위하여 권한 있는 자만이 절차에 따라 부가서비스 운영시스템에 접근할 수 있도록 통제합니다.

④ 시스템의 감사기록

한국전자인증은 부가서비스제공에 관한 운영사항 등에 관한 내역을 감사기록·보존합니다.

⑤ 감사기록의 접근통제

한국전자인증은 부가서비스 운영시스템의 감사기록의 위·변조 및 삭제하는 위협에 대처하기 위하여 권한 있는 자만이 절차에 따라 부가서비스 운영시스템의 감사기록에 접근할 수 있도록 통제합니다.

제7장 인증서 형식

7.1 공동인증서 형식

한국전자인증은 X.509 V3 표준을 준용하는 공동인증서를 발급·공고합니다.

한국전자인증의 공동인증서 프로파일은 다음 표와 같습니다.

1) 기본필드

#	필드명	ASN.1 type	Note	지원여부		비고
				생성	처리	
1	Version	INTEGER	0x2(버전 3)	m	m	
2	Serial Number	INTEGER	자동할당	m	m	
3	Issuer type value	OID printableString 또는 utf8String	X.500, RFC5280 준수 C(Country)는 printableString ,그이외의 속성값은 utf8String	m m m	m m m	
4	Validity notBefore notAfter	UTCTime UTCTime	최상위인증기관 CPS에 명시된 유효기간 준수	m m m	m m m	
5	Subject type value	OID printableString 또는 utf8String	X.500, RFC5280 준수 C(Country)는 printableString 그이외의 속성값은 utf8String	m m m	m m m	
6	Subject Public Key Info algorithm subjectPublicKey	OID BIT STRING		m m m	m m m	
7	Extensions	Extensions		m	m	

2) 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier KeyIdentifier authorityCertIssuer authorityCertSerialNumber	OCTET STRING GeneralNames INTEGER	발급자 공동인증서의 KeyID	n	m m m m	m m m m	
2	Subject Key Identifier	OCTET STRING	subjectPublicKey 정보의 160비트 해시값	n	m	m	
3	Key Usage	BIT STRING	Digital Signature, non-Repudiation	c	m	m	
	Certificate Policy						

4	policyIdentifier policyQualifiers PolicyQualifierId Qualifier CPSuri UserNotice NoticeReference ExplicitText	OID OID IA5String SEQUENCE BMPString	전자서명인증사업자 공동인증서 정책 CPS, UserNotice 전자서명인증사업자 CPS 주소 공동인증서 표시규격 준수	c	m m m m m m - m	m m m m m m - m	[1]
5	Policy Mappings issuerDomainPolicy subjectDomainPolicy	OID OID		-	-	-	
6	Subject Alternative Names	otherName	가입자 한글실명과 VID	n	m	m	
		rfc822Name	가입자 이메일 주소		o	m	[2]
7	Issuer Alternative Names	otherName	전자서명인증사업자 한글실명	n	o	m	
8	Extended Key Usage	OID	보안토큰 식별자	n	o	o	[3]
9	Basic Constraints cA pathLenConstraint	FALSE INTEGER		-	x	x	
10	Policy Constraints requireExplicitPolicy inhibitPolicyMapping	INTEGER INTEGER		-	-	-	
11	Name Constraints			-	-	-	
12	CRL Distribution Point distributionPoint reasons cRLIssuer	DistributionPointName ReasonFlags GeneralNames	CRL 획득 정보 간접CRL 발급시 사용	n	m m - o	m m - m	[4]
13	Authority Information Access accessMethod accessLocation	OID GeneralName	id-ad-calssuers, id-ad-ocsp	n	m m m	m m m	[5]
[1]	전자우편 보안에 사용하고자 하는 경우 non-critical설정, 이외에 critical 설정 권고						
[2]	전자우편 보안에 사용하고자 하는 경우 rfc822Name 생성 권고						
[3]	[KCAC.TS.HSM]의 보안토큰 기반일 경우 보안토큰 식별자(id-kisa-HSM) 사용						
[4]	uri값으로 ldap://hostname[:portnumber]/dn[?attribute] 형식 사용						
[5]	전자우편 보안에 사용하고자 하는 경우 id-ad-calssuers 생성 권고						

공동인증서에 포함된 사항은 다음과 같은 내용을 포함합니다.

❑ 가입자의 이름

- 가입자의 전자서명검증정보
- 가입자와 전자서명인증사업자가 이용하는 전자서명 방식
- 공동인증서의 일련번호
- 공동인증서의 유효기간
- 전자서명인증사업자의 명칭
- 공동인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항
- 가입자가 제3자를 위한 대리권 등을 갖는 경우 이에 관한 사항
- 공동인증서임을 나타내는 표시

7.2 공동인증서 유효성 확인 정보 형식

한국전자인증은 X.509 V2 표준을 준용하는 공동인증서 효력정지 및 폐지목록을 생성·공고합니다.

한국전자인증은 공동인증서의 효력을 정지한 경우 공동인증서 효력정지 및 폐지목록 확장영역 중 폐지 사유코드 필드를 이용하여 당해 공동인증서가 효력정지 되었음을 나타냅니다.

한국전자인증의 공동인증서 효력정지 및 폐지목록 프로파일은 다음 표와 같습니다.

1) 기본필드

#	필드명	ASN.1 type	Note	지원여부		비고
				생성	처리	
1	Version	INTEGER	0x1(버전 2)	m	m	
2	Signature	OID	자동할당	m	m	
3	Issuer type value	 OID printableString 또는 utf8String	X.500, RFC5280 준수 C(Country)는 printableString 그 이외의 속성값은 utf8String	m m m	m m m	
4	This Update	UTCTime	발급시점	m	m	
5	Next Update	UTCTime	전자서명인증사업자 정책에 따름	m	m	
6	Revoked Certificates userCertificate revocationDate crlEntryExtensions	INTEGER UTCTime Extensions		 m m	 m m	[1] [2]
7	CRL Extensions	Extensions		m	m	[3]

[1]	효력정지 및 폐지된 공동인증서가 없을 경우는 Revoked Certificates 필드를 생성하지 않음
[2]	아래 "3) CRL 엔트리 확장필드" 참조
[3]	아래 "2) CRL 확장필드" 참조

2) CRL 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier KeyIdentifier authorityCertIssuer authorityCertSerialNumber	OCTET STRING GeneralNames INTEGER	전자서명인증사업자 공동인증서의 KeyID	n	m	m	
2	Issuer Alternative Name	otherName	전자서명인증사업자 한글실명	n	o	m	
3	CRL Number	INTEGER		n	m	m	
4	Issuing Distribution Point DistributionPointName onlyContainsUserCerts onlyContainsCACerts onlySomeReasons IndirectCRL	IA5string BOOLEAN BOOLEAN BIT STRING BOOLEAN		c	m m - - - o	m m - - - m	[1] [2]
[1]	CRLDP(Certificate Revocation List Distribution Point)와 동일 ※ RFC 2560 참조						
[2]	indirectCRL를 사용할 때는 반드시 "TRUE"로 설정						

3) CRL 엔트리 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Reason Code	ENUMERATED		n	m	m	
2	Hold Instruction Code	OID		n	o	m	
3	Invalidity Date	UTCTime		n	o	m	
4	Certificate Issuer	GeneralNames		c	o	m	

7.3 공동인증서 유효성 확인 서비스 형식

한국전자인증은 인증체계에서 인증서비스 이용의 신뢰성 확보를 위한 공동인증서 유효성 확인 기능을 실시간으로 제공하며, 공동인증서 유효성 확인 서비스용 공동인증서 프로파일의 구성 및 내용은 다음 표와 같습니다.

1) 기본필드

#	필드명	ASN.1 type	Note	지원여부		비고
				생성	처리	
1	Version	INTEGER	0x2(버전 3)	m	m	
2	Serial Number	INTEGER	자동할당	m	m	
3	Issuer type value	 OID printableString 또는 utf8String	X.500, RFC5280 준수 C(Country)는 printableString 그이외의 속성값은 utf8String	m m m	m m m	
4	Validity notBefore notAfter	UTCTime UTCTime	최상위인증기관 CPS에 명시된 유효기간 준수	m m m	m m m	
5	Subject type value	OID printableString 또는 utf8String	X.500, RFC5280 준수 C(Country)는 printableString 그이외의 속성값은 utf8String	m m m	m m m	
6	Subject Public Key Info algorithm subjectPublicKey	OID BIT STRING		m m m	m m m	
7	Extensions	Extensions		m	m	

2) 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier KeyIdentifier authorityCertIssuer authorityCertSerialNumber	OCTET STRING GeneralNames INTEGER	3가지 값을 모두 사용	n	m m m m	m m m m	
2	Subject Key Identifier	OCTET STRING	subjectPublicKey 정보의 160비트 해시값	n	m	m	
3	Key Usage	BIT STRING	Digital Signature, non-Repudiation	c	m	m	
4	Certificate Policy policyIdentifier policyQualifiers PolicyQualifierId Qualifier CPSuri UserNotice NoticeReference	 OID OID IA5String SEQUENCE	 전자서명인증사업자 공동인증서 정책 CPS, UserNotice 전자서명인증사업자 CPS 주소	c	 m m m m m m -	 m m m m m m -	

	ExplicitText	BMPString	공동인증서 표시규격 준수		m	m	
5	Policy Mappings			-	-	-	
6	Subject Alternative Names	otherName	가입자 한글실명	n	m	m	
7	Issuer Alternative Names	otherName	전자서명인증사업자 한글실명	n	o	m	
8	Basic Constraints			-	x	x	
9	Policy Constraints			-	-	-	
10	Name Constraints			-	-	-	
11	Extended Key Usage	OID		c	m	m	
12	CRL Distribution Point distributionPoint reasons cRLIssuer	DistributionPointName ReasonFlags GeneralNames	CRL 획득 정보 간접CRL발급시 사용	n	m m o o	m m m m	[1]
13	Authority Information Access accessMethod accessLocation	OID GeneralName	id-ad-calssuers	n	o	m	[2]
14	OCSP No Check	OID	id-pkix-ocsp-nocheck	n	o	m	[3]
[1]	uri값으로 ldap://hostname[:portnumber]/dn[?attribute] 형식 사용						
[2]	OCSP 서버용 인증서를 전자서명사업자가 발급하는 경우에는 반드시 생성 시점확인용 공동인증서의 경우에는 사용하지 않음						
[3]	OCSP 서버용 shortlived 공동인증서를 발행할 경우 사용 시점확인용 공동인증서의 경우에는 사용하지 않음						

제8장 감사 및 평가

8.1 감사 및 평가 현황

한국전자인증 전자서명인증업무 운영기준 준수 사실의 인정을 받기 위해 매년 1회 법 제10조(평가기관)에 따른 평가기관으로부터 평가를 받습니다.

이와 별도로, 정보통신망법에 따라 방송통신위원회의 본인확인기관 정기점검을 수검합니다.

8.2 평가자의 신원, 자격

평가자의 신원 및 자격은 시행령 제5조(평가기관의 선정기준 및 절차 등)을 따릅니다.

8.3 평가 대상과 평가자의 관계

평가기관은 법령상 과학기술정보통신부에 의해 인정받은 기관으로 평가자와 평가 대상과는 독립성을 유지합니다.

8.4 평가 목적 및 내용

한국전자인증은 법 제9조(인정기관)에 따른 인정기관으로부터 전자서명인증업무 운영기준의 준수 사실을 인정받기 위해 평기기관으로부터 평가를 받습니다. 평가의 내용은 전자서명인증업무 운영기준 준수여부 및 평가기관이 마련한 세부 평가기준을 따릅니다.

8.5 부적합 사항에 대한 조치

한국전자인증은 전자서명인증업무 운영기준 준수사실에 대한 인정을 받을 수 있도록 부적합 사항에 대하여 신속히 조치합니다.

8.6 결과 보고

평가기관은 법 제10조(평가기관)에 따라 전자서명인증업무 운영기준 준수사실에 대해 평가를 수행하고, 그 결과를 인정기관에 제출하여야 합니다.

제9장 전자서명인증업무 보증 등 기타사항

9.1 수수료

9.1.1 공동인증서 수수료

한국전자인증은 개인과 법인/단체/개인사업자에 대하여 공동인증서를 발행하며 수수료는 다음과 같습니다.

발급대상	공동인증서 종류	수수료(원, VAT포함)	
		신규발급/갱신발급	재발급
법인/단체/개인사업자	범용	110,000	5,500
	용도제한용	별도 계약에 의함	없음
개인	범용	4,400	없음
	용도제한용	별도 계약에 의함	없음
서버	범용	1,100,000	110,000

[표1] 공동인증서 수수료

9.1.2 공동인증서비스 수수료

- 신규발급, 갱신발급, 재발급의 경우 상기 [표1]의 수수료를 따릅니다. 다만, 한국전자인증의 정책에 따라 할인 요율을 적용할 수 있습니다.
- 한국전자인증은 필요 시 인증서 상태확인 서비스(OCSP), OCSP Gateway서비스, 시점확인서비스 등의 부가서비스 요금을 별도 부과할 수 있습니다.

서비스 구분	수수료(원/건)	비 고
OCSP	100원	
OCSP Gateway	100원	
시점확인 서비스	500원	

[표2] 부가서비스 수수료

- 상기 부가서비스 수수료는 공동인증서 이용자의 사용량을 고려하여 별도 협약에 따라 조정될 수 있습니다.

9.1.3 전자인증서비스에 대한 환불 정책

가입자는 공동인증서 수수료를 결제 후 (1)14일(발급가능기간) 이내 발급받지 않은 경우, (2)발급받고 사용하지 않은 상태에서 7일 이내인 경우, 최초 신청한 등록대행기관을 통해 환불을 요청 할 수 있으며 수수료를 전

액 환불 받을 수 있습니다. 이 때 공동인증서 발급에 따른 필요경비가 발생하였을 경우에는 해당 비용을 수수료에서 차감하고 환불하며 세부내용은 환불 시 가입자에게 고지됩니다.

9.2 배상

9.2.1 전자서명인증서비스 관련 배상 내용

한국전자인증은 법 제20조(손해배상책임)규정에 따라 인증업무 수행과 관련하여 가입자 또는 공동인증서를 신뢰한 이용자에게 손해를 입힌 때에는 그 손해를 배상합니다. 다만 한국전자인증은 고의 또는 과실없음을 입증하면 그 배상책임이 면제됩니다. 배상 범위는 본 인증업무준칙 9.8 을 따릅니다.

한국전자인증은 가입자의 효력정지 또는 폐지신청 이후 공동인증서의 효력정지 및 폐지목록(CRL) 공고 사이의 시간에 발생한 사고 및 Next Update(다음 인증서의 효력 정지 및 폐지목록(CRL)의 발급시점을 말합니다)이전에 발생한 사고에 대하여도 과실없음을 입증하지 못하는 한 배상책임을 부담합니다.

한국전자인증은 인증업무 수행과 관련하여 가입자 또는 공동인증서를 신뢰한 이용자에게 입힌 손해를 배상하기 위하여 보험에 가입하여야 합니다.

손해배상은 공동인증서 가입자 또는 이용자가 공동인증서를 신뢰함으로써 발생되는 모든 유형의 손해 및 손실에 적용되고, 손해배상의 타당성이 인정된 가입자 또는 이용자에 한해 손해배상 건당 배상총액은 금 5억원을 한도로 합니다.

9.2.2 면책

한국전자인증은 전자서명관련법 및 관련규정을 준수하고 본 인증업무준칙에 명시된 책임과 의무를 준수하였음에도 불구하고 가입자, 이용자 및 등록대행기관 등에서 발생하는 다음과 같은 문제에 대해서는 책임을 지지 않습니다.

- 인증서비스 수행과정 중 다음의 원인으로 가입자와 이용자에게 발생하는 기타 손실의 부분
  - 인증업무준칙에서 정의되지 않은 책임과 의무
  - 인증업무준칙에 명기된 사항 외의 부정확한 정보

- 이용자의 부주의와 무지에 대한 책임
- 공동인증서에 포함된 정보의 완전성, 현재성, 특정 목적에의 적합성 등

- 문제발생 가능성에 대해 인증업무준칙 및 홈페이지 게시판 등을 통해 공지하였음에도 불구하고 가입자와 이용자가 이를 무시하거나 필요한 행동을 취하지 않음으로 인하여 발생하는 손해 또는 손실
- 송수신된 전자문서의 송수신 사실에 대한 부인봉쇄. 단, 부인봉쇄를 위한 근거자료의 생성과 확인은 가능

또한, 전자서명인증사업자 또는 공동인증서 자체의 하자가 아닌 다음과 같은 사유로 인한 가입자와 이용자의 손해에 대해서 책임을 지지 않습니다.

- 가입자 및 이용자의 의무 불이행으로 인한 손해
- 인증서비스 수행 중 한국전자인증의 시스템 장애가 아닌 통신경로상의 장애
- 유효기간이 경과된 공동인증서의 이용에 따른 손해
- 전자서명관련법 및 본 인증업무준칙에서 규정한 범위를 벗어나는 경우에 의한 손해
- 효력정지 또는 폐지된 공동인증서의 이용에 따른 손해
- 한국전자인증이 제공하지 않은 소프트웨어 또는 하드웨어의 장애 등으로 인하여 발생되는 인증서비스의 지연 및 중단에 의한 가입자 및 이용자의 손해
- 전쟁이나 기타 천재지변 등 불가항력적인 사유로 인증서비스를 제공하지 못한 경우
- 기타 한국전자인증의 과오로 인한 사고가 아닌 경우

9.3 영업비밀

한국전자인증은 "부정경쟁방지 및 영업비밀보호에 관한 법률"을 준수하고 있으며, 한국전자인증의 인증서비스 이용 과정에서 취득한 한국전자인증의 영업비밀에 대해 누설하거나 이를 부당하게 이용할 경우 민·형사상의 책임을 부담할 수 있습니다.

9.4 개인정보보호

한국전자인증 및 등록대행기관은 전자서명법규와 정보통신망이용촉진및정보보호등에관한법률, 개인정보보호법의 규정에 따라, 가입자의 정보 수집 시 인증업무 수행에 필요한 최소한의 가입자 정보만을 수집하며, 가입자의 동의 하에서만 개인식별이 가능한 가입자정보를 수집 및 저장합니다. 수집된 사용자 정보

는 암호화 하여 보관됩니다.

제공된 가입자정보는 당해 가입자의 동의 없이 목적 외에 이용되거나 제3자에게 제공될 수 없으며, 가입자의 주민등록번호를 보호하기 위하여 공동인증서 이용기술에서도 가입자의 주민번호를 ISP(Internet Service Provider)에게 제공하지 않습니다. 이에 대한 모든 책임은 한국전자인증과 등록대행기관이 부담합니다. 다만, 다음 각 호의 경우에는 예외로 합니다.

- 인증서비스 제공에 따른 요금정산을 위하여 필요한 경우
- 법령에 특별한 규정이 있는 경우
- 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 필요한 경우로서 특정 개인을 식별할 수 없는 가명정보로 제공하는 경우

한국전자인증 및 등록대행기관은 가입자의 동의를 받아야 할 경우에는 가입자정보관리책임자의 신원(성명, 소속부서, 직위 및 전화번호 기타 연락처), 정보의 수집 목적 및 이용 목적, 제3자에 대한 정보제공관련 사항(제공받는 자, 제공 목적 및 제공할 정보의 내용) 등 개인정보보호법에 따라 동의 내용을 고지하며 가입자는 언제든지 이 동의를 철회할 수 있습니다.

가입자는 언제든지 한국전자인증 및 등록대행기관이 가지고 있는 가입자 자신의 정보에 대해 열람, 오류정정, 삭제를 요청할 수 있으며, 한국전자인증은 이에 대해 지체 없이 필요한 조치를 취하여야 하고, 가입자가 오류의 정정을 요구할 경우, 한국전자인증 및 등록대행기관은 그 오류를 정정할 때까지 당해 가입자 정보를 이용하지 않아야 합니다. 한국전자인증 및 등록대행기관은 가입자 정보 보호를 위하여 관리자를 한정하여 그 수를 최소화하며 가입자 정보의 분실, 도난, 유출, 변조 등으로 인한 가입자의 손해에 대하여 모든 책임을 부담합니다.

한국전자인증 및 등록대행기관 또는 그로부터 가입자 정보를 제공받은 제3자는 가입자정보의 수집 목적 또는 제공받은 목적을 달성한 때에는 당해 가입자정보를 지체 없이 파기하여야 합니다.

9.5 지식재산권

한국전자인증은 지식재산권의 보호와 관련된 법령을 준수합니다.

9.6 보증

한국전자인증은 한국인터넷진흥원에서 한국전자인증을 위해 발급한 전자서명인증사업자용 인증서에 포함된 전자서명검증정보에 합치하는 생성키로 발급한 가입자 공동인증서에 대해 다음 사항을 보장합니다.

- 발급된 공동인증서에 포함된 내용이 등록사실과 오차가 없다는 사실
- 공동인증서 효력정지 및 폐지목록에 대한 내용이 틀림없다는 사실
- 전자서명관련법 및 인증업무준칙의 규정을 준수하여 공동인증서가 발급되었다는 사실

9.7 보증 예외 사항

공동인증서가 가입자 및 이용자의 신용등급, 가입자 관련정보의 불변성 등 상기 사항 이외의 것까지 보장한다는 것을 의미하지는 않습니다. 따라서 이용자에게 공동인증서에 기재된 내용이 가입자의 신용 및 신원정보, 가입자 및 이용자의 특정업무 또는 목적에 합치하는 보증 등을 보장하는 것은 아닙니다.

9.8 보험의 보상 범위

한국전자인증은 인증업무수행과 관련하여 가입자 또는 공동인증서를 신뢰한 이용자에게 손해를 입힌 때에는 배상의 타당성이 인정된 가입자 또는 이용자만 그 손해를 배상합니다.

9.9 배상 한계

한국전자인증은 연간 20억원을 총보상한도로 보험에 의한 손해배상책임을 집니다.

보험에 의한 배상의 한도에는 가입자, 이용자 등 한국전자인증이 발급, 관리, 폐지, 효력정지, 만료한 공동인증서와 관련한 모든 자가 입는 모든 손해가 포함됩니다. 보험에 의한 배상의 한도를 초과하는 배상책임은 당사자간의 합의나 법원의 판결에 따릅니다.

9.10 준칙의 효력

9.10.1 준칙 시행일

본 인증업무준칙은 2021년 9월 6일부터 시행합니다.

9.10.2 준칙의 효력이 종료되는 조건

본 인증업무준칙은 인증업무를 지속할 수 없는 때에 효력이 상실됩니다.

9.11 통지 및 의사소통

한국전자인증은 한국전자인증의 전자서명생성정보에 대한 손상, 노출, 파손, 분실, 도난 등 인증서의 신뢰도 및 유효성에 중대한 영향을 미치는 사실이 발생하거나, 인증업무에 중대한 영향을 미치는 상황이 발생할 경우 한국전자인증의 홈페이지(https://www.crosscert.com)에 공고하는 것을 원칙으로 하며, 필요한 경우에 한해 전자우편으로 통지합니다.

또한 본 인증업무준칙 또는 인증서비스와 관련된 문의가 있을 경우 한국전자인증의 이메일(helpdesk@crosscert.com) 또는 고객센터(1566-0566)을 통해 의사소통을 할 수 있습니다.

9.12 이력 관리

한국전자인증은 전자서명인증업무준칙의 변경 이력을 관리합니다.

9.13 분쟁 해결

9.13.1 관련자에게 전달되는 문서(또는 전자문서)가 법적 효력을 갖기 위한 요건

인증체계 관련자에게 전달되는 문서(또는 전자문서)가 법적 효력을 갖기 위하여는 전자서명관련법규와 본 인증업무준칙을 준수하고 전자서명인증사업자에 의하여 인증된 전자서명이 있어야 합니다.

9.13.2 분쟁을 해결하는 절차

과학기술정보통신부 등 관련정부기관과 한국인터넷진흥원은 전자서명관련법 위반행위 및 인증업무준칙의 준수 여부 등을 검사하고 전자서명관련법 및 기타 관련 법률에 따라 가장 빠른 방법으로 분쟁 해결을 조정할 수 있습니다.

한국전자인증은 가입자 및 이용자간의 분쟁 발생시에는 관련 당사자에게 관련 자료를 분쟁해결 사전에 제출하도록 요구하고 전자서명관련법 및 인증업무준칙의 준수여부 등을 조사하여 조정안을 제시함으로써 합의에 이르도록 유도하고 권고할 수 있습니다. 이 때, 분쟁 발의 또는 관련 당사자는 한국전자인증에 서면으로 심의를 요청해야 하고 동 문서는 관련된 이해 당사자들에게 전달해야만 합니다

분쟁이 발생한 경우에 한국전자인증은 한국인터넷진흥원에 분쟁조정을 요청할 수 있습니다. 이 경우 한국인터넷진흥원은 분쟁 당사자들에게 관련자료를 제출을 요구하고 전자서명관련법 및 인증업무준칙의 준수여부 등을 조사하여 조정안을 제시함으로써 합의에 이르도록 유도하고 시정조치를 권고할 수 있습니다.

9.14 관할 법원

한국전자인증과 가입자 또는 이용자와의 인증업무와 관련한 분쟁이 일어났을 경우에 분쟁의 해결을 위한 제 소송은 관할은 민사소송법의 관할 규정을 따릅니다.

9.15 관련 법의 준수

본 인증업무준칙은 전자서명법, 전자서명법 시행령, 전자서명법 시행규칙을 준수합니다.

9.16 기타 규정

본 인증업무준칙은 대한민국의 관계법령에 따라서 해석되고 적용됩니다.