SignKorea 인증업무준칙

Ver. 4.10

1. 소개

1.1 개요

1.1.1 준칙의 배경 및 목적

인터넷 등 개방형 정보통신시스템을 이용하여 처리되는 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고, 국민생활의 편익을 증진하기 위하여 1999년 2월 5일 전자서명법(법률 제5,792호)이 제정되어 1999년 7월 1일부터 시행되고 있습니다.

(주)코스콤 인증센터(영문명 “SignKorea”, 이하 “SignKorea”라 한다)의 인증업무준칙(이하 “준칙”이라 한다)은 전자서명법(이하 “법”이라 한다), 동법 시행령(이하 “시행령”이라 한다), 동법 시행규칙(이하 “시행규칙”이라 한다)에 따라 규정 된 전자서명인증업무 운영기준(이하 “운영기준”이라 한다)을 준수하는 전자서명인증사업자로 인정 받고, 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 “정보통신망법”이라 한다), 동법 시행령(이하 “정보통신망법 시행령”이라 한다), 동법 시행규칙(이하 “정보통신망법 시행규칙”이라 한다)에 따라 본인확인기관으로 지정 받은 SignKorea가 제공하는 인증서의 발급, 효력정지, 효력회복, 갱신, 재발급, 폐지 등의 인증업무역무(이하 “인증서비스”라 한다)에 필요한 전반적인 사항과 인증서비스와 관련된 책임과 의무에 대한 사항을 정함을 목적으로 합니다.

1.1.2 전자서명인증체계 소개

“전자서명인증체계”라 함은 SignKorea가 인증서를 발급하고, 인증관련 기록을 관리하며, 인증서를 이용한 부가업무 등을 제공하기 위한 체계를 말합니다.

1.1.3 인증기관 소개

SignKorea는 1999년 7월 관련 법령에 의거하여 정보통신환경에서 전자서명 방식을 이용한 안전한 전자문서의 교환 환경을 조성하기 위하여 설립되었으며, 법 제8조(운영기준 준수사실의 인정)에 의거 운영기준 준수 사실을 인정받은 전자서명인증사업자이며, 정보통신망법 제23조의3에 의거 본인확인기관으로 지정 받았습니다.

SignKorea의 인증서비스에 관련된 연락처는 다음과 같습니다.

○ 기관명 : (주)코스콤 인증센터 (영문명 : SignKorea)

○ 주소
  - 본사 : 07330 서울특별시 영등포구 여의나루로4길 21 (여의도동)
  - 센터 : 14119 경기도 안양시 동안구 엘에스로 115번길 26 (호계동)
○ 인터넷 URL : http://www.signkorea.com
○ 전자우편 : signkorea@koscom.co.kr
○ 전화번호 : 1577-7337
○ 팩스번호 : 02) 767-7390

1.1.4 인증서 정의 및 효력

“인증서”라 함은 법 제2조(정의)에 따라 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 증명하기 위하여 SignKorea가 인증서를 발급받고자 하는 자에게 발급하는 전자적 정보를 말합니다. 이 경우 SignKorea는 인증서를 발급받고자 하는 자의 신원을 확인합니다.

SignKorea는 가입자가 제공한 정보가 가입자의 당시 상황과 일치함을 확인한 후에 가입자가 제출한 전자서명검증정보와 관련정보에 인증기관의 전자서명생성정보로 전자서명한 인증서를 발급합니다. 그러므로, SignKorea는 이용자에게 SignKorea의 인증서에 기재된 내용은 인증서 발급신청 당시에 사실임만을 보장하며, 다음 사항을 보증하는 것이 아닙니다.

○ 가입자와 이용자의 특정업무나 목적에 대한 보증
○ 가입자의 신용
○ 가입자 신원정보 등 관련정보의 불변성
○ 기타 SignKorea 업무외 분야 등

법령의 규정 또는 당사자간의 약정에 따라 가입자가 인증서의 전자서명검증정보에 합치하는 전자서명생성정보로 전자서명을 생성하는 경우, 생성된 전자서명은 법 제3조(전자서명의 효력)에 의거 해당문서에 대한 서명, 서명날인 또는 기명날인으로서의 효력을 가집니다.

SignKorea의 인증서는 비대면 상황에서의 전자문서교환, 소프트웨어 검증 등의 전자서명의 생성 및 검증 등 법적인 권리와 의무가 발생하는 분야에서 이용할 수 있습니다.

SignKorea는 별도의 이용금지범위를 정하지는 않지만, 다음과 같은 경우에는 가입자의 인증서 이용을 제한할 수 있습니다.

○ 가입자가 사망, 구속 등으로 신원확인이나 법적인 전자거래가 불가능한 경우
○ 법정대리인의 동의를 필요로 하는 법률행위의 범위에 인증서비스 가입 및 인증서 (재)발급 관련 사항이 포함되어 있음에도 불구하고 피한정후견인이 법정대리인의 동의 없이 서비스에 가입하거나 인증서를 (재)발급 받은 경우
○ 파산선고를 받고 복권되지 아니한 사람

○ 인증서의 유효기간이 경과된 경우
○ 가입자가 타인의 명의 도용 등 부정한 방법으로 인증서를 발급 받았거나 그렇다고 의심 되는 경우
○ SignKorea가 인증서비스와 관련된 보안절차나 인증기관 자신의 전자서명생성정보 유출과 같은 보안상의 이유로 기 발급된 인증서의 이용을 제한할 필요가 있다고 판단하는 경우
○ 기타 SignKorea가 인증서의 이용을 제한할 필요가 있다고 판단하는 경우

1.2 문서의 명칭

당 준칙의 명칭은 SignKorea 인증업무준칙 Ver. 4.10입니다.

1.3 전자서명인증체계 관련자

1.3.1 SignKorea

SignKorea는 법 제8조(운영기준 준수사실의 인정) 등에 의거 정부의 심사를 받아 운영기준 준수사실의 인정을 받은 전자서명인증사업자로 지정된 기관이며 다음의 업무를 수행합니다.
○ 인증서비스 관련 신청서 접수 및 처리
○ 가입자의 신원확인
○ 인증서 및 관련 정보의 제공
○ 인증서비스의 제공
○ 인증서 폐지목록(효력정지 목록 포함)의 제공
○ 등록대행기관의 지정 및 관리
○ 기타 운영기준 준수사실의 인정을 받은 전자서명인증사업자로 수행해야 할 업무

1.3.1.1 SignKorea의 책임과 의무

1.3.1.1.1 정확한 정보의 제공

SignKorea는 다음과 관련하여 정확한 정보 및 사실만을 한국인터넷진흥원에 제공합니다.

○ 인증기관용 인증서 발급(갱신 및 재발급 포함) 신청
○ 인증기관용 인증서 효력정지 및 폐지 신청

1.3.1.1.2 인증서비스 관련정보의 제공

SignKorea는 준칙 및 관련정보를 1.5.3(준칙의 공지 및 가입자 동의 방법)에서 정한 홈페이지를 통해 제공하고 인증서 및 인증서 효력정지와 폐지에 관련된 정보를 디렉토리 또는 웹서버 시스템에 등록하여 가입자와 이용자가 항상 검색할 수 있도록 합니다.

1.3.1.1.3 가입자 정보의 보호

SignKorea는 가입자의 정보를 기밀정보로 분류하고 임의 접근을 제한하며, 가입자의 동의를 얻어 공개하는 정보라 할지라도 타인에 의한 임의 접근 및 변경 또는 삭제를 불허합니다. 단, SignKorea는 법률에서 정한 규정에 의거 타 기관의 요청이 있는 경우에 이를 공개할 수 있습니다.

1.3.1.1.4 전자서명생성정보의 올바른 이용

SignKorea는 다음과 같이 이용목적에 따라 여러 가지 전자서명생성정보와 전자서명검증정보를 만들 수 있습니다. 단, 각 전자서명생성정보와 전자서명검증정보는 해당 분야에만 이용할 수 있습니다.

○ 인증서 발급용으로 만든 전자서명생성정보는 인증서 발급에만 이용한다.
○ 시점확인을 위해 만든 전자서명생성정보는 시점확인을 위해서만 이용한다.
○ 인증서 유효성 확인(OCSP)용으로 만든 전자서명생성정보는 인증서 검증에만 이용한다.

1.3.1.1.5 중요 사실에 대한 통보 및 조치

SignKorea는 SignKorea의 전자서명생성정보에 대한 손상, 노출, 파손, 분실, 도난 등 인증서의 신뢰도 및 유효성에 중대한 영향을 미치는 사실이 발생하거나, SignKorea의 인증업무에 중대한 영향을 주는 상황이 발생한 경우에 해당사실을 SignKorea의 홈페이지를 이용하여 공고하는 것을 원칙으로 하며, 필요한 경우에 한해 전자우편으로 통지합니다.

SignKorea는 통보조치 후에 가입자와 이용자의 피해를 최소화할 수 있는 방법을 강구하여 신속하게 조치합니다.

1.3.1.1.6 관련 법규의 준수

SignKorea는 인증서비스를 수행할 때 전자서명법, 정보통신망법 및 개인정보 보호법 등 관련 법령을 준수합니다.

1.3.1.1.7 검증정보에 대한 보장

SignKorea는 가입자가 제출한 정보 중 인증서비스를 제공하기 위해 필요한 최소한의 정보에 대해서만 사실여부를 확인하며, 해당정보에 대한 사실성을 이용자에게 보장합니다.

1.3.1.1.8 안전한 암호화 소프트웨어 적용

SignKorea는 가입자가 전자서명생성정보를 안전하게 생성·저장할 수 있도록 객관적으로 신뢰할 수 있는 암호화 소프트웨어 및 보안 기술 규격을 적용하며, 가능한 범위(Windows, iOS, Android 등 가입자 단말 환경)에서 이에 대해 신뢰성을 평가하는 것을

원칙으로 합니다.

만약 객관적으로 신뢰성이 검증되지 않은 암호화 소프트웨어 또는 보안 기술 규격을 적용하는 경우, SignKorea는 안전성을 확보하기 위한 충분한 기술적 검증 또는 조치를 취하며, 가입자에 손해 발생 시 이에 대한 책임을 부담합니다.

1.3.2 가입자

가입자는 전자서명법상 가입자로서 SignKorea가 준칙에서 정한 일련의 절차에 따라 SignKorea의 인증서비스에 가입하고 SignKorea가 정한 규격에 적합한 전자서명생성정보와 전자서명검증정보를 생성한 후, SignKorea가 가입자의 전자서명검증정보와 관련 정보에 대해 발급한 인증서를 통해 전자서명생성정보와 전자서명검증정보의 합치성을 확인받으려는 자연인(이하 “개인”이라 한다)과 그 외 법인, 단체 및 개인사업자 등(이하 “법인”이라 한다)을 의미합니다. 단, SignKorea가 필요하다고 판단한 경우에는 가입자를 대신하여 업무를 수행하는 정보통신장비를 가입자에 포함할 수 있습니다.

1.3.2.1 가입자의 책임과 의무

1.3.2.1.1 적정한 인증서의 선택 및 정확한 정보의 제공

가입자는 자신의 목적에 맞는 인증서를 선택해서 신청해야 하며, 인증서비스의 신청과 관련하여 본 준칙에 대해 정확하게 이해해야 하고, 정확한 정보 및 사실만을 SignKorea에 제공하여야 합니다.

1.3.2.1.2 전자서명생성정보의 보호

가입자는 다음과 같이 전자서명생성정보를 보호해야 합니다.

○ 가입자는 자신만이 알고 있는 안전한 전자서명비밀번호 등을 이용하여 전자서명생성정보가 도용되지 않도록 해야 합니다.
○ 가입자는 전자서명생성정보가 저장되어 있는 하드디스크나 USB, 스마트폰 등의 물리적 저장매체의 보안에 대한 책임을 가집니다.

1.3.2.1.3 적절한 조치

가입자는 다음의 상황이 발생하면 신속하게 SignKorea 또는 등록대행기관에 해당 사실을 통보하고 적절한 조치를 수행해야 합니다.

○ 가입자의 신상정보(성명, 전자우편 주소 등)가 변경되는 경우
○ 비밀번호의 유출이나 USB, 스마트폰의 도난 등으로 가입자의 전자서명생성정보가 유출 또는 훼손되었다고 생각되는 경우
○ 인증서 가입자 이외의 제3자가 인증서를 발급, 효력정지, 효력회복, 갱신, 재발급, 폐지

하려는 시도를 한 경우

위와 같은 상황이 발생하면 가입자는 SignKorea 또는 등록대행기관에 해당 인증서의 폐지 또는 재발급을 요청함으로써 가입자의 인증서에 대한 서비스를 중단시키고 필요한 경우에 새로운 인증서를 발급 받습니다.

1.3.2.1.4 유의사항

SignKorea는 가입자가 온라인으로 폐지신청을 하는 경우에 가입자용 인증서 관리프로그램(이하 “관리프로그램”이라 한다)을 이용하여 저장장치의 가입자 전자서명생성정보와 인증서를 파기하는 것을 원칙으로 합니다. 하지만, 가입자가 별도로 백업해둔 전자서명생성정보와 인증서는 가입자가 파기해야 합니다.

1.3.3 대리인

대리인은 개인 가입자의 법정 대리인 또는 법인 가입자가 지정한 법인의 임직원을 의미합니다. 대리인은 위임장 등과 같은 증명서를 지참한 경우에 한하여 가입자를 대리하여 인증서비스를 신청할 수 있습니다.

본 준칙에서 대리인은 가입자에 포함되며, 내용상 가입자와 대리인에 대한 구별이 필요한 경우에 한하여 가입자와 대리인을 별도로 명시합니다.

1.3.4 이용자

이용자는 전자서명법상 이용자로서 SignKorea가 가입자에게 발급한 인증서를 이용하여 가입자의 전자서명생성정보와 전자서명검증정보의 합치성을 확인하려는 개인 또는 법인을 의미합니다.

1.3.4.1 이용자의 책임과 의무

1.3.4.1.1 인증서 이용목적의 이해

이용자는 가입자의 인증서에 대해 이용목적과 이용가능범위에 대해 정확하게 이해해야 합니다. 이용자는 가입자가 보내온 SignKorea의 인증서가 이용자의 목적(금융기관, 공공기관, 정부기관 등에서 가입자의 전자서명을 처리)에 적합한가를 판단해야 합니다.

1.3.4.1.2 인증서 내용 및 유효성의 확인

이용자는 인증서의 이용 전에 유효기간, 용도 등에 대해 가입자의 인증서는 물론 한국인터넷진흥원 및 SignKorea의 인증서에 수록되어 있는 내용을 확인해야하며, 인증서 폐지목록(CRL) 또는 인증서 유효성 확인 서비스(OCSP)를 통해 각 인증서가 효력정지 또는 폐지되어 있는지 확인해야 합니다. 단, 인증서 폐지목록은 주기적으로 생성되는 정보이므로,

이를 통해 실시간 정보를 획득할 수는 없습니다.

1.3.4.1.3 적용 가능한 책임조항 및 보증에 대한 인지

이용자는 이용하려는 인증서의 효력 및 보증범위, 관련 책임조항 등의 내용을 정확하게 인지해야 합니다.

1.3.4.1.4 이용자의 배상책임

이용자는 인증서 이용과 관련하여 이용자의 고의 또는 과실로 가입자에게 손해를 입힌 경우에 가입자에게 그 손해에 대해 배상해야 합니다.

1.3.5 중계서비스기관

중계서비스기관은 SignKorea 및 등록대행기관과 약정을 체결하여 가입자 등록정보 등을 전달하는 시스템(이하 “중계시스템”이라 한다)을 운영하는 자를 말합니다.

1.3.5.1 중계서비스기관의 의무와 책임

1.3.5.1.1 준칙의 이해

중계서비스기관은 준칙을 숙지하고 있어야 하며, 중계서비스를 위해 SignKorea와 맺은 계약서에서 정한 사항을 준수할 책임을 가지며, 다음과 같은 정보에 대해서 SignKorea 및 등록대행기관이 처음 전송한 상태대로 전달할 책임이 있습니다. 또한 중계서비스기관은 다음 각 호의 정보를 복호화하거나 보유하지 못합니다. 중계서비스기관은 중계서비스의 장애에 의해 발생되는 SignKorea, 등록대행기관, 가입자 그리고 이용자가 입은 손해에 대하여 배상할 책임을 지게 됩니다.

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

1.3.5.1.2 중계서비스기관의 의무

중계서비스기관은 가입자 등록정보 등을 SignKorea로 전달하는 경우, 다음 각 호의 사항에 대해서 전자서명인증업무 운영기준에 준하여 중계시스템 및 보호설비를 갖추어야 합니다.

○ 출입통제
○ 물리적 침입 감시
○ 시스템 및 네트워크 보호

1.3.5.1.3 중계서비스기관의 배상책임

중계서비스기관은 중계서비스기관의 고의 또는 과실로 SignKorea에 손해를 입힌 경우에 그 손해에 대해 배상해야 하며, 중계서비스 시스템 오류 등으로 인하여 발생한 가입자 또는 이용자의 손해에 대해서도 배상해야 합니다.

1.3.5.1.4 준칙의 준수

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

1.3.5.1.5 가입자의 개인정보보호

중계서비스기관은 중계서비스 되는 가입자의 개인정보를 보호하고 자료에 대한 보안을 유지할 의무가 있습니다.

1.3.6 등록대행기관

1.3.6.1 등록대행기관의 의무와 책임

1.3.6.1.1 정확한 신원확인

등록대행기관은 준칙을 숙지하고 있어야 하며, 가입자의 신원확인의 정확성에 대한 책임을 가지게 됩니다. 등록대행기관은 신원확인 결과의 실수 및 오류에 의한 가입자와 이용자 그리고 SignKorea의 손해에 대해 책임을 가지게 됩니다.

등록대행기관은 인증서 발급(갱신 및 재발급 포함) 과정에서 인증기관을 대신하여 전자서명생성정보가 가입자에게 속함을 확인하는 경우, 확인 과정 누락 및 오류 등에 의한 가입자와 이용자 그리고 SignKorea의 손해에 대해 책임을 가지게 됩니다.

1.3.6.1.2 중요사실에 대한 공지

등록대행기관은 인증서 신청서를 접수할 때, 가입자에게 인증서의 이용과 관련한 중요사항들을 숙지시켜야 하며, 필요한 경우에 이에 대하여 가입자의 기명날인 또는 서명 등의 확인을 받아야 합니다.

1.3.6.1.3 전자서명생성정보의 접근 보호

등록대행기관이 인증서 발급 과정에서 전자서명비밀번호를 생체정보(지문 등)로 대체하는 서비스를 제공하는 경우, 등록대행기관은 생체인증이 성공적으로 진행된 이후에 가입자가 자신의 전자서명생성정보에 접근하도록 해야 합니다.

등록대행기관은 동 서비스의 안전성과 유효성이 확보될 수 있도록 운영하여야 하며, 서비스에 대한 감사기록을 안전하게 생성・관리하고, SignKorea가 감사기록의 열람을 요청

하는 경우 성실히 협조하여야 합니다.

1.3.6.1.4 등록대행기관의 배상책임

등록대행기관은 등록대행기관의 고의 또는 과실로 SignKorea의 신뢰도에 악영향을 주거나 금전적인 손해를 입힌 경우에 그 손해에 대해 배상해야 하며, 인증서 가입자의 신원확인 오류 등으로 인하여 발생한 가입자 또는 이용자의 손해에 대해서도 배상해야 합니다.

등록대행기관은 인증기관을 대신하여 전자서명생성정보가 가입자에게 속함을 확인하는 경우, 확인 과정 누락 및 오류 등으로 인하여 발생한 가입자 또는 이용자의 손해에 대해서도 배상해야 합니다.

등록대행기관이 다음과 같은 형태로 협조의무를 해태함으로 인하여 SignKorea의 인증업무관련 관리·감독이 원활하게 이루어지지 못한 경우, 등록대행기관은 관련된 손해에 대한 책임을 부담합니다.

○ SignKorea의 신원확인 원본서류의 이송요청에 대해 타당한 사유 없이 거부·부작위 또는 지체
○ SignKorea의 정보통신망을 통한 가입자의 등록정보(전자우편, 휴대전화 번호 등 연락처 포함) 전송요청에 대해 타당한 사유 없이 거부·부작위 또는 지체
○ 기타 위 내용에 준하는 사유

1.3.7 기타 관련자

1.3.7.1 클라우드 공동인증서비스 관련자

SignKorea는 타인증기관과 제휴하여 가입자(타인증기관 가입자 포함)의 신청을 받아 가입자의 인증서(전자서명생성정보 포함)를 클라우드(SignKorea 및 타인증기관이 운영하는 가입자 인증서 보관용 서버)에 보관하는 서비스를 제공합니다.

SignKorea가 제휴한 타인증기관은 한국정보인증㈜, 한국전자인증㈜, ㈜한국무역정보통신입니다.

가입자가 클라우드 공동인증서비스를 이용하는 중 손해를 입을 경우 서비스 이용약관 및 제휴 인증기관 간 협약에 따라 배상합니다.

1.4 인증서 종류

SignKorea는 인증서의 이용범위와 용도에 따라 인증서의 등급을 [표1]과 같이 구분하고 있습니다. 단, SignKorea는 사용빈도에 따른 위험성을 고려하여 일부 등급을 세부적으로 구분할 수 있습니다.

구분		등급	이용범위 및 용도	발급 대상
공동인증서	용도제한용	Special	- 비대면 과정에서의 전자서명 - 비금융기관 및 금융기관에서의 전자문서 교환 - 전자문서의 교환규모가 크거나 내용이 매우 중요한 경우	개인 법인/단체/개인사업자 서버
	범용	Platinum	- 비대면 과정에서의 전자서명 - 비금융기관 및 금융기관에서의 전자문서 교환 ※ 단, 위험도 및 활용도에 따라 구분 가능	개인 법인/단체/개인사업자 서버
	용도제한용	Gold	- 증권(온라인 증권거래 등), 금융투자 및 보험 거래 ・이용 사이트 : “자본시장과 금융투자업에 관한 법률”에 따른 금융투자회사가 제공하는 사이트, 한국예탁결제원이 제공하는 전자주주총회 사이트, “보험업법”에 따른 보험회사가 제공하는 사이트 - 정부 민원업무(전자정부민원서비스 등 정부가 인정하는 분야) 및 인증기관간 합의된 업무 ※ 코스콤이 발급한 용도제한용 인증서는 코스콤 독자 명의로 제공하는 사이트에서 이용 가능	개인 법인/단체/개인사업자
	용도제한용	Silver	- 법인내 직원간의 GroupWare 등을 통한 전자서명 - 특정 서비스 또는 서비스제공업체에 제한된 용도로만 사용 - 정부 민원업무(전자정부민원서비스 등 정부가 인정하는 분야) ※ 이용기관과의 계약에 따라 정부 민원업무는 제외될 수 있음 ※ 코스콤이 발급한 용도제한용 인증서는 코스콤 독자 명의로 제공하는 사이트에서 이용 가능	개인 법인/단체/개인사업자

[표1] 인증서의 등급 및 이용범위

SignKorea는 상기의 인증서 등급별 이용범위 및 용도에 맞게 이용하기를 권장합니다.

SignKorea는 Platinum 등급을 상호연동용 인증서로 발급하며, 인증서의 OID는 발급대상자별로 다음과 같습니다.

- 법인,단체,개인사업자 : 1.2.410.200004.5.1.1.7
- 개인 : 1.2.410.200004.5.1.1.5

SignKorea는 가입자가 인증서를 신청한 일시 또는 인증서를 발급한 일시로부터 일정기간(1년, 2년, 3년)을 인증서의 기본적인 유효기간으로 설정합니다. 다만, 재발급과 갱신 과정을 거친 인증서는 일정기간(1년, 2년, 3년) 미만 혹은 이상이 될 수 있습니다. 또한 가입자 전자서명생성정보의 안전성 및 신뢰성이 확보되는 경우(보안토큰에 발급, 안전한 실행환경(TEE) 기술을 활용하여 발급 등)에는 유효기간을 최대 5년(갱신시 유효기간은 잔여기간 + 5년)으로 설정할 수 있습니다.

구분		유효기간
신규발급		1~5년
재발급	유효기간 내	잔여기간
	유효기간 만료 후	1~5년
갱신		잔여기간 + 1~5년

[표2] 인증서의 유효기간

1.5 준칙의 관리

1.5.1 준칙 관리부서(또는 담당자) 이름 및 연락처

○ 관리부서 : (주)코스콤 인증센터 (영문명 : SignKorea)
○ 인터넷 URL : http://www.signkorea.com
○ 전자우편 : signkorea@koscom.co.kr
○ 전화번호 : 1577-7337
○ 팩스번호 : 02) 767-7390

1.5.2 준칙의 제·개정 사유 및 절차

SignKorea는 다음의 경우에 준칙을 개정합니다.

○ 법 제15조(인증업무준칙의 준수 등) 제1항에 의거 준칙의 변경이 필요할 경우
○ SignKorea가 새로운 업무를 반영하거나 인증서비스를 개선하기 위해 준칙의 내용에 대하여 보완·수정이 필요하다고 판단한 경우

SignKorea는 준칙을 개정할 경우 버전, 사유, 내용 등 개정내역에 대한 기록을 유지·관리합니다.

SignKorea는 최상위인증기관(한국인터넷진흥원)과의 정책 일관성을 위해 필요시 준칙 제· 개정에 대하여 협의할 수 있습니다.

1.5.3 준칙의 공지 및 가입자 동의 방법

SignKorea는 다음의 절차에 따라 준칙을 공고합니다.

○ 개정된 준칙은 새로운 버전이 부여됩니다.
○ 개정된 준칙은 아래의 정보저장위치에 즉시 공고합니다.
○ SignKorea의 준칙 정보저장위치: http://www.signkorea.com/cps.html

가입자는 준칙이 수정되어 공고된 후 2주 이내에 서면 또는 전자서명생성정보로 전자서명한 전자문서, 전화, 전자메일 등의 수단을 통해 이의를 제기할 수 있으며, 그러하지 않은 경우 SignKorea는 가입자가 준칙의 수정에 대하여 동의하는 것으로 간주합니다.

1.6 정의 및 약어

○ DN(Distinguished Name)
인증서 발급자 및 인증서 소유자를 확인하기 위해 사용되는 이름 형식을 말한다.
○ 신뢰당사자
SignKorea의 인증서를 수령하여 당해 인증서를 신뢰하고 사용하는 자를 말한다.

○ 디렉토리
인증서, CRL을 보관하고 신뢰당사자에게 공고 및 검색 서비스를 제공하기 위한 시스템을 말한다.
○ 신원확인
SignKorea가 인증서의 신뢰성 확보를 위하여 인증서 발급, 갱신, 효력정지 및 폐지 등의 신청시 신청인 및 신청 정보의 진정성 등을 확인하는 행위를 말한다.
○ 사고정보
전자금융사고가 발생한 가입자의 정보(이름, 주민등록번호, IP, MAC주소 등)를 말한다.
○ 찾아가는 서비스
인증서 발급에 필요한 등록업무를 인증기관 또는 등록대행기관의 소속 직원이 신청인을 직접 찾아가 가입자에 대한 신원확인을 수행하고 인증서 발급, 재발급 등의 신청을 접수・등록함으로써 발급의 편의를 도와주는 서비스를 말한다.
○ 전자서명비밀번호
전자서명생성정보를 암・복호화하고, 전자서명을 생성하는데 필요한 비밀번호(또는 패스워드)를 말한다.
○ 클라우드
인증기관이 가입자의 신청을 받아 가입자의 인증서(전자서명생성정보 포함)를 보관하기 위해 운영하는 서버를 말한다.
○ 재발급
가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출되어 해당 인증서를 폐지하고 잔여 유효기간으로 새로운 인증서를 발급하거나, 유효기간 만료 후 새로운 인증서를 발급하는 것을 말한다.
○ 갱신
인증서의 유효기간이 만료되기 최대 2개월 전부터 만료 시점 이전에 유효기간을 연장하여 인증서를 발급하는 것을 말한다.

이외 본 준칙에서 사용하는 용어는 관련 법령에서 정의하는 용어를 따릅니다.

2. 전자서명인증업무 관련 정보의 공고

2.1 공고설비

SignKorea는 인증서, 인증서 효력정지 및 폐지목록 등 인증업무와 관련된 정보(이하 “인증업무관련정보”라 한다)를 공고하는 설비를 운영합니다.

2.2 공고방법

SignKorea의 인증업무관련정보를 아래 저장위치에 게시하여 공고합니다.

○ 공고위치: ldap://dir.signkorea.com

2.3 공고주기

SignKorea는 인증서 발급 및 관리 등에 관련된 정보는 처리 후 즉시 공고하며, 인증서 효력정지 및 폐지목록은 최대 24 시간을 주기로 갱신 후 공고합니다. 인증서 효력정지 및 폐지목록의 갱신 주기와 갱신 시점은 변경될 수 있으며, 변경이 발생하는 경우 당해 사실을 SignKorea 홈페이지(http://www.signkorea.com)에 공고합니다.

2.4 공고된 정보에 대한 책임

SignKorea는 본 준칙의 공고방법을 준수하지 않거나, 효력정지 또는 폐지된 인증서의 공고를 누락하여 가입자 또는 이용자에게 손해를 입힌 경우 법 제20조(손해배상책임)에 따른 책임을 집니다.

3. 신원확인

3.1 가입자 이름 표시 방법

SignKorea는 가입자를 구별하기 위해 ITU-T X.500에서 정한 DN(Distinguished Name)을 이용합니다.

SignKorea는 인증서의 발급에 있어 가입자에게 다음과 같은 법적 이름을 허용합니다. 단, SignKorea는 가입자가 별칭 등을 희망하는 경우에 한하여 인증서에 희망이름의 기재를 허용할 수 있습니다.

- 실명, 법인명 등 법적 이름
- 특허청 또는 국제적으로 이와 동등한 기관으로부터 받은 상표권 등(증명서 필요)
- 인터넷 도메인명
- 인터넷 IP 주소
- WWW용 URL
- 전자우편 주소 등

SignKorea는 가입자가 제출한 이름 및 기타 정보 등을 DN으로 구성하여 인증서에 저장합니다. DN은 이용자가 인증서를 확인할 때 기준정보가 되므로 신규 가입자의 DN과 기존 가입자의 DN의 중복성을 확인하여 중복되지 않는 경우에만 인증서를 발급합니다.

SignKorea는 DN이 중복되는 경우에 가입자에게 새로운 DN을 요청하며, 가입자는 SignKorea의 인증서비스에 가입하려면 이에 응해야 합니다. SignKorea는 다양한 이름을 수용하기 위해 특별한 해석규칙을 적용하지 않습니다.

3.2 인증서 신규 발급 시 신원확인

SignKorea 또는 등록대행기관은 인증서를 발급 받고자 하는 자의 신원을 확인하는 때에는 직접 대면(운영기준에 적합한 것으로 인정받은 직접 대면에 준하는 비대면 방법을 포함)하여 실지명의 여부를 확인하고, 신원확인증표에 의하여 본인임을 확인합니다. 다만,

“금융실명거래 및 비밀보장에 관한 법률”에 따른 금융기관에서 실지명의가 확인된 전자금융거래 가입자가 인증서를 발급받으려는 경우에는 정보통신망을 통하여 신원을 확인할 수 있습니다.

3.2.1 대면 신원확인 방법

SignKorea 또는 등록대행기관이 인증서를 발급받고자 하는 자(법인인 경우 대표자)의 신원을 확인하는 때에는 그 자의 명의가 시행규칙 제5조(실지명의 기준의 신원확인 방법)에 의한 실지명의인지 여부를 확인하고, 같은 조에 따른 신원확인증표에 의하여 본인임을 확인합니다.

법인이 대리인을 통하여 신청하는 경우에는 법인의 신원확인증표 외에 대리인의 신원확인증표, 법인 대표자의 위임장, 법인인감증명서를 추가로 확인합니다.

3.2.2 대면에 준하는 비대면 신원확인 방법

SignKorea 또는 등록대행기관은 금융위원회의 「비대면 실명확인 가이드라인」을 준용하여 대면에 준하는 비대면 실명확인 방법으로 인증서를 발급받고자 하는 자의 신원을 확인할 수 있습니다.

신청자가 사업자이고 대표자가 직접 신청하는 경우 아래의 방법으로 신원을 확인할 수 있습니다.

① 본인 명의 휴대폰 인증을 통한 신원확인
- 신청자의 본인 명의 휴대폰 인증을 통해 인적사항을 확인합니다.
- 신청자가 제출한 본인확인수단 관련 정보를 SignKorea로 전송한 뒤 신청자는 SignKorea로부터 본인확인정보 검증결과를 수신하고, 그 결과에 따라 절차를 진행합니다.

② 신원확인증표 촬영본을 통한 신원확인
- 신원확인증표의 촬영본이 원본과 동일함을 확인합니다.
- 신원확인방법은 신원확인증표의 진위를 확인할 수 있는 공공 사이트를 통하여 진위여부를 확인합니다.

③ 계좌인증에 의한 신원확인
- 신청자의 은행계좌를 통해 소액을 송금하거나 송금 받도록 하는 방식입니다.
- 해당 계좌가 신청자 명의의 계좌인지 여부, 신청자가 해당 계좌를 조회하거나 송금할 권한을 보유한 실제 권리자인지 여부를 확인합니다.

④ 서류제출에 의한 신원확인
- 사업자의 신원확인을 위해 사업자등록증명을 제출합니다. 법인의 경우 법인등기사항증명서를 추가로 제출합니다.
- 제출하는 서류(원본 또는 원본과 동일성을 확인할 수 있는 서류)는 신청서 접수일 7일 이내 발급분으로 제한합니다.

신원확인 강화를 위해 안면인증에 의한 신원확인을 추가로 실시할 수 있습니다.

3.2.3 온라인 신원확인 방법

시행령 제9조(신원확인의 방법)에 따라「금융실명거래 및 비밀보장에 관한 법률」에 의한 실지명의가 확인된 전자금융거래 가입자를 대상으로 인증서를 발급하는 경우 그의 동의를 받아 정보통신망을 통하여 신원을 확인할 수 있으며, 확인하는 사항은 다음과 같습니다.

- 전자금융거래 가입자의 계정(ID)과 그 비밀번호 또는 계좌번호와 그 비밀번호
- 전자금융거래 가입자의 주민등록번호
- 금융기관이 전자금융거래를 위하여 가입자에게 제공한 일회용비밀번호(보안카드의 비밀번호 포함) 또는 가입자 본인만이 알 수 있는 두 가지 이상의 정보
- 위에서 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 제외

3.3 인증서 갱신발급, 재발급 및 변경 시 신원확인

3.3.1. 갱신발급 신원확인

SignKorea는 가입자가 SignKorea에 온라인으로 전자서명이 포함된 갱신신청서를 제출하면 새로운 유효기간의 인증서를 새로 발급합니다. 새로 발급된 인증서의 유효기간은 기존 유효기간의 잔여 유효기간을 포함합니다. 이때, 가입자에 대한 신원확인은 가입자의 전자서명을 검증하는 것으로 대신합니다.

3.3.2 재발급 신원확인

SignKorea는 재발급의 경우 가입자에 대한 신원확인은 3.2(인증서 신규발급 시 신원확인)에 준하여 처리합니다.

3.3.3 가입자 등록정보 변경 시 신원확인

SignKorea는 인증서 내에 반영된 가입자 정보의 변경 신청을 처리할 경우에는 3.2(인증서 신규발급 시 신원확인)의 절차를 따르며, 그 외 가입자 등록정보(주소, 전화번호, 전자우편주소 등) 변경 요청 시에는 가입자의 전자서명에 대한 검증으로 신원확인을 대체하여 SignKorea에 등록된 당해 정보를 변경할 수 있습니다.

3.4 인증서 효력정지・효력회복・폐지 시 신원확인

3.4.1 인증서 효력정지 시 신원확인

SignKorea 또는 등록대행기관은 3.2(인증서 신규발급 시 신원확인)에 준하여 가입자 신원을 확인합니다. 가입자가 효력정지 신청을 온라인으로 SignKorea에 신청한 경우에 SignKorea는 가입자의 전자서명으로 신원확인을 대체합니다.

3.4.2 인증서 효력회복 시 신원확인

등록대행기관은 3.2(인증서 신규발급 시 신원확인)에 준하여 가입자 신원을 확인합니다.

3.4.3 인증서 폐지 시 신원확인

등록대행기관은 3.2(인증서 신규발급 시 신원확인)에 준하여 가입자 신원을 확인합니다. 가입자가 폐지 신청을 온라인으로 SignKorea에 신청한 경우에 SignKorea는 가입자의 전자서명으로 신원확인을 대체합니다. 가입자가 SignKorea의 콜센터(1577-7337)로 신고한 경우 사전에 등록된 2가지 이상의 개인정보를 통하여 가입자 본인여부를 확인합니다.

4. 인증서 관리

4.1 인증서 발급 신청

4.1.1 발급 신청 주체

인증서 발급 신청은 개인 및 법인이 신청할 수 있으며, 개인은 본인이 직접 신청하여야 하며, 법인은 당해 법인의 임원 또는 직원이 대리하여 신청할 수 있습니다.

4.1.2 발급 신청 절차

SignKorea의 인증서를 발급 받으려는 자 또는 대리인(이하 “신청자”라 한다)은 신원확인 증표를 지참하고, SignKorea 또는 등록대행기관에 방문하여 인증서 신청서를 제출합니다. 단, 신청자가 SignKorea 및 등록대행기관 홈페이지 등을 통해 찾아가는 서비스(등록대행기관이 신청자를 직접 방문하는 서비스)를 요청할 경우, 등록대행기관이 신청자를 직접 방문하여 신청서를 접수합니다.

SignKorea가 대면에 준하는 비대면의 방법으로 가입자의 신원을 확인할 경우 발급신청에 필요한 신청서는 온라인에서 작성된 전자문서의 형태로, 신청서 이외의 신원확인에 관한 서류는 본 준칙 3.2.2에서 정하는 방식으로 제출 받을 수 있습니다.

제출된 인증서 신청서에 기재된 가입자 정보에 대한 확인 사항은 다음과 같습니다.

- 개인인증서 신청서
  - ○ 성명
  - ○ 주민등록번호
  - ○ 용도 및 등급

○ 전화번호
○ 전자우편주소
○ 기타 SignKorea가 필요로 하는 정보

- 법인인증서 신청서
○ 법인명
○ 사업자등록번호
○ 용도 및 등급
○ 사업자 대표 전화번호
○ 법인 사업장 주소
○ 담당자의 소속 및 직위
○ 담당자 이름 및 담당자 연락처
○ 담당자 전자우편
○ 기타 SignKorea가 필요로 하는 정보

- 서버인증서 신청서
○ URL 또는 IP
○ 용도 및 등급
○ 수량
○ 법인명
○ 사업자 대표 전화번호
○ 법인 사업장 주소
○ 담당자의 소속 및 직위
○ 담당자 이름 및 담당자 연락처
○ 담당자 전자우편
○ 기타 SignKorea가 필요로 하는 정보

4.2 인증서 발급 신청 처리

4.2.1 인증서 발급 신청 접수 및 처리 절차

SignKorea 또는 등록대행기관은 4.1(인증서 발급 신청)에 따른 발급 신청 접수 시 3.2(인증서 신규 발급 시 신원확인)에 따라 신청인에 대한 식별 및 확인을 진행합니다.

SignKorea는 발급 신청 처리 완료시, 인증서 발급을 위한 참조번호 및 인가코드를 신청인에게 부여합니다.

4.2.2 발급 신청에 대한 거절 기준

SignKorea는 가입자의 인증서 발급 신청에 대해 다음에 해당하는 경우 발급을 제한할 수 있습니다.

○ 타인의 명의를 도용하여 신청하였거나 그렇다고 의심되는 경우
○ 신청서에 허위 사실을 기재 또는 허위서류를 첨부하였거나 그렇다고 의심되는 경우
○ 등록대행기관의 업무상 또는 기술상 문제로 인증서를 발급하지 못하는 경우
○ 사고정보를 이용하여 신청 또는 발급하였거나 그렇다고 의심되는 경우
○ 단말기 지정 또는 추가인증 등에 실패한 경우

4.2.3 발급 신청 접수에 대한 처리 기간

SignKorea가 SignKorea의 시스템 또는 등록대행기관을 통해 가입자에게 발급한 참조번호 및 인가코드는 인증서의 종류에 따라 [표3]에서 정한 기간 동안만 유효합니다.

종류 / 발급가능기간	개인인증서	법인인증서	서버인증서
인증서 등록후	25일	25일	25일

[표3] 인증서 발급 가능 기간

단, SignKorea는 가입자가 제출한 정보의 정확성 및 신뢰성에 문제가 있거나 가입자가 인증서 발급 수수료를 지불하지 않는 경우에 인증서 발급을 지연하거나 거부할 수 있으며, 단체 가입 등 가입자의 규모가 큰 경우에는 처리기간이 지연될 수 있습니다.

4.2.4. 인증서 부정발급 방지

SignKorea는 인증서의 부정발급을 방지하기 위해 부정발급 상시 확인 체계를 운영합니다. SignKorea는 부정발급이 예상되는 이상징후를 상시 모니터링하고, 이상징후 발생 시 가입자의 연락처(전자우편 또는 휴대전화 번호)로 이상징후 발생 사실을 통지합니다. 통지를 받은 가입자가 부정발급을 인지하고 SignKorea로 연락하면 인증서 폐지 등 필요한 후속 조치를 취합니다.

4.3 인증서 발급 절차 및 보호조치

4.3.1 가입자의 인증서 발급 신청

가입자는 SignKorea 또는 등록대행기관이 제공하는 인증서 가입자 소프트웨어에 인증서 신청 등록시 부여받은 참조번호와 인가코드를 입력하여 전자서명생성정보와 전자서명검증정보를 생성하고 SignKorea에 인증서 발급을 신청합니다.

상기 발급 신청 과정 중 일부분은 SignKorea 또는 등록대행기관이 제공하는 인증서 가입자 소프트웨어에 의해 자동으로 처리될 수 있습니다.

4.3.2 인증서 발급

SignKorea 또는 등록대행기관은 인증서 발급 신청을 받은 후 인증서를 발급하기 위하여 가입자의 전자서명생성정보로 서명된 인증서 발급신청 정보를 검증함으로 전자서명생성정보가 가입자에게 유일하게 속함을 확인합니다.

SignKorea는 신청자의 DN과 전자서명검증정보를 SignKorea의 전자서명생성정보로 전자서명하여 X.509 버전 3에 따른 인증서를 생성하고 신청자에게 발급한 후, 인증서를 디렉토리에 등재합니다.

4.3.3 가입자 정보의 전송 및 보호조치

SignKorea는 등록대행기관 또는 중계서비스기관을 통하여 인증서를 발급받고자 하는 자의 가입자 정보를 당해 기관과의 업무협약에 따라 정보통신망을 통해 전송받으며, 개인정보를 포함한 가입자 정보는 전자서명 및 암호화를 적용하여 기밀성, 무결성 등을 보장하며, 중계서비스기관을 통하는 경우 중계서비스기관에는 개인정보를 저장하지 않습니다.

4.4 인증서 수령

신청자는 관리프로그램을 통해 SignKorea가 생성한 인증서를 전달받아 인증서와 자신의 전자서명생성정보를 저장할 매체를 선택하고 이를 안전하게 저장해야 합니다. 가입자가 인증서를 인수하는 것은 인증서의 생성시점부터 유효기간 동안 이용자와 SignKorea에게 다음 내용이 사실임을 보증하는 것을 의미합니다.

○ 어떠한 불법 이용자도 가입자의 전자서명생성정보에 접근하지 않았다.
○ 인증서 내의 모든 정보에 대하여 SignKorea가 확인한 사항은 사실이다.
○ 인증서 내의 정보이외에 가입자가 SignKorea에게 통보한 사항은 사실이다.
○ SignKorea가 준칙에서 정한 범위내에서만 인증서를 이용한다.

SignKorea의 인증서를 인수한 신청자는 SignKorea의 가입자가 됩니다. 신청자가 SignKorea의 인증서를 인수하는 것은 SignKorea 및 이용자에게 다음의 원인으로 인한 피해를 입히지 않으며, 그 피해에 대한 보상에 동의하는 것을 의미합니다.

○ 가입자 또는 그 대리인의 허위사실 제공
○ 가입자의 태만 또는 악의로 인한 중요사실의 통보 미비
○ 가입자의 전자서명생성정보 분실・훼손 또는 도난・유출

SignKorea는 가입자의 대리인에 의해서 인증서가 인수된 경우에 가입자와 대리인 모두 상기내용에 대해 동의한 것으로 간주합니다.

4.5 인증서 이용

이용자는 가입자의 인증서를 이용 시 1.3.4.1(이용자의 책임과 의무)의 내용을 준수해야 합니다.

4.6 인증서 갱신발급

4.6.1 갱신 발급 요건

인증서 갱신 발급은 인증서의 유효기간이 만료되기 최대 2개월 전부터 유효기간 만료일까지 전자서명정보와 유효기간이 갱신된 새로운 인증서를 발급하는 것을 말합니다. SignKorea는 갱신처리 과정에서 유효기간 정보와 가입자의 전자서명생성정보는 변경되며 기존의 인증서는 폐지됩니다.

4.6.2 인증서의 갱신발급 및 등재

SignKorea 또는 등록대행기관은 인증서 갱신 발급 신청을 받은 후 인증서를 발급하기 위하여 가입자의 전자서명생성정보로 서명된 인증서 발급신청 정보를 검증함으로 전자서명생성정보가 가입자에게 유일하게 속함을 확인합니다.

SignKorea는 가입자의 갱신된 인증서를 발급하는 즉시 해당 인증서를 디렉토리에 등재하며, 기존 인증서는 디렉토리에서 삭제됩니다.

4.6.3 갱신신청 기간

SignKorea는 가입자 인증서의 유효기간 만료가 최대 2개월 남은 시점부터 갱신 신청을 처리하는 것을 원칙으로 합니다. 다만, SignKorea는 가입자의 편의 등을 고려하여 신청기간을 조정할 수 있습니다.

4.6.4 가입자 정보의 전송 및 보호조치

인증서 갱신 발급 시 가입자 정보의 전송은 4.3.3(가입자 정보의 전송 및 보호조치)을 준하여 처리합니다.

4.6.5 가입자 이름 표시 방법

인증서 갱신 발급 시 가입자 구분을 위한 DN은 3.1(가입자 이름 표시 방법)을 준하여 처리합니다.

4.6.6 인증서의 수령

갱신 발급된 인증서의 수령은 4.4(인증서의 수령)을 준하여 처리합니다.

4.7 인증서 재발급

4.7.1 재발급 요건

SignKorea는 다음의 사유에 해당하는 경우 인증서를 재발급합니다.

○ 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출되어 해당 인증서를 폐지하고 잔여 유효기간으로 새로운 인증서를 발급하는 경우
○ 가입자의 인증서 유효기간 만료 후 새로운 인증서를 발급하는 경우

SignKorea는 1.4 (인증서 종류)의 [표2] (인증서 유효기간)에 따라 유효기간을 설정하고, 새로운 전자서명검증정보에 대해 전자서명하여 새로운 인증서를 생성하여 가입자에게 발급합니다.

4.7.2 재발급 절차

4.7.2.1 재발급 신청

재발급 신청은 4.1(인증서 발급 신청)을 따릅니다.

4.7.2.2 인증서 발급

인증서 재발급은 4.3.2(인증서 발급)을 준하여 처리합니다.

4.7.2.2 가입자 정보의 전송 및 보호조치

인증서 재발급 시 가입자 정보의 전송은 4.3.3(가입자 정보의 전송 및 보호조치)을 준하여 처리합니다.

4.7.2.3 가입자 이름 표시 방법

인증서 재발급 시 가입자 구분을 위한 DN은 3.1(가입자 이름 표시 방법)을 준하여 처리합니다.

4.7.3 인증서의 수령

재발급된 인증서의 수령은 4.4(인증서의 수령)을 준하여 처리합니다.

4.8 인증서 변경

4.8.1 가입자 등록정보 변경 요건

가입자 등록정보 변경은 인증서 내에 반영된 가입자 정보의 변경의 경우는 3.2(인증서 신규발급 시 신원확인)절차를 따르며 그 외의 가입자 등록정보(주소, 전화번호, 전자우편주소 등)가 변경된 경우는 가입자가 등록정보 변경을 요청하여 SignKorea에 등록된 당해 정보를 변경시킬 수 있습니다.

4.8.2 가입자 등록정보 변경 신청

가입자는 SignKorea 홈페이지를 통하여 가입자 정보의 변경을 신청할 수 있으며, SignKorea는 가입자의 전자서명에 대한 검증으로 가입자의 신원확인을 합니다.

SignKorea는 정보통신망을 통하여 가입자 정보 변경 신청을 받는 경우, 가입자의 전자서명 및 암호화를 적용하여 가입자 정보의 기밀성, 무결성 등을 보장합니다.

4.8.3 가입자 이름 표시 방법

인증서 변경 발급 시 가입자 구분을 위한 DN은 3.1(가입자 이름 표시 방법)을 준하여 처리합니다.

4.8.4 인증서의 수령

가입자는 등록정보가 변경된 인증서를 수령하기 위해 4.4(인증서의 수령)을 준하여 처리합니다.

4.9 인증서 효력정지・효력회복・폐지

4.9.1 인증서 효력정지

4.9.1.1 효력정지 요건

SignKorea는 다음과 같은 경우에 인증서의 효력을 즉시 정지시킵니다.

○ 가입자가 인증서의 효력정지를 신청하는 경우

SignKorea는 다음의 경우에는 인증서의 효력을 정지할 수 있습니다.

○ 가입자의 전자서명생성정보에 대한 분실・훼손 또는 도난・유출이 의심되는 경우

SignKorea는 인증서비스 운영상 부득이한 사유가 발생한 경우에는 인증서를 일정시간 정지시킬 수 있습니다.

SignKorea는 인증서의 효력정지 상태를 효력정지 후 6개월까지만 유지할 수 있으며, 6개월 이상 지속되는 경우에는 인증서를 폐지시킵니다. 단, 효력정지 기간 중에 유효기간이 만료되는 경우에는 일반 인증서의 유효기간 만료와 동일하게 간주합니다.

4.9.1.2 효력정지 신청인

가입자 또는 그 대리인만이 인증서의 효력정지를 신청할 수 있습니다.

4.9.1.3 효력정지 신청 절차

SignKorea의 인증서를 소유하고 있는 가입자는 등록대행기관에 방문하지 않고 인증서 관리프로그램을 통해 온라인으로 효력정지를 할 수 있으며, 가입자의 사유로 온라인 신청이 불가능한 경우에는 등록대행기관을 통해 효력정지를 신청할 수 있습니다.

SignKorea는 등록대행기관 또는 중계서비스기관을 통하여 인증서의 효력정지를 하고자 하는 자의 가입자 정보는 정보통신망을 통하여 받는 경우, 전자서명 및 암호화를 적용하여 가입자 정보의 기밀성, 무결성 등을 보장합니다.

4.9.1.4 영향

SignKorea는 가입자가 인증서의 효력을 정지시키는 경우에 인증서의 유효기간 및 종류에 상관없이 그 효력을 신속하게 정지시키지만, 가입자가 정지 이전에 행한 계약 또는 법적 행위의 효력과 의무사항에는 영향을 주지 않습니다.

4.9.2 인증서 효력회복

4.9.2.1 효력회복 요건

SignKorea는 가입자가 인증서 효력정지 후 6개월 이내에 인증서의 효력을 유효한 상태로 변경하기 위해 SignKorea에 인증서 효력회복을 신청한 경우와, SignKorea가 인증서비스 운영상의 부득이한 사유로 효력을 정지시킨 인증서의 효력을 회복해야 하는 경우에 인증서의 효력을 지체없이 회복합니다.

4.9.2.2 효력회복 신청 절차

SignKorea는 효력정지된 인증서의 전자서명검증정보에 합치하는 전자서명생성정보로 만들어진 전자서명은 법적효력이 없는 것으로 간주하기 때문에 가입자는 효력회복을 SignKorea에 온라인으로 신청 할 수 없습니다. 그러므로 가입자는 SignKorea 또는 등록대행기관에 방문하여 효력회복을 신청해야 합니다.

4.9.3 인증서 폐지

4.9.3.1 폐지 요건

SignKorea는 다음의 사유에 해당하는 경우 가입자의 인증서를 폐지합니다.

○ 가입자가 인증서 폐지를 신청하는 경우
○ 가입자의 전자서명생성정보에 대한 분실・훼손 또는 도난・유출된 사실을 인지한 경우

○ 가입자의 사망・실종선고 또는 해산사실을 인지한 경우
○ 가입자가 타인의 명의 도용 등 부정한 방법으로 인증서를 발급받은 사실을 인지한 경우
○ 가입자가 1.3.2.1(가입자의 책임과 의무)에 따른 준칙의 의무사항을 위반한 경우
○ 가입자의 의무사항 준수가 천재지변 및 기타 원인으로 인해 지연되거나 불가능한 경우
○ 착오로 인한 인증서 발급
○ 가입자가 인증서 효력정지 신청일로부터 6개월 내에 효력회복을 신청하지 않은 경우
○ 가입자의 인증서가 사고정보를 이용하여 발급된 사실을 인지한 경우
○ 가입자가 인증서 분실, 부정발급 등으로 SignKorea 콜센터(1577-7337)로 신고하는 경우 등

4.9.3.2 폐지 신청 절차

SignKorea의 인증서를 소유하고 있는 가입자는 등록대행기관에 방문하지 않고 관리프로그램을 통해 온라인으로 폐지 신청을 할 수 있으며, 가입자의 사유로 온라인 신청이 불가능한 경우에는 등록대행기관 또는 SignKorea 콜센터(1577-7337)를 통해 폐지 신청을 할 수 있습니다.

SignKorea 콜센터(1577-7337)를 통한 폐지 신청 접수는 개인용 인증서 가입자에 한합니다.

SignKorea 콜센터(1577-7337)를 통한 폐지는 3.4.3(인증서 폐지 시 신원확인)에 준하여 신원확인 후, 폐지합니다. 폐지된 인증서의 인증서폐지목록(CRL) 등재는 4.9.4(인증서 효력정지 및 폐지목록(CRL) 발행주기 및 공고 소요시간)에 준합니다.

SignKorea는 등록대행기관, SignKorea 콜센터(1577-7337) 또는 중계서비스기관의 정보통신망을 통하여 폐지를 하는 경우, 가입자의 등록정보에 대해 암호화를 적용하여 가입자 정보의 기밀성, 무결성 등을 보장합니다.

4.9.3.3 영향

SignKorea는 가입자가 인증서의 효력을 폐지시키는 경우에 인증서의 유효기간 및 종류에 상관없이 그 효력을 신속하게 폐지시키지만, 가입자가 폐지 이전에 행한 계약 또는 법적 행위의 효력과 의무사항에는 영향을 주지 않습니다.

4.9.4 인증서 효력정지 및 폐지목록(CRL) 발행주기 및 공고 소요시간

인증서 효력정지 및 폐지목록(CRL)은 최대 24시간 단위로 발행하며, 발행시점에 즉시 공고하는 것을 원칙으로 합니다.

4.10 인증서 유효성 확인 서비스(OCSP)

4.10.1 이용 방법

인증서 유효성 확인 서비스(이하 “OCSP”라 한다) 신청자 또는 그 대리인은 서비스 가입을 위해, 사전에 SignKorea에게 이용 등록 신청을 하여야 합니다. OCSP 서비스 가입자 또는 이용자는 SignKorea에서 제공받은 OCSP 클라이언트 소프트웨어 또는, 자신이 보유하고 있는 OCSP 요청 처리가 가능한 소프트웨어를 이용하여 OCSP 요청을 합니다.

4.10.2 이용 조건

SignKorea에서 제공하는 OCSP와 OCSP 클라이언트 소프트웨어는 원칙적으로 유료이며, 이용 요금은 별도의 협의를 통해서 책정됩니다. 또, 가입자 또는 이용자가 온라인상에서 OCSP 요청시 자신의 전자서명생성정보와 인증서로 전자 서명함을 원칙으로 하고 있으며, 표준화된 처리를 위해 OCSP 요청시 RFC2560을 준수하여야 합니다.

4.10.3 이용 계약 해지

OCSP 서비스 가입자 또는 이용자는 SignKorea와 별도의 절차를 거쳐서 이용 계약 해지를 할 수 있습니다.

4.11 서비스 가입 철회

가입자는 인증서비스의 가입을 철회할 수 있습니다. 가입자가 인증서비스 철회를 신청하면 해당 인증서는 즉시 폐지되며, 가입자의 개인정보는 5.5(기록 보존)에 따라 인증서의 효력이 소멸된 날로부터 10년 동안 보관 후 파기합니다.

4.12 기타 부가 서비스

4.12.1 시점확인서비스

SignKorea는 가입자 또는 이용자가 전자문서에 대한 시점확인을 신청하는 경우, 시점확인 서비스를 제공할 수 있습니다. 단, 이용 요금 및 기타 비용은 원칙적으로 유료이며, 구체적인 이용 조건 및 이용 계약 해지는 SignKorea와 별도의 협의를 통해서 정해집니다.
SignKorea는 시점확인시 정확한 국제표준 시각정보를 제공하기 위하여 위성시각수신 장비를 운영합니다.

4.12.2 클라우드 공동인증서비스

클라우드 공동인증서비스는 가입자(타인증기관 가입자 포함)가 클라우드에 가입자 인증서(전자서명생성정보 포함)를 보관하고, 등록된 PC, 모바일 등 다양한 매체에서 인증서를 편리하게 사용하는 서비스입니다.

5. 시설 및 운영 관리

5.1 물리적 보호조치

5.1.1 시설 위치와 구조에 관한 사항

5.1.1.1 시설 위치

SignKorea의 인증시스템을 위한 시설의 위치는 아래와 같습니다.

○ 인증시스템 메인센터 전산실 및 인증 콜센터
- 14119 경기도 안양시 동안구 엘에스로 115번길 26 (호계동)

○ 인증시스템 DR(재해복구) 전산실
- 07329 서울특별시 영등포구 여의나루로 76 (여의도동)

5.1.1.2 시설 구조

SignKorea는 인증서비스 전용의 네트워크, 설비 및 전산실을 운영합니다.

5.1.2 다중출입, 침입감지·경보 및 감시·통제 등 물리적 보호조치에 관한 사항

○ 출입통제 시스템은 신원확인카드, 지문인식 및 무게감지 장치 등을 다중으로 결합하여 통제구역에 대한 접근을 통제한다.
○ 출입통제 시스템과 연계하여 통제구역 출입 내역을 기록하고 정기적으로 그 기록을 검사한다.
○ 이상 상황이 발생하는 경우에 대비하여 다음과 같은 시스템을 설치하고 경보 기능을 갖는 감시통제시스템을 설치·운영한다.
- CCTV 카메라 및 모니터링시스템
- 침입감지시스템
○ 보안경비요원을 배치하여 24시간 보안경비업무를 수행한다.

5.1.3 물리적 잠금장치에 관한 사항

핵심인증시스템은 물리적 접근통제를 위하여 물리적 잠금장치가 있는 보안캐비닛 내에 설치합니다.

5.1.4 화재, 수재, 정전방지 및 방호에 관한 사항

SignKorea는 갑작스러운 정전으로 인한 심각한 피해를 방지하기 위하여 무정전전원공급장치를 이용하며, 별도의 발전기를 설치하여 안정적으로 전원을 공급합니다.

SignKorea는 침수에 대한 핵심인증시스템 등 중요 시스템의 보호를 위하여 바닥으로부터 30cm이상의 위치에 설치합니다.

SignKorea는 화재에 대한 핵심인증시스템 등 중요 시스템의 보호를 위하여 화재 탐지기를 설치하고, 소화시 시스템의 기능에 문제를 야기하지 않는 성분의 휴대용 소화기 및 자동소화설비 등을 설치하였습니다.

5.1.5 항온·항습, 통풍 및 기타 보호설비에 관한 사항

SignKorea는 핵심인증시스템 등 중요 시스템의 보호를 위하여 온도 및 습도를 일정하게 유지하기 위한 항온항습장치를 설치 및 운영하고 있습니다.

5.1.6 시설 및 장비의 폐기처리 절차에 관한 사항

SignKorea는 시설 및 장비 등을 폐기하는 경우에 정보 복구가 불가능한 방법으로 폐기합니다.

5.1.7 원격지 백업설비 안전운영에 관한 사항

SignKorea는 인증서 등의 중요 정보의 원격지 보관을 위해 SignKora 인증센터와 10Km 이상 떨어진 곳에 원격지 백업설비를 운영하고 있으며, 출입통제 시스템, 침입감시시스템 등 보호설비를 구축하여 운영하고 있습니다.

5.2 절차적 보호조치

5.2.1 인증업무에 대한 업무 분장 및 담당자 현황

SignKorea는 인증업무의 안전·신뢰성을 확보하기 위하여 업무를 담당자 역할별로 분리하여 수행하며, SignKorea의 업무 및 담당자는 아래를 포함합니다.

○ 책임자 : 전자서명 인증업무 책임자, 정책 관리자
○ 업무 운영자 : CA 운영자, 키생성 관리자, 시점확인 운영자, OCSP 운영자, 클라우드 공동인증 운영자, 공고 운영자
○ 시스템 및 보안 관리자 : 시스템 관리자, 설치 관리자, 보안 관리자
○ 감사자 : IT감사자

5.2.2 동일인에 의해 동시 수행될 수 없는 인증업무

SignKorea의 인증업무의 업무분리 원칙은 아래를 포함합니다

○ 상기 5.2.1의 “책임자” 업무를 수행하는 인력은 “업무 운영자”, “시스템 및 보안 관리자”, “감사자” 업무 중 1개 이상을 동시에 수행할 수 없습니다.

○ 상기 5.2.1의 “업무 운영자” 업무를 수행하는 인력은 “책임자”, “시스템 관리자”, “설치 관리자”, “IT감사자” 업무 중 1개 이상을 동시에 수행할 수 없습니다.
○ 상기 5.2.1의 “시스템 관리자” 또는 “설치 관리자” 업무를 수행하는 인력은 “책임자”, “업무 운영자”, “IT감사자” 업무 중 1개 이상을 동시에 수행할 수 없습니다.
○ 상기 5.2.1의 “보안 관리자” 업무를 수행하는 인력은 “책임자”, “IT감사자” 업무 중 1개 이상을 동시에 수행할 수 없습니다.
○ 상기 5.2.1의 “IT감사자” 업무를 수행하는 인력은 “책임자”, “업무 운영자”, “시스템 및 보안 관리자” 업무 중 1개 이상을 동시에 수행할 수 없습니다.

5.2.3 인증업무 담당자 인증방법

(주)코스콤 또는 SignKorea는, 신뢰자가 되려는 자에 대한 신원 확인 과정을 수행합니다. 이 과정은 (주)코스콤 또는 SignKorea 채용 담당자의 대면확인과 신분증 또는 신분관련 문서 확인 등을 포함합니다. 추가적인 신원 확인은 당 준칙 5.3.1(인증업무 인력의 자격, 경력 등 요구사항 및 신원확인 절차)에 정해진 바에 따릅니다.

SignKorea는 상기 과정을 통과한 신뢰자에게만 인증업무를 할당하며, 이후 해당 인원에 대해 할당 업무 수행에 필요한 아래의 항목을 제공 또는 부여합니다.

○ 출입용 카드키 등 접근장치
○ 접근이 필요한 공간에 대한 출입 권한
○ 시스템 접근 및 작업 수행을 위한, 계정 및 패스워드 등의 전자적 권한

5.3 인적 보안

5.3.1 인증업무 인력의 자격, 경력 등 요구사항 및 신원확인 절차

SignKorea는 신원을 조회하여 이상이 없는 임직원만 인증 및 보안 관련 업무를 수행하도록 하며, 인증서비스에 관련된 모든 종업원, 협력업체, 자문인력 등과 일부 영업담당, 시스템 관리담당, 지정된 엔지니어 및 SignKorea의 시스템 기반구조 감독을 책임지는 경영진을 대상으로 인적 통제를 수행합니다.

법 제8조 제3항의 결격사유에 해당되는 자는 SignKorea의 임원이 될 수 없습니다.

5.3.2 업무 수행 인력의 교육 및 업무순환에 관한 사항

SignKorea는 업무 수행 인력에 대해 년 1회 이상 외부 또는 내부 정보보호 교육을 이수하도록 하고 있습니다.

5.3.3 비인가된 행위에 대한 처벌에 관한 사항

소속직원의 비인가된 행위에 대하여 코스콤은 인사규정 등 내부 규정이 정하는 바에 따

라 해당 직원을 징계합니다.

5.4 감사 기록

5.4.1 감사기록의 유형 및 보존기간

SignKorea는 다음 로그기록에 대하여 백업한 날로부터 2년 이상 보관합니다. 단, “5.5.1 보존되는 기록의 유형 및 보존기간”에서 10년 보존 대상으로 언급된 항목은 5.5.1에 따릅니다.

○ 인증시스템 서비스 제공기록 및 네트워크 로그기록
○ 출입통제 시스템의 출입관련 감사기록
○ CCTV 시스템의 기록

5.4.2 감사기록 보호조치

SignKorea는 물리적 접근통제와 논리적 접근통제를 통해 감사기록에 대한 접근을 제한하며, 감사기록 중 주요 개인정보에 대해서는 암호화하여 보관합니다.

5.4.3 감사기록 백업주기 및 절차

SignKorea는 인증시스템 중 온라인시스템의 감사기록은 주 1회 이상, 오프라인 시스템과 기타 시스템은 월 1회 이상 백업합니다.

5.5 기록 보존

5.5.1 보존되는 기록의 유형 및 보존기간

SignKorea는 민법, 상법 등 관계 법령에 따라 가입자인증서와 그 효력정지 및 폐지에 관한 기록 등을 당해 인증서의 효력이 소멸된 날부터 10년 동안 보관합니다.

SignKorea는 클라우드 공동인증서비스를 탈퇴한 가입자(1년 이상 미사용한 가입자 포함)의 경우 탈퇴한 날부터 1년 동안 관련 기록을 보관합니다. 단, 민원, 분쟁, 소송 발생 시 법령에 따라 요구되는 기간 동안 또는 해결 시점까지 보관할 수 있습니다.

5.5.2 보존기록의 보호조치

SignKorea는 보존기록에 대해 엄격한 물리적 접근통제 및 절차통제를 적용하여 보안을 유지하고 업무범위에 한해 조회가 가능하도록 합니다. 또한 보존기록의 훼손 및 변질을 방지하기 위해 보존장소에 항온항습기를 설치하고 화재의 발생에 대비하여 화재경보기 등의 보호설비를 설치하여 운영합니다.

5.5.3 보존기록의 백업주기 및 백업절차

SignKorea는 보존기록의 손실과 파괴에 대비하여 복사본을 만들어 물리적으로 격리된 안전한 장소에 저장하는 것을 원칙으로 하며, 이를 위한 백업주기는 월 1회 이상입니다.

5.6 전자서명인증사업자의 전자서명생성정보 갱신

5.6.1 갱신 절차

SignKorea 인증서 유효기간 만료 또는 전자서명인증체계 내의 필요에 의해 SignKorea 인증서를 갱신할 수 있습니다. 갱신 절차는 전자서명인증업무 운영기준을 준수하여 갱신합니다.

5.6.2 갱신 인증서 배포 절차

가입자의 인증서의 안전한 사용을 위해 다음과 같은 절차를 통해 SignKorea 인증서를 배포합니다.

○ 최상위인증기관의 SignKorea 인증서 갱신
○ 갱신된 인증서 수령
○ SignKorea 디렉토리 서버에 갱신된 인증서 게시
○ 각 인증기관에 갱신 통보 및 갱신된 인증서 전달
○ 인증서 이용 기관에 갱신 통보 및 갱신된 인증서 전달
○ 갱신된 인증서 배포 후, 갱신된 전자서명생성정보로 가입자 인증서 발급

5.7 장애 및 재난 복구

5.7.1 인증업무 장애 및 재난 유형별 처리 및 복구 절차

SignKorea는 인증 시스템 및 설비의 장애가 발생한 경우, 2중(또는 다중)으로 설치된 시스템 및 설비를 이용하여 신속하게 복구합니다.

SignKore는 주요 데이터의 손실이 발생하였을 경우 백업된 데이터를 이용하여 복구합니다.

SignKorea는 전자적 침해사고 발생시 코스콤 사내 정보보호 관련 조직과 협력하여 대응 및 조치를 취하고, 필요한 경우 한국인터넷진흥원 또는 금융보안원과 공조합니다.

SignKorea는 장애 또는 재난 상황의 심각성에 따라, 인증업무 운영 조직 외 코스콤 사내의 여러 조직이 참여하는 위기상황대응반을 구성하여 대응합니다.

5.7.2 전자서명인증업무 장애방지 등 연속성 보장 대책

SignKorea는 인증서생성관리, 디렉토리, 실시간 인증서 유효성 확인, 시점확인 등 시스템 이중화, 네트워크 경로 이중화 등을 통해서 인증업무의 연속성을 보장하고 있습니다.

5.8 업무 휴지, 폐지, 종료

자연재해 또는 천재지변이 아닌 SignKorea의 불가피한 사정으로 인하여 인증서비스의 전부 또는 일부를 휴지 또는 폐지, 종료하는 경우에 SignKorea는 법 제15조(전자서명인증업무준칙의 준수 등) 제2항 내지 제3항에 의거 휴지기간 및 휴지일과 폐지일을 정하고 휴지는 휴지일 30일전에, 폐지는 폐지일 60일전에 가입자에게 해당사실을 SignKorea의 홈페이지에 공고하고, 가입자가 인증서 신청 시 등록한 전자우편을 통해 통보합니다.

6. 기술적 보호 조치

6.1 전자서명생성정보 보호

SignKorea는 안전하고 신뢰성 있는 전자서명 알고리즘을 이용하기 위하여 다음과 같은 크기의 키 및 해쉬값을 이용합니다.

○ KCDSA 및 RSA 경우 : 2,048 비트 이상
○ ECDSA 경우 : 224 비트 이상
○ SHA-256 경우 : 256 비트 이상

6.2 전자서명생성정보 보호조치

6.2.1 저장장치

SignKorea는 SignKorea의 전자서명생성정보를 안전하게 저장하기 위하여 봉인, 접근권한 확인 및 전자서명생성정보 유출·변경 방지 기능을 갖춘 저장장치에 암호화하여 저장합니다.

6.2.2 생성. 이용 후 안전한 삭제 방법

SignKorea는 SignKorea의 전자서명생성정보의 생성이 종료된 즉시 시스템 메모리에서 전자서명생성정보를 삭제하고, 전자서명생성정보를 이용할 때 외부노출 위험을 최소화합니다.

6.2.3 파기 방법

SignKorea는 SignKorea 인증서의 유효기간이 만료되거나 전자서명생성정보가 훼손·유출되었을 경우에 해당 전자서명생성정보가 저장된 매체에서 전자서명생성정보를 물리적 논리적으로 복구가 불가능한 방법으로 안전하게 파기합니다.

6.2.4 전자서명검증정보의 이용기간

SignKorea는 해당 전자서명검증정보의 인증서가 유효한 동안에 한해 전자서명생성정보와 전자서명검증정보를 이용합니다.

6.3 전자서명생성정보 및 전자서명검증정보의 관리

SignKorea는 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되는 안전한 키 생성시스템에서 인가된 자만이 SignKorea의 전자서명생성정보와 전자서명검증정보 및 인증서 요청양식을 생성할 수 있도록 합니다.

6.4 데이터 보호 조치

인증서 발급, 시점확인, 인증서 유효성 확인 서비스 등을 위한 SignKorea 전자서명생성정보의 생성은, 전자서명생성정보 유출·변경 방지 기능을 갖춘 장치에서 3인 이상이 공동으로 수행합니다.

SignKorea 는 해당 전자서명생성정보의 훼손, 손실에 대비하여 백업을 수행합니다. 백업 시에도, 전자서명생성정보 유출·변경 방지 기능을 갖춘 장치를 이용합니다. 전자서명생성정보의 백업은, 백업매체를 통해 자동으로 수행합니다.

6.5 시스템 보안 통제

SignKorea는 시스템에 대한 물리적·논리적인 접근을 통제하고 있으며, 원격 시스템 접속을 통한 작업을 원칙적으로 금지하고 있습니다. 또한 시스템 작업시 최소 2인 이상이 공동작업을 수행하도록 규정하고 있습니다.

6.6 시스템 운영 관리

SignKorea는 형상관리시스템을 통해 인증S/W의 변경관리와 버전관리를 수행하고 있습니다.

6.7 네트워크 보호조치

SignKorea는 네트워크를 안전하게 운영하기 위하여 침입차단시스템과 침입탐지시스템을 설치하여 운영하고 있습니다.

6.8 시점확인서비스 보호조치

SignKorea는 시점확인 서비스 제공 시, 시점확인 서비스만을 위한 별도의 전자서명생성정보를 사용하고 있습니다.

SignKorea는 시점확인 서비스 시 정확한 국제표준 시각정보를 제공하기 위하여 위성시각수신 장비를 운영합니다.

6.9 클라우드 공동인증서비스 보호조치

SignKorea는 클라우드 공동인증서비스 제공 시, 서비스 이용자가 등록한 전자서명생성정보를 봉인, 접근권한 확인 및 전자서명생성정보 유출·변경 방지 기능을 갖춘 저장장치에 암호화하여 저장하고 있습니다.

SignKorea는 클라우드 공동인증서비스 제공 시, 서비스 이용자의 탈퇴 혹은 이용자 요청 즉시, 전자서명생성정보를 물리적 논리적으로 복구가 불가능한 방법으로 안전하게 파기합니다.

7. 인증서 형식

7.1 인증서 형식

SignKorea에서 발급하는 인증서는 아래와 같은 사항을 포함하며, 인증서의 프로파일은 [표4]와 같습니다.

○ 가입자의 이름(법인의 경우에는 명칭을 말한다)
○ 가입자의 전자서명검증정보
○ 가입자와 인증기관이 이용하는 전자서명 방식
○ 인증서의 일련번호
○ 인증서의 유효기간
○ 인증기관의 명칭등 인증기관임을 확인할 수 있는 정보
○ 인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항
○ 가입자가 제3자를 위한 대리권등을 갖는 경우 또는 직업상 자격 등의 표시를 요청한 경우 이에 관한 사항
○ 인증서임을 나타내는 표시

■ 기본필드

	필드명	ASN.1 type	Note	지원여부		비고
				생성	처리	
1	버전	INTEGER	0x2(버전3)	m	m	
2	일련번호	INTEGER	자동할당	m	m	
3	서명 알고리즘	OID		m	m	
4	발급자		C(Country)는 printableString, 그 이외의 속성값은 utf8String	m	m	
	type	OID		m	m	
	value	printable 또는 utf8String		m	m	
5	유효기간		인증기관 CPS에 명시된 유효기간 준수	m	m	
	notBefore	UTCTime		m	m	
	notAfter	UTCTime		m	m	
6	소유자		C(Country)는	m	m	

	type	OID	printableString, 그이외의 속성값은 utf8String	m	m	
	value	printable 또는 utf8String		m	m	
7	소유자 공개키 정보			m	m	
	algorithm	OID		m	m	
	subjectPublicKey	BIT STRING		m	m	
8	인증서 확장 필드	Extensions		m	m	

■ 확장필드

	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	발급자 공개키 식별자			n	m	m	
	KeyIdentifier	OCTET STRING	발급자 인증서의 KeyID		m	m	
	authorityCertIssuer	GeneralNames			m	m	
	authorityCertSerialNumber	INTEGER			m	m	
2	소유자 공개키 식별자	OCTET STRING	subjectPublicKey 정보의 160비트 해쉬값	n	m	m	
3	키 사용 목적	BIT STRING	Digital Signature, non-Repudiation	c	m	m	
4	인증서 정책			b			[1]
	policyIdentifier	OID	인증기관 인증서 정책		m	m	
	policyQualifiers				m	m	
	PolicyQualifierId	OID	CPS, UserNotice		m	m	
	Qualifier				m	m	
	CPSuri	IA5String	인증기관 CPS 주소		m	m	
	UserNotice				m	m	
	NoticeReference	SEQUENCE			-	-	
	ExplicitText	BMPString	이 인증서는 공동인증서입니다		m	m	
5	인증서 정책 매핑			-	-	-	
	issuerDomainPolicy	OID					
	subjectDomainPolicy	OID					
6	소유자 대체 명칭	otherName	id-kisa-identifyData에 가입자 한글실명과 VID	n	m	m	
		rfc822Name	가입자 이메일 주소		o	m	[2]
7	발급자 대체 명칭	otherName	id-kisa-identifyData에 인증기관 한글실명	n	o	m	
8	확장 키 사용목적	OID	보안토큰 식별자(id-kisa-HSM)	n	o	o	[3]
9	기본 제한			-	x	x	
	cA	FALSE					
	pathLenConstraint	INTEGER					
10	정책 제한			-	-	-	
	requireExplicitPolicy	INTEGER					
	inhibitPolicyMapping	INTEGER					
11	명칭 제한			-	-	-	
12	인증서 효력정지 및 폐지목록 분배점			n	m	m	
	distributionPoint	DistributionPointName	CRL 획득 정보		m	m	[4]
	reasons	ReasonFlags			-	-	
	cRLIssuer	GeneralNames	간접CRL 발급시 사용		o	m	
13	발급자 정보 접근			n	m	m	[5]
	accessMethod	OID	id-ad-caIssuers, id-ad-ocsp		m	m	
	accessLocation	GeneralName			m	m	
[1]	전자우편 보안에 사용하고 하는 경우 non-critical 설정, 이외에 critical 설정						
[2]	전자우편 보안에 사용하고자 하는 경우 rfc822Name 생성						
[3]	보안토큰 기반일 경우 보안토큰 식별자(id-kisa-HSM) 사용						
[4]	uri 값으로 ldap://hostname[:portnumber]/dn[?attribute]형식 사용						
[5]	전자우편 보안에 사용하고자 하는 경우 id-ad-caIssuers 생성						

c : critical, n : non-critical, m : 생성, o : 선택 , x : 생성하지 않음

[표4] 가입자 전자서명용 인증서 프로파일

7.2 인증서 유효성 확인 정보 형식

SignKorea는 가입자의 인증서를 효력정지・효력회복・폐지하는 경우 [표5]과 같은 프로파일로 인증서 효력정지 및 폐지목록(CRL)을 생성하여 게시하고 있습니다.

■ 기본필드

	필드명	ASN.1 type	Note	지원여부		비고
				생성	처리	
1	버전	INTEGER	0x1(버전 2)	m	m	
2	서명 알고리즘	OID	자동할당	m	m	
3	발급자		C(Country)는 printableString, 그 이외의 속성값은 utf8String	m	m	
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	
4	발급일자	UTCTime	발급시점	m	m	
5	다음 발급일자	UTCTime	인증기관 정책에 따름	m	m	
6	효력정지 및 폐지 목록					[1]
	userCertificate	INTEGER		m	m	
	revocationDate	UTCTime		m	m	
	crlEntryExtensions	Extensions				[2]
7	인증서 효력정지 및 폐지 목록 확장필드	Extensions		m	m	[3]
[1]	효력정지 및 폐지된 인증서가 없을 경우는 Revoked Certificates 필드를 생성하지 않음					
[2]	CRL 엔트리 확장필드 참조					
[3]	CRL 확장필드 참조					

■ CRL 확장필드

	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	발급자 공개키 식별자			n	m	m	
	KeyIdentifier	OCTET STRING	인증기관 인증서의 KeyID				
	authorityCertIssuer	GeneralNames					
	authorityCertSerialNumber	INTEGER					
2	발급자 대체 명칭	otherName	id-kisa-identifyData에 인증기관 한글실명	n	o	m	
3	인증서 효력정지 및 폐지 목록 번호	INTEGER		n	m	m	
4	인증서 효력정지 및 폐지목록 발급분배점			c	m	m	
	DistributionPointName	IA5string			m	m	[1]
	onlyContainsUserCerts	BOOLEAN			-	-	
	onlyContainsCACerts	BOOLEAN			-	-	
	onlySomeReasons	BIT STRING			-	-	
	IndirectCRL	BOOLEAN			o	m	[2]
[1]	CRLDP(Certificate Revocation List Distribution Point)와 동일						
[2]	indirectCRL 를 사용할 때는 반드시 “TRUE”로 설정						

■ CRL 엔트리 확장필드

	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	효력정지 및 폐지 사유	ENUMERATED		n	m	m	
2	효력정지 시 수행 명령	OID		n	o	m	
3	효력정지 및 폐지 일자	UTCTime		n	o	m	
4	인증서 발급자	GeneralNames		c	o	m	

[표5] 가입자 전자서명용 인증서 효력정지 및 폐지목록(CRL) 프로파일

7.3 인증서 유효성 확인 서비스 형식

가입자의 인증서 유효성 확인 서비스(OCSP)에 사용되는 OCSP 서버용 인증서의 프로파일은 [표6]과 같습니다.

■ 기본필드 : 가입자 전자서명용 인증서 프로파일과 동일

■ 확장필드

	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	발급자 공개키 식별자		3가지 값을 모두 사용	n	m	m	
	KeyIdentifier	OCTET STRING			m	m	
	authorityCertIssuer	GeneralNames			m	m	
	authorityCertSerialNumber	INTEGER			m	m	
2	소유자 공개키 식별자	OCTET STRING	subjectPublicKey 정보의 160비트 해쉬값	n	m	m	
3	키 사용 목적	BIT STRING	Digital Signature, non-Repudiation	c	m	m	
4	인증서 정책			c			
	policyIdentifier	OID	인증기관 인증서 정책		m	m	
	policyQualifiers				m	m	
	PolicyQualifierId	OID	CPS, UserNotice		m	m	
	Qualifier				m	m	
	CPSuri	IA5String	인증기관 CPS 주소		m	m	
	UserNotice				m	m	
	NoticeReference	SEQUENCE			-	-	
	ExplicitText	BMPString			m	m	
5	인증서 정책 매핑			-	-	-	
6	소유자 대체 명칭	otherName	id-kisa-identifyData에 가입자 한글실명	n	m	m	
7	발급자 대체 명칭	otherName	id-kisa-identifyData에 발급기관 한글실명	n	o	m	
8	기본 제한			-	x	x	
9	정책 제한			-	-	-	
10	명칭 제한			-	-	-	
11	확장키 용도	OID		c	m	m	
12	인증서 효력정지 및 폐지목록 분배점			n	m	m	
	distributionPoint	DistributionPointName	CRL 획득 정보		m	m	[1]
	reasons	ReasonFlags			o	m	
	cRLIssuer	GeneralNames	간접CRL발급시 사용		o	m	
13	발급자 정보 접근			n	o	m	[2]
	accessMethod	OID	id-ad-caIssuers				
	accessLocation	GeneralName					
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 인증기관이 발급하는 경우에는 반드시 생성 시점확인용 인증서의 경우에는 사용하지 않음
[3]	OCSP 서버용 shortlived 인증서를 발행할 경우 사용 시점확인용 인증서의 경우에는 사용하지 않음

[표6] 인증기관 시점확인 및 OCSP 서버용 인증서 프로파일

8. 감사 및 평가

8.1 감사 및 평가 현황

SignKorea 전체 인증 업무, 시스템 H/W, S/W, 보호설비 등 전반적인 사항에 대해 매년 1회 법 제10조(평가기관)에 따른 평가기관(법 제11조에 따른 국제통용평가 수행기관 포함)으로부터 전자서명인증업무 운영기준 준수 여부에 대한 평가를 받습니다. 또한 정보통신망법에 따라 방송통신위원회의 본인확인기관 정기점검을 수검합니다.

위와 별도로, 연 1회 전자서명인증업무에 대한 내부 감사를 실시합니다.

8.2 평가자의 신원, 자격

8.1(감사 및 평가 현황)에서 평가기관의 평가자 신원 및 자격은 시행령 제5조(평가기관의 선정기준 및 절차 등)를 따릅니다.

내부 감사는 전문성을 갖춘 인력으로 평가자를 구성하여 실시합니다.

8.3 평가 대상과 평가자의 관계

SignKorea는 8.2(평가자의 신원, 자격)에 따른 평가기관의 평가자와 독립성을 유지합니다.

내부 감사는 전자서명인증업무를 담당하는 부서와 독립적인 조직에서 실시합니다.

8.4 평가 목적 및 내용

SignKorea는 법 제9조에 따른 인정기관으로부터 전자서명인증업무 운영기준에 대한 준수사실을 인정받기 위해 평가기관으로부터 평가를 받습니다. 평가의 내용은 전자서명인증업무 운영기준 준수 여부 및 평가기관이 마련한 세부 평가기준에 따릅니다.

내부 감사는 본 준칙의 준수 여부를 확인함을 목적으로 합니다.

8.5 부적합 사항에 대한 조치

SignKorea는 전자서명인증업무 운영기준 준수사실에 대한 인정을 받을 수 있도록, 평가

기관의 평가 결과 발생한 부적합 사항에 대해 조치합니다.

내부 감사를 통해 부적합 사항 발견 시 이에 대한 조치를 실시합니다.

8.6 결과 보고

평가기관은 법 제10조(평가기관)에 따라 전자서명인증업무 운영기준 준수사실에 대한 평가를 수행하고, 그 결과를 인정기관에 제출합니다.

내부 감사 진행 결과는 경영진 및 이해관계자와 공유합니다.

9. 전자서명인증업무 보증 등 기타사항

9.1 수수료

9.1.1 인증서비스 수수료

SignKorea는 가입자와 이용자에게 인증서의 발급, 인증서의 이용, 기타 인증서비스의 제공 등에 대해 수수료를 부과할 수 있습니다. SignKorea의 발급 수수료는 신규 발급과 기존 인증서에 대한 갱신을 대상으로 합니다. SignKorea는 가입자가 등급 및 대상별 수수료에서 정한 수수료를 인증서 발급 전에 납부하는 것을 원칙으로 합니다.

SignKorea는 인증서의 발급대상, 등급, 용도 및 발급구분에 따라 발급 수수료의 기준을 [표7]과 같이 정합니다.

(단위: 원/년, 부가세 별도)

<table>
<tr><td colspan="4">구 분</td><td>수수료</td></tr>
<tr><td rowspan="5">개인</td><td rowspan="3">범용</td><td colspan="2">신규, 갱신</td><td>4,000</td></tr>
<tr><td rowspan="2">재발급</td><td>유효기간 내</td><td>0</td></tr>
<tr><td>유효기간 만료 후</td><td>4,000</td></tr>
<tr><td rowspan="3">용도제한용</td><td>증권/보험용</td><td rowspan="3" colspan="2">별도 계약에 따름</td></tr>
<tr><td>신용카드용</td></tr>
<tr><td>기타</td></tr>
<tr><td rowspan="5">법인, 단체,
개인사업자</td><td rowspan="3">범용</td><td colspan="2">신규, 갱신</td><td>100,000</td></tr>
<tr><td rowspan="2">재발급</td><td>유효기간 내</td><td>0</td></tr>
<tr><td>유효기간 만료 후</td><td>100,000</td></tr>
<tr><td rowspan="3">용도제한용</td><td>증권/보험용</td><td rowspan="3" colspan="2">별도 계약에 따름</td></tr>
<tr><td>신용카드용</td></tr>
<tr><td>기타</td></tr>
<tr><td colspan="3">서버</td><td colspan="2">1,000,000</td></tr>
</table>

[표7] 인증서 발급 수수료(유효기간 1년 기준)

SignKorea는 정부 또는 SignKorea의 정책에 의거 수수료를 면제하거나 할인율을 적용할 수 있으며, 가입자 및 이용자와의 계약 또는 협약 등에 의하여 수수료 부과방법이나 납부시기 등을 변경할 수 있습니다.

SignKorea는 필요한 경우 인증서 발급수수료 이외에 인증서 이용 등에 대한 서비스 수

수료를 부과할 수 있으며, 시점확인서비스, 인증서 유효성 검증서비스 및 기타 인증서비스의 사용에 따른 수수료는 원칙적으로 유료이며 별도의 계약에 따릅니다.

SignKorea는 가입자의 인증서를 재발급 하는 과정에서 가입자 직접 방문 등 신원확인 업무 수행에 따르는 비용을 가입자에게 부과할 수 있습니다.

9.1.2 환불

가입자는 인증서를 발급받지 않았을 경우 등록 신청일로부터 7일 이내, 인증서를 발급받았을 경우 발급일로부터 7일 이내 환불 요구 시 구비서류를 제출하여 수수료를 환불받을 수 있습니다. 이때, 당해 수수료 환급 시 필요경비를 공제할 수 있으며, 가입자의 인증서는 폐지합니다.

9.2 배상

SignKorea는 전자서명인증업무의 수행과 관련하여 가입자 또는 이용자에게 손해를 입힌 경우 그 손해를 배상합니다. 또한 SignKorea는 시행령 제11조(손해배상을 위한 보험 가입)에 따라 연간 또는 건당 최대 25억원(최소 15억원)을 한도로 보험에 가입하고 있습니다.

9.3 영업비밀

전자서명인증체계 관계자는 SignKorea 인증서비스 이용 과정에서 취득한 SignKorea의 영업비밀에 대해 누설하거나 이를 부당하게 이용할 경우 민・형사상의 책임을 부담할 수 있습니다.

9.4 개인정보 보호

SignKorea는 가입자의 개인정보 보호를 위해 개인정보 보호법에 근거한 개인정보 처리방침을 마련하여 준수하고 있습니다. 개인정보 처리방침은 아래의 정보저장위치에 공고되어 있습니다.

○ 개인정보 처리방침 정보저장위치 : http://www.signkorea.com/privacy.html

9.5 지식재산권

SignKorea는 지식재산권의 보호와 관련된 법령을 준수합니다.

9.6 보증

해당사항 없습니다.

9.7 보증 예외 사항

해당사항 없습니다.

9.8 보험의 보상 범위

SignKorea가 가입하고 있는 보험은 SignKorea와 SignKorea가 계약을 체결한 등록대행기관을 담보하고 있습니다.

9.9 배상 한계

SignKorea는 전자서명인증업무 수행과 관련하여 가입자 또는 이용자에게 손해를 입힌 경우 그 손해를 배상합니다. 다만 SignKorea가 고의 또는 과실이 없음을 입증하면 그 배상책임이 면제 됩니다.

9.10 준칙의 효력

9.10.1 준칙의 시행일

제·개정된 준칙은 SignKorea가 준칙 정보저장위치에 공고하는 날로부터 시행합니다.

9.10.2 준칙의 효력 종료 조건

본 준칙은 새롭게 개정된 준칙으로 대체될 경우 효력이 종료됩니다.

9.11 통지 및 의사소통

SignKorea는, SignKorea의 전자서명생성정보에 및 클라우드 서버에 보관하고 있는 가입자의 전자서명생성정보에 대한 손상, 노출, 파손, 분실, 도난 등 인증서의 신뢰도 및 유효성에 중대한 영향을 미치는 사실의 발생 또는 SignKorea의 인증업무에 중대한 영향을 주는 상황의 발생을 인지한 경우에 한국인터넷진흥원에 해당 사실을 신속하게 신고합니다. 또한 해당사실을 SignKorea의 홈페이지(http://www.signkorea.com)를 이용하여 공고하는 것을 원칙으로 하며, 필요한 경우에 한해 전자우편으로 통지합니다.

SignKorea는 통보조치 후에 가입자와 이용자의 피해를 최소화할 수 있는 방법을 강구하여 신속하게 조치합니다.

SignKorea는 인증서비스와 관련된 각종 주요 정보를 홈페이지를 통해 공지합니다.

SignKorea 또는 등록대행기관은 가입자 인증서의 폐지 등 주요 상태변경 발생 시에 기 확보된 가입자의 연락처(전자우편 또는 휴대전화 번호)로 개별 통지합니다.

본 준칙 또는 SignKorea의 인증서비스와 관련한 문의가 있을 경우 SignKorea의 이메일(signkorea@koscom.co.kr) 또는 콜센터(1577-7337)를 통해 의사소통할 수 있습니다.

9.12 이력 관리

본 준칙의 개정 이력은 다음과 같습니다.

○ 2020년 12월 10일 - SignKorea 인증업무준칙 Ver. 4.0 시행
(전자서명법 개정에 따른 기존 인증업무준칙 전부개정)

○ 2021년 7월 15일 - SignKorea 인증업무준칙 Ver. 4.1 시행
(전자서명법 시행령 및 시행규칙 개정에 따른 관련 근거 조항 변경 사항 반영)

○ 2021년 10월 1일 - SignKorea 인증업무준칙 Ver. 4.2 시행
(준칙 개정절차에 최상위인증기관 협의과정 명시, 신원확인 방법 조항 보완, 부가서비스 내용 추가)

○ 2021년 10월 29일 - SignKorea 인증업무준칙 Ver. 4.3 시행
(안전한 암호화 소프트웨어 적용 원칙 명시, 담당자 변경 사항 반영)

○ 2022년 11월 1일 - SignKorea 인증업무준칙 Ver. 4.4 시행
(클라우드 공동인증서비스 관련사항 추가, 배상책임 및 가입자/이용자 책임 부분을 전자서명법과 준칙 취지에 부합하게 보완)

○ 2023년 1월 11일 - SignKorea 인증업무준칙 Ver. 4.5 시행
(용어의 정의 및 관련 법 조항 등 준칙의 개요 현행화, 전자문서의 법적 효력 문구 보완, 배상책임을 전자서명법과 준칙의 취지에 부합하게 보완)

○ 2023년 12월 1일 - SignKorea 인증업무준칙 Ver. 4.6 시행
(용어의 정의 보완, 인증서 용도를 전자서명법 취지에 부합하게 보완, 내부 감사 관련 내용 추가)

○ 2024년 6월 10일 - SignKorea 인증업무준칙 Ver. 4.7 시행
(비대면 신원확인 방법 관련 사항 추가)

○ 2024년 7월 5일 - SignKorea 인증업무준칙 Ver. 4.8 시행
(인증서 유효기간 및 갱신신청 기간 관련 사항 변경)

○ 2024년 12월 3일 - SignKorea 인증업무준칙 Ver. 4.9 시행
(인증서 이용 제한 요건 보완, 가입자 정보 수집 항목 현행화, 대리인 및 이용자 정의 보완, 인증서 부정발급 방지 운영체계 추가, 서비스 가입 철회 절차 보완, 배상 관련 근거법령 표기 삭제 및 배상 한도 구체화)

○ 2025년 3월 28일 - SignKorea 인증업무준칙 Ver. 4.10 시행
(비대면 신원확인 방법 보완)

9.13 분쟁 해결

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

전자서명인증체계 관련자에게 전달되는 문서(또는 전자문서)가 전자서명을 포함하는 경우에 법적 효력을 갖기 위해서는 다음과 같은 요건을 만족해야 합니다.

○ 전자서명은 법 제2조(정의) 제2호 각 목의 요건을 만족해야 함
○ 인증서에 기초한 전자서명인 경우, 전자서명에 사용된 인증서가 유효한 상태이며 정지 또는 폐지 상태가 아니어야 함

전자서명인증체계 관련자에게 전달되는 문서(또는 전자문서)가 전자서명을 포함하지 않는 경우는 전자문서법 제4조에 따른 법적 효력을 갖습니다.

9.13.2 인증업무와 관련된 분쟁을 해결하는 절차

SignKorea의 인증서비스와 관련된 분쟁이 발생하는 경우, 전자서명법 및 관련 법령에 따라 신속하게 분쟁을 해결할 수 있습니다. 가입자 또는 신뢰당사자는 9.11(통지 및 의사소통)의 의사소통 방법을 통해 SignKorea에 분쟁 해결을 위한 연락을 취할 수 있습니다.

9.14. 관할법원

SignKorea와 가입자 또는 신뢰당사자와의 인증업무와 관련한 분쟁해결을 위하여 SignKorea의 본사 소재지를 관할하는 법원을 관할법원으로 합니다.

본 준칙은 대한민국의 전자서명법 및 관계 법령에 따라서 해석되고 적용됩니다.

9.15 관련 법률 준수

전자서명인증체계 관련자는 대한민국의 전자서명법 및 관계 법령을 준수해야 합니다.

9.16 기타 규정

해당사항 없음

부칙 (2020.12.10.)

본 준칙은 2020년 12월 10일부터 시행합니다.

부칙 (2021.07.15.)
본 준칙은 2021년 7월 15일부터 시행합니다.

부칙 (2021.10.01.)
본 준칙은 2021년 10월 1일부터 시행합니다.

부칙 (2021.10.29.)
본 준칙은 2021년 10월 29일부터 시행합니다.

부칙 (2022.11.01.)
본 준칙은 2022년 11월 1일부터 시행합니다.

부칙 (2023.01.11.)
본 준칙은 2023년 1월 11일부터 시행합니다.

부칙 (2023.12.01.)
본 준칙은 2023년 12월 1일부터 시행합니다.

부칙 (2024.06.10.)
본 준칙은 2024년 6월 10일부터 시행합니다.

부칙 (2024.07.05.)
본 준칙은 2024년 7월 5일부터 시행합니다.

부칙 (2024.12.03.)
본 준칙은 2024년 12월 3일부터 시행합니다.

부칙 (2025.03.28.)
본 준칙은 2025년 3월 28일부터 시행합니다.