(붙임 2)

YESKEY 전자서명인증업무준칙

Version 5.11

본 전자서명인증업무준칙은 금융결제원이 발급하는
인증서의 발급·이용 등에 관한 전반적인 사항 및
금융결제원 전자서명인증업무(YESKEY) 관련 당사자의
의무와 책임을 규정한 것으로서 전자서명 관련법규를 준수합니다.

금융결제원 금융인증센터

ⓒCOPYRIGHT 2021 YESKEY ALL RIGHTS RESERVED

- 제·개정 이력 -

구 분	개정일	시행일	구 분	개정일	시행일
제 정	2000. 8.29.	2000. 8.29.	개정	2016.06.15.	2016.07.01.
개 정	2001. 7. 5.	2001. 7. 5.		2016.09.19.	2016.10.15.
	2001.12.17.	2001.12.17.		2016.11.03.	2016.11.25.
	2002. 3.12.	2002. 3.12.		2017.02.10.	2017.02.20.
	2002. 8.21.	2002. 9. 5.		2017.07.07.	2017.07.17.
	2002.12.27.	2003. 1.13.		2017.10.13.	2017.10.23.
	2004. 3.31.	2004. 6.12.		2018.07.31.	2018.08.10.
	2004. 9.16.	2004.10. 1.		2018.08.30.	2018.09.10.
	2005. 2.21.	2005. 3. 8.		2019.07.01.	2019.07.15.
	2005.11.17.	2005.12. 2.		2020.11.10.	2020.12.10.
	2005.12.29.	2006. 1.13.		2021.04.28.	2021.04.28.
	2006. 6.14.	2006. 7. 1.	전문개정	2021.10.18.	2021.10.18.
	2006. 6.30.	2006. 8. 1.	개정	2021.11.10.	2021.11.10.
전문개정	2007. 5.21.	2007. 8. 1.		2021.12. 8.	2021.12. 9.
개정	2009.10. 7.	2009.10.22.		2022.01.25.	2022.01.26.
	2010. 6. 3.	2010. 7. 1.		2022.04.13.	2022.04.13.
	2011. 3. 9.	2011. 3.28.		2022.08.16.	2022.08.16.
	2011. 9. 8.	2011. 9.30.		2023.06.02.	2023.06.02.
	2013. 8.27.	2013. 9.26.		2023.07.17	2023.07.17
	2013.10.25.	2013.12.16.		2024.05.31	2024.05.31
	2014.10.17.	2014.11.17.		2024.08.27	2024.08.27
	2015.07.15.	2015.08.15.		2025.01.02	2025.01.06
	2016.03.10.	2016.04.01.		2025.12.01	2025.12.01

- 목 차 -

1. 소개 ····· 1

1.1. 개요 ····· 1

1.1.1. 준칙의 배경 및 목적 ····· 1

1.1.2. 전자서명인증체계 ····· 1

1.2. 준칙의 명칭 ····· 1

1.3. 전자서명인증체계 관련자 ····· 2

1.3.1. 과학기술정보통신부 ····· 2

1.3.2. 인터넷진흥원 ····· 2

1.3.3. 결제원 ····· 3

1.3.4. 등록대행기관 ····· 5

1.3.5. 가입자 ····· 7

1.3.6. 이용자 ····· 8

1.4. 인증서 종류 ····· 9

1.4.1. 인증서 종류 ····· 9

1.4.2. 이용범위 및 제한 ····· 10

1.5. 준칙의 관리 ····· 11

1.5.1. 준칙 관리부서 및 연락처 ····· 11

1.5.2. 준칙의 개정 ····· 11

1.5.3. 준칙의 공지 ····· 12

1.6. 정의 및 약어 ····· 12

1.6.1. 정의 ····· 12

1.6.2. 약어 ····· 13

2. 전자서명인증업무 관련 정보의 공고 ····· 14
2.1. 공고설비 ····· 14
2.2. 공고방법 ····· 14
2.3. 공고 주기 ····· 14
2.4. 공고된 정보에 대한 책임 ····· 14
3. 신원확인 ····· 15
3.1. 가입자 이름 표시 방법 ····· 15
3.2. 신원확인 ····· 15
3.2.1. 신규발급 시 신원확인 ····· 15
3.2.2. 갱신발급, 재발급 및 변경 시 신원확인 ····· 18
3.2.3. 효력정지, 효력회복 및 폐지 시 신원확인 ····· 18
4. 인증서 관리 ····· 19
4.1. 인증서 발급 신청 ····· 19
4.1.1. 신청 주체 ····· 19
4.1.2. 신청등록 절차 ····· 19
4.2. 인증서 발급 신청 처리 ····· 19
4.2.1. 신청 처리 절차 ····· 19
4.2.2. 발급제한 ····· 19
4.3. 인증서 발급 절차 및 보호조치 ····· 20
4.3.1. 인증서 발급 절차 ····· 20
4.3.2. 가입자정보의 전송 ····· 21
4.4. 인증서 수령 ····· 22

4.5. 인증서 이용 ····· 22

4.6. 인증서 갱신발급 ····· 23

4.6.1. 갱신발급 요건 ····· 23
4.6.2. 갱신발급 절차 ····· 23

4.7. 인증서 재발급 ····· 24

4.7.1. 재발급 요건 ····· 24
4.7.2. 재발급 절차 ····· 24

4.8. 인증서 변경 ····· 25

4.8.1. 가입자 등록정보 변경 요건 ····· 25
4.8.2. 가입자 등록정보 변경 절차 ····· 25

4.9. 인증서 효력정지·효력회복·폐지 ····· 25

4.9.1. 효력정지 사유 ····· 25
4.9.2. 효력회복 공고 ····· 26
4.9.3. 효력회복 기간의 제한 ····· 26
4.9.4. 폐지 사유 ····· 26
4.9.5. 인증서 효력정지 및 폐지목록(CRL)의 갱신과 공고 ····· 27
4.9.6. 강제 폐지에 따른 공지 ····· 27
4.9.7. 부정발급 및 이상거래 모니터링 ····· 27

4.10. 실시간 인증서 상태확인(OCSP) 서비스 ····· 28

4.11. 서비스 가입 철회 ····· 28

4.12. 기타 부가 서비스 ····· 28

4.12.1. 시점확인서비스 ····· 28

5. 시설 및 운영 관리 ····· 29

5.1. 물리적 보호조치 ····· 29

5.1.1. 물리적 접근 통제 ····· 29

5.1.2. 수해 방지 ····· 30
5.1.3. 화재 예방 ····· 30
5.1.4. 전원 ····· 30
5.1.5. 방호 ····· 30
5.1.6. 항온항습, 통풍 ····· 31
5.1.7. 기타 보호설비 ····· 31
5.1.8. 매체 저장 ····· 31
5.1.9. 시설 및 장비의 폐기 처리 ····· 31
5.1.10. 원격지 백업설비 안전운영 ····· 31
5.2. 절차적 보호조치 ····· 32
5.2.1. 전자서명인증업무에 대한 업무 분장 ····· 32
5.2.2. 동일인에 의해 동시 수행될 수 없는 전자서명인증업무 ····· 32
5.2.3. 업무 담당자 현황 및 인증 방법 ····· 33
5.3. 인적 보안 ····· 33
5.3.1. 전자서명인증업무 인력의 자격, 경력 등 요구사항 ····· 34
5.3.2. 전자서명인증업무 교육, 업무순환에 관한 사항 ····· 34
5.3.3. 비인가된 행위에 대한 처벌에 관한 사항 ····· 34
5.4. 감사 기록 ····· 35
5.4.1. 감사기록의 유형 및 보존기간 ····· 35
5.4.2. 감사기록 보호조치 ····· 35
5.4.3. 감사기록 백업주기 및 절차 ····· 35
5.5. 기록 보존 ····· 36
5.5.1. 보존기록의 유형 및 보존기간 ····· 36
5.5.2. 보존기록의 보호조치 ····· 36
5.5.3. 보존기록의 백업주기 및 백업절차 ····· 36
5.6. 전자서명인증사업자의 전자서명생성정보 갱신 ····· 36
5.7. 장애 및 재해복구 ····· 37
5.7.1. 전자서명인증업무 장애 유형 ····· 37

5.7.2. 전자서명인증업무 장애 유형별 복구 ····· 37
5.7.3. 전자서명인증업무 장애방지 등 연속성 보장 대책 ····· 38
5.8. 업무 휴지, 폐지, 종료 ····· 38
5.8.1. 전자서명인증업무 휴지 ····· 38
5.8.2. 전자서명인증업무 폐지 ····· 39
6. 기술적 보호 조치 ····· 40
6.1. 전자서명생성정보 보호 ····· 40
6.2. 전자서명생성정보 보호조치 ····· 40
6.2.1. 전자서명생성정보 저장장치 ····· 40
6.2.2. 전자서명생성정보 생성·사용 후 안전한 삭제 방법 ····· 40
6.2.3. 전자서명생성정보 파기 방법 ····· 40
6.2.4. 전자서명생성정보 백업 ····· 40
6.3. 전자서명생성정보 및 전자서명검증정보의 관리 ····· 41
6.4. 데이터 보호 조치 ····· 41
6.5. 시스템 보안 통제 ····· 41
6.6. 시스템 운영 관리 ····· 42
6.7. 네트워크 보호조치 ····· 42
6.8. 부가서비스 보호조치 ····· 43
7. 인증서 형식 ····· 43
7.1. 인증서 형식 ····· 44
7.1.1. 인증서 프로파일 ····· 44
7.1.2. 전자서명의 생성 ····· 46
7.2. 인증서 유효성 확인 정보 형식 ····· 46

7.2.1. 인증서 효력정지 및 폐지목록(CRL) 프로파일 ····· 46
7.2.2. 실시간 인증서 상태확인(OCSP) 서비스용 인증서 프로파일 ····· 47

8. 평가 및 감사 ····· 49

8.1. 평가 및 감사 현황 ····· 49

8.2. 평가자 및 감사자의 신원, 자격 ····· 49

8.3. 평가 대상과 평가자의 관계 및 감사 대상과 감사자의 관계 ····· 49

8.4. 평가 및 감사 목적, 내용 ····· 49

8.5. 부적합 사항에 대한 조치 ····· 50

8.6. 결과 보고 ····· 50

9. 전자서명인증업무 보증 등 기타사항 ····· 51

9.1. 수수료 ····· 51

9.1.1. 인증서 발급・갱신 수수료 ····· 51
9.1.2. 인증서 접근 수수료 ····· 51
9.1.3. 인증서 유효 여부 확인 수수료 ····· 52
9.1.4. 기타 서비스에 대한 수수료 ····· 52
9.1.5. 환불 ····· 52

9.2. 배상 ····· 52

9.3. 영업비밀 ····· 52

9.4. 개인정보 보호 ····· 53

9.4.1. 개인정보 수집 및 이용목적 ····· 53
9.4.2. 전자서명인증업무 관련정보의 보호범위 및 책임 ····· 53
9.4.3. 개인정보보호를 위한 조치 ····· 54

9.4.4. 개인정보보호에 대한 처리방침 ····· 54
9.5. 지식재산권 ····· 54
9.6. 보증책임 ····· 55
9.7. 보증 예외 사항 ····· 55
9.8. 보험의 보상 범위 ····· 55
9.9. 배상 한계 ····· 55
9.10. 준칙의 효력 ····· 55
9.11. 통지 및 의사소통 ····· 56
9.12. 이력 관리 ····· 56
9.13. 분쟁 해결 ····· 56
9.13.1. 관련자에게 전달되는 문서(또는 전자문서)가 법적 효력을 갖기 위한 요건 ····· 56
9.13.2. 분쟁을 해결하는 절차 ····· 56
9.14. 관할법원 ····· 57
9.15. 관련 법률 준수 ····· 57
9.16. 기타 규정 ····· 57

1. 소개

1.1. 개요

1.1.1. 준칙의 배경 및 목적

금융결제원(이하 “결제원”이라 한다)은 인터넷 등 개방형 정보통신망을 이용하여 처리되는 전자문서의 안전 및 신뢰성을 확보하기 위하여 제정된 전자서명법에 따라 금융기관과 함께 전자서명인증시스템을 구축·운영하고 있습니다.

본 전자서명인증업무준칙(이하 “준칙”이라 한다)은 전자서명법(이하 “법”이라 한다), 동법 시행령(이하 “시행령”이라 한다), 동법 시행규칙(이하 “시행규칙”이라 한다), 과학기술정보통신부 전자서명인증업무 운영기준(이하 “운영기준”이라 한다)에 근거하여 전자서명인증서(이하 “인증서”라 한다) 발급 및 관리, 운영정책 및 절차 등 결제원이 제공하는 전자서명인증업무에 관련된 전반적인 사항과 전자서명인증업무 관련 당사자의 책임과 의무에 관한 사항을 정함을 목적으로 합니다.

1.1.2. 전자서명인증체계

전자서명인증에 관한 정책의 수립, 시행 및 감독은 과학기술정보통신부가 관장하고 있으며, 결제원 전자서명인증업무는 한국인터넷진흥원(이하 “인터넷진흥원”이라 한다)을 최상위인증기관으로 하여 전자서명인증체계가 구성되어 있습니다.

결제원은 신청인의 신원확인 등의 등록업무를 등록대행기관에 위임할 수 있으며, 전자서명인증업무의 이용주체로 가입자, 가입신청자(결제원으로부터 인증서를 발급받으려는 자), 이용자가 있습니다.

1.2. 준칙의 명칭

본 준칙은 YESKEY 전자서명인증업무준칙이라 합니다.

1.3. 전자서명인증체계 관련자

전자서명인증체계 관련자는 안전하고 신뢰할 수 있는 인증서의 발급·이용·관리를 위하여 신의성실로 상호 협조해야 합니다.

1.3.1. 과학기술정보통신부

과학기술정보통신부는 전자서명 인증관리체계의 안전성·신뢰성 있는 운영을 위한 정책·감독기관으로서 다음의 업무를 수행합니다.

- 전자서명 인증관리체계의 안전·신뢰성 있는 구축 및 운영을 위한 정책수립
- 전자서명인증업무 운영기준(이하 “운영기준”이라 한다) 마련 및 고시
- 전자서명인증사업자의 운영기준 준수 여부에 대한 평가기준·절차 수립
- 전자서명인증사업자의 운영기준 준수여부 평가를 수행하는 기관(이하 “평가기관”이라 한다)의 선정기준·절차 등 업무수행방법 수립과 평가기관 선정, 고시 및 취소
- 운영기준 준수사실의 인정에 관한 업무를 수행하는 기관(이하 “인정기관”이라 한다) 지정
- 운영기준 준수사실의 인정을 받은 전자서명인증사업자(이하 “인정사업자”)에 대한 검사 및 시정명령
- 운영기준에 부합한다고 인정하는 국제적으로 통용되는 평가(이하 “국제통용평가”라 한다)의 선정 및 고시

1.3.2. 인터넷진흥원

인터넷진흥원은 법 제9조(인정기관)에 따라 지정된 인정기관으로서 다음의 업무를 수행합니다.

- 운영기준 준수사실의 인정을 받으려는 전자서명인증사업자가 법 제8조에 따른 자격을 갖추었는지 여부를 확인하여 운영기준 준수사실의 인정 여부 결정, 증명서 발급 및 공고

- 법 제11조에 따른 전자서명인증사업자의 국제통용평가 인정 여부 결정 및 증명서 발급 및 공고
- 시행령 제3조에 따른 운영기준 준수사실 인정의 취소
- 운영기준 준수여부 평가를 신청한 전자서명인증사업자에 대하여 세부 평가기준, 평가 범위, 평가 일정 및 평가 참관에 관한 사항 등을 평가기관과 협의
- 전자서명인증 관련 기술개발·보급 및 표준화 연구
- 전자서명인증 관련 제도 연구
- 전자서명인증 최상위 인증기관

1.3.3. 결제원

결제원은 전자서명인증사업자로서 다음의 업무를 수행합니다.

- 전자서명인증업무 이용 신청접수 및 처리
- 가입자 신원확인
- 인증서 발급, 인증서 재발급, 인증서 갱신, 가입자정보 변경, 인증서 효력정지, 인증서 효력회복, 인증서 폐지 등의 업무
- 인증서 목록, CRL 등 인증서 관련 정보 공고
- 시점확인서비스
- 등록대행기관의 운영
- 기타 전자서명인증사업자로서 필요하다고 인정되는 업무

결제원의 책임 및 의무사항은 다음과 같습니다.

1.3.3.1. 정확한 정보 제공

결제원은 가입자 및 이용자에게 인증서의 신뢰성이나 유효성에 영향을 미칠 수 있는 다음의 정보를 YESKEY 홈페이지 또는 결제원 디렉토리시스템에 공고하여 그 사실을 확인할 수 있도록 합니다.

- 전자서명인증업무 휴지·정지 또는 폐지
- 준칙
- 인증서에 대한 정보
  - 가입자 인증서
  - 가입자 CRL
- 전자서명인증업무 운영기준 준수사실의 인정
- 기타 전자서명인증업무 수행관련 정보 등

1.3.3.2. 전자서명생성정보의 보호

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

1.3.3.3. 전자서명생성정보 안전조치

결제원은 결제원 전자서명생성정보의 분실·훼손, 도난·유출 등 인증서의 신뢰성이나 유효성에 영향을 미치는 사유가 발생한 사실을 인지하는 경우 가입자에게 이를 통보하며 필요한 경우 당해 전자서명생성정보로 발급한 가입자의 인증서를 폐지합니다.

결제원은 결제원이 보관하는 가입자 전자서명생성정보의 분실·훼손, 도난·유출 등 인증서의 신뢰성이나 유효성에 영향을 미치는 사유가 발생한 사실을 인지하는 경우 가입자에게 이를 통보하며 해당 전자서명생성정보 및 인증서를 효력정지 또는 폐지합니다.

결제원은 전자서명생성정보의 분실·훼손, 도난·유출 등 인증서의 신뢰성이나 유효성에 영향을 미치는 사유가 발생한 사실을 인지하는 경우 즉시 당해 사실을 YESKEY 홈페이지에 공고하며, CRL을 갱신하고, 이용자가 갱신된 CRL을 이용할 수 있도록 합니다. 그리고 결제원은 전자서명인증업무의 신뢰성·유효성을 확보할 수 있는 대책을 강구합니다.

1.3.3.4. 등록대행기관 운영

결제원은 등록대행기관이 가입자 인증서 이용신청 접수 및 신원확인 등의 전자서명인증업무를 처리함에 있어 안전성과 유효성이 확보될 수 있도록 운영하며 등록대행기관의 요건, 의무, 책임, 업무처리 등에 관하여는 별도로 정한 규약 및 시행세칙에 의합니다.

1.3.3.5. 신원확인

결제원은 법 제14조(신원확인)에 따라 가입자의 신원을 확인하며, 관련 서류를 요구할 수 있습니다.

1.3.3.6. 안전한 암호 알고리즘의 사용

결제원은 신뢰할 수 있는 인증을 획득한 암호화 모듈 및 보안 기술규격을 적용하는 것을 원칙으로 하며, 암호알고리즘, 암호모듈 및 키 운영, 암호알고리즘이 적용되는 메커니즘 등과 같은 전자서명인증시스템 암호 운영 관련 전반에서 안전성을 확보하기 위해 충분한 기술적, 정책적 노력을 취해야하며, 그렇지 않은 사유로 인해 가입자 또는 이용자에게 손해가 발생하였을 때에도 책임을 부담합니다.

1.3.4. 등록대행기관

등록대행기관은 인증서 발급, 효력정지, 효력회복, 폐지 등 신청접수 및 신원확인 등의 업무를 수행하며, 가입자의 편의를 위하여 여러 지역에 지정되어 있습니다.

결제원의 등록대행기관은 국민은행 등 은행권(농협·수협중앙회 포함), 새마을금고중앙회, 신용협동조합중앙회 등이며 결제원은 등록대행기관을 추가로 지정·운영할 수 있고 이 경우 “2.2 공고방법 - 등록대행기관 목록”에 공고합니다.

등록대행기관의 책임 및 의무사항은 다음과 같습니다.

1.3.4.1. 인증서 이용신청 접수 및 중요 내용 설명

등록대행기관은 정당한 사유없이 인증서 발급, 재발급, 갱신발급, 효력정지, 효력회복, 폐지 등의 인증서 관련 신청접수를 거부할 수 없습니다. 또한「약관의 규제에 관한 법률」제3조(약관의 작성 및 설명의무 등)에 따라 중요한 내용을 가입자가 이해할 수 있도록 설명하여야 합니다.

1.3.4.2. 신원확인

등록대행기관은 법 제14조(신원확인)에 따라 가입자의 신원을 확인하며, 관련 서류를 요구할 수 있습니다. 등록대행기관은 참가기관 자체적으로 확인했거나 행정안전부 등 관련 기관으로부터 전달받은 정보를 통해 가입자가 사망 등의 사유로 더 이상 인증서를 이용할 수 없는 상태임이 확인된 즉시 결제원에 그 사실을 알립니다.

1.3.4.3. 전자서명생성정보의 접근보호

전자서명생성정보의 비밀번호를 생체정보(지문 등) 또는 가입자만이 아는 정보(PIN 등)로 대체하는 경우, 등록대행기관은 생체인증 또는 가입자만이 아는 정보의 인증이 유효한 경우 가입자가 저장·관리하는 전자서명생성정보에 접근할 수 있는 서비스를 제공할 수 있습니다.

등록대행기관은 동 서비스의 안전성과 유효성이 확보될 수 있도록 운영하여야 하며, 서비스에 대한 감사기록을 안전하게 생성·관리하고, 결제원이 감사기록의 열람을 요청하는 경우 성실히 협조하여야 합니다.

1.3.4.4. 책임

등록대행기관이 전자서명인증업무규약을 위반하여 전자서명인증업무에 중대한 지장을 초래하였을 경우 결제원은 해당 등록대행기관에 대하여 적절한 제재를 가할 수 있습니다. 또한 인증서 가입자의 신원확인 오류 등 등록대행기관의 고의 또는 과실로 인하여 발생한 가입자 또는 이용자의 손해에 대하여는 등록대행기관이 그 손해를 배상할 책임이 있습니다.

1.3.5. 가입자

가입자는 전자서명생성정보에 대하여 결제원으로부터 전자서명인증을 받은 자(인증서를 발급받으려는 가입신청자를 포함)를 말합니다.

사업자번호를 보유한 사업자(개인 또는 법인)의 경우 해당 사업자의 임직원인 대리인이 인증서를 발급받을 수 있으며, 대리인은 가입자의 위임장 등과 같은 관련 서류를 지참한 경우에 한하여 가입자를 대리하여 인증업무를 신청할 수 있습니다.

본 준칙에서는 대리인 및 가입신청자를 가입자에 포함하며, 구별이 필요한 경우에 한하여 별도로 명시합니다.

가입자의 책임 및 의무사항은 다음과 같습니다.

1.3.5.1. 정확한 정보제공

가입자는 다음사항에 대하여 정확한 정보를 결제원과 등록대행기관에 제공하여야 하며, 결제원 또는 등록대행기관이 신원확인을 위하여 관련 서류를 요청하는 경우 가입자는 성실히 협조하여야 합니다. 또한 주민등록번호 등 주요정보가 변경되었을 경우 결제원과 등록대행기관에 변경사실을 즉시 통보하여야 합니다.

- 인증서 발급 신청
- 인증서 재발급 신청
- 인증서 갱신발급 신청
- 인증서 효력정지, 효력회복 및 폐지 신청
- 가입자정보 변경 등

1.3.5.2. 인증서의 목적에 적합한 사용

가입자는 정당한 용도 및 제한(제한이 따르는 경우)에 맞게 인증서를 사용하여야 합니다. 그리고 인증서를 사용하여 전자서명을 제공할 때에는, 당해 인증서에 포함된 전자서명검증정보에 합치하는 전자서명생성정보를 사용하여야 합니다.

1.3.5.3. 전자서명생성정보의 보호

가입자는 신뢰할 수 있는 소프트웨어나 하드웨어를 이용하여 전자서명정보를 생성하며 생성된 전자서명생성정보 및 접근통제수단이 분실·훼손 또는 도난·유출되지 않도록 안전하게 보관·관리하여야 합니다.

효력정지기간 중에도 가입자가 전자서명생성정보를 보유하는 동안에는 전자서명생성정보를 안전하게 보관·관리하여야 하며 보유를 원치 않을 경우에는 저장된 모든 전자서명생성정보를 완전히 삭제하여야 합니다.

1.3.5.4. 전자서명생성정보 안전조치

가입자는 전자서명생성정보가 분실·훼손 또는 도난·유출되었거나 안전하지 않다고 인지하는 경우 즉시 결제원 또는 등록대행기관에 관련사실을 통보하여 결제원이 당해 인증서를 폐지할 수 있도록 협조하여야 합니다.

1.3.6. 이용자

이용자는 결제원이 발급한 인증서를 이용하여 가입자의 전자서명생성정보와 전자서명검증정보의 합치 여부를 확인하는 자를 말합니다.

이용자의 책임 및 의무사항은 다음과 같습니다.

1.3.6.1. 인증서의 사용목적 이해

이용자는 결제원이 가입자에게 발급한 인증서의 이용목적 및 이용가능 범위(제한 포함)를 이해하여야 합니다.

1.3.6.2. 인증서의 유효성 확인

이용자는 인증서 기재사항 등에 의하여 전자서명의 진위여부를 확인하기 위하여 다음의 조치를 취하여야 합니다.

- 인증서 유효여부의 확인
- 인증서의 정지 또는 폐지 여부의 확인
- 인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항에 대한 확인
- 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격 등의 표시를 요청한 경우 이에 관한 사항에 대한 확인

1.4. 인증서 종류

1.4.1. 인증서 종류

결제원은 개인과 사업자/단체에(게) 공동인증서와 금융인증서를 발급합니다. 공동인증서와 전자서명생성정보는 가입자가 선택한 설비에 저장되고, 금융인증서와 전자서명생성정보는 결제원의 저장장소에 암호화하여 저장됩니다.

인증서의 유효기간은 공동인증서는 발급일로부터 1년, 금융인증서는 발급일로부터 최대 3년입니다. 다만, 보안매체(금융IC카드, 보안토큰, USIM 등)에 발급된 공동인증서의 유효기간은 최대 4년이며, 안전한 실행환경(TEE 등) 기반에 보안토큰 방식으로 작동하는 보안영역용 공동인증서 또는 이에 준하는 보안성을 갖춘 공동인증서의 유효기간은 최대 3년입니다. 대면업무용 금융인증서의 유효기간은 최대 3시간입니다. 또한 서버용 공동인증서의 유효기간은 발급일로부터 1년 또는 2년입니다.

결제원에서 가입자 유형별 발급하는 인증서의 종류 및 용도는 다음과 같습니다.

구 분			용 도
개인	금융인증서	범용	· 전자서명 및 본인확인 관련 제반업무
		대면업무용	· 대면 서비스(금융마이데이터, 오픈뱅킹서비스 가입) 이용을 위한 전자서명 및 본인확인 관련 업무
	공동인증서	범용	· 전자서명 및 본인확인 관련 제반업무
		은행/신용카드/보험용	· 금융, 공공 및 정부민원 전자서명 관련 업무 · 본인확인 관련 제반업무
		기타	· 특정인에게 발급되어 지정된 분야에 제한적으로 사용
사업자	금융인증서	금융공공용	· 금융, 공공 및 정부민원 전자서명 관련 업무
		전자세금용	· 국세청 민원 및 전자세금계산서업무 · 외부감사 및 준법감시를 위한 전자채권채무 조회 및 기업 회계감사자료 조회업무 · 관세청 민원 및 전자통관 업무
		기 타	· 특정인에게 발급되어 지정된 분야에 제한적으로 사용
	공동인증서	범 용	· 전자서명 관련 제반업무
		은행/신용카드/보험용	· 금융, 공공 및 정부민원 전자서명 관련 업무
		전자세금용	· 국세청 민원 및 전자세금계산서업무 · 외부감사 및 준법감시를 위한 전자채권채무 조회 및 기업 회계감사자료 조회업무
		조달청 원클릭용	· 조달청 비축원자재 구매업무
		금융위원회 CTR용	· 금융위원회 고액현금거래 보고업무
		서버용	· 인터넷뱅킹, 지급결제중계, 온라인쇼핑몰 등 인터넷에서 서버를 이용하여 서비스를 제공하는 업무
		기 타	· 특정인에게 발급되어 지정된 분야에 제한적으로 사용

※ 사업자 인증서는 사업자번호를 보유한 사업자/단체인 경우 발급 가능

1.4.2. 이용범위 및 제한

결제원이 발급한 인증서는 “1.4.1”의 인증서 종류별 용도에 따라 금융기관업무, 정부민원업무, 전자문서 관련 제반업무 등에 사용할 수 있습니다. 앞의 전자거래에서의 인증서 사용은 정당한 권한을 가진 가입자가 인증서의 발급용도에 맞게 인증서를 사용하는 것을 말합니다. 일정횟수 이상 비밀번호 오류 등 인증업무 관련 보안상의 우려가 있는 경우 결제원은 기발급된 인증서의 사용을 제한

할 수 있습니다.

1.5. 준칙의 관리

1.5.1. 준칙 관리부서 및 연락처

- 관리부서 : 결제원 금융인증센터
- 전자우편 : yeskey@kftc.or.kr
- 주소 : 13556, 경기도 성남시 분당구 정자일로 213번길 9
- 전화 : 1577-5500
- FAX : (02)531-3109

1.5.2. 준칙의 개정

결제원은 전자서명인증업무 개선을 위하여 준칙의 변경이 필요하다고 판단한 경우 이를 개정할 수 있습니다. 본 준칙의 제·개정 시에는 인증업무 관리책임자의 승인을 받아 개정합니다.

결제원은 준칙이 제·개정된 경우 다음의 내용을 포함한 준칙의 제·개정 관련 기록을 유지·관리하여야 합니다.

- 준칙 버전
- 적용 업무 및 범위의 개요
- 준칙의 제·개정 기록
  - 제·개정된 기존 준칙의 규정
  - 제·개정 내용
  - 제·개정 사유 등

결제원은 최상위인증기관과의 정책 일관성을 위해 필요시 준칙 제·개정에 대하여 협의할 수 있습니다.

1.5.3. 준칙의 공지

결제원은 개정된 준칙을 아래의 정보저장위치에 즉시 공고합니다.

- 준칙 정보저장위치 : http://www.yeskey.or.kr/cps.htm

가입자는 변경된 준칙이 공고된 후 30일(공고일 포함) 내에 전자우편(e-mail) 또는 전자서명생성정보로 전자서명한 전자문서 등 서면으로 이의를 제기할 수 있습니다.

1.6. 정의 및 약어

1.6.1. 정의

1.6.1.1. 법 용어 정의

본 준칙에서 사용되는 주요 용어들은 “9.15”의 전자서명인증 관련법규에 정의되어 있습니다.

1.6.1.2. 용어의 정의

본 준칙을 위하여 다음과 같이 용어를 정의합니다.

- 디렉토리시스템 : 인증서, CRL을 보관하고 신뢰당사자에게 공고 및 검색 서비스를 제공하기 위한 것으로 ITU-T X.500 표준을 준수하는 시스템을 말합니다.
- 사고정보 : 전자금융사고 또는 인증서 유출 등이 발생한 기기정보(IP 및 MAC주소 등) 및 개인정보(이름, 주민등록번호 등)를 말합니다.
- YESKEY 인증서비스 : 결제원이 제공하는 전자서명인증서비스를 말합니다.
- 단말기 지정 : 단말기(PC, 스마트폰 등)의 기기정보를 등록대행기관에 등록하고, 인증서 발급시 가입자가 등록한 단말기인지 여부를 확인하여 가입자의 신원을 확인하는 방법을 말합니다.
- 추가인증 : 휴대폰 SMS인증, 2채널 인증 등과 같이 단말기 지정 이외의 수단으로 가입자의 신원을 확인하는 방법을 말합니다.
- 2채널 인증 : 서로 다른 두 가지 이상의 통신경로를 이용하여 가입자의 신

원을 확인하는 방법을 말합니다.

1.6.2. 약어

본 준칙에서는 다음의 약어가 사용됩니다.

- CRL : Certificate Revocation List, 인증서 효력정지 및 폐지목록
- DN : Ditinguished Name, 식별명칭

2. 전자서명인증업무 관련 정보의 공고

2.1. 공고설비

인증서 발급 및 관리에 관한 정보와 CRL 등의 인증서 상태정보에 관련된 정보의 공고설비 운영주체는 결제원입니다. 결제원은 관련법령에 따라 공고설비를 운영하며, 이를 준수하지 않아 가입자 또는 이용자에게 손해를 입힌 때에는 법 제20조(손해배상책임)에 따른 책임을 집니다.

2.2. 공고방법

인증서, 인증서 효력정지 및 폐지목록 등 인증업무와 관련된 정보는 인터넷을 통해 공고하며, 공고위치는 다음과 같습니다.

- 공고위치 : ldap://ds.yessign.or.kr:389/, ldap://ds.yessign.or.kr:1389/
- 실시간 인증서 상태확인 정보 : http://ocsp.yessign.org:4612
- 등록대행기관 목록 : https://www.yeskey.or.kr/ra.htm,
  https://www.yeskey.or.kr/shortcut/issuer

2.3. 공고 주기

인증서 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 YESKEY홈페이지(http://www.yeskey.or.kr)에 공고합니다.

2.4. 공고된 정보에 대한 책임

결제원이 효력정지되거나 폐지된 인증서의 공고를 누락하여 가입자 또는 이용자에게 손해를 입힌 때에는 법 제20조(손해배상책임)에 따른 책임을 집니다.

3. 신원확인

3.1. 가입자 이름 표시 방법

결제원이 발급하는 인증서는 DN으로 서로 구분될 수 있습니다. DN은 가입자 실명과 가입자 ID를 포함합니다. 가입자 ID는 결제원과 등록대행기관의 업무규약에 따라 등록대행기관, 가입자, 인증서 사용용도에 따라 유일하게 부여됩니다.

결제원은 인증서 신청등록시 가입신청자가 등록한 명칭으로 인증서, CRL 내의 기본영역에 사용될 명칭을 구성하며 당해 명칭의 구성방식은 국내·국제 표준을 따릅니다. 가입신청자가 신청등록시 등록 가능한 명칭은 실명을 원칙으로 합니다.

3.2. 신원확인

3.2.1. 신규발급 시 신원확인

결제원 또는 등록대행기관은 가입신청자의 신원을 확인합니다. 결제원 또는 등록대행기관은 대면 또는 대면에 준하는 비대면 실지명의 확인 절차를 통해 가입 신청자의 신원을 확인하거나,「금융실명거래 및 비밀보장에 관한 법률」에 의거 금융기관에서 실지명의가 확인된 전자금융거래 가입자가 인증서를 발급받으려는 경우 정보통신망을 통하여 온라인으로 신원을 확인할 수 있습니다.

3.2.1.1. 대면 신원확인에 의한 발급

결제원 또는 등록대행기관이 직접 대면하여 가입신청자의 신원을 확인하는 때에는 시행규칙 제5조(실지명의 기준의 신원확인 방법)에 의거 신원확인증표에 의하여 실지명의인지 여부와 부착된 사진으로 본인임을 확인합니다.

사업자의 경우 대표자 전원의 신원을 확인하고, 사업자가 대리인을 통하여 신청하는 경우에는 사업자의 신원확인증표 외에 대리인의 신원확인증표, 대표자의 위임장, 법인인감증명서를 추가로 확인합니다.

특히, 서버용 인증서의 경우 인터넷에서 전자거래서비스를 제공하는 가입신청자가 관련 서류를 소지하고 결제원을 방문하여 신원확인하며 결제원이 신원확인시 필요로 하는 서류는 다음과 같습니다.

- 대표자가 신청하는 경우
  - · 서버인증서 이용신청서
  - · 당해 서비스에 대한 사업자등록증 사본
  - · 법인인감증명서, 법인등기부등본
  - · 도메인 실존여부 확인서류(도메인네임 등록필증 사본)
  - · 대표자 신원확인증표 등
- 대리인을 통하여 신청하는 경우
  - · 서버인증서 이용신청서
  - · 당해 서비스에 대한 사업자등록증 사본
  - · 법인인감증명서, 법인등기부등본
  - · 도메인 실존여부 확인서류(도메인네임 등록필증 사본)
  - · 대리인 신원확인 증표
  - · 대표자의 위임장 등

다만, 개인사업자인 경우는 법인인감증명서, 법인등기부등본은 제외합니다.

3.2.1.2. 비대면 신원확인에 의한 발급

결제원 또는 등록대행기관은 다음의 비대면 방식을 이용하여 가입신청자의 신원을 확인할 수 있습니다.

- 결제원 또는 등록대행기관은 아래의 신원확인방법으로 가입신청자의 실지명의를 확인합니다. 아래의 신원확인방법에 의한 발급 대상은 개인 및 개인사업자에 한정됩니다.

· 실명확인증표 확인 : 개인은 가입신청자의 실명확인증표를 확인하며, 개인사업자는 대표자의 실명확인증표 및 사업자등록증명원을 확인

· 계좌인증 또는 영상통화 (택1) : 가입신청자에 대한 계좌를 인증하거나 가입신청자와 영상통화를 하는 방식 중에서 선택하여 본인을 확인

(계좌인증) 계좌로 소액을 이체하여 입금내역을 확인한 후 인증값을 입력하도록 하거나 계좌비밀번호를 입력하는 등의 방법으로 계좌를 확인. 개인은 가입신청자의 계좌를 확인하며 개인사업자는 대표자의 계좌를 확인

(영상통화) 영상통화 등을 통해 가입신청자의 영상과 그 사람이 제출한 실명확인증표상의 사진을 비교·대조하는 방식으로 본인을 확인. 영상통화는 개인은 가입신청자를 확인하며, 개인사업자는 대표자를 확인

· 본인확인수단 활용 : 인증서, 아이핀, 휴대폰 등 본인확인수단을 이용하여 본인을 확인. 개인은 가입신청자의 본인확인수단을 확인하며, 개인사업자는 대표자의 본인확인수단을 확인

- 결제원 또는 등록대행기관은 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 온라인으로 신원을 확인할 수 있으며, 온라인 신원확인 정보는 다음과 같습니다.

· 전자금융거래 가입자의 계정(ID)과 그 비밀번호 등 로그인 정보 또는 계좌번호와 그 비밀번호

· 전자금융거래 가입자의 주민등록번호, 사업자번호, 외국인등록번호 등 식별번호

· 금융기관이 전자금융거래를 위하여 가입자에게 제공한 일회용비밀번호(보안카드의 비밀번호 포함) 또는 가입자 본인만이 알 수 있는 두 가지 이상의 정보

· 신용카드정보 등 전자금융거래 가입자의 신원을 확인할 수 있는 정보. 다만, 전자금융거래 가입자가 사업자, 단체, 해외체류자, 외국인 또는 점자보안카드 사용자(해당 정보 확인에 동의한 점자보안카드 사용자는 제외한다)인 경우는 제외

3.2.2. 갱신발급, 재발급 및 변경 시 신원확인

3.2.2.1. 갱신발급 시 신원확인

인증서 갱신은 가입자의 기존 전자서명정보가 유효할 때 신청 가능하므로, 결제원은 가입자의 신원확인을 인증서 갱신신청내역의 가입자 전자서명으로 합니다. 이때 가입자는 비밀번호 등 전자서명생성정보 접근통제 수단을 이용하여 전자서명을 생성함으로써 전자서명생성정보 소유를 증명할 수 있습니다.

인증서 갱신신청시 가입자의 기존 등록정보가 변경된 경우 결제원 및 등록대행기관은 필요에 따라 변경정보에 대한 증빙자료를 요구할 수 있습니다.

3.2.2.2. 재발급 시 신원확인

인증서 재발급은 “3.2.1 신규발급 신원확인”을 따릅니다.

3.2.2.3. 변경 시 신원확인

결제원은 가입자의 신원확인을 가입자 등록정보 변경신청내역의 가입자 전자서명으로 합니다.

3.2.3. 효력정지, 효력회복 및 폐지 시 신원확인

인증서 효력정지 및 폐지의 신청은 결제원 또는 등록대행기관에 하여야 하며, 신원확인은 "3.2.1 신규발급 시 신원확인"을 준용하거나 또는 전자서명을 이용하는 방법으로 신원확인을 합니다. 다만, "3.2.1 신규발급 시 신원확인" 중 온라인 신원확인을 사용하는 경우 2가지 이상의 정보를 확인합니다.

인증서 효력회복 신청은 결제원 또는 등록대행기관에 하여야 하며, 신원확인은 "3.2.1 신규발급 시 신원확인"을 준용합니다.

4. 인증서 관리

4.1. 인증서 발급 신청

4.1.1. 신청 주체

국내에 거주하는 개인(재외국민 및 외국인 포함), 사업자/단체는 인증서 발급을 신청할 수 있습니다.

4.1.2. 신청등록 절차

가입신청자는 등록대행기관의 전자금융거래 이용매체 또는 YESKEY 홈페이지를 이용하거나 등록대행기관 또는 결제원을 직접 방문하여 가입신청 등록을 할 수 있습니다.

4.2. 인증서 발급 신청 처리

4.2.1. 신청 처리 절차

결제원과 등록대행기관은 법에 따라 가입신청자의 신원을 확인합니다. 이때, 비대면 신원확인방식의 안전성 및 신뢰성을 제고하기 위하여 단말기 지정 또는 추가인증 등을 통해 가입신청자의 신원확인을 강화할 수 있습니다.

신원 확인이 완료되면 가입신청자는 등록대행기관의 전자금융거래 이용매체 또는 YESKEY 홈페이지를 통하여 인증서 발급을 신청등록합니다. 인증서 발급은 신청등록일 당일 포함 7일 내에만 가능하며 7일이 경과한 후에는 다시 인증서 발급 신청등록을 해야 합니다.

4.2.2. 발급제한

결제원과 등록대행기관은 다음 각 호의 어느 하나에 해당하는 경우에 인증서 발급을 제한합니다.

- 타인의 명의를 도용하여 신청한 경우
- 신청서에 허위 사실을 기재 또는 허위서류를 첨부한 경우
- 등록대행기관의 업무상 또는 기술상 문제로 인증서를 발급하지 못하는 경우
- 사고정보를 이용하여 신청 또는 발급한 경우
- 단말기 지정 또는 추가인증 등에 실패한 경우
- 가입자가 사망 등의 사유로 더 이상 인증서를 이용할 수 없는 상태임이 확인된 경우
- 위 각 호에 준하는 사유가 인정되는 경우로서 피해의 발생 또는 확대 방지를 위한 경우

4.3. 인증서 발급 절차 및 보호조치

4.3.1. 인증서 발급 절차

4.3.1.1. 가입신청자의 인증서 발급요청

가입신청자는 인증서 신청등록일 당일 포함 7일 내에 결제원 또는 등록대행기관 홈페이지에 접속하여 인증서 발급에 필요한 가입자 소프트웨어를 사용하여 전자서명생성정보를 생성한 후, 발급 신청시 부여받은 인가코드, 참조번호 등과 가입자정보를 이용하여 전자서명검증정보가 포함된 발급신청내역을 전송합니다.

이때 인증서 발급신청내역에 포함된 전자서명검증정보가 가입신청자가 소유하고 있는 전자서명생성정보와 합치되는지를 확인하기 위하여 발급신청내역은 해당 전자서명생성정보로 전자서명되며 상기 발급신청 과정 중 특정부분은 가입자 소프트웨어에 의해 자동으로 처리될 수 있습니다.

4.3.1.2. 결제원의 인증서 발급

인증서 발급신청을 받은 결제원은 인증서를 발급하기 전에 인증서 발급신청 내용에 대해 다음의 검증을 실시함으로써 전자서명생성정보가 가입신청자에게 유일하게 속함을 확인합니다.

- 인가코드, 참조번호, 신청내용 등을 이용한 가입신청자 및 전문 위변조 확인
- 가입신청자가 제출한 전자서명검증정보의 유일성 확인
- 가입신청자가 제출한 전자서명검증정보에 합치하는 전자서명생성정보의 소유여부 확인
- 인증서에 등록될 정보의 정확성 확인

결제원은 인증서 발급신청 내용에 대한 검증 후, 인증서 발급신청이 정당한 가입신청자에게 다음의 사항이 포함된 인증서를 결제원의 전자서명생성정보로 전자서명하여 발급합니다. 그리고 결제원 디렉토리시스템 등에 공고합니다.

- 가입자의 명칭
- 가입자의 전자서명검증정보
- 가입자와 결제원이 이용하는 전자서명 방식
- 인증서의 일련번호
- 인증서의 유효기간
- 인증서 발급자인 결제원의 명칭
- 인증서의 이용범위 또는 용도를 제한하는 경우에 이에 관한 사항 등

4.3.1.3. 관련 표준의 준수

결제원은 전자서명생성정보 생성 시 관련 표준에 따라 안전한 암호 알고리즘 또는 안전한 암호화 장치를 이용하여 전자서명생성정보를 생성합니다.

4.3.2. 가입자정보의 전송

결제원과 등록대행기관 간의 모든 가입자정보는 결제원과 등록대행기관의 업무규약에 따라 정보통신망을 통해 전송됩니다. 정보통신망을 통해 전송되는 결제원과 등록대행기관 간의 모든 가입자정보는 전자서명을 통해 위변조 여부를 확인하며 암호화하여 안전하게 전송함으로써 가입자정보의 기밀성, 무결성 등을 보장합니다.

4.4. 인증서 수령

가입신청자는 가입자 소프트웨어를 통해 결제원이 발급한 인증서를 전달받아, 인증서와 자신의 전자서명생성정보를 저장할 매체를 선택하고, 이를 안전하게 저장·관리해야 합니다. 금융인증서의 경우 가입자의 인증서와 전자서명생성정보는 결제원 저장장소에 암호화되어 안전하게 저장됩니다.

4.5. 인증서 이용

가입자는 발급받은 인증서의 용도에 따라 유효기간을 확인하여 인증서를 이용하도록 유의하여야 합니다.

대면업무용 금융인증서 이용자는 가입자가 인증서를 안전한 환경에서 이용할 수 있도록 해야 하며, 전자서명생성 및 제공 과정이 가입자의 통제 하에 이루어질 수 있도록 유의하여야 합니다.

4.5.1. 사업자 금융인증서 사용권한 위임 및 이용

사업자 금융인증서 가입자는 해당 금융인증서를 직원 등 타인에게 사용권한을 위임하여 이용하게 할 수 있습니다. 사업자 금융인증서 가입자는 이용 권한이 있는 자에 한하여 사업자 금융인증서의 사용권한이 위임될 수 있도록 유의하여야 합니다.

4.5.2. 사업자 금융인증서 사용권한 위임 절차

위임 요청자는 추가인증을 완료한 후 사용권한 위임 대상 인증서 정보를 입력합니다. 이어서 필수정보(이름, 직책, 소속부서, 사유 등)를 기재함으로써 위임을 신청합니다. 사업자 금융인증서 가입자는 해당 요청을 확인하고 요청자의 신원을 검증한 뒤 사용권한의 위임 승인 또는 거절 여부를 결정합니다.

4.6. 인증서 갱신발급

4.6.1. 갱신발급 요건

인증서 갱신은 인증서의 유효기간이 만료되기 최대 3개월 전부터 유효기간 만료일까지 전자서명정보와 유효기간이 갱신된 동일한 종류의 새로운 인증서를 발급하는 것을 말합니다. 갱신발급된 인증서는 기존 인증서의 유효기간을 승계하고 해당 인증서 종류에 따라 유효기간이 연장됩니다.

4.6.2. 갱신발급 절차

4.6.2.1. 가입자의 갱신발급 신청

가입자는 결제원 또는 등록대행기관에 접속 또는 방문하여 가입자 소프트웨어 또는 등록대행기관 소프트웨어로 전자서명정보를 생성하고 인증서 갱신신청내역을 전송합니다. 결제원은 수신한 갱신신청내역을 검증하고, 그 결과에 따라 인증서 갱신내역을 가입자에게 전송합니다. 인증서 갱신내역은 다음과 같은 내용을 포함합니다.

- 새로 생성한 전자서명검증정보
- 새로 생성한 전자서명생성정보로 전자서명된 정보
- 기존 전자서명생성정보로 상기 내용을 전자서명한 정보
- 기존 인증서 정보 등

4.6.2.2. 결제원의 인증서 갱신발급

인증서 갱신신청을 받은 결제원은 인증서를 갱신하기 전에 인증서 갱신신청내역에 포함된 내용에 대해 다음의 검증을 실시함으로써 전자서명생성키가 가입자에게 유일하게 속함을 확인합니다.

- 가입자가 제출한 전자서명검증정보의 유일성 확인
- 가입자가 제출한 전자서명검증정보로 전자서명을 검증하여 전자서명검증정

보에 합치하는 전자서명생성정보의 소유여부 확인

- 기존 전자서명생성정보로 생성한 전자서명을 검증하여 가입자 신원확인

결제원은 인증서 갱신신청내역에 포함된 내용을 검증하여 정당한 가입자인 경우 인증서를 갱신합니다. 결제원은 갱신한 인증서를 가입자에게 전송하고 결제원 디렉토리시스템 등에 공고합니다.

갱신 발급된 인증서의 DN은 기존 인증서의 DN을 승계합니다.

4.6.2.3. 가입자의 인증서 수령

가입자가 갱신발급된 인증서를 인수하는 절차는 "4.4 인증서 수령" 절차를 준용합니다.

4.6.2.4. 가입자정보의 전송

가입자정보의 전송방법은 "4.3.2 가입자정보의 전송"을 준용합니다.

4.7. 인증서 재발급

4.7.1. 재발급 요건

인증서 재발급은 가입자가 자신의 인증서를 분실하였거나 전자서명생성정보의 노출, 손상 등이 우려되어 현재 이용중인 인증서를 폐지하고 새로운 인증서를 다시 발급 받는 것을 말합니다. 재발급된 인증서의 유효기간은 인증서 재발급 일로부터 재발급 이전 인증서의 유효기간 만료일까지이며, 인증서가 재발급되면 기존의 인증서는 자동 폐지됩니다.

4.7.2. 재발급 절차

인증서 재발급은 “4.1 인증서 발급 신청 등록”, “4.2 인증서 발급 신청 처리”, “4.3 인증서 발급절차 및 보호조치” 및 “4.4 인증서 수령”을 준용합니다.

4.8. 인증서 변경

4.8.1. 가입자 등록정보 변경 요건

가입자 등록정보 변경은 인증서 내에 반영된 가입자정보 이외의 가입자 등록정보(주소, 전자우편주소, 전화번호 등)가 변경된 경우 가입자가 등록정보 변경을 요청하여 결제원에 등록된 당해 정보를 변경시키는 것을 말합니다.

4.8.2. 가입자 등록정보 변경 절차

가입자 등록정보 변경은 가입자가 직접 결제원에 인터넷으로 신청하며, 가입자정보의 전송방법은 “4.3.2 가입자정보의 전송”을 준용합니다.

4.9. 인증서 효력정지·효력회복·폐지

인증서 효력정지는 인증서 유효기간 동안 가입자의 신청에 의해 인증서의 효력을 일정기간 정지하는 것을 말합니다.

인증서 효력회복은 효력이 정지된 인증서에 대하여 가입자가 효력회복을 신청하였을 경우 유효기간 내에서 당해 인증서의 효력을 회복시키는 것을 말합니다.

인증서 폐지는 인증서 유효기간 만료 전에 가입자의 신청 또는 결제원 전자서명인증업무 수행의 안전성, 보안성, 신뢰성 등을 위한 부득이한 사유로 인해 인증서의 효력을 강제로 종료하는 것을 말합니다.

인증서 효력정지, 효력회복 및 폐지의 신청은 가입자가 결제원 또는 등록대행기관에 하여야 하며, 결제원은 해당 신청이 접수된 경우 이를 즉시 처리합니다.

4.9.1. 효력정지 사유

결제원은 가입자의 인증서 효력정지 신청이 있는 경우 당해 인증서의 효력을 정지시킬 수 있습니다.

4.9.2. 효력회복 공고

인증서의 효력이 회복된 경우 결제원은 CRL에서 당해 인증서를 삭제하여 CRL을 공고합니다.

4.9.3. 효력회복 기간의 제한

인증서의 효력이 정지한 날로부터 6월이 경과하여도 효력회복이 되지 않은 인증서는 가입자의 동의없이 자동으로 폐지됩니다.

4.9.4. 폐지 사유

결제원은 다음의 사유가 발생한 경우 당해 인증서를 폐지합니다.

- 가입자가 인증서 폐지를 신청한 경우
- 가입자의 사망, 해산 등의 사유가 발생한 경우
- 피한정후견인이 법정대리인의 동의를 필요로 하는 법률행위 범위에 인증서 발급이 포함되어 있음에도 불구하고 법정대리인의 동의 없이 인증서를 발급받은 경우
- 인증서의 유효기간이 경과된 경우
- 가입자가 명의도용 등 부정한 방법으로 인증서를 발급받은 경우
- 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출된 경우
- YESKEY 인증서비스 보안 유지 및 향상을 위하여 필요한 경우
- 가입자명, 고유식별정보 등 가입자의 주요 정보가 결제원에 등록된 정보와 불일치할 경우
- 금융인증서를 보관하는 클라우드 계정 전화번호가 불법적으로 사용되는 경우
- 가입자가 개인 금융인증서를 삭제하는 경우
- 기타 가입자가 이용약관을 준수하지 않은 경우

4.9.5. 인증서 효력정지 및 폐지목록(CRL)의 갱신과 공고

결제원은 가입자 인증서의 효력정지 및 폐지 결과를 반영하여 최대 24시간 주기로 CRL을 갱신하고, 갱신 즉시 YESKEY 홈페이지(https://www.yeskey.or.kr) 또는 결제원 디렉토리 시스템에 공고합니다. 단, 인증서 효력정지 및 폐지목록은 주기적으로 생성되는 정보이므로, 이를 통해 실시간 정보를 획득할 수는 없습니다.

4.9.6. 강제 폐지에 따른 공지

결제원은 "4.9.4 폐지 사유"에 따라 가입자의 동의 없이 인증서를 폐지한 경우 당해 가입자에게 전자우편 또는 전화(문자메시지 포함) 등을 이용하여 해당 사실을 통지합니다.

4.9.7. 부정발급 및 이상거래 모니터링

결제원은 전자서명법, 전자서명법 시행령 및 전자서명법 시행규칙과 전자서명 인증업무 운영기준에 의거 인증서의 부정발급 또는 인증서비스 이상거래 여부를 상시 24시간 365일 모니터링하며, 이상 징후가 탐지될 경우 인증서의 발급을 차단하거나 이용을 제한할 수 있습니다.

- 부정발급 모니터링은 인증서가 가입자 외의 제3자에 의해 무단으로 발급되는 것을 탐지하여 부정발급 시도를 사전에 차단하는 것을 의미합니다.

- 이상거래 모니터링은 MO인증 및 인증서비스 등이 이용자 외의 제3자에 의해 무단으로 이용되는 것을 탐지하여, 부정 이용을 제한하는 것을 의미합니다.

- 결제원은 부정발급 및 이상거래 모니터링을 위해 사용한 가입자 및 이용자 정보를 안전하게 관리하고 적법한 범위 내에서 부정발급 및 이상거래 모니터링 목적으로만 사용합니다.

- 발급 및 이용이 제한된 경우, 발급받은 기관을 직접 방문하시거나 결제원을 방문 또는 유선으로 본인확인을 거친 경우에만 제한을 해제할 수 있습니다.

4.10. 실시간 인증서 상태확인(OCSP) 서비스

실시간 인증서 상태확인(OCSP)서비스란 가입자가 이용자에게 접속하여 자신의 인증서를 제출하면 이용자는 전자서명을 검증하고 인증서 일련번호를 결제원 OCSP(Online Certificate Status Protocol) 시스템에 전송하며, 결제원은 가입자가 제출한 인증서의 유효성을 실시간으로 검증하여 검증결과를 이용자에 회신하는 서비스입니다.

이용자는 결제원과 이 서비스 이용계약을 체결하고 서버인증서를 발급받아 자신의 웹서버에 설치하여야 합니다. 이와 관련된 S/W는 결제원의 기술협력사로부터 지원받을 수 있습니다.

이 서비스 이용수수료는 월단위로 이용건수에 비례하여 부과되며, 이용계약 해지 등 세부사항은 해당 계약내용에 따릅니다.

4.11. 서비스 가입 철회

가입자의 서비스 가입 철회는 “4.9 인증서 효력정지·효력회복·폐지”의 인증서 폐지 절차를 준용하며, “5.5 기록 보존”을 준용하여 해당 가입자의 전자서명인증업무 관련 정보를 보존합니다.

4.12. 기타 부가 서비스

4.12.1. 시점확인서비스

결제원은 법 제18조(전자문서의 시점확인)에 따라 전자문서가 결제원에 제시된 시점을 전자서명하여 확인시켜주는 시점확인서비스를 제공할 수 있습니다.

이용자는 이 서비스 이용약관에 동의하고 시점확인 S/W를 자신의 서버에 설치하여야 하며, 이와 관련된 S/W는 결제원의 기술협력사로부터 지원받을 수 있습니다. 기타 이용방법, 이용조건 및 이용계약 해지 등 세부사항은 해당 약관내용에 따릅니다.

5. 시설 및 운영 관리

5.1. 물리적 보호조치

결제원은 가입자의 등록정보 관리시스템, 전자서명키 생성·관리시스템, 인증서 생성·발급·관리시스템, 인증서 실시간상태조회시스템, 시점확인시스템 등(이하 "인증시스템"이라 한다)의 보안성 제고를 위하여 세부사항을 정합니다.

5.1.1. 물리적 접근 통제

결제원은 외부인의 침입이나 불법적 접근 또는 화재 등의 물리적 위협으로부터 인증시스템 등이 설치된 장소를 다음과 같이 안전하게 보호합니다.

- 결제원의 인증시스템은 별도의 통제구역 내에 설치·운영
- 결제원의 출입통제 시스템은 신원확인카드, 지문인식 등을 다중으로 결합하여 통제구역에 대한 접근통제
- 결제원은 하드웨어 보수 등의 업무수행을 위하여 비인가자가 인증시스템 운영실 등에 출입할 경우에 반드시 담당관리자가 동행
- 결제원은 출입통제시스템과 연계하여 통제구역 출입내역을 기록하고 정기적으로 그 기록을 검토
- 결제원은 다음의 감시통제시스템을 설치하며 이상상황 발생시 경보 및 인접시설간 유·무선 연락기능을 확보

  · CCTV 카메라 및 모니터링시스템

  · 침입감지시스템

- 결제원은 2인 이상의 청원경찰을 배치하여 보안경비업무 수행

5.1.2. 수해 방지

결제원은 침수로부터 인증시스템을 안전하게 보호하기 위하여 바닥으로부터 최소 30cm이상의 위치에 설치하며 누수의 감지 및 신속한 대처를 위하여 누수경보기를 이용합니다.

5.1.3. 화재 예방

결제원은 인증시스템 운영실 등에 화재예방을 위하여 화재 탐지기, 휴대용 소화기, 자동소화설비 등을 설치하고 있습니다.

5.1.4. 전원

결제원은 갑작스러운 정전으로 인한 시스템의 심각한 피해를 방지하기 위하여 무정전전원공급장치를 이용하며, 별도의 자가발전기를 설치하여 안정적으로 전원을 공급합니다.

5.1.5. 방호

인증시스템이 운영되는 시스템실의 외벽은 전자서명인증업무의 제공에 필수적으로 요구되는 인증시스템을 외부 침입으로부터 보호할 수 있도록 설계합니다.

- 외벽은 천장, 바닥을 통한 외부 침입이 불가능하도록 마감
- 인증시스템과 타 시스템을 분리할 수 있도록 시스템실내 케이지 설계
- 창문이 있는 경우 강화유리 또는 강화필름으로 코팅한 유리를 사용

5.1.6. 항온항습, 통풍

인증시스템 운영실은 적정용량의 항온항습장치를 설치 운영하며, 통풍창은 사람이 통과할 수 있을 경우 차폐막을 설치합니다.

5.1.7. 기타 보호설비

인증시스템 운영실 내에 물리적인 침입을 감지하고 이를 경보하여 주는 장치를 다음과 같이 설치합니다.

- 운영실내에 진동감지장치, 음향감지장치 등의 침입감지장치 설치
- 침입감지장치에 이상이 생겼을 경우 이를 감지하는 기능
- 침입감지장치가 침입을 감지하였을 경우 관리자에게 즉각 알리는 기능

5.1.8. 매체 저장

결제원은 주요 매체를 접근이 제한된 장소의 내화금고에 저장하여 물리적으로 접근을 통제합니다.

5.1.9. 시설 및 장비의 폐기 처리

결제원은 시설 및 장비 등을 폐기하는 경우 물리적, 논리적으로 정보복구가 불가능한 방법으로 폐기합니다.

5.1.10. 원격지 백업설비 안전운영

결제원은 인증서 등 중요정보 보관을 위해 10km 이상 떨어진 곳에 원격지 백업설비를 운영하고 있으며, 출입통제시스템, 침입감지장치 등 보호설비를 구축・운영하고 있습니다.

5.2. 절차적 보호조치

5.2.1. 전자서명인증업무에 대한 업무 분장

결제원은 전자서명인증업무의 안전성과 신뢰성을 확보하기 위하여 결제원 소속 직원으로 전자서명인증업무 수행인력을 역할별로 분리하여 운용하며, 해당 인력은 “5.3.1 전자서명인증업무 인력의 자격, 경력 등 요구사항”에서 정한 자격 및 경력을 갖추어야 합니다.

- 결제원은 모든 보호조치를 계획, 감독, 통제하는 관리책임자를 지정
- 결제원은 인증업무 정책을 관리하는 정책관리자를 지정
- 결제원은 모든 보호조치의 실행을 담당하는 보안관리자를 지정
- 결제원은 주요시설의 유지·관리를 위하여 인증시스템 관리, 네트워크 관리 등을 담당하는 전문인력(관련분야 2년 이상 경력자)인 보안실무자를 1인 이상 확보
- 결제원은 가입자의 등록정보관리, 인증서 생성·발급·관리, 시점확인 기능 등을 지원하는 인증시스템의 설치 운영 및 유지보수에 2인 이상의 직원을 배치하여 공동으로 업무를 수행

5.2.2. 동일인에 의해 동시 수행될 수 없는 전자서명인증업무

결제원은 전자서명인증업무 운영시의 신뢰성 및 보안성 확보를 위하여 다음과 같이 업무분리 원칙을 준수합니다.

- 결제원 전자서명생성정보 생성 업무는 3인 이상이 공동으로 수행
- 가입자 전자서명생성정보 생성 업무와 인증서 발급 및 관리 업무는 2인 이상이 공동으로 수행
- 동일 시스템에 대한 운영 및 감사업무는 동일하지 않은 자가 각각 수행

5.2.3. 업무 담당자 현황 및 인증 방법

5.2.3.1. 업무 담당자 현황

구 분	담당자
인증업무 관리책임자	금융인증센터장
정책관리자	인증제도팀장 인증서비스팀장
보안관리자	인증시스템실장 인증운영팀장
보안실무자	인증운영팀
가입자관리자	인증서비스팀
키생성관리자	인증운영팀
금고관리자	인증운영팀
사업담당자	인증제도팀 인증서비스팀
개발자	인증개발팀
운영자	인증운영팀
감사관리자	감사실
고객센터	고객지원실

5.2.3.2. 인증 방법

결제원의 전자서명인증업무 담당자는 신원확인카드, 지문인식 등 다중으로 결합되어 보호되는 통제구역을 통과한 후에 방화벽 및 서버보안 소프트웨어로 보호되는 시스템을 관리할 수 있습니다.

5.3. 인적 보안

결제원은 직원 채용시 신원조사를 실시하고 있으며, 인증시스템 운영인력의 자격과 자질을 주기적으로 조사하고 동 사항의 유지여부를 지속적으로 관리합니다.

5.3.1. 전자서명인증업무 인력의 자격, 경력 등 요구사항

결제원은 전자서명인증업무에 필요한 시설 및 장비의 운영인력으로서 다음의 요건을 갖춘 자를 10인 이상 확보합니다.

- 정보통신기사·정보처리기사 및 전자계산기조직응용기사 이상의 국가기술자격 또는 이와 동등 이상의 자격이 있다고 과학기술정보통신부가 인정하는 자격을 갖출 것
- 과학기술정보통신부가 정하여 고시하는 정보보호 또는 정보통신 운영·관리 분야에서 2년 이상 근무한 경력이 있을 것

5.3.2. 전자서명인증업무 교육, 업무순환에 관한 사항

- 결제원은 보호조치에 대하여 소속직원이 관련내용을 숙지할 수 있도록 내부교육 등의 필요한 조치를 취합니다.
- 결제원은 보안관리자 및 보안실무자, 인증시스템을 관리하는 직원이 연 1회 이상 정보보호관련 내부 또는 외부교육을 이수하도록 합니다.
- 결제원은 인증시스템을 관리하는 직원에 대하여 업무상 지득한 기밀사항의 준수에 관한 서약서를 작성하여 날인하도록 합니다.
- 결제원은 업무환경의 변화 등으로 인하여 보호조치의 수정·보완이 필요한 경우, 이를 지체없이 보완합니다.
- 결제원은 인증시스템을 관리하는 직원이 인사이동 또는 퇴직하는 경우에는 내부규정에 따라 계정삭제 및 저장매체 반납 등의 적절한 조치를 취하도록 합니다.

5.3.3. 비인가된 행위에 대한 처벌에 관한 사항

소속직원의 비인가된 행위에 대하여 결제원은 인사규정 등 내부 규정이 정하는 바에 따라 해당 직원을 징계합니다.

5.4. 감사 기록

5.4.1. 감사기록의 유형 및 보존기간

결제원은 인증시스템에서 발생한 다음의 사건에 대한 세부내역을 감사기록에 2년간 보존합니다.

- 가입자정보의 입력・접근・변경・삭제
- 전자서명정보의 생성・접근・파기
- 인증서의 생성・발급・갱신・효력정지・폐지
- 가입자 인증서의 등록 및 관리
- 전자문서의 시점확인
- 인증시스템의 시작과 종료
- 계정의 추가 및 삭제
- 사용자 권한 변경
- 로그인(login) 및 로그오프(logoff)
- 기타 인증시스템 관리자의 주요 활동

5.4.2. 감사기록 보호조치

결제원의 감사관리자는 인증시스템의 감사기록을 조회하고 관리합니다. 각 시스템의 감사기록은 감사관리자가 총괄 관리하며, 시스템의 각 업무관리자는 각자의 업무에 대한 감사기록만을 열람할 수 있습니다.

5.4.3. 감사기록 백업주기 및 절차

결제원은 감사기록을 매일 백업받아 하드디스크 이외의 저장매체에 보존합니다.

5.5. 기록 보존

5.5.1. 보존기록의 유형 및 보존기간

결제원은 다음의 업무와 관련된 내역을 당해 인증서 효력이 소멸된 날로부터 10년 동안 기록·보존합니다.

- 인증서 발급 및 관리 등 전자서명인증업무
- 결제원 전자서명인증시스템 등의 운영업무

5.5.2. 보존기록의 보호조치

결제원은 보존기록의 위·변조 및 훼손 등을 방지하기 위하여 다음과 같이 보존기록을 보호합니다.

- 전자문서는 전자서명하여 안전하게 보관합니다.
- 일반문서는 잠금장치가 설치된 캐비닛에 보관합니다.

문서관리자는 모든 보존기록을 관리하며, 기타 관리자들은 자신의 업무범위 내의 보존기록만을 조회할 수 있습니다.

결제원은 “5.5.1”의 기록을 전자서명인증업무를 수행하는 시설과 해당 시설로부터 10Km이상의 원격지 저장설비에 각각 1부씩 보존합니다.

보존기간이 만료된 기록은 복구 불가능하도록 안전하게 파기합니다.

5.5.3. 보존기록의 백업주기 및 백업절차

결제원은 보존기록을 매일 일별 백업받아 보존합니다.

5.6. 전자서명인증사업자의 전자서명생성정보 갱신

결제원의 전자서명생성정보가 갱신되면 결제원은 갱신된 결제원 인증서를 디렉토리시스템에 게시함으로써 이용자에게 배포하고, 가입자 인증서 발급·갱신·

재발급시 결제원 인증서를 내려줌으로써 가입자에게 배포합니다.

5.7. 장애 및 재해복구

결제원은 인증시스템 장애, 전자서명생성정보 유출 등에 따른 전자서명인증업무의 중단 또는 그와 동등한 사고와 지진·홍수·화재 등 재해에 대비하여 신속한 대응 및 복구체제를 구축하고 있습니다.

5.7.1. 전자서명인증업무 장애 유형

다음의 장애 유형은 “주의”의 비상상황 등급으로 분류합니다.

- 해킹 등 침해사고에 의한 일부 가입자 전자서명생성정보 유출
- 인증시스템의 장애, 오작동 등으로 인한 장애
- 웜·바이러스, Dos 공격 등으로 인한 장애

다음의 장애 유형은 “경계”의 비상상황 등급으로 분류합니다.

- 전자서명생성정보(백업 포함) 손상
- 해킹 등 침해사고에 의한 대량의 가입자 전자서명생성정보 유출
- 실시간 인증서 상태확인 서비스 장애
- 인증서 발급서비스 장애

다음의 장애 유형은 “심각”의 비상상황 등급으로 분류합니다.

- 가입자 인증서 발급에 사용하는 전자서명생성정보 유출
- 해킹 등 참해사고에 의한 가입자 전자서명생성정보가 대량 유출되어 부정사용되는 사고 발생

5.7.2. 전자서명인증업무 장애 유형별 복구

- 웜·바이러스, Dos 공격 등으로 인한 장애의 경우 관련 침입차단시스템을 이용하여 해당 IP 및 포트를 차단하고, 침입탐지시스템을 통한 모니터링 강

화조치를 취합니다.

- 해킹으로 인한 가입자 인증서 유출의 경우 유출된 가입자의 인증서를 폐지하고 가입자에게 통보합니다.
- 웜·바이러스, Dos 공격 및 해킹 등에 대비하여 방화벽, 침입탐지시스템, 보안S/W, ID, PASSWORD 관리 및 S/W의 최신패치로 방어하며, 피해 발생시 백업데이터로 복구합니다.
- 인증시스템을 이중화로 구성·운영하며 백업센터를 운영함으로써 지진·홍수·화재 등 재해 및 장애에 대비합니다.
- 논리적 장애 발생 시 장애이전시점 복구 기능을 이용하여 복구합니다.
- 시스템 접근 가능 IP통제, 서버보안S/W 설정 등으로 주요 자원에 대한 접근통제 및 복구체제를 구성합니다.

5.7.3. 전자서명인증업무 장애방지 등 연속성 보장 대책

- 결제원은 인증시스템을 이중화하여 무정지 운영체제를 구축하고 백업센터를 운영하여 장애의 방지에 최선의 노력을 다합니다.
- 결제원은 가입자 인증서 등의 주요 데이터의 훼손·멸실이 발생하였을 경우 백업된 자료를 이용하여 신속히 복구하여 서비스의 연속성을 보장합니다.
- 결제원은 전자서명인증업무 운영인력을 주야간으로 운영하여 연중 무휴로 전자서명인증업무를 제공합니다.

5.8. 업무 휴지, 폐지, 종료

5.8.1. 전자서명인증업무 휴지

자연재해 또는 천재지변이 아닌 불가피한 사정으로 결제원이 전자서명인증업무의 전부 또는 일부를 휴지하고자 하는 때에는 휴지기간을 정하여 휴지하고자

하는 날의 30일전까지 전자우편, 홈페이지 등을 통해 가입자에게 요금의 반환, 가입자의 개인정보 폐기 등 가입자 보호조치 내용을 포함하여 업무의 휴지를 통보합니다.

5.8.2. 전자서명인증업무 폐지

자연재해 또는 천재지변이 아닌 불가피한 사정으로 결제원이 전자서명인증업무를 폐지하고자 하는 때에는 폐지하고자 하는 날의 60일전까지 전자우편, 홈페이지 등을 통해 가입자에게 요금의 반환, 가입자의 개인정보 폐기 등 가입자 보호조치 내용을 포함하여 업무의 폐지를 통보합니다. 결제원이 전자서명인증업무를 폐지할 경우 “5.5 기록 보존”을 준용하여 해당 가입자의 전자서명인증업무 관련 정보를 10년간 보존 후 폐기합니다.

6. 기술적 보호 조치

6.1. 전자서명생성정보 보호

- 결제원은 인가된 자만이 전자서명생성정보를 생성할 수 있도록 합니다.
- 결제원은 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되는 안전한 키 생성시스템에서 전자서명생성정보를 생성합니다.

6.2. 전자서명생성정보 보호조치

6.2.1. 전자서명생성정보 저장장치

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

6.2.2. 전자서명생성정보 생성·사용 후 안전한 삭제 방법

결제원은 전자서명생성정보의 생성 및 사용이 종료된 후 지체 없이 시스템 메모리에서 전자서명생성정보를 삭제합니다.

6.2.3. 전자서명생성정보 파기 방법

결제원은 인증서의 유효기간이 만료되거나 전자서명생성정보가 훼손·유출되었을 경우 당해 전자서명생성정보를 복구 불가능하도록 완전히 삭제합니다.

6.2.4. 전자서명생성정보 백업

결제원은 전자서명생성정보에 대해 원본 이외에 백업본 2부를 작성하여, 1부는 주센터의 내화금고에 보관하고 나머지 1부는 재해복구센터의 내화금고에 보관합니다.

6.3. 전자서명생성정보 및 전자서명검증정보의 관리

결제원은 전자서명생성정보의 분실·훼손·도난·유출 방지를 위하여 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되는 안전한 키 생성시스템에서 인가된 자만이 전자서명생성정보를 생성하여 보관할 수 있도록 합니다.

6.3.1. 분실신고 접수시 처리

가입자로부터 분실신고를 접수한 경우 결제원은 지체없이 가입자의 신원을 확인하고 가입자의 신청에 따라 즉시 폐지 등의 처리를 한 후 가입자에게 통보합니다.

6.4. 데이터 보호 조치

전자서명생성정보의 유출방지를 위하여 전자서명생성정보 생성에 직접적으로 연관된 데이터는 전자서명생성정보 생성 즉시 메모리에서 삭제되며, 기타 데이터를 이용하여 전자서명생성정보를 유추하는 것은 불가능합니다.

6.5. 시스템 보안 통제

- 결제원은 인증시스템을 2중화하여 구성합니다.
- 결제원은 전자서명인증업무와 관련된 주요 프로그램 또는 프로세스의 동작 여부를 점검할 수 있는 시스템을 설치 운영합니다.
- 결제원은 루트관리자의 권한을 제한할 수 있는 소프트웨어를 설치합니다.
- 결제원은 인증시스템의 운영에 필요한 프로그램만을 설치합니다.
- 결제원은 인증시스템의 운영체제에서 불필요한 사항은 삭제합니다.
- 결제원은 인증시스템 운영체제의 문제점 해결을 위한 최신의 패치를 설치하여 운영합니다.
- 결제원은 인증시스템을 잠금장치가 장착된 보안캐비넷에 보관하고, 장금장치의 열쇠는 별도의 보관함을 마련하여 관리합니다.

- 결제원은 인증시스템에 대한 논리적인 접근통제를 설정합니다.
- 결제원은 인증시스템의 추가/폐기/변경(운영체제의 변경, 패치 등)에 관한 사항을 관리대장에 기록하고 유지합니다.
- 결제원은 인증시스템의 추가/폐기/변경에 관한 사항을 내부 지침에 의거 관리합니다.
- 결제원은 서비스 방해공격을 방지하기 위하여 침입탐지시스템을 사용합니다.

6.6. 시스템 운영 관리

결제원은 전자서명인증 S/W의 형상관리 등 인증시스템의 운영에 대한 형상관리를 합니다.

- 인증시스템의 S/W 등록에 대한 형상관리
- 인증시스템의 변경사항 등 운영관리에 대한 형상관리

6.7. 네트워크 보호조치

- 결제원은 인증 네트워크를 이중화하여 구성하여 장애에 대비하고, 침입차단 및 침입탐지시스템을 사용하여 네트워크를 보호합니다.
- 결제원은 침입차단 및 침입탐지시스템을 설치합니다.
- 결제원은 네트워크회선을 전자서명인증역무 제공을 위하여 별도의 회선을 사용합니다.
- 결제원은 침입차단 및 침입탐지시스템에 해당 기능의 소프트웨어만 설치합니다.
- 결제원은 침입탐지시스템의 데이터베이스를 주기적으로 갱신하고, 네트워크관리시스템을 이용하여 인증시스템을 지속적으로 모니터링합니다.
- 결제원은 로그기록을 주기적으로 분석하여 침입시도, 네트워크 부하 등을 파악하고 이에 적절하게 대처합니다.
- 결제원은 침입차단 및 침입탐지시스템에 대한 논리적인 접근통제를 설정합니다.

- 결제원은 침입차단 및 침입탐지시스템에 대한 추가/폐기/변경에 관한 사항을 관리대장에 기록하고 유지합니다.
- 결제원은 침입차단 및 침입탐지시스템의 추가/폐기/변경에 관한 사항을 내부지침에 의거 관리합니다.

6.8. 부가서비스 보호조치

결제원은 “5.1.1 인증시스템 운영실의 격실분리에 관한 사항”에 따라 인증서 상태확인 기능을 제공하는 시스템 및 시점확인 기능을 제공하는 시스템 운영시 다른 설비와는 별도의 운영실로 분리하는 등 보호조치를 마련하여 시행하고 있습니다.

7. 인증서 형식

7.1. 인증서 형식

7.1.1. 인증서 프로파일

결제원이 발급하는 가입자 인증서는「전자서명 인증서 프로파일 기술규격」을 준수하며 다음의 내용을 포함합니다.

1) 기본필드

#	필드명	ASN.1 타입	지원여부		Note	비고
			생성	처리		
1	Version	INTEGER	m	m	0x02 (버전 3)	
2	Serial Number	INTEGER	m	m	자동할당	
3	Signature	OID	m	m		
4	Issuer		m	m	[KCAC.TS.DN] 준수 C(Country)는 printableString, 그이외의 속성값은 utf8String	
	type	OID	m	m		
	value	printableString 또는 utf8String	m	m		
5	Validity		m	m	인증서 유효기간	
	notBefore	UTCTime	m	m		
	notAfter	UTCTime	m	m		
6	Subject		m	m	[KCAC.TS.DN] 준수 C(Country)는 printableString, 그이외의 속성값은 utf8String	
	type	OID	m	m		
	value	printableString 또는 utf8String	m	m		
7	Subject Public Key Info		m	m		
	algorithm	OID	m	m	전자서명인증체계 알고리즘 기술규격 준수	
	subjectPublicKey	BIT STRING	m	m		
8	Extensions	Extensions	m	m		[1]

[1] 아래 “2) 확장필드” 참조

2) 확장필드

#	필드명	ASN.1 타입	C	지원여부		Note	비고
				생성	처리		
1	Authority Key Identifier		n	m	m		
	keyIdentifier	OCTET STRING		m	m	발급자 인증서의 KeyID	
	authorityCertIssuer	GeneralNames		m	m		
	authorityCertSerialNumber	INTEGER		m	m		
2	Subject Key Identifier	OCTET STRING	n	m	m	subjectPublicKey 정보의 160비트 해쉬값	
3	Key Usage	BIT STRING	c	m	m	전자서명, 부인봉쇄	
4	Certificate Policy		c	m	m		
	policyIdentifier	OID		m	m	인증서 정책	
	policyQualifiers			m	m		
	PolicyQualifierId	OID		m	m	CPS, UserNotice	
	Qualifier			m	m		
	CPSuri	IA5String		m	m	준칙의 URI	
	UserNotice			m	m		
	NoticeReference	SEQUENCE		-	-		
	ExplicitText	BMPString		m	m	인증서 표시규격 준수	
5	Policy Mappings		-	-	-		
6	Subject Alternative Names	otherName	n	m	m	id-kisa-identifyData에 가입자 한글실명과 VID	
		rfc822Name		o	m		
7	Issuer Alternative Names	otherName	n	o	m	id-kisa-identifyData에 인증기관 한글실명	
8	Extended Key Usage	OID	n	o	o	id-kisa-HSM	
9	Basic Constraints		-	x	x		
10	Policy Constraints		-	-	-		
11	Name Constraints		-	-	-		
12	CRL DistributionPoint		n	m	m		
	distributionPoint	DistributionPoint Name		m	m	CRL 획득 정보	
	reasons	ReasonFlags		-	-		
	cRLIssuer	GeneralNames		o	m	간접 CRL발급시 사용	
13	Authority Information Access		n	m	m		
	accessMethod	OID		m	m	id-ad-ocsp	
	accessLocation	GeneralNames		m	m	OCSP URI	

7.1.2. 전자서명의 생성

결제원 전자서명은 공개키 알고리즘 적용으로 전자서명생성정보를 제어할 수 있는 가입자만이 전자서명을 생성할 수 있습니다. 결제원은 전자서명생성정보에 비밀번호 등의 접근통제수단을 적용하여 가입자(또는 가입자의 서명 권한을 위임받은 자) 이외의 다른 자가 가입자의 전자서명생성정보에 접근할 수 없도록 가입자 인증 및 접근통제 기능을 제공합니다.

7.2. 인증서 유효성 확인 정보 형식

7.2.1. 인증서 효력정지 및 폐지목록(CRL) 프로파일

결제원이 생성하는 CRL은「전자서명 인증서 효력정지 및 폐지목록 프로파일 기술규격」을 준수하며 다음의 내용을 포함합니다.

1) 기본필드

#	필드명	ASN.1 타입	지원여부		Note	비고
			생성	처리		
1	Version	INTEGER	m	m	0x01 (버전 3)	
2	Signature	OID	m	m		
3	Issuer		m	m	[KCAC.TS.DN] 준수 C(Country)는 printableString, 그이외의 속성값은 utf8String	
	type	OID	m	m		
	value	printableString 또는 utf8String	m	m		
4	This Update	UTCTime	m	m	CRL 생성시점	
5	Next Update	UTCTime	m	m	CRL 다음 갱신예정 시점	
6	Revoked Certificates		m	m		[1]
	userCertificate	INTEGER	m	m		
	revocationData	UTCTime	m	m		
	crlEntryExtensions	Extensions	m	m		[2]
7	CRL Extensions	Extensions	m	m		[3]

[1] 효력정지 및 폐지된 인증서가 없는 경우 Revoked Certificates 필드를 생성하지 않음

[2] 아래 “3) CRL 엔트리 확장필드” 참조

[3] 아래 “2) CRL 확장필드” 참조

2) CRL 확장필드

#	필드명	ASN.1 타입	C	지원여부		Note	비고
				생성	처리		
1	Authority Key Identifier		n	m	m		
	keyIdentifier	OCTET STRING		m	m	인증기관 인증서의 KeyID	
	authorityCertIssuer	GeneralNames		m	m		
	authorityCertSerialNumber	INTEGER		m	m		
2	Issuer Alternative Names	otherName	n	o	m	id-kisa-identifyData에 인증기관 한글실명	
3	CRL Number	INTEGER	n	m	m		
4	Issuing DistributionPoint		c	m	m		
	DistributionPointName	IA5String		m	m	CRL 획득 정보	[1]
	onlyContainsUserCerts	BOOLEAN		-	-		
	onlyContainsCACerts	BOOLEAN		-	-		
	onlySomeReasons	BIT STRING		-	-		
	IndirectCRL	BOOLEAN		o	m		[2]

[1] CRLDP 와 동일 ([KCAC.TS.DSCP] 참조)

[2] IndirectCRL을 사용할 때는 반드시 “TRUE”로 설정

3) CRL 엔트리 확장필드

#	필드명	ASN.1 타입	C	지원여부		Note	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		

7.2.2. 실시간 인증서 상태확인(OCSP) 서비스용 인증서 프로파일

결제원은 인터넷진흥원으로부터 다음과 같은 내용을 포함하는 실시간 인증서 상태확인 서비스용 인증서를 발급받아 사용합니다.

1) 기본필드

“7.1 인증서형식, 1) 기본필드”와 동일합니다.

2) 확장필드

#	필드명	ASN.1 타입	C	지원여부		Note	비고
				생성	처리		
1	Authority Key Identifier		n	m	m	세가지 값을 모두 사용	
	keyIdentifier	OCTET STRING		m	m		
	authorityCertIssuer	GeneralNames		m	m		
	authorityCertSerialNumber	INTEGER		m	m		
2	Subject Key Identifier	OCTET STRING	n	m	m	subjectPublicKey 정보의 160비트 해쉬값	
3	Key Usage	BIT STRING	c	m	m	전자서명, 부인봉쇄	
4	Certificate Policy		c	m	m		
	policyIdentifier	OID		m	m	인증서 정책	
	policyQualifiers			m	m		
	PolicyQualifierId	OID		m	m	CPS, UserNotice	
	Qualifier			m	m		
	CPSuri	IA5String		m	m	OCSP인증서를 발급한 인증기관의 준칙 URI	
	UserNotice			m	m		
	NoticeReference	SEQUENCE		-	-		
	ExplicitText	BMPString		m	m	인증서 표시규격 준수	
5	Policy Mappings		-	-	-		
6	Subject Alternative Names	otherName	n	m	m	id-kisa-identifyData에 가입자 한글실명과 VID	
7	Issuer Alternative Names	otherName	n	o	m	id-kisa-identifyData에 인증기관 한글실명	
8	Extended Key Usage	OID	c	m	m		
9	Basic Constraints		-	x	x		
10	Policy Constraints		-	-	-		
11	Name Constraints		-	-	-		
12	CRL DistributionPoint		n	m	m		
	distributionPoint	DistributionPointName		m	m	CRL URI	
	reasons	ReasonFlags		o	m		
	cRLIssuer	GeneralNames		o	m	간접 CRL발급시 사용	
13	Authority Information Access		n	o	m		
	accessMethod	OID				id-ad-ocsp	
	accessLocation	GeneralNames					
14	OCSP No Check	OID	n	o	m	id-pkix-ocsp-nocheck	

8. 평가 및 감사

8.1. 평가 및 감사 현황

결제원은 전자서명법 및 동법 시행령에 따라 인정기관으로부터 운영기준 준수사실의 인정을 받기 위해 매년 평가기관에 평가를 받습니다.

또한, 전자서명인증업무는 중립적이며 신뢰성 있는 결제원 내부의 독립된 감사조직으로부터 연 1회 이상 감사를 받습니다.

8.2. 평가자 및 감사자의 신원, 자격

운영기준 준수사실 평가자의 신원 및 자격은 전자서명법 시행령을 따릅니다.

결제원 내부 감사는 결제원 감사규정에 따른 자격을 갖춘 자가 실시합니다.

8.3. 평가 대상과 평가자의 관계 및 감사 대상과 감사자의 관계

운영기준 준수사실 평가기관은 전자서명법 시행령에 따라 평가 업무의 독립성, 객관성, 공정성 및 신뢰성을 확보할 수 있는 기관으로 결제원과 독립성을 유지하여야 합니다.

결제원 내부감사는 전자서명인증업무와 독립된 조직에서 실시합니다.

8.4. 평가 및 감사 목적, 내용

결제원은 인정기관으로부터 운영기준의 준수사실을 인정받기 위하여 평가를 받으며, 평가내용은 과학기술정보통신부가 고시한 전자서명인증업무 운영기준에 의거하여 평가기관이 정한 세부평가 기준에 따릅니다.

결제원 내부 감사 조직은 전자서명인증업무 수행 관련 제반 사항 및 준칙 준수 여부 등에 대하여 감사합니다.

8.5. 부적합 사항에 대한 조치

결제원이 운영기준의 준수사실을 인정받고 전자서명법 제17조 각호의 어느 하나에 해당하는 경우, 과학기술정보통신부 장관은 기간을 정하여 시정을 명할 수 있습니다. 결제원은 기간 내에 시정명령을 이행하여야 합니다.

결제원 내부 감사 과정에서 부적합 사항 등이 발생할 경우, 인증업무 관리책임자는 결제원 감사규정에 따른 후속 조치를 실시합니다.

8.6. 결과 보고

평가기관은 결제원의 운영기준 준수사실에 대해 평가를 하고 그 결과를 인정기관에 제출하여야 합니다.

내부 감사 결과는 결제원 감사규정에 따라 감사 조직의 결재권자에 보고됩니다.

9. 전자서명인증업무 보증 등 기타사항

9.1. 수수료

결제원은 가입자 또는 이용자에게 전자서명인증서비스 제공에 따른 수수료를 부과할 수 있으며, 결제원 또는 등록대행기관은 판단에 따라 수수료를 면제하거나 할인요율을 적용할 수 있습니다.

9.1.1. 인증서 발급·갱신 수수료

결제원 또는 등록대행기관은 인증서를 발급하거나 갱신할 때 아래 표와 같이 수수료를 받으며, 재발급의 경우 수수료를 받지 않습니다.

(단위 : 원/년, 부가세 별도)

구 분			수수료
개인	금융인증서	범용	무료
		대면업무용	
	공동인증서	범용	4,000
		은행/신용카드/보험용	무료
		기타	무료
사업자	금융인증서	금융공공용	4,000
		전자세금용	4,000
		기타	용도별 상이(별도 계약)
	공동인증서	범 용	100,000
		은행/신용카드/보험용	4,000
		전자세금용	4,000
		조달청 원클릭용	무료
		금융위원회 CTR용	4,000
		서버용	1,000,000
		기 타	용도별 상이(별도 계약)

9.1.2. 인증서 접근 수수료

결제원은 인증서를 열람·확인하는 이용자에게 수수료를 부과하지 않습니다.

9.1.3. 인증서 유효 여부 확인 수수료

결제원은 인증서의 유효 여부를 확인하려는 이용자에게 아래 표와 같이 수수료를 받습니다.

구분	효력정지 및 폐지목록(CRL) 조회	실시간 인증서 상태확인(OCSP) 서비스
수수료	무료	별도계약에 따름

9.1.4. 기타 서비스에 대한 수수료

결제원은 필요한 경우 기타 서비스에 대한 수수료를 부과할 수 있습니다.

9.1.5. 환불

결제원과 등록대행기관은 가입자가 인증서 발급신청일 당일 포함 7일 이내에 발급신청을 취소하는 경우와 인증서 발급일 당일 포함 7일 이내에 발급을 취소하는 경우에 한하여 수수료를 환불하고, 당해 인증서를 폐지합니다. 다만, 결제원과 등록대행기관은 수수료를 환불할 때 필요 경비를 공제할 수 있습니다.

또한 인증서 발급신청일 또는 발급일 당일 포함 7일이 경과하였더라도 결제원 또는 등록대행기관 귀책사유로 인한 가입자의 환불 요구에 대해서는 수수료를 환불하고, 당해 인증서를 폐지합니다.

9.2. 배상

결제원은 전자서명인증업무의 수행과 관련하여 가입자 또는 이용자에게 손해를 입힌 경우에는 그 손해를 배상합니다.

9.3. 영업비밀

결제원, 이용자, 가입자 및 등록대행기관은 상호 영업비밀을 보호합니다.

9.4. 개인정보 보호

9.4.1. 개인정보 수집 및 이용목적

YESKEY 인증서비스에서는 인증서 발급 및 관리, 전자서명인증서비스 관련 각종 공고 및 통보, 인증서 부정발급 확인·부정사용 방지 및 단말기 지정 등의 목적을 위해 법, 시행령 및 시행규칙에서 규정한 정보 등 다음과 같이 최소한의 개인정보를 수집하고 있습니다.

- 수집하는 개인정보 항목 : 성명, 전자우편(E-mail)주소, 전화번호 또는 휴대전화번호, 인증서 담당자 정보(부서, 전화번호, 팩스번호, 전자우편주소), 대리인정보(신원확인증표 사본, 부서, 전화번호)
- 수집하는 고유식별정보 항목 : 주민등록번호, 여권번호, 외국인등록번호 등 신원확인증표 상의 개인정보
- 수집하는 기기정보 : IP 및 MAC주소, HDD Serial, USB Serial, OS버전, 웹브라우저버전 등

9.4.2. 전자서명인증업무 관련정보의 보호범위 및 책임

결제원과 등록대행기관은 전자서명인증업무 수행과정에서 얻게 되는 다음의 자료를 결제원이 제공하는 전자서명인증서비스의 이용 외에는 다른 목적으로 이용하거나 임의로 제3자에게 제공하지 않습니다. 다만, 사법기관 등 제3자가 법률에서 정한 요건 및 절차에 따라 정보제공을 요청하는 경우 이를 따를 수 있습니다.

- 가입자의 개인정보(본인의 동의가 있거나 인증서 및 디렉토리시스템에 공개된 내용은 제외)
- 전자서명인증업무 관련 전문 기록과 전문에 대한 로그
- 결제원에서 생성 또는 보관하는 전자서명인증업무 관련 감사자료
- 재해복구대책
- 결제원 전자서명인증업무 운영관련 보안조치

9.4.3. 개인정보보호를 위한 조치

개인정보는 접근·관리에 필요한 최소인원으로 사용자를 지정한 후 비밀번호를 통해 철저히 관리하고 있으며, YESKEY 홈페이지는 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 다음과 같은 조치를 취하고 있습니다.

- 암호화 알고리즘 등을 적용함으로써 개인정보의 보관 및 송수신 네트워크의 안전성 확보
- 컴퓨터 바이러스에 의한 피해방지를 위한 백신프로그램 연계
- 키보드 입력값에 대한 해킹방지를 위해 키보드보안장치 설치 및 운영

9.4.4. 개인정보보호에 대한 처리방침

YESKEY 인증서비스의 개인정보보호에 관한 사항은 개인정보처리방침을 수립하여 시행하고 있으며, 동 내용은 YESKEY 홈페이지에서 확인하실 수 있습니다.

9.5. 지식재산권

다음 사항에 대한 지식재산권은 저작권법 등 관련법률에 따라 결제원에 귀속됩니다.

- 결제원이 개발한 소프트웨어 및 하드웨어
- 준칙
- 결제원 명칭
  - 법인명
  - 전자서명인증업무명(YESKEY, yessign)
- 결제원이 전자서명하여 송신한 전자문서
- CRL

9.6. 보증책임

해당 사항 없습니다.

9.7. 보증 예외 사항

해당 사항 없습니다.

9.8. 보험의 보상 범위

결제원은 전자서명인증업무의 수행과 관련하여 결제원의 고의 또는 과실로 발생하는 사고로 인한 손해배상을 담보하기 위하여 연간 및 건당 총 보상액 한도가 25억원인 책임보험에 가입하고 있습니다.

9.9. 배상 한계

결제원은 전자서명인증업무의 수행과 관련하여 가입자 또는 이용자에게 손해를 입힌 경우에는 그 손해를 배상합니다. 다만, 결제원이 고의 또는 과실이 없음을 입증하면 그 배상책임이 면제됩니다.

9.10. 준칙의 효력

준칙이 개정되면 개정전 내용은 개정 준칙의 효력발생일에 그 효력이 상실됩니다. 본 개정준칙은 2025년 1월 6일부터 효력이 발생합니다.

9.11. 통지 및 의사소통

결제원은 관련자와의 전자서명인증서비스와 관련된 주요 정보의 통지 및 의사소통 수단으로 홈페이지, 전자우편 또는 전화를 사용합니다.

9.12. 이력 관리

준칙의 제·개정 이력은 준칙의 포함되어 준칙과 함께 관리됩니다.

9.13. 분쟁 해결

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

전자서명인증체계 관련자에게 전달되는 전자서명(또는 전자문서)는 아래와 같이 법적 효력을 갖습니다.

- 전자서명법 제3조(전자서명의 효력)의 각 항에 따른 사항
- 전자문서법 제4조(전자문서의 효력)의 각 항에 따른 사항

9.13.2. 분쟁을 해결하는 절차

전자서명인증업무와 관련하여 결제원과 가입자 또는 이용자간 분쟁이 발생한 경우 법 제22조(분쟁의 조정)에 따라 전자문서·전자거래분쟁조정위원회에 조정을 신청하여 관련 절차에 따라 신속한 방법으로 분쟁을 해결할 수 있습니다.

9.14. 관할법원

전자서명인증업무 관련 분쟁이 발생할 경우 그 관할기관은 결제원 본사 소재지를 관할하는 지방법원이 됩니다.

9.15. 관련 법률 준수

이 준칙에 명시되지 아니한 사항에 대해서 “1.3”의 전자서명인증체계 관련자는 전자서명법, 정보통신망법, 개인정보 보호법 등 관계법령 및 이용약관을 준수합니다.

9.16. 기타 규정

본 준칙은 대한민국의 관계법령에 따라 해석되고 적용됩니다.

부 칙(2023. 7. 17.)

이 준칙은 2023. 7. 17.부터 시행합니다.

부 칙(2024. 05. 31.)

이 준칙은 2024. 05. 31.부터 시행합니다.

부 칙(2024. 08. 27.)

이 준칙은 2024. 08. 27.부터 시행합니다.

부 칙(2025. 01. 02.)

이 준칙은 2025. 1. 6.부터 시행합니다.

부 칙(2025. 12. 01.)

이 준칙은 2025. 12. 01.부터 시행합니다.