

yesign 공인인증업무준칙

Version 3.6

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

금융결제원 전자인증부

©COPYRIGHT 2013 yesign ALL RIGHTS RESERVED

구 분	개정일	시행일
제 정	2000. 8.29.	2000. 8.29.
개 정	2001. 7. 5.	2001. 7. 5.
	2001.12.17.	2001.12.17.
	2002. 3.12.	2002. 3.12.
	2002. 8.21.	2002. 9. 5.
	2002.12.27.	2003. 1.13.
	2004. 3.31.	2004. 6.12.
	2004. 9.16.	2004.10. 1.
	2005. 2.21.	2005. 3. 8.
	2005.11.17.	2005.12. 2.
	2005.12.29.	2006. 1.13.
	2006. 6.14.	2006. 7. 1.
	2006. 6.30.	2006. 8. 1.
전문개정	2007. 5.21.	2007. 8. 1.
개정	2009.10. 7.	2009.10.22.
	2010. 6. 3.	2010. 7. 1.
	2011. 3. 9.	2011. 3.28.
	2011. 9. 8.	2011. 9.30.
	2013. 8.27.	2013. 9.26.
	2013. 10.25	2013. 12.16.

- 목 차 -

- 1. 개요 1
 - 1.1 배경 및 목적 1
 - 1.1.1 준칙의 배경 및 목적 1
 - 1.1.2 전자서명인증체계 1
 - 1.1.3 결제원 1
 - 1.1.4 공인인증서 정의 및 효력 2
 - 1.2 준칙의 명칭 3
 - 1.3 공인전자서명인증체계 관련자 3
 - 1.3.1 미래창조과학부 3
 - 1.3.2 인터넷진흥원 3
 - 1.3.3 결제원 4
 - 1.3.4 등록대행기관 4
 - 1.3.5 가입자 5
 - 1.3.6 이용자 5
 - 1.3.7 결제원의 의무 5
 - 1.3.8 등록대행기관의 의무 및 책임 7
 - 1.3.9 가입자의 의무 7
 - 1.3.10 이용자의 의무 9
 - 1.4 준칙의 관리 10
 - 1.4.1 준칙 관리부서 및 연락처 10
 - 1.4.2 준칙의 개정 10
 - 1.4.3 준칙의 신고 및 적용 10
 - 1.4.4 준칙의 공지 11
 - 1.4.5 가입자 동의 11
 - 1.5 정의 및 약어 11
 - 1.5.1 정의 11
 - 1.5.2 약어 12

- 2. 공인인증서 종류 및 수수료 13
 - 2.1 공인인증서 종류 13
 - 2.2 공인인증업무 수수료 13
 - 2.2.1 공인인증서 발급·갱신 수수료 14
 - 2.2.2 공인인증서 접근 수수료 14
 - 2.2.3 공인인증서 유효 여부 확인 수수료 14
 - 2.2.4 기타 서비스에 대한 수수료 14
 - 2.3 환불 15
- 3. 공인인증업무 16
 - 3.1 공인인증서 발급 신청 16
 - 3.1.1 신청 주체 16
 - 3.1.2 발급 절차 16
 - 3.1.3 발급 제한 16
 - 3.2 공인인증서 신규발급 17
 - 3.2.1 신원확인 17
 - 3.2.2 신규발급 절차 18
 - 3.3 공인인증서 갱신발급 20
 - 3.3.1 갱신발급 요건 20
 - 3.3.2 갱신발급 절차 21
 - 3.4 공인인증서 재발급 22
 - 3.4.1 재발급 요건 22
 - 3.4.2 재발급 절차 22
 - 3.5 가입자 등록정보 변경 22
 - 3.5.1 가입자 등록정보 변경 요건 22
 - 3.5.2 가입자 등록정보 변경 절차 22
 - 3.6 공인인증서 효력정지·효력회복·폐지 23
 - 3.6.1 효력정지 사유 23
 - 3.6.2 폐지 사유 23
 - 3.6.3 효력정지 및 폐지 신청과 신원확인 24

3.6.4 공인인증서 효력정지 및 폐지목록(CRL)의 갱신과 공고	24	5.1.7 항온항습, 동풍	38
3.6.5 강제 폐지에 따른 공지	24	5.1.8 기타 보호설비	38
3.6.6 효력회복 신청과 신원확인	25	5.1.9 매체 저장	38
3.6.7 효력회복 공고	25	5.1.10 시설 및 장비의 폐기 처리	38
3.6.8 효력회복 기간의 제한	25	5.1.11 원격지 백업설비 안전운영	38
3.7 인증서유효성확인(OCSP)서비스	25	5.2 절차적 보호조치	39
3.8 시점확인서비스	26	5.2.1 공인인증업무에 대한 업무 분장	39
3.9 공인인증서 프로파일	27	5.2.2 공인인증업무 담당자 인증 방법	39
3.10 공인인증서 효력정지 및 폐지목록(CRL) 프로파일	29	5.2.3 동일인에 의해 동시 수행될 수 없는 공인인증업무	39
3.11 인증서유효성확인(OCSP) 서비스용 공인인증서 프로파일	31	5.3 기술적 보호조치	40
3.12 공인인증기관의 전자서명키 갱신	33	5.3.1 전자서명정보 생성	40
3.13 공인인증업무 휴지 및 폐지	33	5.3.2 전자서명정보의 크기 및 해쉬값	40
3.13.1 공인인증업무 휴지	33	5.3.3 전자서명생성정보 저장장치	40
3.13.2 공인인증업무 폐지	33	5.3.4 전자서명생성정보 생성·사용 후 안전한 삭제 방법	40
3.14 공인인증업무 정지 및 지정취소	33	5.3.5 전자서명생성정보 파기 방법	40
4. 공인인증업무 관련정보의 공고	35	5.3.6 전자서명생성정보 사용기간	40
4.1 공고 설비	35	5.3.7 공인인증시스템 구성 및 관리 등 시스템 보호에 관한 사항	41
4.2 공고 방법	35	5.3.8 공인인증 S/W 형상관리 등 운영관리에 관한 사항	41
4.2.1 주요정보 공고위치	35	5.3.9 네트워크의 구성 및 운영 등 네트워크 보호에 관한 사항	42
4.2.2 공고 빈도	35	5.3.10 시점확인서비스 등 부가서비스 운영에 대한 보호조치	42
5. 공인인증업무 시설 및 장비 보호조치	36	5.4 인적 보안	42
5.1 물리적 보호조치	36	5.4.1 공인인증업무 인력의 자격, 경력 등 요구사항	43
5.1.1 공인인증시스템 운영실의 격실분리에 관한 사항	36	5.4.2 공인인증업무 교육, 업무순환에 관한 사항	43
5.1.2 물리적 접근 통제	36	5.4.3 비인가된 행위에 대한 처벌에 관한 사항	43
5.1.3 수해 방지	37	5.5 감사 기록	44
5.1.4 화재 예방	37	5.5.1 감사기록의 유형 및 보존기간	44
5.1.5 전원	37	5.5.2 감사기록 보호조치	44
5.1.6 방호	37	5.5.3 감사기록 백업주기 및 절차	44
5.6.3 보존기록의 백업주기 및 백업절차	45	5.6 기록 보존	45
5.7 장애 및 재해복구	45	5.6.1 보존기록의 유형 및 보존기간	45
5.7.1 공인인증업무 장애 및 재해 유형별 신고·복구	46	5.6.2 보존기록의 보호조치	45
5.7.2 공인인증업무 장애 유형	46	6.7 관련법의 준수	52
5.7.3 공인인증업무 장애 유형별 신고절차	46	6.7 공인인증업무준칙의 효력	53
5.7.4 공인인증업무 장애 유형별 복구	47		
5.7.5 공인인증업무 장애방지 등 연속성 보장 대책	47		
6. 공인인증업무 보증 등 기타사항	48		
6.1 보증	48		
6.1.1 보증 책임	48		
6.1.2 보증 제한	48		
6.2 배상	48		
6.2.1 배상 책임	48		
6.2.2 책임 제한	48		
6.2.3 배상 한도	49		
6.3 분쟁 해결	49		
6.3.1 준거법	49		
6.3.2 재판 관할	49		
6.3.3 분쟁을 해결하는 절차	49		
6.3.4 공인전자서명인증체계 관련자에게 전달되는 문서(또는 전자문서)가 법적 효력을 갖기 위한 요건	50		
6.4 개인정보보호	50		
6.4.1 공인인증업무 관련정보의 보호범위 및 책임	50		
6.4.2 개인정보보호를 위한 조치	50		
6.4.3 개인정보 수집 및 이용목적	51		
6.4.4 개인정보보호에 대한 처리방침	51		
6.5 감사 및 점검 등	51		
6.5.1 시설 및 장비에 대한 심사	51		
6.5.2 정기점검	52		

1. 개요

1.1 배경 및 목적

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 공인인증기관으로 지정받아 금융기관과 함께 공인인증시스템을 구축·운영하고 있습니다.

본 공인인증무준칙(이하 “준칙”이라 한다)은 전자서명법(이하 “법”이라 한다), 동법 시행령(이하 “시행령”이라 한다), 동법 시행규칙(이하 “시행규칙”이라 한다), 한국인터넷진흥원(이하 “인터넷진흥원”이라 한다) 공인인증무준칙에 근거하여 공인인증서 발급 및 관리, 운영정책 및 절차 등 결제원이 제공하는 공인인증업무에 관련된 전반적인 사항과 공인인증업무 관련 당사자의 책임과 의무에 관한 사항을 정함을 목적으로 합니다.

1.1.2 전자서명인증체계

공인인증에 관한 정책의 수립, 시행 및 감독은 **미래창조과학부**가 관장하고 있으며, 최상위인증기관으로서 인터넷진흥원과 그 아래 5개 공인인증기관으로 전자서명인증체계가 구성되어 있습니다.

공인인증기관은 신청인의 신원확인 등의 등록업무를 등록대행기관에 위임할 수 있으며, 공인인증업무의 이용주체로 가입자, 가입신청자(결제원으로부터 공인인증서를 발급받으려는 자), 이용자가 있습니다.

1.1.3 결제원

결제원은 민법 제32조(비영리법인의 설립과 허가)에 따라 1986년 6월 2일 설립된 비영리사단법인으로서 **금융기관간 공동 네트워크**를 운영하며, 어음교환, 지로, 금융공동망을 통해 금융기관간 자금이체 등 지급결제 업무를 수행하는 기관으로서 2000년 4월 12일 법 제4조(공인인증기관의 지정)에 따라 정부로부터

1

1.2 준칙의 명칭

본 준칙은 yes sign 공인인증무준칙이라 합니다.

1.3 공인전자서명인증체계 관련자

공인전자서명인증체계 관련자는 안전하고 신뢰할 수 있는 전자서명 공인인증서의 발급·이용·관리를 위하여 신의성실로 상호 협조해야 합니다.

1.3.1 미래창조과학부

미래창조과학부는 전자서명 인증관리체계(PKI, Public Key Infrastructure)의 안전성·신뢰성 있는 운영을 위한 정책·감독기관으로서 다음의 업무를 수행합니다.

- 전자서명 인증관리체계의 안전·신뢰성 있는 구축 및 운영을 위한 정책수립
- 공인인증기관 지정, 검사, 지정명령, 업무정지 및 지정취소
- 인터넷진흥원과 공인인증기관의 전자서명 관련법규 준수여부에 대한 관리·감독
- 외국정부와 전자서명의 상호인증 등

1.3.2 인터넷진흥원

인터넷진흥원은 법 제25조(전자서명인증관리업무)에 따라 지정된 전자서명인증관리센터로서 다음의 업무를 수행합니다.

- 법 제4조의 규정에 의하여 공인인증기관을 지정하는 경우 공인인증기관으로 지정받고자 하는 자가 갖추어야 할 시설 및 장비에 대한 심사 지원
- 법 제14조제1항의 규정에 의한 공인인증기관에 대한 검사 지원
- 법 제18조제3의 규정에 의한 보호조치에 대한 심사 및 기술 지원
- 법 제19조제2항의 규정에 의한 시설 및 장비의 안전운영 여부에 관한 점검
- 공인인증기관에 대한 공인인증서 발급·관리 등 공인인증업무
- 전자서명인증 관련 기술개발·보급 및 표준화 연구

3

공인인증기관으로 지정받아 공인인증무를 제공하고 있습니다. 결제원의 공인인증업무에 관련된 연락처는 다음과 같습니다.

- 주소 : 463-811, 경기도 성남시 분당구 정자일로 213번길 9
- 인터넷 URL : <http://www.yessign.or.kr>
- 전자우편 : yessign@kftc.or.kr
- 전화번호 : 1577-5500
- 팩스번호 : 02)531-3109

1.1.4 공인인증서 정의 및 효력

1.1.4.1 정의

공인인증서란 법 제15조의 규정에 따라 공인인증기관이 발급하는 것으로, 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말합니다.

결제원은 가입자가 공인인증서 신청시 등록대행기관에 제공한 가입자정보와 일치함을 확인한 후, 가입자가 제출한 전자서명검증정보와 관련정보에 공인인증기관의 전자서명생성정보로 전자서명한 공인인증서를 발급합니다. 따라서 동 공인인증서에 기재된 사실은 가입자의 발급신청 당시를 기준으로 하는 것이며, 가입자의 신용, 가입자 관련정보의 불변성 등을 보장하지 않습니다.

1.1.4.2 효력

결제원이 발급한 공인인증서는 법 제16조(공인인증서의 효력의 소멸 등)에서 정한 소멸 등의 사유가 발생하는 경우를 제외하고는 효력을 인정받으며, 소멸 등의 사유가 발생하는 경우 당해 공인인증서의 효력은 소멸 또는 정지됩니다.

1.1.4.3 이용범위 및 제한

결제원이 발급한 공인인증서는 전자거래에 사용할 수 있습니다. 앞의 전자거래에서의 공인인증서 사용은 정당한 권한을 가진 가입자가 공인인증서의 발급용도에 맞게 공인인증서를 사용하는 것을 말합니다. 그러하지 아니한 경우나 공인인증업무 관련 보안상의 우려가 있는 경우 결제원은 기발급된 공인인증서의 사용을 제한할 수 있습니다.

2

- 전자서명인증 관련 제도 연구 및 상호인증 등 국제협력 지원
- 공인인증업무 폐지 또는 지정취소된 공인인증기관의 가입자 공인인증서 등 인수
- 공인인증서 분실신고 접수 및 동 내역의 공인인증기관알 전송
- 그 밖에 전자서명인증관리업무와 관련하여 필요한 사항

1.3.3 결제원

결제원은 법 제4조(공인인증기관의 지정) 및 제8조(공인인증기관의 업무수행)에 따라 지정된 공인인증기관으로서 다음의 업무를 수행합니다.

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

1.3.4 등록대행기관

등록대행기관은 공인인증서 발급, 효력정지, 효력회복, 폐지 등 신청접수 및 신원확인 등의 업무를 수행하며, 가입자의 편의를 위하여 여러지역에 지정되어 있습니다.

결제원의 등록대행기관은 국민은행 등 은행권(농협·수협중앙회 포함), 새마을금고중앙회, 신용협동조합중앙회 등이며 결제원은 등록대행기관을 추가로 지정·운영할 수 있고 이 경우 “4.2.1 주요정보 공고위치 - 등록대행기관 목록”에 공고합니다.

4

1.3.5 가입자

가입자는 등록대행기관 및 결제원으로부터 공인인증서를 발급받은 자(발급받으려는 가입신청자를 포함)를 말합니다.

법인의 경우 대리인이 공인인증서를 발급받을 수 있으며, 대리인은 가입자의 위임장 등과 같은 관련 서류를 지참한 경우에 한하여 가입자를 대리하여 공인인증업무 신청할 수 있습니다. 하지만 대리인이 가입자(본인)를 대신하여 전자서명을 할 수는 없습니다.

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

1.3.6 이용자

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

1.3.7 결제원의 의무

1.3.7.1 정확한 정보 제공

결제원은 법 제22조의2(공인인증서의 관리 등)에 따라 가입자 및 이용자에게 공인인증서의 신뢰성이나 유효성에 영향을 미칠 수 있는 다음의 정보를 yessign 홈페이지(<http://www.yesign.or.kr>) 또는 결제원 디렉토리시스템에 공고하여 그 사실을 확인할 수 있도록 합니다.

- 공인인증기관 지정
- 공인인증업무 휴지·정지 또는 폐지
- 공인인증기관 지정취소
- 공인인증기관 업무의 양도·양수·합병
- 준칙
- 공인인증서에 대한 정보
 - 가입자 공인인증서
 - 가입자 CRL
- 기타 공인인증업무 수행관련 정보 등

5

1.3.8 등록대행기관의 의무 및 책임

1.3.8.1 공인인증서 이용신청 접수 및 중요 내용 설명

등록대행기관은 법 제7조(인증업무의 제공 등)에 따라 정당한 사유없이 공인인증서 발급, 재발급, 갱신발급, 효력정지, 효력회복, 폐지 등의 공인인증서 관련 신청접수를 거부할 수 없습니다. 또한 「약관의 규제에 관한 법률」 제3조(약관의 작성 및 설명의무 등)에 따라 중요한 내용을 고객이 이해할 수 있도록 설명하여야 합니다.

1.3.8.2 신원확인

등록대행기관은 법 제15조(공인인증서의 발급)에 따라 가입자의 실지명의를 확인하며, 관련 서류를 징구할 수 있습니다.

1.3.8.3 책임

등록대행기관이 전자거래공인인증업무규약을 위반하여 공인인증업무에 중대한 지장을 초래하였을 경우 결제원은 해당 등록대행기관에 대하여 적절한 제재를 가할 수 있습니다. 또한 공인인증서 가입자의 신원확인 오류 등으로 인하여 발생한 가입자 또는 이용자의 손해에 대하여는 전자금융거래배상책임보험 보통약관이 정하는 바에 따라 배상합니다.

1.3.9 가입자의 의무

1.3.9.1 정확한 정보제공

가입자는 법 제15조(공인인증서의 발급)에 따라 다음사항에 대하여는 정확한 정보를 결제원과 등록대행기관에 제공하여야 합니다. 아울러 결제원 또는 등록대행기관이 신원확인을 위하여 관련 서류를 요청하는 경우 가입자는 성실히 협조하여야 합니다.

- 공인인증서 발급 신청
- 공인인증서 재발급 신청
- 공인인증서 갱신발급 신청
- 공인인증서 효력정지, 효력회복 및 폐지 신청

7

1.3.7.2 전자서명생성정보의 보호

결제원은 법 제21조(전자서명생성정보의 관리)에 따라 신뢰할 수 있는 소프트웨어나 하드웨어 등을 이용하여 안전한 방법으로 결제원 전자서명생성정보를 생성하며 생성된 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리합니다.

1.3.7.3 전자서명생성정보 사용의 제한

결제원은 법 제8조(공인인증기관의 업무수행)에 따라 공인인증무무를 제공함에 있어서 인터넷진흥원으로부터 인증받은 전자서명검증정보에 합치하는 전자서명생성정보를 사용합니다.

1.3.7.4 전자서명생성정보 안전조치

결제원은 법 제21조(전자서명생성정보의 관리)에 따라 결제원 전자서명생성정보의 분실·훼손, 도난·유출 등 공인인증서의 신뢰성이나 유효성에 영향을 미치는 사유가 발생한 사실을 인지하는 경우 인터넷진흥원 및 가입자에게 이를 통보하며 필요한 경우 당해 전자서명생성정보로 발급한 가입자의 공인인증서를 폐지합니다.

결제원은 즉시 당해 사실을 yesign 홈페이지(<http://www.yesign.or.kr>)에 공고하며, CRL을 갱신하고, 이용자가 갱신된 CRL을 이용할 수 있도록 하고, 결제원은 공인인증업무의 신뢰성·유효성을 확보할 수 있는 대책을 강구합니다.

1.3.7.5 등록대행기관 운영

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

1.3.7.6 신원확인

결제원은 법 제15조(공인인증서의 발급)에 따라 가입자의 실지명의를 확인하며, 관련 서류를 징구할 수 있습니다.

6

- 가입자정보 변경 등

1.3.9.2 공인인증서의 합목적적 사용

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

1.3.9.3 전자서명생성정보의 보호

가입자는 법 제21조(전자서명생성정보의 관리)에 따라 신뢰할 수 있는 소프트웨어나 하드웨어를 이용하여 전자서명정보를 생성하며 생성된 전자서명생성정보가 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.

가입자의 전자서명생성정보 보호의무 위반으로 인한 결과의 책임은 전적으로 가입자에게 있습니다.

1.3.9.4 전자서명생성정보 안전조치

가입자는 법 제21조(전자서명생성정보의 관리)에 따라 전자서명생성정보가 분실·훼손 또는 도난·유출되었거나 안전하지 않다고 인지하는 경우 지체없이 결제원 또는 등록대행기관에 관련사실을 통보하여 결제원이 당해 공인인증서를 폐지할 수 있도록 협조하여야 합니다.

1.3.9.5 결제원의 면책보장

가입자는 공인인증서 사용과 공개에 있어 다음의 사유로 인하여 발생하는 모든 책임과 비용에 대하여는 결제원의 면책을 보장합니다. 본 의무는 가입자의 공인인증업무 신청을 접수한 때부터 시작되며 공인인증서 만료(폐지 포함)후 10년 동안 지속됩니다.

- 가입자가 그릇되게 제공한 정보

8

- 가입자가 태만 또는 고의로 제공하지 않은 변경된 정보
- 가입자의 전자서명생성정보 관리 부주의(정보 노출, 분실, 변조 등)

1.3.9.6 배상책임

가입자는 공인인증서 사용과 관련하여 가입자의 고의 또는 과실로 결재원 또는 등록대행기관에게 손해를 입힌 경우 결재원 또는 등록대행기관에게 그 손해를 배상해야 합니다.

1.3.10 이용자의 의무

1.3.10.1 공인인증서의 사용목적 이해

이용자는 결재원이 가입자에게 발급한 공인인증서의 이용목적 및 이용가능 범위(제한 포함)를 이해하여야 합니다. 이용자의 과실로 인한 손해는 전적으로 이용자의 책임입니다.

1.3.10.2 공인인증서의 유효성 확인

이용자는 공인인증서 기재사항 등에 의하여 공인전자서명의 진위여부를 확인하기 위하여 다음의 조치를 취하여야 합니다.

- 공인인증서 유효여부의 확인
- 공인인증서의 정지 또는 폐지 여부의 확인
- 공인인증서의 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

1.3.10.3 배상책임

이용자는 공인인증서 사용과 관련하여 이용자의 고의 또는 과실로 결재원 또는 가입자에게 손해를 입힌 경우 결재원 또는 가입자에게 그 손해를 배상해야 합니다.

1.4 준칙의 공지

결재원은 개정된 준칙을 아래의 정보저장위치에 즉시 공고합니다.

- 준칙 정보저장위치 : <http://www.yessign.or.kr/cps.htm>

1.4.5 가입자 동의

가입자는 변경된 준칙이 공고된 후 30일(공고일 포함) 내에 서면으로(또는 전자서명생성정보로 전자서명한 전자문서로) 이의를 제기하지 아니한 경우 결재원은 가입자가 변경된 준칙에 동의한 것으로 봅니다.

1.5 정의 및 약어

1.5.1 정의

1.5.1.1 법 용어 정의

본 준칙에서 사용되는 주요 용어들은 “6.6”의 공인전자서명 관련법규에 정의되어 있습니다.

1.5.1.2 용어의 정의

본 준칙을 위하여 다음과 같이 용어를 정의합니다.

- 디렉토리시스템 : 공인인증서, CRL을 보관하고 신뢰당사자에게 공고 및 검색 서비스를 제공하기 위한 것으로 ITU-T X.500 표준을 준수하는 시스템을 말합니다.
- 사고정보 : 전자금융사고 또는 공인인증서 유출 등이 발생한 기기정보(IP 및 MAC주소 등) 및 개인정보(이름, 주민등록번호 등)를 말합니다.
- yessign서비스 : 법에 의거 공인인증기관으로 지정받은 결재원이 제공하는 공인인증서비스를 말합니다.
- 단말기 지정 : 단말기(PC, 스마트폰 등)의 기기정보를 등록대행기관에 등록하고, 공인인증서 발급시 가입자가 등록된 단말기인지 여부를 확인하여 가입자의 신원을 확인하는 방법을 말합니다.

1.4 준칙의 관리

1.4.1 준칙 관리부서 및 연락처

관리부서 : 결재원 전자인증부

전자우편 : yessign@kftc.or.kr

주소 : 463-811, 경기도 성남시 분당구 정자일로 213번길 9

전화 : 1577-5500

FAX : (02)531-3109

1.4.2 준칙의 개정

결재원은 법 제6조(공인인증업무준칙 등)에 따라 미래창조과학부가 준칙의 변경을 명한 경우 또는 결재원 원장이 공인인증업무 개선을 위하여 준칙의 변경이 필요하다고 판단한 경우 이를 개정할 수 있습니다.

본 준칙의 제·개정권자는 결재원 원장입니다.

결재원은 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

1.4.3 준칙의 신고 및 적용

결재원은 법 제6조(공인인증업무준칙 등)에 따라 제·개정된 준칙을 적용하기 15일 전까지 미래창조과학부에 신고합니다.

1.4.4 준칙의 공지

결재원은 개정된 준칙을 아래의 정보저장위치에 즉시 공고합니다.

- 준칙 정보저장위치 : <http://www.yessign.or.kr/cps.htm>

1.4.5 가입자 동의

가입자는 변경된 준칙이 공고된 후 30일(공고일 포함) 내에 서면으로(또는 전자서명생성정보로 전자서명한 전자문서로) 이의를 제기하지 아니한 경우 결재원은 가입자가 변경된 준칙에 동의한 것으로 봅니다.

1.5 정의 및 약어

1.5.1 정의

1.5.1.1 법 용어 정의

본 준칙에서 사용되는 주요 용어들은 “6.6”의 공인전자서명 관련법규에 정의되어 있습니다.

1.5.1.2 용어의 정의

본 준칙을 위하여 다음과 같이 용어를 정의합니다.

- 디렉토리시스템 : 공인인증서, CRL을 보관하고 신뢰당사자에게 공고 및 검색 서비스를 제공하기 위한 것으로 ITU-T X.500 표준을 준수하는 시스템을 말합니다.
- 사고정보 : 전자금융사고 또는 공인인증서 유출 등이 발생한 기기정보(IP 및 MAC주소 등) 및 개인정보(이름, 주민등록번호 등)를 말합니다.
- yessign서비스 : 법에 의거 공인인증기관으로 지정받은 결재원이 제공하는 공인인증서비스를 말합니다.
- 단말기 지정 : 단말기(PC, 스마트폰 등)의 기기정보를 등록대행기관에 등록하고, 공인인증서 발급시 가입자가 등록된 단말기인지 여부를 확인하여 가입자의 신원을 확인하는 방법을 말합니다.

- 추가인증 : 휴대폰 SMS인증, 2체널 인증 등과 같이 단말기 지정 이외의 수단으로 가입자의 신원을 확인하는 방법을 말합니다.

- 2체널 인증 : 서로 다른 두 가지 이상의 통신경로를 이용하여 가입자의 신원을 확인하는 방법을 말합니다.

1.5.2 약어

본 준칙에서는 다음의 약어가 사용됩니다.

- CRL : Certificate Revocation List, 공인인증서 효력정지 및 폐지목록
- DN : Distinguished Name, 식별명칭

2. 공인인증서 종류 및 수수료

2.1 공인인증서 종류

결제원은 개인과 법인/단체(개) 범용 인증서, 용도제한용 인증서를 발급합니다. 결제원이 발급하는 공인인증서의 유효기간은 발급일로부터 1년입니다. 다만, **서비용 공인인증서의 유효기간은 발급일로부터 1년 또는 2년입니다.**

구분	OID	용도
개인	범용 1.2.410.200005.1.1.1	· 금융기관업무 · 정부민원업무 · 기타 전자문서 관련 제한업무
	용도제한용 은행/신용카드/보험용 1.2.410.200005.1.1.4	· 조회, 자금이체 등 은행업무(개별 및 공동업무) · 조회, 각종 신청 등 보험업무 · 조회, 각종 신청 등 신용카드업무 · 정부민원업무
법인/단체	범용 1.2.410.200005.1.1.5	· 금융기관업무 · 정부민원업무 · 기타 전자문서 관련 제한업무
	은행/신용카드/보험용 1.2.410.200005.1.1.2	· 조회, 자금이체 등 은행업무(개별 및 공동업무) · 조회, 각종 신청 등 보험업무 · 조회, 각종 신청 등 신용카드업무 · 정부민원업무
	전자세금용 1.2.410.200005.1.1.6.8	· 전자세금계산서업무 · 국세청 제공 민원업무
	용도제한용 조달청원클릭용 1.2.410.200005.1.1.6.3	· 조달청 비록원자재 구매업무
	금융위원회 CTR용 1.2.410.200005.1.1.6.5	· 금융위원회 고액현금거래 보고업무
	서비용 1.2.410.200005.1.1.3	· 인터넷뱅킹, 지급결제중계, 온라인쇼핑몰 등 인터넷에서 서비를 이용하여 서비스를 제공하는 업무
	기타 1.2.410.200005.1.1.6.X 및 1.2.410.200005.1.1.7.X	· 특정인에게 발급되어 지정된 분야에 제한적으로 사용

※ 개인사업자로서 전자입찰 등의 업무에 참여하고자 하는 경우 법인 인증서를 발급받을 수 있습니다.
※ 전자서명법 제4조 제4항에 의한 제공업무의 구분지정에도 불구하고 2006년 7월 1일 이전 범용 인증서를 발급받은 가입자에 대해서는 범용 인증서 이용을 보장합니다.

2.2 공인인증업무 수수료

결제원은 법 제28조(요금 부과)에 따라 가입자 또는 이용자에게 필요한 수수료

2.3 환불

결제원과 등록대행기관은 가입자가 공인인증서 발급신청일로부터 7일 이내에 발급신청을 취소하는 경우와 공인인증서 발급일로부터 7일 이내에 발급을 취소하는 경우에 한하여 수수료를 환불하고, 당해 공인인증서를 폐지합니다. 다만, 결제원과 등록대행기관은 수수료를 환불할 때 필요 경비를 공제할 수 있습니다.

또한 공인인증서 발급신청일 또는 발급일로부터 7일이 경과하였다라도 결제원 또는 등록대행기관 귀책사유로 인한 가입자의 환불 요구에 대해서는 수수료를 환불하고, 당해 공인인증서를 폐지합니다.

를 부과할 수 있습니다.

그리고 결제원 또는 등록대행기관은 판단에 따라 수수료를 면제하거나 할인요율을 적용할 수 있습니다.

2.2.1 공인인증서 발급·갱신 수수료

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

(단위 : 원/년, 부가세 별도)

구분	개인		법인/단체						
	범용	용도제한용	범용	용도제한용					
		은행/신용카드/보험용		은행/신용카드/보험용	전자세금용	조달청원클릭용	금융위원회 CTR용	서비용	기타
수수료	4,000	무료	100,000	4,000	4,000	무료	4,000	1,000,000	용도별 상이 (별도 계약)

2.2.2 공인인증서 접근 수수료

결제원은 공인인증서를 열람·확인하는 이용자에게 수수료를 부과하지 않습니다.

2.2.3 공인인증서 유효 여부 확인 수수료

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

구분	효력정지 및 폐지목록(CRL) 조회	공인인증서 유효성확인(OCSP) 서비스
수수료	무료	별도계약에 따름

2.2.4 기타 서비스에 대한 수수료

결제원은 필요한 경우 기타 서비스에 대한 수수료를 부과할 수 있습니다.

3. 공인인증업무

3.1 공인인증서 발급 신청

3.1.1 신청 주체

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

3.1.2 발급 절차

- 가입신청자는 등록대행기관을 직접 방문하여 본인확인을 거친 후 전자금융거래 가입신청을 하여야 합니다. 다만, 이미 등록대행기관의 신원확인을 마친 기존 전자금융거래 가입자는 그러하지 아니합니다.
- 가입신청자가 주민등록증 등 신원확인증표를 지참하고 결제원 또는 등록대행기관을 직접 방문하여 공인인증서 신청서를 제출함으로써, 가입신청을 할 수도 있습니다.
- 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.
- 가입신청자는 등록대행기관의 전자금융거래 이용매체 또는 yes sign 홈페이지를 통하여 공인인증서 발급을 신청합니다.
- 가입신청자는 결제원이 발급한 공인인증서를 원하는 매체에 저장합니다.

3.1.3 발급 제한

결제원과 등록대행기관은 다음 각 호의 어느 하나에 해당하는 경우에 공인인증서 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 공인인증서를 발급하지 못하는 경우
- 사고정보를 이용하여 신청 또는 발급하였거나 그렇다고 의심되는 경우
- 단말기 지정 또는 추가인증 등에 실패한 경우

3.2 공인인증서 신규발급

3.2.1 신원확인

결재원 또는 등록대행기관은 가입신청자의 신원을 확인합니다. 이 경우 결재원 또는 등록대행기관은 원칙적으로 직접 대면하여 신원을 확인하나, 「금융실명거래 및 비밀보장에 관한 법률」에 의거 금융기관에서 실지명의가 확인된 전자금융거래 가입자가 공인인증서를 발급받으려는 경우에는 정보통신망을 통하여 신원을 확인할 수 있습니다.

3.2.1.1 대면신원확인에 의한 발급

결재원 또는 등록대행기관이 직접 대면하여 가입신청자의 신원을 확인하는 때에는 시행규칙 제13조의2(신원확인 기준 및 방법) 및 제13조의3(신원확인증표)에 의거 신원확인증표에 의하여 실지명의인지 여부와 부착된 사진으로 본인임을 확인합니다.

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

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

- 대표자가 신청하는 경우
 - 서버인증서 이용신청서
 - 당해 서비스에 대한 사업자등록증 사본

17

- 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 온라인신원확인에 의한 발급

시행규칙 제13조의2(신원확인 기준 및 방법) 제4항에 의거 등록대행기관을 통하여 발급되는 범용 및 은행/신용카드/보험용의 경우 「금융실명거래 및 비밀보장에 관한 법률」에 의한 실지명의가 확인된 전자금융거래 가입자를 대상으로 비대면 신원확인방식으로 발급될 수 있습니다.

온라인신원확인 정보는 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 또한 등록대행기관은 비대면 신원확인방식의 안전성 및 신뢰성을 제고하기 위하여 단말기 지정 또는 추가인증 등을 통해 가입신청자의 신원확인을 강화할 수 있습니다.

3.2.2 신규발급 절차

3.2.2.1 가입신청자의 공인인증서 발급신청

가입신청자는 공인인증서 신청등록 후 7일(신청일 포함)내에 결재원 또는 등록

18

대행기관 홈페이지에 접속하여 공인인증서 발급에 필요한 가입자 소프트웨어를 사용하여 전자서명정보를 생성한 후, 신청등록시 부여받은 인가코드, 참조번호 등의 가입자정보를 이용하여 전자서명검증정보가 포함된 발급신청내역을 전송합니다.

이때 공인인증서 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.

인가코드, 참조번호의 노출 우려 및 신원확인의 유효성 보장을 위하여 공인인증서 발급신청은 신청등록 후 7일(신청일 포함)내에만 가능하며 7일이 경과한 후에는 다시 공인인증서 신청등록을 해야 합니다.

3.2.2.2 결재원의 공인인증서 발급

공인인증서 발급신청을 받은 결재원은 공인인증서를 발급하기 전에 공인인증서 발급신청 내용에 대해 다음의 검증을 실시함으로써 전자서명생성기가 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
- 공인인증서에 등록될 정보의 정확성 확인

결재원은 공인인증서 발급신청 내용에 대한 검증 후, 공인인증서 발급신청이 정당한 가입신청자에게 다음의 사항이 포함된 공인인증서를 발급·전송합니다. 그리고 결재원 디렉토리시스템 등에 공고합니다.

- 가입자의 명칭
- 가입자의 전자서명검증정보
- 가입자와 결재원이 이용하는 전자서명 방식
- 공인인증서의 일련번호
- 공인인증서의 유효기간

19

- 공인인증서 발급자인 결재원의 명칭
 - 공인인증서의 이용범위 또는 용도를 제한하는 경우에 이에 관한 사항 등
- 결재원이 발급하는 공인인증서는 DN으로 서로 구분될 수 있습니다. DN은 가입자 실명과 가입자 ID를 포함합니다. 가입자 ID는 결재원과 등록대행기관의 업무규약에 따라 등록대행기관, 가입자, 공인인증서 사용용도에 따라 유일하게 부여됩니다.

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

3.2.2.3 가입신청자의 공인인증서 수령

가입신청자는 가입자 소프트웨어를 통해 결재원이 발급한 공인인증서를 전달받아, 공인인증서와 자신의 전자서명생성정보를 저장할 매체를 선택하고, 이를 안전하게 저장·관리해야 합니다.

3.2.2.4 가입자정보의 전송

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

3.3 공인인증서 갱신발급

3.3.1 갱신발급 요건

공인인증서 갱신은 공인인증서의 유효기간이 만료되기 1개월 전부터 유효기간 만료일까지 전자서명정보와 유효기간이 갱신된 동일한 종류의 새로운 공인인증서를 발급하는 것을 말합니다. 새로 발급된 공인인증서의 유효기간은 기존 공인

20

인증서 유효기간을 승계하여 기존 공인인증서 만료시각 이후로부터 1년입니다.

3.3.2 갱신발급 절차

3.3.2.1 가입자의 갱신발급 신청 및 신원확인

가입자는 결제원 또는 등록대행기관에 접속하여 가입자 소프트웨어로 전자서명 정보를 생성하고 공인인증서 갱신신청내역을 전송합니다. 공인인증서 갱신내역은 다음과 같은 내용을 포함합니다.

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

공인인증서 갱신은 가입자의 기존 전자서명정보가 유효할 때 신청 가능하므로, 결제원은 가입자의 신원확인을 공인인증서 갱신신청내역의 가입자 전자서명으로 합니다. 인증서 갱신신청시 가입자의 기존 등록정보가 변경된 경우 결제원 및 등록대행기관은 필요에 따라 변경정보에 대한 증빙자료를 요구할 수 있습니다.

3.3.2.2 결제원의 공인인증서 갱신발급

공인인증서 갱신신청을 받은 결제원은 공인인증서를 갱신하기 전에 공인인증서 갱신신청내역에 포함된 내용에 대해 다음의 검증을 실시함으로써 전자서명생성기가 가입자에게 유일하게 속함을 확인합니다.

- 가입자가 제출한 전자서명검증정보의 유일성 확인
- 가입자가 제출한 전자서명검증정보로 전자서명을 검증하여 전자서명검증정보에 합치하는 전자서명생성정보의 소유여부 확인
- 기존 전자서명생성정보로 생성한 전자서명을 검증하여 가입자 신원확인

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

갱신 발급된 공인인증서의 DN은 기존 공인인증서의 DN을 승계합니다.

21

원확인을 가입자 등록정보 변경신청내역의 가입자 전자서명으로 합니다.

가입자정보의 전송방법은 "3.2.2.4 가입자정보의 전송"을 준용합니다.

3.6 공인인증서 효력정지·효력회복·폐지

공인인증서 효력정지는 공인인증서 유효기간 동안 가입자의 신청에 의해 공인인증서의 효력을 일정기간 정지하는 것을 말합니다.

공인인증서 효력회복은 효력이 정지된 공인인증서에 대하여 가입자가 효력회복을 신청하였을 경우 유효기간 내에서 당해 공인인증서의 효력을 회복시키는 것을 말합니다.

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

3.6.1 효력정지 사유

결제원은 가입자의 공인인증서 효력정지 신청이 있는 경우 당해 공인인증서의 효력을 정지시킬 수 있습니다.

3.6.2 폐지 사유

결제원은 법 제18조(공인인증서의 폐지) 및 "1.3.7 결제원의 의무"에서 정한 사항에 따라 다음의 사유가 발생한 경우 당해 공인인증서를 폐지합니다.

- 가입자가 공인인증서 폐지를 신청한 경우
- 가입자의 사망, 해산 등의 사유가 발생한 경우
- 피성년후견인이 법정대리인의 동의 없이 공인인증서를 발급받은 경우
- 피한정후견인이 법정대리인의 동의를 필요로 하는 법률행위 범위에 공인인증서 발급이 포함되어 있음에도 불구하고 법정대리인의 동의 없이 공인인증서를 발급받은 경우
- 공인인증서의 유효기간이 경과된 경우

23

3.3.2.3 가입자의 공인인증서 수령

가입자가 갱신발급된 공인인증서를 인수하는 절차는 "3.2.2.3 가입신청자의 공인인증서 수령" 절차를 준용합니다.

3.3.2.4 가입자정보의 전송

가입자정보의 전송방법은 "3.2.2.4 가입자정보의 전송"을 준용합니다.

3.4 공인인증서 재발급

3.4.1 재발급 요건

공인인증서 재발급은 가입자가 자신의 공인인증서를 폐지 또는 분실하였거나 전자서명생성정보의 노출, 손상 등이 우려되어 새로운 공인인증서를 다시 발급받는 것을 말합니다. 재발급된 공인인증서의 유효기간은 공인인증서 재발급일로부터 재발급 이전 공인인증서의 유효기간 만료일까지입니다.

3.4.2 재발급 절차

공인인증서 재발급은 "3.2.1 신원확인" 및 "3.2.2 신규발급 절차"를 준용합니다.

3.5 가입자 등록정보 변경

3.5.1 가입자 등록정보 변경 요건

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

3.5.2 가입자 등록정보 변경 절차

가입자 등록정보 변경은 결제원에 인터넷으로 신청하며, 결제원은 가입자의 신

22

원확인을 가입자 등록정보 변경신청내역의 가입자 전자서명으로 합니다.

가입자정보의 전송방법은 "3.2.2.4 가입자정보의 전송"을 준용합니다.

3.6 공인인증서 효력정지·효력회복·폐지

공인인증서 효력정지는 공인인증서 유효기간 동안 가입자의 신청에 의해 공인인증서의 효력을 일정기간 정지하는 것을 말합니다.

공인인증서 효력회복은 효력이 정지된 공인인증서에 대하여 가입자가 효력회복을 신청하였을 경우 유효기간 내에서 당해 공인인증서의 효력을 회복시키는 것을 말합니다.

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

3.6.1 효력정지 사유

결제원은 가입자의 공인인증서 효력정지 신청이 있는 경우 당해 공인인증서의 효력을 정지시킬 수 있습니다.

3.6.2 폐지 사유

결제원은 법 제18조(공인인증서의 폐지) 및 "1.3.7 결제원의 의무"에서 정한 사항에 따라 다음의 사유가 발생한 경우 당해 공인인증서를 폐지합니다.

- 가입자가 공인인증서 폐지를 신청한 경우
- 가입자의 사망, 해산 등의 사유가 발생한 경우
- 피성년후견인이 법정대리인의 동의 없이 공인인증서를 발급받은 경우
- 피한정후견인이 법정대리인의 동의를 필요로 하는 법률행위 범위에 공인인증서 발급이 포함되어 있음에도 불구하고 법정대리인의 동의 없이 공인인증서를 발급받은 경우
- 공인인증서의 유효기간이 경과된 경우

23

- 가입자가 부정한 방법으로 공인인증서를 발급받았거나 그렇다고 의심되는 경우

- 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출된 경우

- yessign서비스 보안 유지 및 향상을 위하여 필요한 경우

- 기타 가입자가 준칙의 주요 의무나 주요 사항을 준수하지 않은 경우

3.6.3 효력정지 및 폐지 신청과 신원확인

3.6.3.1 효력정지 및 폐지신청서 처리

공인인증서 효력정지 및 폐지의 신청은 결제원 또는 등록대행기관에 하여야 하며, 신원확인은 "3.2.1 신원확인"을 준용합니다. 결제원은 효력정지 및 폐지신청이 접수된 경우 이를 즉시 처리합니다.

3.6.3.2 분실신고 접수시 처리

인터넷진흥원을 통해 분실신고를 접수한 경우 인터넷진흥원은 분실신고정보를 결제원에 전송하고, 결제원은 가입자 여부를 확인하여 그 결과를 인터넷진흥원에 통보합니다. 결제원은 분실신고자가 결제원의 가입자인 경우 지체없이 전자서명인증무지침 제7조에 따라 가입자의 신원을 확인하고 가입자의 신청에 따라 즉시 폐지 등의 처리를 한 후 그 결과를 인터넷진흥원에 통보합니다. 인터넷진흥원을 통해 접수된 분실신고의 접수시각은 결제원 시스템에 접수된 시각으로 합니다.

3.6.4 공인인증서 효력정지 및 폐지목록(CRL)의 갱신과 공고

결제원은 가입자 공인인증서의 효력정지 및 폐지 결과를 반영하여 최대 24시간 주기로 CRL을 갱신하고, 갱신 즉시 yessign홈페이지(<http://www.yessign.or.kr>) 또는 결제원 디렉토리시스템에 공고합니다.

3.6.5 강제 폐지에 따른 공지

결제원은 "3.6.2 폐지 사유"에 따라 가입자의 동의없이 공인인증서를 폐지한 경우 당해 가입자에게 전자우편 또는 전화 등을 이용하여 해당 사실을 통지합니다.

24

3.6.6 효력회복 신청과 신원확인

공인인증서 효력회복 신청은 결제원 또는 등록대행기관에 하여야 하며, 신원확인인 "3.2.1 신원확인"을 준용합니다. 결제원은 효력회복 신청이 접수된 경우 이를 즉시 처리합니다.

3.6.7 효력회복 공고

공인인증서의 효력이 회복된 경우 결제원은 CRL에서 당해 공인인증서를 삭제하여 CRL을 공고합니다.

3.6.8 효력회복 기간의 제한

법 제17조(공인인증서의 효력정지 등)에 따라 공인인증서의 효력이 정지한 날로부터 6월이 경과하여도 효력회복이 되지 않은 공인인증서는 가입자의 동의없이 자동으로 폐지됩니다.

3.7 인증서유효성확인(OCSP)서비스

인증서유효성확인(OCSP)서비스란 가입자가 이용자에게 접속하여 자신의 공인인증서를 제출하면 이용자는 전자서명을 검증하고 공인인증서 일련번호를 결제원 OCSP(Online Certificate Status Protocol) 시스템에 전송하며, 결제원은 고객이 제출한 공인인증서의 유효성을 실시간으로 검증하여 검증결과를 이용자에게 회신하는 서비스로서, 이용자는 이 서비스를 이용하여 결제원의 yesign 공인인증서 뿐만 아니라 다른 공인인증기관에서 발급한 공인인증서의 유효성도 실시간으로 검증할 수 있습니다.

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.

3.9 공인인증서 프로파일

결제원이 발급하는 가입자 공인인증서는 「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	
	type	OID	m	m	C(Country)는 printableString,	
4	value	printableString 또는 utf8String	m	m	그이외의 속성값은 utf8String	
	Validity		m	m		
5	notBefore	UTCTime	m	m	인증서 유효기간	[1]
	notAfter	UTCTime	m	m		
6	Subject		m	m	[KCAC.TS.DN] 준수	
	type	OID	m	m	C(Country)는 printableString,	
6	value	printableString 또는 utf8String	m	m	그이외의 속성값은 utf8String	
	Subject Public Key Info		m	m		
7	algorithm	OID	m	m	전자서명인증체계 알고리즘 기술규격 준수	
	subjectPublicKey	BIT STRING	m	m		
8	Extensions		m	m		[2]

[1] 준칙 "2.1 공인인증서 종류", "3.3 공인인증서 갱신발급", "3.4 공인인증서 재발급"에 명시된 유효기간

[2] 아래 "2) 확장필드" 참조

3.8 시점확인서비스

결제원은 법 제20조(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.

2) 확장필드

#	필드명	ASN.1 타입	C	지원여부	Note	비고
				생성	처리	
1	Authority Key Identifier			m	m	
	keyIdentifier	OCTET STRING	n	m	m	발급자 인증서의 KeyID
	authorityCertIssuer	GeneralNames		m	m	
1	authorityCertSerialNumber	INTEGER		m	m	
	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			m	m	
	policyIdentifier	OID		m	m	인증서 정책 [1]
	policyQualifiers			m	m	
	PolicyQualifierId	OID		m	m	CPS, UserNotice
	Qualifier			m	m	
	CPSuri	IASString		m	m	준칙의 URI
	UserNotice			m	m	
NoticeReference	SEQUENCE		-	-		
4	ExplicitText	BMPString		m	m	공인인증서 표시규격 준수
	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 공인인증기관 한글실명
8	Extended Key Usage	OID	n	o	o	id-kisa-HSM [2]
9	Basic Constraints			-	x	x
10	Policy Constraints			-	-	-
11	Name Constraints			-	-	-
12	CRL DistributionPoint			m	m	
	distributionPoint	DistributionPointName	n	m	m	CRL 획득 정보
	reasons	ReasonFlags		-	-	
	cRLIssuer	GeneralNames		o	m	간접 CRL발급시 사용
13	Authority Information Access			m	m	
	accessMethod	OID	n	m	m	id-ad-ocsp
	accessLocation	GeneralNames		m	m	OCSP URI

[1] 인증서 정책은 준칙 "2.1 공인인증서 종류" 참조

[2] [KCAC.TS.HSM]의 보안토큰 기반일 경우 보안토큰 식별자(id-kisa-HSM) 사용

3.10 공인인증서 효력정지 및 폐지목록(CRL) 프로파일

결재원이 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	
	type	OID	m	m	C(Country)는 printableString, C(Country)는 printableString, 그이외의 속성값은 utf8String	
	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		
	crfEntryExtensions	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

3.11 인증서유효성확인(OCSP) 서비스용 공인인증서 프로파일

결재원은 인터넷진흥원으로부터 다음과 같은 내용을 포함하는 인증서유효성확인 서비스용 공인인증서를 발급받아 사용합니다.

1) 기본필드

“3.9 공인인증서 프로파일, 1) 기본필드”와 동일합니다.

2) CRL 확장필드

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

[1] CRLDP 와 동일 ([KCAC.TS.DSCDP] 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	

2) 확장필드

#	필드명	ASN.1 타입	C	지원여부	Note	비고
				생성	처리	
1	Authority Key Identifier			m	m	
	keyIdentifier	OCTET STRING	n	m	m	제거지 않음 모두 사용
	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, 부인부채
4	Certificate Policy			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 공인인증기관의 준칙 URI
	UserNotice			m	m	
	NoticeReference	SEQUENCE		-	-	
	ExplicitText	BMPString		m	m	공인인증서 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 공인인증기관 한글실명
8	Extended Key Usage	OID	c	m	m	
9	Basic Constraints			-	x	x
10	Policy Constraints			-	-	-
11	Name Constraints			-	-	-
12	CRL DistributionPoint			m	m	
	distributionPoint	DistributionPointName	n	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-oid-ocsp [1]
	accessLocation	GeneralNames		-	-	
14	OCSP No Check	OID	n	o	m	id-pkix-ocsp-nocheck [2]

[1] 공인인증기관이 발급하는 경우에는 반드시 생성

[2] shortlived 인증서를 발행할 경우 사용

3.12 공인인증기관의 전자서명키 갱신

결재원의 전자서명키가 갱신되면 결재원은 갱신된 결재원 공인인증서를 디렉토리 시스템에 게시함으로써 이용자에게 배포하고, 가입자 공인인증서 발급·갱신·재발급시 결재원 공인인증서를 내려줌으로써 가입자에게 배포합니다.

3.13 공인인증업무 휴지 및 폐지

3.13.1 공인인증업무 휴지

자연재해 또는 천재지변이 아닌 불가피한 사정으로 결재원이 공인인증업무의 전부 또는 일부를 휴지하고자 하는 때에는 휴지기간을 정하여 휴지하고자 하는 날의 30일전까지 이를 가입자에게 통보하고 미래창조과학부에 신고합니다.

휴지기간은 법 제10조(인증업무의 휴지·폐지 등)에 의거 6월을 초과할 수 없습니다.

3.13.2 공인인증업무 폐지

자연재해 또는 천재지변이 아닌 불가피한 사정으로 결재원이 공인인증업무를 폐지하고자 하는 때에는 폐지하고자 하는 날의 60일전까지 이를 가입자에게 통보하고 미래창조과학부에 신고합니다.

이때 결재원은 가입자의 공인인증서와 그 효력정지 및 폐지에 관한 기록(이하 "가입자인증서 등"이라 함)을 다른 공인인증기관에게 인계합니다. 다만, 부득이한 사유로 인하여 가입자인증서 등을 인계할 수 없는 경우에는 그 사실을 미래창조과학부에 지체없이 신고합니다. 이 경우 미래창조과학부는 인터넷진흥원에 대하여 당해 공인인증기관의 가입자인증서 등을 인수하도록 명할 수 있습니다.

3.14 공인인증업무 정지 및 지정취소

미래창조과학부는 공인인증기관이 다음에 해당하는 경우에는 6월 이내의 기간

33

4. 공인인증업무 관련정보의 공고

4.1 공고 설비

공인인증서 발급 및 관리에 관한 정보와 CRL 등의 공인인증서 상태정보에 관련된 정보의 공고설비 운영주체는 결재원입니다. 결재원은 관련법령에 따라 공고설비를 운영하며, 이를 준수하지 않아 가입자 또는 이용자에게 손해를 입힌 때에는 법 제26조(배상책임)에 따른 책임을 집니다.

4.2 공고 방법

4.2.1 주요정보 공고위치

공인인증서, 공인인증서 효력정지 및 폐지목록 등 공인인증업무와 관련된 정보의 공고위치는 다음과 같습니다.

- 공고위치 : [ldap://ds.yessign.or.kr:389/](http://ds.yessign.or.kr:389/)
- 공인인증서 유효성 상태정보 : <http://ocsp.yessign.org:4612>
- 등록대행기관 목록 : <http://www.yessign.or.kr/ra.htm>

4.2.2 공고 빈도

공인인증서 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 yessign홈페이지(<http://www.yessign.or.kr>)에 공고합니다. 효력정지되거나 폐지된 공인인증서의 공고 누락에 따라 가입자 또는 이용자에게 손해를 입힌 때에는 법 제26조(배상책임)에 따른 책임을 집니다.

35

을 정하여 공인인증업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있습니다. 다만, '사외 기타 부정한 방법으로 지정을 받은 경우'와 '공인인증업무의 정지명령을 받은 자가 그 명령에 위반하여 공인인증업무를 정지하지 아니한 경우'에는 지정을 취소합니다.

- 사외 기타 부정한 방법으로 법 제4조의 규정에 의한 지정을 받은 경우
- 공인인증업무의 정지명령을 받은 자가 그 명령에 위반하여 공인인증업무를 정지하지 아니한 경우
- 법 제4조의 규정에 의한 지정을 받은 날부터 6월 이내에 공인인증업무를 개시하지 아니하거나 6월 이상 계속하여 공인인증업무를 휴지한 경우
- 법 제6조제4항의 규정에 의한 공인인증업무준칙 변경명령에 위반한 경우
- 법 제11조의 규정에 의한 시정명령을 정당한 사유없이 이행하지 아니한 경우

지정이 취소된 경우 가입자인증서 등의 인계에 관한 사항은 "3.13.2 공인인증업무 폐지"를 준용합니다.

34

5. 공인인증업무 시설 및 장비 보호조치

5.1 물리적 보호조치

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

5.1.1 공인인증시스템 운영실의 격실분리에 관한 사항

결재원은 다음의 공인인증시스템을 별도의 운영실로 분리합니다.

- 가입자정보 관리 기능을 제공하는 시스템, 공인인증기관 전자서명키 관리, 공인인증서 생성·발급 기능을 제공하는 시스템은 동일 운영실에 설치할 수 있으나 다른 시스템과는 별도 운영실로 분리
- 공인인증서 공고기능을 제공하는 시스템은 다른 시스템과는 별도 운영실로 분리
- 공인인증서 상태확인 기능을 제공하는 시스템, 시점확인 기능을 제공하는 시스템은 동일 운영실에 설치할 수 있으나 다른 설비와는 별도 운영실로 분리

5.1.2 물리적 접근 통제

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

- 결재원의 공인인증시스템은 별도의 통제구역 내에 설치·운영
- 결재원의 출입통제 시스템은 신원확인카드, 지문인식, 무게감지장치 등을 다중으로 결합하여 통제구역에 대한 접근통제
- 결재원은 공인인증시스템의 물리적 접근통제를 위하여 보안캐비닛 내에 설치
- 결재원은 하드웨어 보수 등의 업무수행을 위하여 외부인이 공인인증시스템

36

- 운영실 등에 출입할 경우에 반드시 담당관리자가 동행
- 결재원은 출입통제시스템과 연계하여 통제구역 출입내역을 기록하고 정기적으로 그 기록을 검토
- 결재원은 다음의 감시통제시스템을 설치하며 이상상황 발생시 경보 및 인접시설간 유·무선 연락기능을 확보
 - CCTV 카메라 및 모니터링시스템
 - 침입감지시스템
- 결재원은 2인 이상의 청원경찰을 배치하여 보안경비업무 수행

5.1.3 수해 방지

결재원은 침수로부터 공인인증시스템을 안전하게 보호하기 위하여 바닥으로부터 최소 30cm 이상의 위치에 설치하며 누수의 감지 및 신속한 대처를 위하여 누수경보기를 이용합니다.

5.1.4 화재 예방

결재원은 공인인증시스템 운영실 등에 화재예방을 위하여 화재 탐지기, 휴대용 소화기, 자동소화설비 등을 설치하고 있습니다.

5.1.5 전원

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

5.1.6 방호

공인인증시스템 운영실의 외벽은 공인인증업무의 제공에 필수적으로 요구되는 공인인증시스템을 외부 침입으로부터 보호할 수 있도록 설계합니다.

- 외벽 재질은 벽돌 또는 철근 콘크리트로 축조되어 있거나, 철골구조물에 3T 이상의 철판으로 용접
- 외벽은 천장, 바닥까지 완벽하게 마감

37

5.2 절차적 보호조치

5.2.1 공인인증업무에 대한 업무 분장

결재원은 공인인증업무의 안전성과 신뢰성을 확보하기 위하여 결재원 소속직원으로 공인인증업무 수행인력을 역할별로 분리하여 운용하며, 해당 인력은 “5.4.1 공인인증업무 인력의 자격, 경력 등 요구사항”에서 정한 자격 및 경력을 갖추어야 합니다.

- 결재원은 모든 보호조치를 계획, 감독, 통제하는 관리책임자를 지정
- 결재원은 모든 보호조치의 실행을 담당하는 보안관리자를 지정
- 결재원은 주요시설의 유지관리를 위하여 공인인증시스템 관리, 네트워크 관리 등을 담당하는 전문인력(관련분야 2년 이상 경력자)인 보안실무자를 1인 이상 확보
- 결재원은 가입자의 등록정보관리 기능을 지원하는 공인인증시스템의 설치 운영 및 유지보수에 2인 이상의 직원을 배치하여 공동으로 업무를 수행
- 결재원은 공인인증서 생성·발급·관리 기능을 지원하는 공인인증시스템의 설치 운영 및 유지보수에 2인 이상의 직원을 배치하여 공동으로 업무를 수행

5.2.2 공인인증업무 담당자 인증 방법

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

5.2.3 동일인에 의해 동시 수행될 수 없는 공인인증업무

결재원은 공인인증업무 운영시의 신뢰성 및 보안성 확보를 위하여 다음과 같이 업무분리 원칙을 준수합니다.

- 키 생성 업무는 3인 이상이 공동으로 수행
- 공인인증서 발급 및 관리 업무는 2인 이상이 공동으로 수행
- 동일 시스템에 대한 운영 및 감사업무는 동일하지 않은 자가 각각 수행

39

- 운영실을 분리할 수 있도록 공인인증시스템 운영실의 내벽을 설계
- 창문이 있는 경우 강화유리 또는 강화필름으로 코팅한 유리를 사용

5.1.7 향온향습, 통풍

공인인증시스템 운영실은 적정용량의 향온향습장치를 설치 운영하며, 통풍장은 사람이 통과할 수 있을 경우 차폐막을 설치합니다.

5.1.8 기타 보호설비

공인인증시스템 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

5.1.9 매체 저장

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

5.1.10 시설 및 장비의 폐기 처리

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

5.1.11 원격지 백업설비 안전운영

결재원은 공인인증서 등 중요정보 보관을 위해 10km 이상 떨어진 곳에 원격지 백업설비를 운영하고 있으며, 출입통제시스템, 침입감지장치 등 보호설비를 구축·운영하고 있습니다.

38

5.3 기술적 보호조치

5.3.1 전자서명정보 생성

- 결재원은 인가된 자만이 전자서명정보를 생성할 수 있도록 합니다.
- 결재원은 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로 부터 보호되는 안전한 키 생성시스템에서 전자서명정보를 생성합니다.

5.3.2 전자서명정보의 크기 및 해쉬값

결재원은 안전하고 신뢰할 수 있는 전자서명 알고리즘을 사용하기 위하여 다음 크기의 정보 및 해쉬값을 이용합니다.

- RSA 및 KCDSA 경우 : 2048 비트 이상
- HAS-160 및 SHA-1 경우 : 160 비트
- SHA-256 경우 : 256 비트

5.3.3 전자서명생성정보 저장장치

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

5.3.4 전자서명생성정보 생성·사용 후 안전한 삭제 방법

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

5.3.5 전자서명생성정보 파기 방법

결재원은 공인인증서의 유효기간이 만료되거나 전자서명생성정보가 훼손·유출되었을 경우 당해 전자서명생성정보의 저장매체를 물리적으로 완전히 파기합니다.

5.3.6 전자서명생성정보 사용기간

결재원 및 가입자의 전자서명생성정보는 당해 공인인증서가 유효한 기간 동안

40

사용할 수 있습니다.

5.3.7 공인인증시스템 구성 및 관리 등 시스템 보호에 관한 사항

- 결제원은 공인인증시스템을 2중화하여 구성합니다.
- 결제원은 공인인증업무와 관련된 주요 프로그램 또는 프로세스의 동작여부를 점검할 수 있는 시스템을 설치 운영합니다.
- 결제원은 루트관리자의 권한을 제한할 수 있는 소프트웨어를 설치합니다.
- 결제원은 공인인증시스템의 운영에 필요한 프로그램을 설치합니다.
- 결제원은 공인인증시스템의 운영체제에서 불필요한 사항은 삭제합니다.
- 결제원은 공인인증시스템 운영체제의 문제점 해결을 위한 최신의 패치를 설치하여 운영합니다.
- 결제원은 공인인증시스템을 잠금장치가 장착된 보안캐비닛에 보관하고, 잠금장치의 열쇠는 별도의 보관함을 마련하여 관리합니다.
- 결제원은 공인인증시스템에 대한 논리적인 접근통제를 설정합니다.
- 결제원은 공인인증시스템의 추가/폐기/변경(운영체제의 변경, 패치 등)에 관한 사항을 관리대장에 기록하고 유지합니다.
- 결제원은 공인인증시스템의 추가/폐기/변경에 관한 사항을 내부 지침에 의거 관리합니다.
- 결제원은 서비스 방해공격을 방지하기 위하여 침입탐지시스템을 사용합니다.
- 결제원은 네트워크 보안을 위하여 「국가기관용 정보통신망 침입차단시스템 평가기준·지침」을 충족하는 침입차단시스템을 사용합니다.

5.3.8 공인인증 S/W 형상관리 등 운영관리에 관한 사항

결제원은 공인인증 S/W의 형상관리 등 공인인증시스템의 운영에 대한 형상관리를 합니다.

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

41

5.4.1 공인인증업무 인력의 자격, 경력 등 요구사항

결제원은 공인인증업무에 필요한 시설 및 장비의 운영인력으로서 다음의 요건을 갖춘 자를 12인 이상 확보합니다.

- 정보통신기사·정보처리기사 및 전자계산기조직응용기사 이상의 국가기술자격 또는 이와 동등 이상의 자격이 있다고 미래창조과학부가 인정하는 자격을 갖춘 것
- 미래창조과학부가 정하여 고시하는 정보보호 또는 정보통신 운영·관리 분야에서 2년 이상 근무한 경력이 있을 것
- 인터넷진흥원에서 실시하는 공인인증업무에 관한 시설 및 장비의 운영, 비상복구대책 및 침해사고의 대응 등에 관한 교육과정을 이수할 것

5.4.2 공인인증업무 교육, 업무순환에 관한 사항

- 결제원은 보호조치에 대하여 소속직원이 관련내용을 숙지할 수 있도록 내부교육 등의 필요한 조치를 취합니다.
- 결제원은 보안관리자 및 보안실무자, 공인인증시스템을 관리하는 직원이 연 1회 이상 정보보호관련 내부 또는 외부교육을 이수하도록 합니다.
- 결제원은 공인인증시스템을 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 공인인증시스템을 관리하는 직원이 인사이동 또는 퇴직하는 경우에는 내부규정에 따라 계정삭제 및 저장매체 반납 등의 적절한 조치를 취하도록 합니다.

5.4.3 비인가된 행위에 대한 처벌에 관한 사항

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

43

5.3.9 네트워크의 구성 및 운영 등 네트워크 보호에 관한 사항

- 결제원은 공인인증 네트워크를 이중화하여 구성하여 장애에 대비하고, 침입차단 및 침입탐지시스템을 사용하여 네트워크를 보호합니다.
- 결제원은 침입차단 및 침입탐지시스템을 「공인인증기관의 시설 및 장비 등에 관한 규정」에 따라 설치합니다.
- 결제원은 네트워크회선을 공인인증업무 제공을 위하여 별도의 회선을 사용합니다.
- 결제원은 침입차단 및 침입탐지시스템에 해당 기능의 소프트웨어만 설치합니다.
- 결제원은 침입탐지시스템의 데이터베이스를 주기적으로 갱신하고, 네트워크관리시스템을 이용하여 공인인증시스템을 지속적으로 모니터링합니다.
- 결제원은 로그기록을 주기적으로 분석하여 침입사도, 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 내부 지침에 의거 관리합니다.

5.3.10 시점확인서비스 등 부가서비스 운영에 대한 보호조치

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

5.4 인적 보안

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

42

5.5 감사 기록

5.5.1 감사기록의 유형 및 보존기간

결제원은 공인인증시스템에서 발생한 다음의 사건에 대한 세부내역을 감사기록에 10년 이상 보존합니다.

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

5.5.2 감사기록 보호조치

결제원의 감사관리자는 공인인증시스템의 감사기록을 조회하고 관리합니다.

각 시스템의 감사기록은 감사관리자가 총괄 관리하며, 시스템의 각 업무관리자는 각자의 업무에 대한 감사기록만을 열람할 수 있습니다.

5.5.3 감사기록 백업주기 및 절차

결제원은 감사기록을 매일 일별백업받아 하드디스크 이외의 저장매체에 보존합니다.

44

5.6 기록 보존

5.6.1 보존기록의 유형 및 보존기간

결재원은 법 제22조(인증업무에 관한 기록의 관리)에 따라 다음의 업무와 관련된 내역을 당해 공인인증서 효력이 소멸된 날로부터 10년 동안 기록·보존합니다.

- 공인인증서 발급 및 관리 등 공인인증업무
- 결재원 공인인증시스템 등의 운영업무

5.6.2 보존기록의 보호조치

결재원은 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.

결재원은 “5.6.1”의 기록을 공인인증업무 수행하는 시설과 해당 시설로부터 10Km이상의 원격지 저장설비에 각각 1부씩 보존합니다.

5.6.3 보존기록의 백업주기 및 백업절차

결재원은 보존기록을 매일 일별백업받아 보존합니다.

5.7 장애 및 재해복구

결재원은 공인인증시스템 장애, 전자서명 생성정보 유출 등에 따른 공인인증업무의 중단 또는 그와 동등한 사고와 지진·홍수·화재 등 재해에 대비하여 신속한 대응 및 복구체제를 구축하고 있습니다.

45

5.7.1 공인인증업무 장애 유형별 복구

- 월·바이러스, Dos 공격 등으로 인한 장애의 경우 관련 침입차단시스템을 이용하여 해당 IP 및 포트를 차단하고, 침입탐지시스템을 통한 모니터링 강화조치를 취합니다.
- 해킹으로 인한 가입자 공인인증서 유출의 경우 유출된 가입자의 공인인증서를 폐지하고 가입자에게 통보합니다.
- 월·바이러스, Dos 공격 및 해킹 등에 대비하여 방화벽, 침입탐지시스템, 보안S/W, ID, PASSWORD 관리 및 S/W의 최신패치로 방어하며, 피해 발생 시 백업데이터로 복구합니다.
- 공인인증시스템을 이중화로 구성·운영하며 백업센터를 운영함으로써 지진·홍수·화재 등 재해 및 장애에 대비합니다.
- 논리적 장애 발생 시 장애이진시점 복구 기능을 이용하여 복구합니다.
- 시스템 접근 가능 IP통제, 서버보안S/W 설정 등으로 주요 자원에 대한 접근통제 및 복구체제를 구성합니다.

5.7.5 공인인증업무 장애방지 등 연속성 보장 대책

- 결재원은 공인인증시스템을 이중화하여 무정지 운영체제를 구축하고 백업센터를 운영하여 장애의 방지에 최선의 노력을 다합니다.
- 결재원은 가입자 공인인증서 등의 주요 데이터의 훼손·멸실이 발생하였을 경우 백업된 자료를 이용하여 신속히 복구하여 서비스의 연속성을 보장합니다.
- 결재원은 공인인증업무 운영인력을 주야간으로 운영하여 연중 무휴로 공인인증업무를 제공합니다.

47

5.7.1 공인인증업무 장애 및 재해 유형별 신고·복구

결재원은 「공인인증업무 비상대응 실무 매뉴얼」에 의하여 장애 및 재해 유형별로 미래창조과학부 및 인터넷진흥원에 신고합니다.

5.7.2 공인인증업무 장애 유형

다음의 장애 유형은 “주의”의 비상상황 등급으로 분류합니다.

- 해킹 등 침해사고에 의한 일부 가입자 전자서명생성정보 유출
- 공인인증시스템의 장애, 오작동 등으로 인한 장애
- 월·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
- 공인인증서유효성확인서비스 장애
- 공인인증서 발급서비스 장애

다음의 장애 유형은 “심각”의 비상상황 등급으로 분류합니다.

- 가입자 공인인증서 발급에 사용하는 전자서명생성정보 유출
- 해킹 등 침해사고에 의한 가입자 전자서명생성정보가 대량 유출되어 부정 사용되는 사고 발생
- 공인인증서유효성확인서비스 장애

5.7.3 공인인증업무 장애 유형별 신고절차

- 결재원은 “주의” 등급의 비상상황의 경우 인터넷진흥원에 신고하고 자체 비상대응조치를 취합니다.
- 결재원은 “경계” 등급의 비상상황의 경우 인터넷진흥원에 신고하고 인터넷진흥원 비상대응팀에 참여하며, 자체 비상대응조치를 취합니다.
- 결재원은 “심각” 등급의 비상상황의 경우 인터넷진흥원에 신고하고 미래창조과학부 비상대응본부에 참여하며, 자체 비상대응조치를 취합니다.

46

6. 공인인증업무 보증 등 기타사항

6.1 보증

6.1.1 보증 책임

결재원은 결재원이 발급한 공인인증서와 관련하여 다음의 내용을 보증합니다.

- 공인인증서 내에 포함된 내용은 발급신청 당시를 기준으로 결재원에 등록된 사실임
- 가입자의 공인인증서는 법, 시행령, 시행규칙을 준수하며, 준칙에 따라 발급됨
- CRL 내용의 정확함

6.1.2 보증 제한

결재원은 법, 시행령, 시행규칙 및 준칙 “6.1.1 보증책임”에서 정한 사항 이외의 사항, 즉 가입자의 신용, 가입자정보의 불변성 등을 보증하지 않습니다.

6.2 배상

6.2.1 배상 책임

결재원은 법, 시행령, 시행규칙 및 준칙의 규정을 위반하여 가입자 또는 공인인증서를 신뢰한 이용자에게 손해를 입힌 경우 법 제26조(배상책임)에 따라 손해배상 한도에서 그 손해를 배상합니다.

6.2.2 책임 제한

결재원은 결재원이 발급한 공인인증서 및 공인인증업무와 관련하여 발생하는 배상책임 이외의 것에 대해서는 책임을 지지 않습니다. 또한, 결재원은 법 제26조(배상책임)에 따라 결재원이 과실없음을 입증한 경우에는 그 배상책임이 면

48

제됩니다.

6.2.3 배상 한도

결재원은 결재원이 발급하는 공인인증서의 종류의 구분 없이 공인인증서마다 연간 및 건당 25억원을 한도로 손해배상책임을 집니다.

공인인증서로 인해 발생하는 손해배상액은 민법 제398조(배상액의 예정)에 따라 위 배상한도를 초과하지 않습니다. 동 배상한도에는 가입자, 이용자 등 결재원이 발급한 공인인증서와 관련한 모든 손해가 포함됩니다.

6.3 분쟁 해결

6.3.1 준거법

본 준칙은 대한민국의 관계법령에 따라 해석되고 적용됩니다.

6.3.2 재판 관할

공인인증업무 관련 분쟁이 발생할 경우 그 관할기관은 결재원 본사 소재지를 관할하는 지방법원이 됩니다.

6.3.3 분쟁을 해결하는 절차

공인인증업무와 관련하여 결재원과 가입자 또는 이용자간 분쟁이 발생한 경우 미래창조과학부는 결재원의 법, 시행령, 시행규칙 및 준칙 준수여부 등을 조사하고 관련법령의 절차에 따라 신속한 방법으로 분쟁을 해결할 수 있습니다. 이 경우 결재원은 관련 당사자의 서면요청에 의해 관련 자료를 제공할 수 있습니다.

49

- 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

6.4.3 개인정보 수집 및 이용목적

yes sign서비스에서는 인증서 발급 및 관리, 인증서비스 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, e-mail주소, 주소, 전화번호, 휴대전화번호
- 수집하는 고유식별정보 항목 : 주민등록번호
- 수집하는 기기정보 : IP 및 MAC주소, HDD Serial, USB Serial, OS버전, 웹 브라우저버전, 스마트폰 고유정보 등

6.4.4 개인정보보호에 대한 처리방침

yes sign서비스의 개인정보보호에 관한 사항은 개인정보처리방침을 수립하여 시행하고 있으며, 동 내용은 yes sign 홈페이지에서 확인하실 수 있습니다.

6.5 감사 및 점검 등

6.5.1 시설 및 장비에 대한 심사

결재원은 공인인증기관 지정 시 심사를 받은 시설 및 장비를 이용하여 공인인증업무를 수행하고 있습니다.

결재원 공인인증업무 수행을 위한 시설 및 장비의 변경이 필요한 경우 이를 미래창조과학부에 신고하여 변경 내용의 적절성을 확인받은 후 공인인증업무에 적용하고 있습니다. 단, 침해사고, 자연재해, 시스템 오류 등으로 인하여 긴급한 조치가 필요한 경우에는 변경 내용을 미리 적용할 수 있으며 적용 후 7일 이내에 신고할 수 있습니다.

51

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

공인전자서명인증체계 관련자에게 전달되는 문서(또는 전자문서)가 법적 효력을 갖기 위해서는 다음과 같은 요건을 만족해야 합니다.

- 공인인증서에 기초한 전자서명을 포함하며, 전자서명은 법 제2조(정의) 제3호 각목의 요건을 갖출 것
- 전자서명에 사용된 공인인증서가 유효한 상태이며, 정지 또는 폐지상태가 아닐 것

6.4 개인정보보호

6.4.1 공인인증업무 관련정보의 보호범위 및 책임

결재원과 등록대행기관은 공인인증업무 수행과정에서 얻게 되는 다음의 자료에 대하여 법 제24조(개인정보의 보호)를 준수하며, 이를 위반할 경우 관련 법률이 정하는 바에 따라 책임을 집니다. 그러나, 결재원과 등록대행기관은 제3자가 법률에서 정한 요건 및 절차에 따라 정보공개를 요구하는 경우 이를 따를 수 있습니다.

- 가입자의 개인정보(본인의 동의가 있거나 공인인증서 및 디렉토리시스템에 공개된 내용은 제외)
- 공인인증업무 관련 전문 기록과 전문에 대한 로그
- 결재원에서 생성 또는 보관하는 공인인증업무 관련 감사자료
- 재해복구대책
- 결재원 공인인증업무 운영관련 보안조치

6.4.2 개인정보보호를 위한 조치

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

50

6.5.2 정기점검

결재원은 공인인증업무 수행을 위한 시설 및 장비의 안전운영 여부를 인터넷진흥원으로부터 매년 정기적으로 점검을 받고 있습니다.

점검은 다음과 같은 사항에 대해 이루어집니다.

- 공인인증업무
- 전자서명키 관리
- 기타 공인인증업무
- 시설 및 장비의 관리
- 문서 및 기록의 관리
- 공인인증업무 시험운영 및 정보제공
- 네트워크 및 시스템 보안
- 물리적 보안
- 재해방지
- 관리적 보안 및 비상계획

6.6 관련법의 준수

“1.3”의 공인전자서명인증체계 관련자가 준수하여야 하는 법률규정은 다음과 같습니다.

- 법
- 시행령
- 시행규칙
- 미래창조과학부 고시
 - 전자서명인증업무지침
 - 공인인증기관의 시설 및 장비 등에 관한 규정
 - 공인인증기관의 보호조치에 관한 규정
 - 공인인증업무준칙 작성표준

52

다음 사항에 대한 지식재산권은 저작권법 등 관련법률에 따라 결재원에 귀속됩니다.

- 결재원이 개발한 소프트웨어 및 하드웨어
- 준칙
- 결재원 명칭
 - 법인명
 - 공인인증업무명(yesign)
- 결재원이 생성한 전자서명정보
- CRL

가입자 공인인증서의 경우 공인인증서 이용과정에서의 분배 등은 허용되나 결재원의 허락 없이 다수가 접근 가능한 장소에 공인인증서를 공개하는 것은 금지합니다.

6.7 공인인증업무준칙의 효력

준칙이 개정되면 개정된 내용은 개정 준칙의 효력발생일에 그 효력이 상실됩니다.

본 개정준칙은 **2013년 12월 16일**부터 효력이 발생합니다.