한국전자인증㈜ 전자서명인증사업자

공동인증서

전자서명 인증 업 무 준 칙

- Certification Practice Statement -

Version 6.1

한 국 전 자 인 증 주 식 회 사

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

- 제·개정 이력 -

버전	개정일	시행일	개정 사유
Ver 1.1	2002. 02 .19	2002. 03 .16	제정
Ver 1.2	2002. 08. 19	2002. 10. 10	개정
Ver 1.3	2002. 10. 19	2002. 11. 04	개정
Ver 1.4	2004. 05. 09	2004. 05. 24	개정
Ver 1.5	2004. 09. 13	2004. 09. 29	개정
Ver 1.6	2007. 03. 20	2007. 04. 08	개정
Ver 2.0	2007. 05. 21	2007. 07. 21	개정
Ver 2.1	2009. 05. 06	2009. 05. 28	개정
Ver 2.2	2011. 03. 11	2011. 03. 26	- 공인인증업무준칙 작성표준에 따른 수정
Ver 2.3	2012. 02. 02	2012. 02. 22	- 기타 정책 변경 반영
Ver 2.4	2013. 09. 05	2013. 09. 16	- 기타 정책 변경 반영
Ver 2.5	2014. 04. 23	2014. 05. 17	- 정의 및 약어 항목 추가 - 정기점검에 따른 수정
Ver 2.6	2016. 06. 16	2016. 07. 01	- 사전동의 받은 대상 관련 항목 추가
Ver 2.7	2016. 07. 06	2016. 07. 20	- 전자서명법 시행규칙 개정에 따른 내용 반영
Ver 2.8	2017. 02. 13	2017. 02. 28	- 인증기관 간 합의된 업무 추가
Ver 2.9	2017. 10. 30	2017. 11. 09	- 전자서명법 시행규칙 개정에 따른 내용 반영
Ver 3.0	2019. 08. 29	2019. 09. 12	- 공고 정보 현행화 - 암호 키 길이 변경 (KISA 권고사항)
Ver 4.0	2020. 11. 26	2020. 12. 10	- 전자서명법 개정에 따른 명칭 변경
Ver 5.0	2021. 08. 23	2021. 09. 06	- 전자서명인증업무준칙 작성방법 개정에 따른 조항 재배치
Ver 5.1	2021. 10. 22	2021. 11. 05	- 불필요 항목 삭제
Ver 5.2	2021. 11. 01	2021. 11. 16	- 전자서명인증업무의 수행에 필요한 사항 수정 및 추가 / 불필요 항목 삭제
Ver 5.3	2021. 12. 08	2021. 12. 23	- 전자서명인증업무의 수행에 필요한 사항 수정 및 추가 / 불필요 항목 삭제

Ver 5.4	2022. 11. 03	2022. 12. 05	- 제·개정 이력표 추가 - 신규 서비스 내용 추가 (클라우드 공동인증서비스, 비대면 신원확인 절차) - 정의 및 약어 항목 수정 - 그 외 기타 정책 변경 반영
Ver 5.5	2022. 12. 16	2023. 01. 09	- 4.12.2 클라우드 공동인증서비스 항목 수정 - 9.13 분쟁 해결 항목 수정
Ver 5.6	2023. 06. 28	2023. 08. 04	- 3.2.1 신원확인 방법 수정 - 3.2.1.5 대면에 준하는 비대면 신원확인 방법 수정
Ver 5.7	2023. 10. 23	2023. 12. 20	- 5.2.1 내부감사자 역할 추가 - 1.3.5.2 , 1.3.6.2 , 9.2.1.3 , 9.2.1.4 , 9.2.2 배상책임 및 면책 관련 항목 삭제 - 4.12.2 클라우드 공동인증서비스 항목 삭제 - 3.2.1.5 대면에 준하는 비대면 신원확인 방법 수정 - 그 외 일부 조항 문구 수정
Ver 5.8	2024. 08. 05	2024. 08. 28	- 전자서명인증업무의 수행에 필요한 사항 현행화 (3.2.1, 3.2.1.5, 5.1.1, 5.8)
Ver 5.9	2024. 11. 20	2024. 12. 04	- 전자서명인증업무의 수행에 필요한 사항 추가 및 삭제, 일부 조항 문구 수정 (1.3.1 / 1.3.4.2 / 3.2.1.2 / 3.2.1.3 / 3.2.1.5 / 4.1.1.2 / 6.1 / 9.2.1.1 / 9.2.1.2 / 9.6 / 9.13.1)
Ver 6.0	2025. 07. 17	2025. 08. 05	- 전자서명인증업무의 수행에 필요한 사항 추가 , 일부 조항 문구 수정 (1.3.4 / 1.4 / 3.2.1.5 / 9.1.1)
Ver 6.1	2025. 11. 04	2025. 12. 30	- 전자서명인증업무의 수행에 필요한 사항 현행화 및 일부 조항 문구 수정 (1.3.5.2 / 1.5.3 / 3.2.1.2 / 3.2.1.5 / 4.2.2 / 4.4 / 4.9.1.4 / 5.4.2 / 5.5.3 / 8장 / 9.1.3 / 9.2.1.1)

목 차

제1장 소 개

1.1 개요

1.1.1 준칙의 배경 및 목적

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

1.1.2 전자서명인증체계 소개

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

1.2 인증업무준칙의 명칭

본 인증업무준칙은 한국전자인증 공동인증서 전자서명 인증업무준칙 버전(version) 6.1입니다.

1.3 전자서명인증체계 관련자

1.3.1 과학기술정보통신부

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

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

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

1.3.2 한국인터넷진흥원

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

- 운영기준 준수사실의 인정을 받으려는 전자서명인증사업자가 법 제8조(운영기준 준수 사실의 인정)에 따른 자격을 갖추었는지 인정 여부 결정 및 증명서 발급 및 공고
- 법 제11조(국제통용평가)에 의한 전자서명인증사업자의 국제통용평가 인정 여부 결정 및 증명서 발급 및 공고
- 시행령 제3조(운영기준 준수사실 인정의 취소)에 의한 운영기준 준수사실 인정의 취소
- 운영기준 준수여부 평가를 신청한 전자서명인증사업자에 대하여 세부 평가 기준, 평가 범위, 평가 일정 및 평가 참관에 관한 사항 등을 평가기관과 협의
- 법 제21조(전자서명인증 정책의 지원 등)에 의한 전자서명인증 정책 지원

인증체계의 최상위 인증기관(Rootca)은 한국인터넷진흥원으로 인증체계 관리 및 운영하는 업무를 수행합니다

1.3.3 한국전자인증

1.3.3.1 역할

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

- 가입자의 신원확인
- 인증서비스 관련 제반 신청서 접수 및 처리
- 등록대행기관의 지정과 관리 및 운영

- 시점확인 서비스의 제공
- 공동인증서 발급(신규/재발급/갱신), 효력정지, 효력회복, 폐지 등의 인증서비스의 제공
- 공동인증서 목록, 공동인증서 효력정지 및 폐지목록 등 공동인증서 관련 정보 공고
- 인증업무준칙 공고
- 공동인증서 관련 정보 공고
- 기타 인증서비스와 관련된 업무

1.3.3.2 책임과 의무

① 관련 법규 및 인증업무준칙의 준수

한국전자인증은 인증서비스를 수행하는 동안 전자서명관련법을 준수합니다.

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

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

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

② 인증서비스의 제공

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

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

③ 인증서비스의 보장

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

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

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

④ 가입자의 개인정보 보호 및 자료의 보안 유지

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

⑤ 전자서명생성정보의 올바른 이용

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

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

⑥ 전자서명생성정보의 보호

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

1.3.4 등록대행기관

1.3.4.1 역할

한국전자인증은 한국전자인증을 대신하여 가입자에 대한 신원확인을 수행하고 공동인증서 발급, 효력정지, 효력회복 또는 폐지 등의 신청을 접수·등록 업무를 수행하거나, 전자적 방식으로 수집된 인증서 신청정보의 안전한 관리 및 신청 절차의 적정성 확보와 관련된 업무를 수행하는 자 (이하 "등록대행기관"이라 한다)를 지정하여 운영할 수 있습니다. 등록대행기관의 업무는 다음과 같습니다.

- 공동인증서 발급(신규/재발급/갱신), 폐지, 효력정지 및 효력회복 신청 접수 및 등록
- 인증서비스 신청인의 신원확인 업무
- 전자적 방식으로 처리되는 인증서 신청정보의 검토·관리 및 관련 절차의 적정성 확보
- 기타 인증서비스와 관련하여 한국전자인증이 위임한 업무

1.3.4.2 책임과 의무

① 인증업무준칙의 이해

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

② 가입자의 신원확인

등록대행기관은 공동인증서를 발급받고자 하는 자에 대하여 전자서명관련법에서 정하는 신원확인의 기준 및 방법에 따라 신원을 확인합니다.

③ 배상과 책임

등록대행기관은 법령에 정한 사항을 위반하여 한국전자인증, 가입자 또는 이용자에게 손해를 입힌 경우 그 손해에 대해 배상하여야 할 책임이 있습니다.

④ 인증업무준칙의 준수

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

⑤ 가입자의 개인정보보호

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

1.3.5 가입자

1.3.5.1 역할

가입자는 전자서명생성정보에 대하여 한국전자인증으로부터 전자서명인증을 받은 자를 말합니다.

1.3.5.2 책임과 의무

① 정확한 정보의 제공

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

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

② 전자서명생성정보의 관리

가입자는 자신의 전자서명생성정보를 안전하게 보관관리하고, 이를 분실훼손 또는 도난유출되거나 훼손될 수 있는 위험을 인지한 때에는 그 사실을 즉시 한국전자인증에게 통보하여야 합니다. 이 경우 가입

자는 지체 없이 이용자에게 한국전자인증에 통보한 내용을 고지하여야 합니다.

③ 공동인증서의 관리

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

1.3.6 이용자

1.3.6.1 역할

이용자는 한국전자인증이 제공하는 전자서명인증서비스를 이용하는 자를 말합니다.

1.3.6.2 책임과 의무

① 이용자의 준수사항

이용자는 가입자의 인증서에 대해 이용목적과 이용 가능 범위에 대해 정확하게 이해해야 하며, 인증서 기재사항 등에 의하여 전자서명의 진위여부를 확인하기 위하여 다음의 조치를 취하여야 합니다.

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

1.4 공동인증서 종류

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

발급대상	공동인증서 종류	용도(이용범위)	유효 기간
법인/단체/개인사업자	범용	-일반 전자상거래 -금융기관 업무 -정부 전자조달 /민원업무 -국세청 전자 세금계산서/민원업무	1년, 2년, 3년
	용도제한용	-전자계약 업무 -전자세금계산서 업무 -은행, 보험 및 신용카드 업무 -원산지 증명 업무 -조달 비축물자 업무	
	서버용	-온라인상 서버를 통해 인증서비스를 이용하는 업무	
개인	범용	-일반 전자상거래 -금융기관 업무 -정부 민원업무	
	용도제한용	-은행, 보험 및 신용카드 업무 -정부 민원업무 -EMR 전자서명 업무 -내부 업무용	

[표] 공동인증서의 종류, 용도 및 유효기간

1.5 인증업무준칙의 관리

1.5.1 인증업무준칙의 관리부서 및 연락처

본 인증업무준칙의 관리는 한국전자인증 공동인증사업본부에서 담당하며 연락처는 다음과 같습니다.

(전화: 02-3019-5623 팩스: 02-3019-5656 전자우편: gca@crosscert.com)

1.5.2 인증업무준칙의 개정 사유

한국전자인증은 다음의 사유가 발생한 경우에 인증업무준칙을 개정합니다.

- 법 제15조(전자서명인증업무준칙의 준수 등) 제1항에 의거 준칙의 변경이 필요할 경우
- 한국전자인증에서 제공하는 인증서비스의 내용이나 절차가 변경되었거나 신규로 제공하는 인증관련 서비스로 인해 인증업무준칙의 변경이 필요하다고 판단된 경우

1.5.3 인증업무준칙의 제·개정 절차 및 공고

한국전자인증은 전자서명인증업무의 개선을 위하여 준칙의 변경이 필요하다고 판단하는 경우, 준칙의 관리부서 및 인증업무 담당부서의 상호 협의 후 전자서명인증 업무 총괄(전자인증사업본부장)의 승인을 받아 제·개정하며, 그 사항이 관련기관 또는 최상위인증기관(한국인터넷진흥원 등)에 중대한 영향을 미치거나 협의가 필요한 경우에는 관련자와 사전 협의를 거쳐 진행합니다.

한국전자인증은 다음 각 호의 사항이 포함된 준칙을 작성하여 한국전자인증의 웹사이트(https://www.crosscert.com/glca/01_5_05_2.jsp)에 게시하는 방법으로 공고합니다. 준칙 중 다음 각목의 내용을 변경한 때도 또한 같습니다.

가. 전자서명인증서비스의 종류
나. 전자서명인증서비스의 요금, 이용범위 및 유효기간 등 이용조건
다. 전자서명인증업무의 수행방법 및 절차
라. 그 밖에 전자서명인증업무의 수행에 필요한 사항

1.5.4 인증업무준칙 개정에 대한 가입자 동의 방법

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

1.6 정의 및 약어

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

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

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

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

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

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

전자서명: 다음 각 목의 사항을 나타내는 데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말합니다.

1) 서명자의 신원

2) 서명자가 해당 전자문서에 서명하였다는 사실

전자서명검증정보: 전자서명을 검증하기 위하여 이용하는 전자적 정보를 말합니다.

전자서명생성정보: 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말합니다.

전자서명키: 전자서명생성정보와 이에 합치하는 전자서명검증정보를 말합니다.

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

가입자: 전자서명생성정보에 대하여 전자서명인증사업자로부터 전자서명인증을 받은 자를 말합니다.

이용자: 전자서명인증사업자가 제공하는 전자서명인증서비스를 이용하는 자를 말합니다.

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

기타 용어의 정의는 전자서명법에 따릅니다.

제2장 전자서명인증업무 관련 정보의 공고

2.1 공고설비

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

2.2 공고방법

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

한국전자인증의 전자서명인증업무관련정보의 저장·공고위치는 다음과 같습니다.

한국전자인증 관련 정보

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

2.3 공고 주기

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

2.4 공고된 정보에 대한 책임

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

제3장 신원확인

3.1 가입자 이름(Distinguished Name)의 표시 방법

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

① DN의 표현방법

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

- 개인 실명, 법인명 등 법적 이름
- 전자우편 주소

② DN의 유일성 보장방법

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

3.2 공동인증서 신규 발급 시 신원확인

3.2.1 신원확인 방법

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

- 신규가입자는 직접 대면(운영기준에 적합한 것으로 인정받은 직접 대면에 준하는 비대면 방법을 포함)에 의한 신원확인을 실시하는 것을 원칙으로 합니다.
- 시행규칙 제5조(실지명의 기준의 신원확인 방법)에 의거하여 신원확인을 합니다.
- 한국전자인증이 정한 신원확인 절차를 거친 가입자에게만 공동인증서를 발급합니다.
- 한국전자인증은 재외동포청과 업무 협의를 통해 각국 재외공관에서 공동인증서 발급서비스를 제공하고 있습니다. 각 공관의 실무관은 한국전자인증이 정한 신원확인 절차를 거쳐 가입자의 신원확인

및 신청 내용을 확인합니다.

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

3.2.1.1 개인용 인증서

- 일반인 (성년)
  - 인증서비스 신청서
  - 신원확인증표 사본 앞면 (원본지참)
    - 주민등록증 발급대상자는 주민등록증
    - 다만, 주민등록증에 의하여 확인하는 것이 곤란한 경우에는 국가기관, 지방자치단체 또는 「교육기본법」에 따른 학교의 장이 발급한 것으로서 실지명의의 확인이 가능한 증표 또는 주민등록번호를 포함한 주민등록표 초본과 신분을 증명할 수 있는 증표
- 미성년자
  - 인증서비스 신청서
  - 미성년자와 법정대리인의 신원확인증표 사본 앞면 (원본지참)
    - 미성년자와 법정대리인의 주민등록증
    - 다만, 주민등록증에 의하여 확인하는 것이 곤란한 경우에는 국가기관, 지방자치단체 또는 「교육기본법」에 따른 학교의 장이 발급한 것으로서 실지명의의 확인이 가능한 증표 또는 주민등록번호를 포함한 주민등록표 초본과 신분을 증명할 수 있는 증표 또는
    - 주민등록증 발급대상자가 아닌 자는 주민등록번호를 포함한 주민등록표 초본과 법정대리인의 가목의 증표 또는 실지명의의 확인이 가능한 증표・서류
  - 법정대리인의 동의서
  - 미성년자와 법정대리인의 관계를 증명할 수 있는 증명 서류 (주민등록등본, 가족관계증명서 등)
- 재외국민
  - 인증서비스 신청서
  - 주민등록표(주민등록법 제6조에 따라 주민등록이 된 재외국민의 경우, 원본지참) 또는
  - 여권 사본 (원본지참) 또는
  - 재외국민등록증 사본 (원본지참)
- 외국인
  - 인증서비스 신청서

- □ 출입국관리법에 의한 등록외국인기록표에 기재된 성명 및 등록번호를 확인할 수 있는 신원확인증표 (원본지참)
- □ 다만, 외국인등록증이 발급되지 아니한 자의 경우에는 여권 또는 신분증에 기재된 성명 및 번호를 확인할 수 있는 신원확인증표 (원본지참)

3.2.1.2 사업자용 인증서

① 대표자 본인이 한국전자인증 또는 등록대행기관을 방문하여 공동인증서 발급신청을 할 경우

■ 법인

- □ 인증서비스 신청서
- □ 법인의 신원확인증표
  - 사업자등록증이나 납세번호를 부여 받은 문서 또는 그 사본
- □ 대표자의 신원확인증표 사본 앞면 (원본지참)
  - 본 인증업무준칙 3.2.1.1의 신원확인 증표를 준용합니다.

■ 단체

- □ 인증서비스 신청서
- □ 단체의 신원확인증표
  - 해당 단체를 대표하는 자의 실지명의를 확인할 수 있는 증표・서류
  - 고유번호 또는 납세번호를 부여 받은 경우에는 고유번호 또는 납세번호를 부여 받은 문서나 그 사본
- □ 대표자의 신원확인증표 사본 앞면 (원본지참)
  - 본 인증업무준칙 3.2.1.1의 신원확인 증표를 준용합니다.

■ 개인사업자

- □ 인증서비스 신청서
- □ 사업자 등록증 사본
- □ 대표자의 신원확인증표 사본 앞면 (원본지참)
  - 본 인증업무준칙 3.2.1.1의 신원확인 증표를 준용합니다.

② 대리인이 한국전자인증 또는 등록대행기관을 방문하여 공동인증서 발급신청을 하는 경우에는 본 인증업무준칙 3.2.1.3와 같습니다.

3.2.1.3 대리인이 신청하는 경우

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

- 인증서비스 신청서
- 본 인증업무준칙 3.2.1.2에서 정한 사업자의 신원확인증표
- 위임장 (인감날인)
- 법인 인감증명서 (개인사업자는 대표자의 인감증명서)
- 대리인의 신분확인증표 사본 앞면 (원본지참)
  - 본 인증업무준칙 3.2.1.1의 신원확인 증표를 준용합니다.

3.2.1.4 실지명의가 확인된 전자금융거래 가입자가 신청하는 경우

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

- 개인용 인증서를 신청하는 경우의 신원확인

- 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
- 이외 전자금융거래 가입자의 본인확인 수단 등 신원을 확인할 수 있는 정보

- 사업자용 인증서를 신청하는 경우의 신원확인

- 전자금융거래 가입자의 계정(ID)과 그 비밀번호 또는 계좌번호와 그 비밀번호
- (개인사업자) 전자금융거래 가입자의 주민등록번호, 사업자등록번호 또는
- (법인/단체) 전자금융거래 가입자의 사업자등록번호
- 금융기관이 전자금융거래를 위하여 가입자에게 제공한 일회용 비밀번호(보안카드의 비밀번호 포함) 또는 가입자 본인만이 알 수 있거나 소유한 두 가지 이상의 정보

3.2.1.5 대면에 준하는 비대면 신원확인 방법

한국전자인증은 대면에 준하는 비대면의 방법으로 신원확인을 할 수 있습니다. 신청자가 개인인 경우 신

청자의 신원을 확인하며, 사업자의 경우 사업자 및 사업자 대표자의 신원을 확인합니다. 사업자의 신원확인은 사업자등록증명 서류와 법인(법인인 단체 포함)의 경우에는 추가로 법인등기사항전부증명서를 통해 확인합니다.

신청자는 한국전자인증에 원본과 동일성을 확인할 수 있는 서류의 스캔본 또는 촬영본(이하 '스캔본 등')을 제출합니다. 한국전자인증은 서류의 진위를 확인할 수 있는 공공 사이트를 이용하여 신청자가 제출한 스캔본 등을 심사하고, 적합한 경우 별도의 원본을 요구하지 않을 수 있습니다.

한국전자인증이 대면에 준하는 비대면 신원확인을 하는 경우 그 방법은 아래와 같습니다.
그 방법은 연속적으로 이루어지며, 도중에 중단된다면 처음부터 다시 진행해야 합니다.

❑ 개인용 인증서를 신청하는 경우의 신원확인

① 본인 명의 휴대폰 인증을 통한 신원확인

- 신청자의 본인 명의 휴대폰 인증을 통해 인적사항을 확인합니다.
- 신청자가 제출한 본인확인수단 관련 정보를 한국전자인증으로 전송한 뒤 신청자는 한국전자인증으로부터 본인확인정보 검증결과를 수신하고, 그 결과에 따라 절차를 진행합니다.

② 신원확인증표 스캔본 등을 통한 신원확인

- 신원확인증표의 스캔본 등이 원본과 동일함을 확인합니다.
- 신원확인방법은 신원확인증표의 진위를 확인할 수 있는 공공 사이트를 통하여 진위여부를 확인합니다.
- 한국전자인증은 신원확인증표의 진위여부를 확인하기 위해 신원확인증표의 직접 촬영본 등을 요구할 수 있습니다.

③ 계좌인증에 의한 신원확인

- 실명 확인이 완료된 신청자의 금융계좌를 통해 소액을 송금하거나 송금 받도록 하는 방식입니다.
- 해당 계좌가 신청자 명의의 계좌인지 여부, 신청자가 해당 계좌를 조회하거나 송금할 권한을 보유한 실제 권리자인지 여부를 확인합니다.

❑ 사업자용 인증서를 신청하는 경우의 신원확인

사업자인 법인/단체 및 개인사업자는 비대면 신원확인 방법으로 인증서를 신청할 수 있으며, 아래 절차에 따라 대표자와 사업자의 신원을 확인합니다.

① 본인 명의 휴대폰 인증을 통한 신원확인

- 신청자의 본인 명의 휴대폰 인증을 통해 인적사항을 확인합니다.

- 신청자가 제출한 본인확인수단 관련 정보를 한국전자인증으로 전송한 뒤 신청자는 한국전자인증으로부터 본인확인정보 검증결과를 수신하고, 그 결과에 따라 절차를 진행합니다.

② 신원확인증표 스캔본 등을 통한 신원확인

- 신원확인증표의 스캔본 등이 원본과 동일함을 확인합니다.
- 신원확인방법은 신원확인증표의 진위를 확인할 수 있는 공공 사이트를 통하여 진위여부를 확인합니다.
- 한국전자인증은 신원확인증표의 진위여부를 확인하기 위해 신원확인증표의 직접 촬영본 등을 요구할 수 있습니다.

③ 셀카인증을 통한 신원확인

- 신원확인증표의 진위 확인이 완료된 후, 신청자가 본인의 얼굴을 촬영(셀카)하여 제출합니다.
- 제출된 셀카는 신분증의 사진과 비교하여 동일인 여부를 확인하기 위한 용도로 사용됩니다.
- 얼굴 인식 기술과 관리자 검수를 통해, 신분증 상의 인물과 실제 촬영된 인물이 동일인임을 확인합니다.

④ 서류 제출을 통한 사업자 신원확인

- 사업자의 신원확인을 위하여 사업자등록증명 서류를 제출하여야 하며, 법인(법인인 단체 포함)의 경우에는 추가로 법인등기사항전부증명서를 제출하여야 합니다.
- 제출하는 서류는 전자문서 형태로 신청서 접수일 7일이내 발급분으로 제한합니다.

3.2.2 가입자의 전자서명생성정보 소유증명 방법

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

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

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

3.3 공동인증서 갱신 발급, 재발급 및 변경 시, 신원확인

3.3.1 갱신발급 신원확인 방법 및 절차

① 신원확인 방법 및 절차

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

3.3.2 재발급 신원확인 방법 및 절차

① 신원확인 방법 및 절차

공동인증서 재발급은 본 인증업무준칙 3.2.1에 따라 신원확인을 합니다.

3.3.3 변경 신원확인 방법 및 절차

① 신원확인 방법 및 절차

한국전자인증은 공동인증서 내에 반영된 등록정보를 가입자가 변경하고자 하는 때에는 본 인증업무준칙 3.2.1에 따라 신원확인을 합니다. 그 외 가입자 등록정보(주소, 전화번호, 전자우편주소 등) 변경 요청 시에는 가입자의 전자서명에 대한 검증으로 신원확인을 대체하여 한국전자인증에 등록된 해당 정보를 변경할 수 있습니다.

3.3.4 갱신발급, 재발급 및 변경 시 가입자의 전자서명생성정보 소유증명 방법

본 인증업무준칙 3.2.2을 준용합니다.

3.4 공동인증서 효력정지·효력회복·폐지 시, 신원확인

3.4.1 효력정지 신원확인 방법 및 절차

① 가입자가 직접 방문하는 경우

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

② 가입자가 정보통신망을 이용하여 직접 효력정지 하는 경우

효력정지를 신청하고자 하는 가입자는 정보통신망을 이용하여 "인증서 효력정지"를 선택한 후 가입자가 보유한 전자서명생성정보를 이용하여 전자서명을 하고, 한국전자인증은 전자서명한 정보를 검증하는 과정을 통하여 신원확인 후 효력정지를 합니다.

3.4.2 효력회복 신원확인 방법 및 절차

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

3.4.3 폐지 신원확인 방법 및 절차

① 가입자가 직접 방문하는 경우

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

② 가입자가 정보통신망을 이용하여 직접 폐지하는 경우

폐지를 신청하고자 하는 가입자는 정보통신망을 이용하여 "인증서 폐지"를 선택한 후 가입자가 보유한 전자서명생성정보를 이용하여 전자서명을 하고, 한국전자인증은 전자서명한 정보를 검증하는 과정을 통하여 신원확인 후 폐지를 합니다.

한국전자인증은 인증서 폐지 처리에 대해 가입자에게 SMS 또는 유선으로 고지합니다.

제4장 인증서 관리

4.1 공동인증서 발급 신청

4.1.1 공동인증서 발급 신청 주체 및 신청 절차

① 공동인증서 신청 주체는 법인/단체/개인사업자 또는 개인이며, 이 신청 주체가 직접 혹은 대리인을 통하여 한국전자인증 또는 등록대행기관에 본 조의 공동인증서 발급 신청서류를 제출하여 신청합니다.

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

4.1.1.1 개인에 대한 신원확인

개인에 대한 신원확인의 경우 본 인증업무준칙 3.2.1에 따른 공동인증서 발급 신청 서류에 의해 제출된 제반 서류상의 성명과 주민등록번호의 확인뿐만 아니라 개인의 신원확인증표에 첨부된 사진 등에 의하여 본인 여부를 확인합니다. 다만, 당해 신청인이 제시한 신원확인증표의 사진에 의하여 본인여부의 식별이 곤란한 경우에는 다른 신원확인증표를 대체적으로 사용할 수 있습니다.

4.1.1.2 사업자에 대한 신원확인

사업자에 대한 신원확인의 경우 본인증업무준칙 3.2.1에 따른 공동인증서 발급 신청 서류에 의해 제출된 서류상의 명칭, 대표자 성명, 사업자등록번호 등에 의하여 진위여부를 확인하며, 당해 사업자의 대표자에 대하여도 신원을 확인합니다. 다만, 대리인이 신청하는 경우 그 대리인으로부터 대표자의 위임장을 제출받고 당해 대리인의 신원을 확인합니다.

4.1.1.3 실지명의가 확인된 전자금융거래 가입자의 신원확인 방법

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

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

이 경우는 아래 사항을 확인합니다.

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

② 전자금융거래 가입자의 주민등록번호

③ 금융기관이 전자금융거래를 위하여 가입자에게 제공한 일회용비밀번호(보안카드의 비밀번호를 포

함한다) 또는 가입자 본인만이 알 수 있는 두 가지 이상의 정보

4.2 공동인증서 발급 신청 처리

4.2.1 인증서 발급 신청 접수 및 처리 절차

한국전자인증 또는 등록대행기관은 공동인증서 발급 신청 정보 및 신청서류를 확인하고 가입 신청자의 신원확인을 마친 후 참조번호와 인가코드를 가입 신청자에게 전달합니다.

4.2.2 인증서 발급 신청에 대한 거절 기준

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

- 타인명의의 신청
- 가입신청서의 내용을 허위로 기재하였거나 허위서류를 첨부하여 가입신청을 하였을 경우
- 납부할 인증수수료를 인증업무준칙에서 정한 기간 내 납부하지 아니한 경우
- 제출된 서류만으로 신원확인이 곤란하거나 불가능한 경우
- 사고정보를 이용하여 발급 신청하였을 경우
- 전자서명관련법 또는 기타 관계 법령에 위반하거나 부정하게 행사할 목적으로 타인에게 양도 또는 대여하기 위하여 공동인증서 발급을 신청한 경우

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

4.2.3 인증서 발급 신청 접수에 대한 처리 기간

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

- 가입신청자의 신원확인정보가 일치하지 않은 경우
- 신청서류의 진위여부를 확인할 수 없거나 식별이 어려운 경우

4.3 공동인증서 발급 절차 및 보호 조치

4.3.1 인증서 발급 절차

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

한국전자인증은 공동인증서 발급 시 다음 사항을 확인한 후 공동인증서를 발급합니다.

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

발급된 공동인증서는 발급과 동시에 한국전자인증의 디렉토리에 등재됩니다.

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

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

4.4 공동인증서 수령

가입신청자는 가입자 소프트웨어를 통해 공동인증서와 자신의 전자서명생성정보를 저장할 매체를 선택하고, 공동인증서의 비밀번호를 입력하여 발급받습니다.

4.5 공동인증서 이용

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

4.6 공동인증서 갱신발급

4.6.1 갱신발급 요건, 신청주체 및 신청절차

① 요건

가입자는 기존에 사용하던 공동인증서의 유효기간이 만료되기 60일 전부터 기존 공동인증서의 전자서명키(전자서명생성정보/전자서명검증정보)과 동일한 종류의 새로운 공동인증서 갱신발급을 신청할 수 있습니다. 갱신 발급된 공동인증서는 갱신발급 시점부터 효력이 발생하여 기존 공동인증서 만료시각 이후로부터 1년 또는 공동인증서의 종류에 따라 2년 또는 3년의 유효기간만큼 연장됩니다. 기존 발급된 인증서는 갱신시점에 자동 폐지됩니다.

② 신청주체 및 신청절차

가입자가 정보통신망으로 공동인증서 갱신신청을 하면 한국전자인증은 다음의 검증을 실시함으로써 전자서명생성키가 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

한국전자인증은 공동인증서 갱신신청내역에 포함된 내용을 검증하여 정당한 가입자인 경우 인증서를 갱신합니다. 갱신된 공동인증서는 발급과 동시에 한국전자인증의 디렉토리에 등재됩니다. 갱신 발급된 인증서의 DN은 기존 인증서의 DN을 승계합니다.

4.6.2 가입자가 갱신 발급된 공동인증서를 수령하는 방법

본 인증업무준칙의 4.4를 준용합니다.

4.7 공동인증서 재발급

4.7.1 재발급 요건, 신청주체 및 발급절차

① 요건

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

② 신청주체 및 신청절차

가입자가 한국전자인증 또는 등록대행기관을 방문하거나 대면에 준하는 비대면 방식을 통하여 본 인증업무준칙 3.2.1에 따른 재발급 신청서류를 제출하면 한국전자인증 및 등록대행기관은 신원확인 절차를 수행한 후에 공동인증서를 재발급합니다.

공동인증서가 재발급되면 기존의 공동인증서는 자동적으로 폐지되며 신규로 재발급된 공동인증서의 유효기간은 기존 공동인증서의 최초 발급 시 설정된 유효기간 중 사용기간일수를 공제한 잔여기간으로 설정되며 유효 만료 기일은 변동이 없습니다. 공동인증서 재발급의 발급절차 및 보호조치는 본 인증업무준칙 4.3을 준용합니다.

4.7.2 가입자가 재발급된 공동인증서를 수령하는 방법

본 인증업무준칙 4.4를 준용합니다.

4.8 공동인증서 변경

4.8.1 가입자 정보가 변경된 인증서 발급 요건, 신청주체 및 신청절차

① 요건

가입자가 공동인증서의 상호 변경 등 공동인증서에 포함된 정보변경으로 새로운 공동인증서를 신청해야

할 필요가 있을 경우에 기존의 공동인증서를 폐지하고 새로운 공동인증서를 발급 신청할 수 있습니다.
그 외 가입자 등록정보(주소, 전화번호, 전자우편주소 등) 변경 요청 시에는 가입자의 전자서명에 대한 검증으로 신원확인을 대체하여 한국전자인증에 등록된 해당 정보를 변경할 수 있습니다.

② 신청주체 및 신청절차

가입자가 공동인증서의 상호 변경 등 공동인증서에 포함된 정보 변경의 경우에는 한국전자인증 또는 등록대행기관을 방문하거나 대면에 준하는 비대면 방식을 통하여 본 인증업무준칙 3.2.1에 따른 정보변경 신청서류를 제출하면 한국전자인증 및 등록대행기관은 신원확인 절차를 수행한 후에 새로운 공동인증서를 발급합니다.

새로운 공동인증서가 발급되면 기존의 공동인증서는 자동적으로 폐지되며 새로운 공동인증서의 유효기간은 기존 공동인증서의 최초 발급 시 설정된 유효기간 중 사용기간일수를 공제한 잔여기간으로 설정되며 유효 만료 기일은 변동이 없습니다. 공동인증서 변경 발급절차 및 보호조치는 본 인증업무준칙 4.3을 준용합니다.

4.8.2 가입자가 정보가 변경된 공동인증서를 수령하는 방법

본 인증업무준칙 4.4를 준용합니다.

4.9 공동인증서 효력정지·효력회복·폐지

4.9.1 신청요건, 신청주체 및 신청절차

4.9.1.1 공동인증서 효력정지 요건 및 신청주체

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

4.9.1.2 공동인증서 효력정지 신청절차

① 가입자가 직접 방문하는 경우

한국전자인증 및 등록대행기관을 직접 방문하여 효력정지를 신청할 수 있습니다.

② 가입자가 정보통신망을 이용하여 직접 효력정지 하는 경우

효력정지를 신청하고자 하는 가입자는 정보통신망을 이용하여 "인증서 효력정지"를 선택한 후 가입자가 보유한 전자서명생성정보를 이용하여 전자서명을 하고, 한국전자인증은 전자서명한 정보를 검증하는 과정을 통하여 신원확인 후 효력정지를 합니다.

4.9.1.3 공동인증서 효력회복 요건, 신청주체 및 신청절차

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

가입자가 한국전자인증 또는 등록대행기관을 방문하여 본 인증업무준칙 3.2.1에 따른 효력회복 신청서를 제출하면 한국전자인증 및 등록대행기관은 신원확인 절차를 수행한 후에 가입자의 공동인증서에 대한 효력회복을 시킵니다.

4.9.1.4 공동인증서 폐지 요건 및 신청주체

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

- 가입자 또는 그 대리인이 공동인증서 갱신발급, 재발급, 변경, 폐지를 신청한 경우
- 가입자가 기망 기타 부정한 방법으로 공동인증서를 발급받은 사실을 인지한 경우
- 가입자의 공동인증서가 사고정보를 이용하여 발급된 사실을 인지한 경우
- 가입자의 사망·실종선고 또는 해산사실을 인지한 경우
- 가입자의 전자서명생성정보가 분실훼손 또는 도난·유출된 사실을 인지한 경우
- 본 인증업무준칙 4.9.1.1의 규정에 따라 효력이 정지된 공동인증서에 대한 효력회복신청이 공동인증서의 효력이 정지된 날로부터 6개월 이내에 없는 경우
- 한국전자인증의 전자서명생성정보가 유출된 경우

4.9.1.5 공동인증서 폐지 신청절차

① 가입자가 직접 방문하는 경우

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

② 가입자가 정보통신망을 이용하여 직접 폐지하는 경우

폐지를 신청하고자 하는 가입자는 정보통신망을 이용하여 "인증서 폐지"를 선택한 후 가입자가 보유한 전자서명생성정보를 이용하여 전자서명을 하고, 한국전자인증은 전자서명한 정보를 검증하는 과정을 통하여 신원확인 후 폐지를 합니다.

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

본 인증업무준칙 4.3.2를 준용합니다.

4.9.3 신청접수부터 해당 인증서 효력정지·효력회복 또는 폐지까지 소요되는 처리시간

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

- 가입자의 신원확인정보가 일치하지 않은 경우
- 신청서류의 진위여부를 확인할 수 없거나 식별이 어려운 경우

4.9.4 공동인증서 효력정지 및 폐지목록(CRL) 발행 주기

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

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

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

4.9.6 공동인증서 효력정지 상태 유지 가능 기간

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

4.10 공동인증서 유효성 확인 서비스(OCSP)

4.10.1 공동인증서 유효성 확인 서비스 이용 방법, 이용 조건

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

한국전자인증의 공동인증서 유효성 확인 서비스 신청자 또는 그 대리인은 서비스 가입을 위해 한국전자인증에 공동인증서 유효성 확인 서비스 등록 신청을 하여야 합니다.

한국전자인증의 공동인증서 유효성 확인 서비스 가입자 또는 이용자는 한국전자인증에서 제공 받은 공동인증서 유효성 확인 소프트웨어 또는 자신이 보유한 소프트웨어를 이용하여 공동인증서 유효성 확인을 요청합니다.

한국전자인증의 공동인증서 유효성 확인 서비스는 유료이며, 서비스 이용 수수료, 기타 제공 조건 등 세부사항은 해당 계약 내용에 따릅니다.

4.10.2 공동인증서 유효성 확인 서비스 이용계약 해지

가입자가 공동인증서 유효성 확인 서비스를 해지하고자 하는 경우에는 한국전자인증에 해지 의사를 통보할 수 있으며, 한국전자인증은 계약의 내용에 따라 계약해지를 진행합니다.

4.11 서비스 가입 철회

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

4.12 기타 부가 서비스

4.12.1 시점 확인 서비스

4.12.1.1 이용 방법

한국전자인증은 가입자 또는 이용자에게 시점확인 서비스를 제공할 수 있습니다.

한국전자인증의 시점 확인 서비스 신청자 또는 그 대리인은 서비스 가입을 위해 한국전자인증에 시점 확인 서비스 등록 신청을 하여야 합니다. 등록절차 후 시점 확인용 계정이 포함된 시점 확인 서비스 등록확인서를 신청자 또는 그 대리인에게 교부합니다.

한국전자인증의 시점 확인 서비스 가입자 또는 이용자는 한국전자인증에서 제공받은 시점 확인 소프트웨어 또는 자신이 보유하고 있는 소프트웨어를 이용하여 자신의 시점 확인 계정을 확인 받은 후 해당 데이터에 대한 시점 확인을 요청합니다.

한국전자인증의 시점 확인 서비스는 유료이며, 서비스 이용 수수료, 기타 제공 조건 등 세부사항은 해당 계약 내용에 따릅니다.

4.12.1.2 이용계약 해지

가입자가 시점 확인 서비스를 해지하고자 하는 경우에는 한국전자인증에 해지 의사를 통보할 수 있으며, 한국전자인증은 계약의 내용에 따라 계약해지를 진행합니다.

제5장 시설 및 운영 관리

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

5.1 물리적 보호조치

5.1.1 시설 위치와 구조에 관한 사항

한국전자인증의 핵심인증시스템을 위한 시설의 위치는 아래와 같습니다.

○ 핵심인증시스템 메인센터

- 경기도 수원시 영통구 광교로 145 차세대융합기술연구원 A동 6층

○ 핵심인증시스템 백업센터

- 서울특별시 구로구 디지털로31길 61 드림마크원 4층

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

5.1.2 물리적 보호조치에 관한 사항

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

- 한국전자인증 메인센터는 권한 있는 자만이 출입이 허가됩니다.
- 한국전자인증의 출입통제 시스템은 소지기반/생체기반의 출입통제장치를 다중으로 결합하여 핵심인증시스템 및 통제구역에 대한 접근을 통제합니다.
- 한국전자인증은 특별한 경우(하드웨어 보수 등의 업무수행)를 제외하고는 외부인의 출입을 삼가며 하드웨어 보수 등의 이유로 통제구역 내에 외부인의 출입이 필요할 경우는 반드시 담당관리자가 동행하도록 합니다.
- 한국전자인증은 24시간 출입통제를 감시 및 통제하며 메인센터 내에 출입하는 모든 인원에 대하여 출입내역을 기록하고 매월 1회 출입기록을 백업장치에 저장 및 이를 안전한 장소에 보관합니다.
- 한국전자인증은 24시간 감지가 가능한 보안·감시 장치를 설치 운영하며, 침입감지 및 이상 상황 발생 시 경보 기능을 갖는 감시통제시스템을 설치·운영합니다.
  - 출입구 및 인증센터의 모든 주요 장소에 CCTV 카메라 설치

□ 24시간 감시가 가능한 관제시스템 설치·운영

□ 외부로부터의 불법적인 침입에 대비하여 인증센터 전체를 포함하는 침입감지 장치 설치

❑ 한국전자인증은 인가된 보안경비업체와 계약하여 24시간 보안체제를 운영합니다.

5.1.3 물리적 잠금장치에 관한 사항

한국전자인증은 시스템 보호 및 물리적 접근통제를 위하여 보안캐비닛(잠금장치 렉) 내에 핵심인증시스템을 설치·운영합니다.

5.1.4 화재, 수재, 정전 방지 및 방호에 관한 사항

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

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

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

5.1.5 항온·항습, 통풍 및 기타 보호설비에 관한 사항

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

5.1.6 시설 및 장비의 폐기처리 절차에 관한 사항

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

5.1.7 원격지 백업설비 안전운영에 관한 사항

한국전자인증은 전자서명인증사업자 인증서, 인증서비스를 제공하는데 사용되는 중요한 저장매체, 가입자 공동인증서, 공동인증서 효력정지 및 폐지목록 등을 화재, 홍수로부터 안전하게 보호하기 위하여 매일 1회 백업하여 원격지 저장 설비에 5년간 보관하며 공동인증서 효력정지 및 폐지목록 등은 공동인증서의 효력이 소멸된 날로부터 5년간 보관합니다.
원격지 저장 설비를 보호하기 위하여 다음과 같은 물리적 보호조치를 수행합니다.

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

5.2 절차적 보호조치

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

한국전자인증은 전자서명인증업무의 안정성 및 신뢰성을 확보하기 위해 역할별로 업무를 분리하여 수행합니다.
전자서명인증업무 수행을 위해 필요한 업무의 종류와 그 업무 분장에 관한 사항은 내부문서인 "전자서명인증 업무지침" 과 "전자서명인증서비스 업무분장표"에 따라 수행합니다.

한국전자인증은 내부감사자를 지정하고, 전자서명인증업무 관리체계가 효과적으로 운영되는지를 점검

하기 위한 관리체계 점검기준, 범위, 주기, 점검인력 자격요건 등을 포함한 관리체계 점검을 연 1회 이상 수행합니다. 내부감사자는 법적 요구사항 및 수립된 정책에 따라 전자서명인증업무 관리체계가 독립적이고 효과적으로 운영되는지를 점검하기 위한 내부감사를 실시합니다.

5.2.2 동일인에 의해 동시 수행될 수 없는 전자서명인증업무

한국전자인증은 다음의 업무가 동일인에 의해 동시 수행되지 않도록 하여야 합니다.

- 한국전자인증이 자신의 전자서명키를 생성하는 경우 (3인 이상)
- 한국전자인증이 다음 각호의 시스템을 설치, 운영 및 유지, 보수하는 경우 (2인 이상)
  - 가입자의 등록정보관리 기능을 지원하는 시스템
  - 공동인증서 생성, 발급, 관리 기능을 지원하는 시스템
  - 시점확인 기능을 지원하는 시스템

5.2.3 업무 담당자 현황 및 담당자 인증방법

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

5.3 인적 보안

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

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

5.3.2 업무 수행 인력의 교육 및 업무순환에 관한 사항

한국전자인증은 인증서비스의 안전한 운영을 위하여 인증업무를 각 시스템 및 기능별로 서로 다른 직원이 수행하도록 역할을 내부문서인 "전자서명인증 업무지침" 과 "전자서명인증서비스 업무분장표" 따라 분리하여 수행하고 있으며, 한 직원이 여러 가지 인증업무를 수행할 경우 인증서비스 보안상 문제가 없도

록 업무순환 하고 있습니다.

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

5.3.3 비인가된 행위에 대한 처벌에 관한 사항

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

5.4 감사 기록

5.4.1 감사기록의 유형 및 보존기간

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

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

한국전자인증은 전자서명인증업무 운영과 관련된 기록 및 인증시스템에서 생성되는 기록의 이상유무를 확인하며, 감사기록은 5년간 보관합니다.

5.4.2 감사기록 보호조치 및 감사기록 백업주기 및 절차

각 시스템의 감사기록에 대한 총괄관리는 감사관리자가 수행하며, 시스템의 각 업무관리자는 각자의 업무에 대한 감사기록만을 열람할 수 있습니다.
한국전자인증은 변경된 내역 및 전체 데이터를 매일 1회 백업합니다.

5.5 기록 보존

5.5.1 보존되는 기록의 유형 및 보존기간

한국전자인증은 다음 업무와 관련된 내역을 기록, 보존합니다.

- 가입자의 인증서 발급 및 관리 등 전자서명인증업무
- 한국전자인증 인증시스템 등의 운영 업무

본 조의 기록보존 대상은 당해 공동인증서의 효력이 소멸한 날로부터 5년 동안 보존하는 것을 원칙으로 합니다. 단, 전자서명법(법률 제17354호) 부칙 제5조(공인인증업무 등에 관한 경과조치) 제2항에 의거 전자서명법 개정전 발급된 유효한 공인인증서에 대해서는 유효기간 만료일로부터 10년간 보관합니다.

5.5.2 보존기록의 보호조치

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

5.5.3 보존기록의 백업주기 및 백업절차

한국전자인증은 보존기록에 대해 물리적 및 절차적, 인적 통제가 되고 있는 지정된 백업 장치를 통해 매일 1회 전체 백업을 수행합니다.
또한 천재지변 및 기타 재난 발생시 보존기록의 손실 및 파괴에 대비하여 2벌 백업을 수행하며, 메인 설비 및 원격지 저장설비에 각각 1벌씩 백업 저장합니다.

5.6 전자서명인증사업자의 전자서명생성정보 갱신

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

5.7 장애 및 재난 복구

5.7.1 전자서명인증업무 장애 및 재해 유형별 처리 및 복구 절차

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

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

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

5.7.2 전자서명인증업무 장애방지 등 연속성 보장 대책

한국전자인증은 안정적인 인증서비스 제공에 노력합니다.

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

한국전자인증은 감사기록, 인증서비스 관련 자료, 가입자 공동인증서 등을 매일 1회 백업하여 원격지 저장 설비에 5년 보관합니다.

5.8 업무 휴지, 폐지, 종료

한국전자인증의 사정으로 인하여 인증서비스의 전부 또는 일부를 휴지 또는 폐지하고자 하는 경우에 한

국전자인증은 휴지기간 및 휴지일과 폐지일을 정하고 휴지는 휴지하고자 하는 날 30일 전까지, 폐지는 폐지하고자 하는 날 60일 전까지 법 제15조(전자서명인증업무준칙의 준수 등) 규정에 따라 가입자에게 해당 사실을 통보합니다.

가입자에게 통보하는 방법은 한국전자인증의 홈페이지(https://www.crosscert.com)와 서면, 전자우편, 팩스, 전화 또는 이와 유사한 방법 중 하나 이상의 방법으로 통보합니다. 통보 및 게시하는 내용에는 요금의 반환, 가입자의 개인정보 폐기 등 가입자 보호조치를 포함하여 함께 통보합니다. 요금의 반환은 본 인증업무준칙 9.1.3의 환불 정책에 따라 환불하며, 개인정보 폐지는 관련 법령에 따라 파기합니다.

제6장 기술적 보호 조치

6.1 전자서명생성정보 보호

한국전자인증은 인가된 자만이 전자서명생성정보를 생성할 수 있도록 합니다. 전자서명생성정보 생성 작업은 물리적 침해 등으로부터 보호되는 하드웨어보안장치(HSM)를 사용하고, 다자인증 통제(최소 3명 이상) 하에서 전자서명생성정보를 생성합니다.

한국전자인증은 안전하고 신뢰할 수 있는 인증서비스를 제공하기 위해 HMAC-DRBG 및 RSA2048 알고리즘을 이용하여 전자서명키를 생성합니다. 공동인증서는 SHA256 With RSA 알고리즘으로 서명되며, 전자서명생성정보는 SEED 알고리즘을 이용하여 암호화를 합니다.

6.2 전자서명생성정보 보호 조치

6.2.1 전자서명생성정보의 저장 시 보호조치

한국전자인증은 한국전자인증의 전자서명생성정보를 안전하게 저장하기 위하여 봉인, 접근권한 확인 및 전자서명생성정보 유출, 변경 방지 기능을 갖춘 하드웨어보안장치(HSM)에 저장합니다.

6.2.2 전자서명생성정보의 생성, 이용 시 보호조치

한국전자인증은 한국전자인증의 전자서명생성정보 활성화 작업 시 다자인증 통제(최소 3명 이상)하에서

합니다.

6.2.3 전자서명생성정보의 생성, 이용 후 안전한 삭제 방법

한국전자인증은 한국전자인증의 전자서명생성정보의 생성 및 이용이 종료된 후 다자인증 통제(최소 3명 이상) 하에서 지체 없이 전자서명생성정보를 삭제합니다.

6.2.4 전자서명생성정보 백업 보관 시 보호조치

한국전자인증은 한국전자인증의 전자서명생성정보에 대해 원본 이외에 백업본 2부를 작성하여, 1부는 메인센터의 내화금고에 보관하고 나머지 1부는 백업센터의 내화금고에 보관합니다.

6.3 전자서명생성정보 및 전자서명검증정보의 관리

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

6.4 데이터 보호 조치

한국전자인증은 한국전자인증의 전자서명생성정보를 생성 작업 시 다자인증 통제(최소 3명 이상) 하에서 안전한 하드웨어보안장치(HSM)를 사용하여 생성하며, 해당 전자서명생성정보가 분실, 훼손 또는 도난, 유출되지 않도록 HSM에 안전하게 저장합니다.

6.5 시스템 보안 통제

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

6.6 시스템 운영 관리

한국전자인증은 다음 각호의 시설 및 장비에 대하여 형상관리를 하여야 합니다.

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

6.7 네트워크 보호조치

한국전자인증은 내/외부의 네트워크를 통한 불법적인 침입 및 정보유출을 방지하기 위하여 침입차단시스템을 사용하며 서비스 방해 공격을 방지하고 인증서생성관리시스템, OCSP시스템, 디렉토리 시스템, 시점확인시스템 (이하 "핵심인증시스템"이라 한다) 등 모든 핵심인증시스템 및 인증운영관련시스템에 대한 침입을 탐지하기 위하여 침입탐지 시스템을 설치·운영합니다. 구성된 네트워크 회선은 서로 다른 ISP(Internet Service Provider)로부터 제공되도록 이중화하여 구성하였으며 하나의 네트워크 회선에 문제가 발생할 경우 다른 회선으로 자동 전환되도록 구성합니다.

6.8 시점확인서비스 보호조치

한국전자인증은 본 인증업무준칙 5.1에 따라 시점확인 기능을 제공하는 시스템은 핵심인증시스템실과 별도로 운영실을 분리하는 보호조치를 마련하고 시행하고 있습니다.

제7장 인증서 형식

7.1 공동인증서 형식

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

한국전자인증의 공동인증서 프로파일은 다음 표와 같습니다.

1) 기본필드

	필드명	ASN.1 type	Note	지원여부	비고

#				생성	처리	
1	Version	INTEGER	0x2(버전 3)	m	m	
2	Serial Number	INTEGER	자동할당	m	m	
3	Issuer		X.500, RFC3280 준수 C(Country)는 printableString, 그 이외의 속성값은 utf8String	m	m	
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	
4	Validity		전자서명인증사업자 CPS에 명시된 유효기간 준수	m	m	
	notBefore	UTCTime		m	m	
	notAfter	UTCTime		m	m	
5	Subject		X.500, RFC3280 준수 C(Country)는 printableString 그 이외의 속성값은 utf8String	m	m	
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	
6	Subject Public Key Info			m	m	
	algorithm	OID		m	m	
	subjectPublicKey	BIT STRING		m	m	
7	Extensions	Extensions		m	m	

2) 확장필드

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

	NoticeReference	SEQUENCE			–	–	
	ExplicitText	BMPString	공동인증서 표시규격 준수		m	m	
5	Policy Mappings			–	–	–	
	issuerDomainPolicy	OID					
	subjectDomainPolicy	OID					
6	Subject Alternative Names	otherName	id-kisa-identifyData에 가입자 한글실명과 VID	n	m	m	
		rfc822Name	가입자 이메일 주소		o	m	
7	Issuer Alternative Names	otherName	id-kisa-identifyData에 전자서명인증사업자 한글실명	n	o	m	
8	Extended Key Usage	OID	id-kisa-HSM	n	o	o	
9	Basic Constraints			–	x	x	
	cA	FALSE					
	pathLenConstraint	INTEGER					
10	Policy Constraints			–	–	–	
	requireExplicitPolicy	INTEGER					
	inhibitPolicyMapping	INTEGER					
11	Name Constraints			–	–	–	
12	CRL Distribution Point			n	m	m	[1]
	distributionPoint	DistributionPointName	CRL 획득 정보		m	m	
	reasons	ReasonFlags			–	–	
	cRLIssuer	GeneralNames	간접CRL 발급시 사용		o	m	
13	Authority Information Access			n	m	m	
	accessMethod	OID	id-ad-calssuers, id-ad-ocsp		m	m	
	accessLocation	GeneralName			m	m	
[1]	uri값으로 ldap://hostname[:portnumber]/dn[?attribute] 형식 사용						

공동인증서에 포함된 사항은 다음과 같은 내용을 포함합니다.

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

7.2 공동인증서 유효성 확인 정보 형식

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

한국전자인증의 공동인증서 효력정지 및 폐지목록 프로파일은 다음 표와 같습니다.

1) 기본필드

#	필드명	ASN.1 type	Note	지원여부		비고
				생성	처리	
1	Version	INTEGER	0x1(버전 2)	m	m	
2	Signature	OID	자동할당	m	m	
3	Issuer		X.500, RFC3280 준수 C(Country)는 printableString, 그 이외의 속성값은 utf8String	m	m	
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	
4	This Update	UTCTime	발급시점	m	m	
5	Next Update	UTCTime	전자서명인증사업자 정책에 따름	m	m	
6	Revoked Certificates					[1]
	userCertificate	INTEGER		m	m	
	revocationDate	UTCTime		m	m	
	crlEntryExtensions	Extensions				[2]
7	CRL Extensions	Extensions		m	m	[3]
[1]	효력정지 및 폐지된 공동인증서가 없을 경우는 Revoked Certificates 필드를 생성하지 않음					
[2]	아래 "3) CRL 엔트리 확장필드" 참조					
[3]	아래 "2) CRL 확장필드" 참조					

2) CRL 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier			n	m	m	
	KeyIdentifier	OCTET STRING	전자서명인증사업자 공동인증서의 KeyID				
	authorityCertIssuer	GeneralNames					
	authorityCertSerialNumber	INTEGER					

2	Issuer Alternative Name	otherName	id-kisa-identifyData에 전자서명인증사업자한글실명	n	o	m	
3	CRL Number	INTEGER		n	m	m	
4	Issuing Distribution Point			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 ※ [KCAC.TS.CERTPROF] 참조						
[2]	indirectCRL를 사용할 때는 반드시 "TRUE"로 설정						

3) CRL 엔트리 확장필드

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

7.3 공동인증서 유효성 확인 서비스 형식

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

1) 기본필드

#	필드명	ASN.1 type	Note	지원여부		비고
				생성	처리	
1	Version	INTEGER	0x2(버전 3)	m	m	
2	Serial Number	INTEGER	자동할당	m	m	
3	Issuer		X.500, RFC3280 준수 C(Country)는 printableString, 그 이외의 속성값은 utf8String	m	m	
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	

4	Validity		전자서명인증사업자 CPS에 명시된 유효기간 준수	m	m	
	notBefore	UTCTime		m	m	
	notAfter	UTCTime		m	m	
5	Subject		X.500, RFC3280 준수 C(Country)는 printableString 그 이외의 속성값은 utf8String	m	m	
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	
6	Subject Public Key Info			m	m	
	algorithm	OID		m	m	
	subjectPublicKey	BIT STRING		m	m	
7	Extensions	Extensions		m	m	

2) 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier			n	m	m	
	KeyIdentifier	OCTET STRING	3가지 값을 모두 사용		m	m	
	authorityCertIssuer	GeneralNames			m	m	
	authorityCertSerialNumber	INTEGER			m	m	
2	Subject Key Identifier	OCTET STRING	subjectPublicKey 정보의 160비트 해시값	n	m	m	
3	Key Usage	BIT STRING	Digital Signature, non-Repudiation	c	m	m	
4	Certificate Policy			c			
	policyIdentifier	OID	전자서명인증사업자 공동인증서 정책		m	m	
	policyQualifiers				m	m	
	PolicyQualifierId	OID	CPS, UserNotice		m	m	
	Qualifier				m	m	
	CPSuri	IA5String	전자서명인증사업자 CPS주소		m	m	
	UserNotice				m	m	
	NoticeReference	SEQUENCE			-	-	
	ExplicitText	BMPString	공동인증서 표시규격 준수		m	m	
5	Policy Mappings			-	-	-	
6	Subject Alternative Names	otherName	id-kisa-identifyData에 가입자한글실명	n	m	m	
7	Issuer Alternative Names	otherName	id-kisa-identifyData에 전자서명인증사업자한글실명	n	o	m	
8	Basic Constraints			-	x	x	
9	Policy Constraints			-	-	-	

10	Name Constraints			–	–	–	
11	Extended Key Usage	OID		c	m	m	
12	CRL Distribution Point			n	m	m	
	distributionPoint	DistributionPointName	CRL 획득 정보		m	m	
	reasons	ReasonFlags			o	m	
	cRLIssuer	GeneralNames	간접CRL발급시사용		o	m	
13	Authority Information Access			n	m	m	
	accessMethod	OID	id-ad-caIssuers		m	m	
	accessLocation	GeneralName			m	m	
14	OCSP No Check	OID	id-pkix-ocsp-nocheck	n	o	m	

제8장 감사 및 평가

8.1 감사 및 평가 현황

한국전자인증은 전자서명인증업무 운영기준 준수 사실의 인정을 받기 위해 매년 1회 전자서명법 제10조에 따라 평가기관으로부터 평가를 받으며, 정보통신망법에 따라 방송통신위원회의 본인확인기관 정기점검을 수검합니다.

이와 별도로, 전자서명인증업무의 독립성 및 신뢰성 유지를 위해 업무분장 내 내부감사업무를 수행할 내부감사자를 지정하며, 매년 1회이상 내부감사를 수행합니다.

8.2 평가자의 신원, 자격

평가자의 신원 및 자격은 시행령 제5조(평가기관의 선정기준 및 절차 등)을 따릅니다.
내부감사는 전문 역량을 갖춘 독립된 인력에 의해 수행됩니다.

8.3 평가 대상과 평가자의 관계

평가기관은 법령상 과학기술정보통신부에 의해 인정받은 기관으로 평가자와 평가 대상과는 독립성을 유지합니다.
내부감사는 인증업무 담당 부서와는 독립된 조직의 전문 인력이 수행하며, 이를 통해 인증업무와의 독립성을 엄격히 유지합니다.

8.4 평가 목적 및 내용

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

내부감사자는 인증업무와 정책·법규 준수 여부, 보안통제 운영 실태, 위험관리 체계 등을 점검하고 경영진 또는 정보보호 최고책임자(CISO)에게 보고함으로써 신뢰성과 투명성을 확보합니다.

8.5 부적합 사항에 대한 조치

한국전자인증은 전자서명인증업무 운영기준 준수사실에 대한 인정을 받을 수 있도록 부적합 사항에 대하여 신속히 조치합니다.
내부감사자는 내부감사 결과를 경영진 또는 정보보호 최고책임자(CISO)에게 보고하여, 결함에 대한 신속한 조치를 요구합니다.

8.6 결과 보고

평가기관은 법 제10조(평가기관)에 따라 전자서명인증업무 운영기준 준수사실에 대해 평가를 수행하고, 그 결과를 인정기관에 제출하여야 합니다.
내부감사자는 내부감사 수행 결과를 경영진 또는 정보보호 최고책임자(CISO)에게 보고합니다.

제9장 전자서명인증업무 보증 등 기타사항

9.1 수수료

9.1.1 공동인증서 수수료

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

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

[표1] 공동인증서 수수료

9.1.2 공동인증서비스 수수료

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

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

[표2] 부가서비스 수수료

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

9.1.3 전자인증서비스에 대한 환불 정책

가입자는 공동인증서를 발급가능기간 내에 발급받지 않았을 경우에는 발급가능기간만료일로부터 14일 이내, 인증서를 발급 받았을 경우에는 발급일로부터 7일 이내에 한국전자인증 홈페이지 또는 등록대행기관을 통해 발급 취소 신청 및 수수료 환불을 요청할 수 있습니다. 이 때 공동인증서 발급에 따른 필요경비가

발생하였을 경우에는 해당 비용을 수수료에서 차감하고 환불하며, 가입자의 공동인증서는 폐지합니다.

9.2 배상

9.2.1 전자서명인증서비스 관련 배상 내용

9.2.1.1 한국전자인증의 배상책임

한국전자인증은 법 제20조(손해배상책임)규정에 따라 전자서명인증업무의 수행과 관련하여 가입자 또는 이용자에게 손해를 입힌 경우에는 그 손해를 배상합니다.

한국전자인증은 신뢰할 수 있는 암호화 모듈 및 보안 기술 규격 적용을 원칙으로 합니다. 신뢰할 수 없는 암호화 모듈 또는 기술 규격을 적용하는 경우 한국전자인증은 안정성을 확보하기 위한 기술적 검토 또는 조치를 취하며, 이에 대한 책임을 부담합니다.
한국전자인증은 인증업무 수행과 관련하여 가입자 또는 공동인증서를 신뢰한 이용자에게 입힌 손해를 배상하기 위하여 보험에 가입되어 있습니다.

9.2.1.2 등록대행기관의 배상책임

등록대행기관은 한국전자인증으로부터 위탁 받은 업무를 수행하면서 전자서명관련법, 본 인증업무준칙 및 한국전자인증과 체결한 계약을 위반하여 한국전자인증, 가입자와 이용자에게 손해를 입히면 그 손해를 배상합니다.

9.3 영업비밀

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

9.4 개인정보보호

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

제공된 가입자 정보는 가입자의 동의 및 법에서 정한 경우를 제외하고는 목적 외에 이용되거나 제3자에게 제공될 수 없으며, 이러한 의무 위반시 한국전자인증은 가입자에 대해 손해배상 책임을 집니다.

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

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

한국전자인증은 개인정보보호와 관련하여 별도의 '개인정보처리방침'을 정하여 운영하고 있으며, 자세한 사항은 한국전자인증 홈페이지에서 확인할 수 있습니다.
- 개인정보처리방침 정보저장 위치: https://www.crosscert.com/glca/01_5_05.jsp

9.5 지식재산권

한국전자인증은 지식재산권의 보호와 관련된 법령을 준수합니다.

9.6 보증

본 인증업무준칙에서 정한 사항 외에 기타 보증사항은 없습니다.

9.7 보증 예외 사항

한국전자인증은 전자서명관련법 및 인증업무준칙에서 정한 사항 이외의 사항 즉, 가입자 신용, 가입자 관련 정보의 불변성 등을 보증하지 않습니다.

9.8 보험의 보상 범위

한국전자인증은 전자서명인증업무의 수행과 관련하여 전자서명법 제20조(손해배상책임)에 따라 연간 총 보상한도가 20억원인 보험에 가입하고 있습니다.

9.9 배상 한계

한국전자인증은 전자서명법 제20조(손해배상책임)에 따라 전자서명인증업무 수행과 관련하여 한국전자인증의 고의 또는 과실로 가입자 또는 이용자에게 손해를 입힌 경우에는 그 손해를 배상합니다. 다만, 한국전자인증의 고의 또는 과실 없음을 입증하면 그 배상책임이 면제됩니다.

9.10 준칙의 효력

준칙이 개정되면 개정 전 내용은 개정 준칙의 효력 발생일에 그 효력이 종료됩니다.
제·개정된 준칙은 한국전자인증이 준칙 정보저장위치에 공고하는 날로부터 시행합니다.

9.11 통지 및 의사소통

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

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

9.12 이력 관리

한국전자인증은 전자서명인증업무준칙의 변경 이력을 관리합니다.

9.13 분쟁 해결

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

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

- 전자문서 및 전자거래 기본법 제4조(전자문서의 효력)

9.13.2 분쟁을 해결하는 절차

전자서명인증업무와 관련하여 한국전자인증과 가입자 또는 이용자간 분쟁이 발생한 경우 한국전자인증의 이메일(helpdesk@crosscert.com) 또는 고객센터(1566-0566)을 통해 의사소통을 할 수 있으며, 법 제22조(분쟁의 조정)에 따라 전자문서전자거래분쟁조정위원회에 조정을 신청하여 관련 절차에 따라 신속한 방법으로 분쟁을 해결할 수 있습니다.

9.14 관할 법원

한국전자인증과 가입자 또는 이용자와의 인증업무와 관련한 분쟁이 일어났을 경우에 분쟁의 해결을 위하여 한국전자인증의 본사 소재지를 관할하는 법원을 관할법원으로 합니다.

9.15 관련 법의 준수

본 인증업무준칙은 전자서명법, 전자서명법 시행령, 전자서명법 시행규칙 및 관련 법령을 준수합니다.

9.16 기타 규정

본 인증업무준칙은 대한민국의 관계법령에 따라서 해석되고 적용됩니다.