뱅크사인(BankSign) 공동인증업무준칙

본 공동인증업무준칙은 금융회사가 블록체인 기술을 적용하여 공동으로 제공하는 인증서의 발급, 이용 등에 관한 전반적인 사항과 인증업무 관련 당사자의 의무와 책임 등을 규정하고 있습니다.

금융결제원 인증기획부

준칙 제·개정 이력표

구분	제·개정일	시행일	비고
제정	2018.7.23.	2018.8.27.	은행연합회 준칙 제정
개정	2020.12.31	2020.12.31	금융결제원 준칙 개정

- 목 차 -

1. 개요

1.1. 배경 및 목적

1.1.1. 준칙의 배경 및 목적

사단법인 금융결제원(이하 '결제원'이라 합니다)과 금융회사는 인터넷 등 개방형 정보통신망 환경 하에서 처리되는 전자금융거래의 안전성과 편의성을 제고하기 위해 은행연합회와 국내 은행이 2018년 구축한 블록체인 공동 시스템(이하 "블록체인시스템"이라 합니다)을 인수하여 2021년 1월 1일부터 블록체인 기반의 공동인증서비스(이하 "뱅크사인"이라 합니다)를 운영하고 있습니다.

본 공동인증업무준칙(이하 "준칙"이라 합니다)은 인증서의 발급 및 관리, 운영정책 등 블록체인시스템 운영과 뱅크사인 이용에 관한 전반적인 사항과 이해 당사자의 책임과 의무에 관한 사항 등을 정함을 목적으로 합니다.

1.1.2. 전자서명 인증체계

블록체인시스템과 뱅크사인에 관한 정책의 수립, 시행 및 감독은 블록체인시스템에 참여한 금융회사(이하 '참가기관'이라 합니다.)와 결제원으로 구성된 의결기구에서 관장하고 있으며, 각 참가기관이 인증업무를 수행하고, 결제원은 관리기관 역할을 수행하는 방식으로 전자서명 인증체계는 구성되어 있습니다.

각 참가기관은 동일한 정책과 기술요건으로 인증서를 발급하고, 각 참가기관이 발급한 인증서를 상호인정(Mutual Recognition)하는 인증체계를 구성합니다.

뱅크사인의 이용주체로는 가입자, 참가기관 및 이용기관이 있습니다.

1.1.3. 결제원 소개

결제원은 1910년 설립한 경성수형교환소를 모태로 1986년 6월에 개편하여 발족한 비영리사단법인으로서 자금결제와 정보유통을 원활하게 함으로써 건전한 금융거래의 유지·발전을 도모하고, 금융회사 이용자의 편의를 제고하는 등 금융 산업 발전에 기여할 목적으로 설립되었습니다.

결제원의 뱅크사인업무와 관련된 연락처는 다음과 같습니다.

- 주소 : (135-758) 서울특별시 강남구 테헤란로 202(역삼동 717번지)
- 인터넷 URL : http://www.kftc.or.kr
- 전자우편 : hkoo@kftc.or.kr

- 전화번호 : 02-531-7791

1.1.4. 인증서 정의 및 효력

1.1.4.1. 정의

인증서는 블록체인시스템에 참여한 참가기관이 발급하는 것으로, 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말합니다.

참가기관은 가입자가 인증서 발급 신청 시 참가기관에 등록된 가입자 본인임을 확인한 후 가입자가 제출한 전자서명검증정보와 관련정보에 참가기관의 전자서명생성정보로 전자서명하여 인증서를 발급합니다. 인증서에 기재된 사실은 가입자의 발급신청 당시를 기준으로 하는 것이며, 가입자의 신용, 가입자 관련정보의 불변성 등을 보장하지 않습니다.

아울러, 블록체인시스템에 참여한 참가기관들은 상호 신뢰 가능한 인증체제를 구축하기 위해 참가기관 인증서를 발급하여 블록체인시스템에 게시하고 있습니다.

참가기관 인증서는 가입자의 인증서 발급에 사용하는 참가기관의 전자서명생성정보가 해당 참가기관에 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말합니다.

참가기관은 안전한 절차에 따라 참가기관 인증서를 발급하고, 블록체인시스템에 게시하여 참가기관들이 이를 확인할 수 있도록 합니다. 참가기관 인증서 발급과정에서 생성한 참가기관의 전자서명생성정보는 발급시스템에 보관하지 않습니다.

1.1.4.2. 효력

인증서는 다음에서 정한 사유가 발생하는 경우를 제외하고는 효력을 인정받으며, 다음의 사유가 발생하는 경우에는 해당 인증서의 효력은 소멸되고 블록체인시스템에서도 사용이 정지됩니다.

- 인증서의 유효기간이 경과한 경우
- 인증서가 폐기된 경우

1.1.4.3. 이용범위 및 제한

인증서는 참가기관과 결제원의 전자금융거래 등에 사용할 수 있습니다. 또한, 협약 등을 통해 공공기관, 전자상거래업체 등(이하 “이용기관”이라 합니다)으로도 사용범위가 확대될 수 있습니다.

인증서 사용은 정당한 권한을 가진 가입자가 인증서의 발급용도에 맞게 인증서를 사

용하는 것을 말합니다. 그렇지 않은 경우나 인증업무 관련 보안상의 우려가 있는 경우 참가기관은 기 발급된 인증서의 사용을 제한할 수 있습니다.

1.2. 준칙의 명칭

본 준칙은 뱅크사인(BankSign) 공동인증업무준칙이라 합니다.

1.3. 전자서명 인증체계 관련자

전자서명 인증체계 관련자는 안전하고 신뢰할 수 있는 전자서명 인증서의 발급·이용·관리를 위해 신의·성실로 상호 협조해야 합니다.

1.3.1. 의결기구

블록체인시스템 및 뱅크사인 운영에 관한 정책 수립 등은 참가기관과 결제원으로 구성된 결제원의 총회, 이사회, 위원회 등의 의결기구에서 관장하며, 다음 사항을 심의·의결합니다.

- 블록체인시스템의 구축 및 운영에 관한 정책 수립
- 뱅크사인 운영에 관한 중요 사항
- 예산의 수립 및 분담방법에 관한 사항
- 업무 참가에 대한 승인 및 취소, 시정명령에 관한 사항

이용기관 협약에 관한 사항은 참가기관과 결제원이 협의하거나 결제원의 뱅크사인업무 소관 위원회에서 정할 수 있습니다.

1.3.2. 참가기관

참가기관은 뱅크사인업무 참가기관으로서 다음의 업무를 수행합니다.

- 인증업무의 안전·신뢰성 보장을 위한 준칙 수립 및 준수
- 가입자 신원확인
- 인증서 발급, 폐기 등의 업무
- 인증서 및 폐기정보 등 관련 정보를 블록체인시스템에 게시
- 기타 참가기관으로서 필요하다고 인정되는 업무

1.3.3. 결제원

결제원은 뱅크사인업무 관련 다음의 업무를 수행합니다.

- 블록체인시스템 구축 및 운영 정책 방안에 대한 의결기구 상정
- 뱅크사인 운영 현안에 대한 의결기구 상정
- 참가기관 신청접수, 승인 및 취소, 제재사항에 대한 의결기구 상정
- 인증업무의 안전·신뢰성 보장을 위한 준칙 수립 지원
- 준칙에 따른 참가기관의 시설 및 장비에 대한 기준 수립 지원
- 준칙에 따른 보호조치에 대한 공동심의기준 수립 지원
- 인증서 이용범위 확대 방안 연구 및 대외 협력
- 타업권 블록체인 인증체계 연동을 위한 표준화 협의
- 참가기관 인증서 발급 지원
- 인증업무 관련 콜센터 운영
- 기타 뱅크사인업무와 관련하여 필요한 사항

1.3.4. 가입자

가입자는 참가기관으로부터 인증서를 발급받은 자(발급 신청자 포함)를 말합니다.

1.3.5. 이용기관

이용기관은 참가기관을 제외하고, 전자민원 서비스 등을 제공하기 위해 인증서를 이용하는 기관으로 인증서를 이용하여 가입자의 전자서명생성정보와 전자서명검증정보의 합치 여부를 확인하는 기관을 말합니다.

1.3.6. 참가기관 및 결제원의 의무

1.3.6.1. 정확한 정보 제공

참가기관 및 결제원은 가입자와 이용기관에게 인증서의 신뢰성이나 유효성에 영향을 미칠 수 있는 다음의 정보를 홈페이지 공고 또는 블록체인시스템에 게시하여 그 사실을 확인할 수 있도록 합니다.

- 홈페이지에 공고
  · 준칙
  · 기타 인증업무 관련 중요 정보 등
- 블록체인시스템에 게시
  · 인증서
  · 인증서 폐기 정보

1.3.6.2. 전자서명생성정보의 보호

참가기관은 신뢰할 수 있는 소프트웨어나 하드웨어 등을 이용하여 안전한 방법으로 참가기관의 참가기관 인증서와 전자서명생성정보를 생성합니다. 참가기관은 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리합니다.

참가기관은 공동인증앱을 통해 가입자의 전자서명생성정보를 안전하게 생성해야 합니다. 또한, 암호 알고리즘에 따라 이를 암호화하여 스마트폰등의 안전한 영역에 인증서와 전자서명생성정보를 저장합니다.

1.3.6.3. 전자서명생성정보 사용의 제한

참가기관은 인증업무를 수행함에 있어서 게시한 참가기관 인증서의 전자서명검증정보에 합치하는 전자서명생성정보를 사용합니다.

1.3.6.4. 전자서명생성정보 안전조치

참가기관은 인증기관 전자서명생성정보의 분실·훼손, 도난·유출 등 인증서의 신뢰성이나 유효성에 영향을 미치는 사유가 발생한 사실을 인지하는 경우 가입자에게 이를 통보하며, 필요한 경우 해당 전자서명생성정보로 발급한 가입자의 인증서를 폐기하고 폐기정보를 블록체인시스템에 게시합니다.

1.3.6.5. 신원확인

참가기관은 인증서 발급을 위해 준칙(3.인증업무)에 따라 가입자의 신원을 확인하며, 관련 정보를 요구할 수 있습니다.

1.3.7. 가입자의 의무

1.3.7.1. 정확한 정보제공

가입자는 참가기관이 지정한 절차에 따라 다음 사항에 대해 정확한 정보를 참가기관에 제공해야 합니다. 아울러, 참가기관이 신원확인을 위해 관련 정보를 요청하는 경우 가입자는 성실히 협조해야 합니다.

- 뱅크사인 이용 신청 (또는 인증서 발급 신청)
- 뱅크사인 이용 해지 신청 (또는 인증서 폐기 신청)

1.3.7.2. 인증서의 합목적적 사용

가입자는 정당한 용도 및 제한(제한이 따르는 경우)에 맞게 인증서를 사용해야 합니다. 그리고 인증서를 사용하여 전자서명을 제공할 때에는, 해당 인증서에 포함된 전자

서명검증정보에 합치하는 전자서명생성정보를 사용해야 합니다.

1.3.7.3. 전자서명생성정보의 보호

가입자는 결제원이 제공하는 신뢰할 수 있는 공동인증앱을 이용하여 전자서명생성정보를 생성하며, 생성된 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 보관·관리해야 합니다.

가입자의 전자서명생성정보 보호의무 위반으로 인한 결과의 책임은 전적으로 가입자에게 있습니다.

1.3.7.4. 전자서명생성정보 안전조치

가입자는 전자서명생성정보가 분실·훼손 또는 도난·유출되었거나 안전하지 않다고 인지하는 경우, 지체 없이 공동인증앱을 통해 인증서 폐기요청을 하거나 참가기관에 관련사실을 통보하여 해당 인증서를 폐기할 수 있도록 협조해야 합니다.

1.3.7.5. 참가기관 및 결제원의 면책보장

가입자는 인증서 사용과 공개에 있어 다음의 사유로 인하여 발생되는 모든 책임과 비용에 대해는 참가기관 및 결제원의 면책을 보장합니다. 본 의무는 가입자의 인증서 발급요청을 받은 때부터 시작되며 인증서 만료(폐기 포함)후 5년 동안 지속됩니다.

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

1.3.7.6. 배상책임

가입자는 인증서 사용과 관련하여 가입자의 고의 또는 과실로 참가기관 또는 결제원에 손해를 입힌 경우 참가기관 또는 결제원에게 그 손해를 배상해야 합니다.

1.3.8. 이용기관의 의무

1.3.8.1. 인증서의 사용목적 이해

이용기관은 참가기관이 가입자에게 발급한 인증서의 이용목적 및 이용범위(제한 포함)를 이해해야 합니다. 이용기관의 과실로 인한 손해는 전적으로 이용기관의 책임입니다.

1.3.8.2. 인증서의 유효성 확인

이용기관은 인증서 기재사항 등에 의하여 전자서명의 진위여부를 확인하기 위해 다음의 조치를 취해야 합니다.

- 인증서 유효 여부의 확인
- 인증서 폐기 여부의 확인

1.3.8.3. 배상책임

이용기관은 인증서 사용과 관련하여 이용기관의 고의 또는 과실로 참가기관, 결제원 또는 가입자에게 손해를 입힌 경우 참가기관, 결제원 또는 가입자에게 그 손해를 배상해야 합니다.

1.4. 준칙의 관리

1.4.1. 준칙 관리부서 및 연락처

결제원은 준칙 관리부서 및 연락처를 각각 지정하여 관련 당사자가 알 수 있도록 홈페이지 등에 게시합니다.

1.4.2. 준칙의 제·개정

인증업무의 개선을 위해 준칙의 변경이 필요한 경우 이를 개정할 수 있습니다.

본 준칙의 제·개정권자는 결제원의 뱅크사인업무 담당 부서장입니다.

결제원은 준칙이 제·개정된 경우 다음의 내용을 포함한 준칙의 제·개정 관련 기록을 유지·관리해야 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 공지

참가기관과 결제원은 준칙을 홈페이지 등에 게시하여 관련 당사자가 열람할 수 있도록 하며, 준칙이 개정된 경우에도 개정 준칙을 홈페이지 등에 즉시 공고합니다.

- 준칙 정보저장위치 : http://www.kftc.or.kr

1.4.4. 가입자 동의

가입자가 변경된 준칙이 공고된 후 30일(공고일 포함) 내에 서면(전자문서 포함)으로 이의를 제기하지 아니한 경우 변경된 준칙에 동의한 것으로 봅니다.

1.5. 용어의 정의 및 약어

1.5.1. 용어의 정의

본 준칙을 위해 다음과 같이 용어를 정의합니다.

- “전자문서”라 함은 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말합니다.
- “전자서명”이라 함은 서명자가 해당 전자문서에 서명하였음을 나타내는데 이용하기 위해 해당 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말합니다.
- “전자서명생성정보”라 함은 전자서명을 생성하기 위해 이용하는 전자적 정보를 말합니다.
- “전자서명검증정보”라 함은 전자서명을 검증하기 위해 이용하는 전자적 정보를 말합니다.
- “인증”이라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말합니다.
- “인증서”라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말합니다.
- “인증업무”라 함은 전자서명생성정보의 인증, 인증 관련 기록의 관리 등 전자서명 인증서비스를 제공하는 업무를 말합니다.
- “참가기관”이라 함은 인증업무를 수행하는 기관으로서, 블록체인시스템에 참여한 금융회사를 말합니다.
- “관리기관”이라 함은 블록체인시스템 및 뱅크사인의 정책, 운영, 대외협력 등을 지원하는 기관으로서, 블록체인시스템에 참여한 결제원을 말합니다.
- “이용기관”이라 함은 전자민원 등의 서비스를 제공하기 위해 인증서를 이용하는 기관으로, 참가기관이 아닌 기관이 가입자의 전자서명생성정보와 전자서명검증정보의 합치 여부를 확인하는 자를 말합니다.
- “가입자”라 함은 참가기관으로부터 전자서명생성정보를 인증받은 개인을 말합니다.
- “서명자”라 함은 전자서명생성정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말합니다.
- “인증업무시설”이라 함은 인증업무에 필요한 제반 시설을 말합니다.

- “블록체인 공동 시스템”이라 함은 여러 참가기관이 공동으로 인증업무를 수행하기 위해 블록체인 기반으로 구축한 인증시스템으로 전자서명생성정보의 생성, 인증서의 생성, 인증서의 등록 및 폐기 정보 공유 등의 기능을 합니다.
- “개인정보”라 함은 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함합니다)를 말합니다.
- “참가기관앱”이라 함은 가입자가 스마트폰 등 휴대용 정보처리장치(이하 “스마트폰등”이라 합니다)를 통해 사용자 인증(로그인)과 전자금융거래를 수행하는 앱을 말합니다.
- “공동인증앱”이라 함은 가입자가 스마트폰등을 통해 인증서의 발급 및 폐기, 인증서 비밀번호 설정 등 인증서 관련 사항을 처리하는 앱을 말합니다.
- “연계정보”라 함은 서비스 연계를 위해 본인확인기관(아이핀 발급기관 등)에서 부여하는 개인식별정보를 말합니다.
- “가상식별번호”라 함은 인증서를 이용한 본인확인 시 주민등록번호 또는 외국인등록번호(이하 “주민등록번호등”이라 합니다)를 이용하여 해당 정보의 노출 없이 안전하게 관련 정보를 생성하고 검증하기 위한 값을 말합니다.

1.5.2. 약어

본 준칙에서는 다음의 약어가 사용됩니다.

- DN : Distinguished Name, 식별명칭
- CN : Common Name, 객체이름
- BCID : Blockchain ID, 전자지갑 Address
- CI : Connecting Information, 연계정보
- VID : Virtual ID, 가상식별번호
- RSA : Rivest, Shamir, Adleman, 소인수분해기반의 공개키암호
- ECC : Elliptic Curve Cryptography, 타원곡선암호
- CC : Common Criteria, 공통평가기준

2. 인증서 종류 및 수수료

2.1. 인증서 종류

인증서 종류에는 참가기관 인증서와 가입자용 인증서가 있습니다.

참가기관 인증서는 결제원에서 정한 안전한 절차와 방법을 통해 참가기관이 발급합니다. 참가기관 인증서는 각 참가기관이 1개씩 발급하며, 참가기관 인증서의 유효기간은 발급일로부터 30년입니다.

가입자용 인증서(이하 “인증서”라 합니다)는 참가기관이 개인에게 발급합니다. 인증서는 개인당 1개씩 발급되고, 복사되지 않으며, 재발급 시 기존 인증서는 자동 폐기됩니다. 인증서의 유효기간은 발급일로부터 3년입니다.

2.2. 인증업무 수수료

참가기관은 가입자 또는 이용기관에게 수수료를 부과할 수 있으며, 참가기관의 판단에 따라 수수료를 면제하거나 할인요율을 적용할 수 있습니다.

2.2.1. 인증서 발급 수수료

참가기관은 인증서를 발급할 때 발급 수수료를 부과할 수 있습니다. 단, 개인 가입자에게는 발급 수수료 면제를 원칙으로 합니다.

2.2.2. 인증서 이용 수수료

블록체인시스템에 참가기관 및 관리기관으로 참여한 참가기관과 결제원 상호간에는 인증서 열람, 확인 및 유효성검증 관련 수수료를 부과하지 않습니다.

참가기관은 위 참가기관 및 관리기관 외의 이용기관(공공기관, 전자금융업자 등)에게 인증서 이용 수수료를 부과할 수 있습니다. 수수료에 관한 사항은 자체적으로 정하거나 결제원과 협의 또는 의결기구에서 정하는 바에 따릅니다.

2.2.3. 기타 서비스에 대한 수수료

참가기관은 필요한 경우 기타 서비스에 대한 수수료를 부과할 수 있습니다.

2.3. 환불

참가기관이 인증서 발급 수수료를 부과하는 경우, 가입자가 인증서 발급일로부터 7

일 이내에 발급을 취소하는 경우에 한하여 수수료를 환불합니다. 이 때, 참가기관은 필요 경비를 공제할 수 있습니다. 다만, 참가기관의 귀책사유로 인한 가입자의 환불 요구에 대해서는 7일이 경과한 후에도 환불이 가능합니다.

이용기관에 대한 인증서 이용 수수료는 환불하지 않는 것을 원칙으로 합니다.

3. 인증업무

3.1. 발급 대상 및 제한

3.1.1. 발급 대상

참가기관은 국내에 거주하는 개인(재외국민, 국내거소 외국인 포함)에 대해 인증서를 발급하고 있습니다. 다만, 기술변화 등에 의한 뱅크사인 운영 정책 변경에 따라, 인증서 발급 대상이 확대 또는 제한될 수 있습니다.

3.1.2. 발급 제한

참가기관은 다음 중 어느 하나에 해당하는 경우 인증서 발급을 제한할 수 있습니다.

- 타인의 명의를 도용하여 신청하였거나 그렇다고 의심되는 경우
- 참가기관의 업무상 또는 기술상 문제로 인증서를 발급하지 못하는 경우
- 필수 동의 항목에 동의하지 않은 경우
- 추가인증 등에 실패한 경우

3.2. 인증서 신규 발급

3.2.1. 전제 조건

인증서 발급을 위해 가입자는 다음의 전제조건을 만족해야 합니다.

- 인증서 발급 참가기관[주)]의 계좌 보유
- 인증서 발급 참가기관[주)]의 전자금융거래 가입
- 스마트폰등(Android 4.1. 이상, iOS 8.0 이상) 보유

주) 농협은행의 경우 농업협동조합법상 조합 포함, 수협은행의 경우 수산업협동조합법상 조합 포함

3.2.2. 신규발급 절차

3.2.2.1. 인증서 발급신청

인증서 발급 신청은 스마트폰등의 참가기관앱을 통해 합니다.

참가기관앱은 다음의 절차를 통해 발급을 진행합니다.

- 공동인증앱 설치

– 참가기관앱에서 동의 확인

· (필수) 뱅크사인 공동인증서비스 이용 약관 동의

· (필수) 개인정보 수집 및 이용 동의

· (필수) 개인정보 제3자 제공 동의

– (필수) 휴대폰 본인 확인

– (필수) 계좌비밀번호 입력

– (필수) 보안매체(OTP, 보안카드 등) 입력

– (필수) 인증수단 설정 : (기본)비밀번호, (추가 택1)패턴/지문/추가안함

참가기관은 휴대폰 본인 확인 절차를 통해 가입자 식별을 위한 주민등록번호등을 확인할 수 있어야 하며, 주민등록번호등을 확인할 수 없는 경우에는 주민등록번호등을 직접 입력받는 등 주민등록번호등을 확인할 수 있는 별도의 조치를 취해야 합니다.

참가기관앱은 휴대폰 본인 확인 과정을 통해 가입자를 식별하고 계좌를 화면에 제공(일부 마스킹처리)하여 계좌비밀번호만 입력 받습니다.

참가기관은 신원확인방식의 안전성 및 신뢰성을 제고하기 위해 OTP 등 보안매체 추가인증을 통해 가입자의 신원확인을 강화할 수 있습니다.

3.2.2.2. 참가기관의 발급

참가기관은 인증서를 발급하기 전에 가입자가 휴대폰본인확인 절차를 통해 제공한 연계정보(CI, Connecting Information)를 기반으로 가입자를 식별할 수 있어야 합니다. 가입자를 식별할 수 없는 경우, 가입자로부터 주민등록번호등을 입력받아 처리하고, 이 경우에는 사전에 주민등록번호등의 수집 동의를 받아야 합니다.

참가기관은 가입자의 계좌비밀번호 확인을 통해 가입자의 계좌 보유 여부를 확인한 후 인증서 발급을 시작합니다.

참가기관앱은 인증서 발급에 필요한 사용자 정보를 안전한 방법으로 공동인증앱에 전달하고, 공동인증앱은 전자서명생성정보 및 전자서명검증정보를 생성하고 표준절차에 따라 인증서를 발급합니다.

공동인증앱은 제출된 사용자 정보를 기반으로 다음의 내용을 보장해야 합니다.

– 인증정보 송·수신간 재사용 방지

– 전자서명생성정보와 전자서명검증정보의 합치성 검증

– 개인정보 암호화 후 블록체인시스템에 저장

– 인증서 발급 및 블록체인시스템에 게시

– 참가기관앱에 인증서 발급 결과 전송

인증서는 DN으로 서로 구분되며, DN내 CN은 다중서명방식의 블록체인주소를 사용합니다. 이 주소는 블록체인아이디(BCID)로 블록체인시스템에서 인증서를 획득하거나 인증서 상태검증을 하는 주소로 사용합니다.

3.2.2.3. 가입자의 인증서 수령

가입자는 공동인증앱을 통해 참가기관이 발급한 인증서 정보를 전달받아, 인증서 정보와 자신의 전자서명생성정보를 저장하고, 이를 안전하게 저장·관리 합니다.

3.2.2.4. 가입자 인증서 정보의 전송

가입자의 인증서 정보는 개인정보 제3자 제공 동의에 따라 블록체인시스템을 통해 각 참가기관에 공유되며, 각 참가기관은 블록체인시스템을 통해 공유되는 가입자의 인증서 정보를 블록체인아이디를 통해서 접근할 수 있습니다. 1인당 1인증서 정보, 인증서 상태정보 등은 인증서가 발급되는 시점부터 관리됩니다.

3.3. 타기관 이용

3.3.1. 전제 조건

타기관 이용은 인증서 발급 참가기관이 아닌 참가기관(이하 “이용등록기관”라 합니다)에서 인증서를 사용하는 것을 말합니다. 가입자는 이용등록기관에서 고객확인 절차를 거친 후 기 발급받은 인증서를 이용할 수 있습니다. 고객확인 절차는 이용등록기관의 계좌 보유 여부를 확인하기 위한 절차로서 발급과 동일하게 다음의 전제조건을 만족해야 합니다.

- 인증서 이용등록기관[주)]의 계좌 보유(또는 이용등록기관의 서비스 가입자)
- 인증서 이용등록기관[주)]의 전자금융거래 가입
- 스마트폰등(Android 4.1. 이상, iOS 8.0 이상) 보유

주) 농협은행의 경우 농업협동조합법상 조합 포함, 수협은행의 경우 수산업협동조합법상 조합 포함

3.3.2. 타기관 이용 절차

이용등록기관의 참가기관앱은 다음의 절차를 통해 고객확인을 진행합니다.

- 참가기관앱에서 동의 확인
  · (필수) 공동인증서비스 이용 약관 동의
- (필수) 휴대폰 본인 확인
- (필수) 기 설정한 인증수단으로 로그인(비밀번호, 패턴, 지문 등)

참가기관은 휴대폰 본인 확인 절차를 통해 가입자의 주민등록번호등을 확인할 수 있어야 하며, 확인이 불가능하여 주민등록번호등을 입력받는 참가기관의 경우 사전에 주민등록번호등의 수집 동의를 받아야 합니다.

공공기관 등 참가기관 외 이용기관에 인증서를 등록하고자 하는 경우 국가본인확인기관의 연계정보(CI) 또는 가상식별번호(VID)를 이용한 고객 식별방안을 마련해야 합니다.

3.4. 인증서 폐기

인증서 폐기는 인증서의 유효기간이 경과되어 효력을 정지하거나, 인증서 유효기간 만료 전이라도 가입자의 신청 또는 참가기관 인증업무 수행의 안전성, 보안성, 신뢰성 등을 위한 부득이한 사유로 인해 인증서의 효력을 강제로 종료하는 것을 말합니다.

3.4.1. 폐기 사유

참가기관은 다음의 사유가 발생한 경우 해당 인증서를 폐기합니다.

- 인증서의 유효기간이 경과된 경우
- 가입자가 인증서 폐기를 신청한 경우
- 가입자가 사망한 경우
- 피성년후견인이 성년후견인의 동의 없이 인증서를 발급받은 경우
- 피한정후견인이 한정후견인의 동의가 필요한 법률행위 범위에 인증서 발급이 포함되어 있음에도 불구하고, 한정후견인의 동의 없이 인증서를 발급받은 경우
- 가입자가 부정한 방법으로 인증서를 발급받았거나 그렇다고 의심되는 경우
- 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출된 경우
- 참가기관의 서비스 보안 유지 및 향상을 위해 필요한 경우
- 기타 가입자가 법·규정, 준칙 등에 명시된 주요 의무를 준수하지 않은 경우

3.4.2. 폐기신청과 신원확인

3.4.2.1. 폐기신청 시 처리

인증서 폐기는 본인이 인증서를 소유하고 있는 경우와 스마트폰등의 분실 또는 공동인증앱 삭제 등의 사유로 인증서를 소유하고 있지 않은 경우에 모두 가능합니다. 폐기신청은 인증서를 발급한 참가기관 또는 인증서를 이용했던 참가기관에서 할 수 있으며, 다음과 같이 신청할 수 있습니다.

- 인증서를 소유하고 있는 경우, 참가기관앱을 통해 인증서 폐기신청 후 공동인증앱에서 전자서명하면 즉시 폐기
- 인증서를 소유하지 않은 경우, 참가기관 콜센터를 통해 본인확인 후 폐기

참가기관은 폐기신청이 접수된 경우 이를 즉시 처리하고 그 결과를 블록체인시스템에 게시 합니다.

3.4.2.2. 분실신고 접수 시 처리

참가기관은 인증서 분실신고가 접수된 경우, 참가기관 내부규정에 따라 지체 없이 가입자의 신원을 확인하고 인증서를 폐기 처리한 후 그 결과를 블록체인시스템에 게시 합니다.

3.4.3. 인증서 폐기정보의 갱신과 공고

참가기관은 인증서 폐기 결과를 반영하여 폐기정보를 갱신하고, 갱신 즉시 블록체인시스템에 게시합니다.

3.4.4. 강제 폐기에 따른 공지

참가기관은 “3.4.1 폐기 사유”에 따라 가입자의 동의 없이 인증서를 폐기한 경우 해당 가입자에게 공동인증앱 등을 이용하여 폐기 내용을 통지합니다.

3.5. 인증서 프로파일

참가기관이 발급하는 인증서는 「전자서명 인증서프로파일 기술규격」을 준수하며 다음의 내용을 포함합니다.

– 기본필드

#	필드명	ASN.1타입	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	인증서 발급자 서명 알고리즘 SHA256해시값을 RSA 전자서명	
4	Issuer		m	m	인증서 발급자 DN 예)“CN=전자지갑_ID, OU=Bank_Code, O=banksign,C=KR”	
	type	OID	m	m		
	value	printableString 또는 utf8String	m	m		
5	Validity		m	m	인증서유효기간(3년)	
	notBefore	UTCTime	m	m		
	notAfter	UTCTime	m	m		
6	Subject		m	m	인증서 가입자 DN 예)“CN=전자지갑_ID, OU=Bank_Code, O=banksign,C=KR”	
	type	OID	m	m		
	value	printableString 또는 utf8String	m	m		
7	Subject Public Key Info		m	m	주체키 식별자	
	algorithm	OID	m	m	전자서명인증체계 알고리즘 기술규격 준수	
	subjectPublicKey	BIT STRING	m	m	공개키	
8	Extension	Extensions	m	m		[1]

[1] 아래 “2) 확장필드” 참조

– 확장필드

#	필드명	ASN.1타입	C	지원여부		Note	비고
				생성	처리		
1	Authority Key Identifier	OCTET STRING	n	m	m	발급자 공개키 식별자 CA의 PublicKey 정보의 160비트 해시값	
2	Subject Key Identifier	OCTET STRING	n	m	m	소유자 공개키 식별자 subjectPublicKey 정보의 160비트 해시값	
3	Key Usage	BIT STRING	c	m	m	키 사용 목적 (전자서명, 부인봉쇄)	
4	Certificate Policy		c	m	m	인증서정책	
	policyIdentifier	OID		o	m	인증서정책 OID	[1]
	policyQualifiers			m	m		
	PolicyQualifierId	OID		m	m	CPS, UserNotice	
	Qualifier			m	m		
	CPSuri	IA5String		m	m	준칙의 URI	
	UserNotice			m	m	사용자공지사항	
5	Subject Alternative Names	otherName	n	o	m	인증서 사용자 대체이름(VID)	[2]

[1] 정책은 결제원 OID체계에 따름

[2] 가입자 한글실명 제외

3.6. 인증업무 휴지 및 폐기

3.6.1. 인증업무 휴지

참가기관이 자연재해 또는 천재지변이 아닌 불가피한 사정으로 인증업무의 전부 또는 일부를 휴지하고자 하는 때에는 휴지기간을 정하여 휴지 예정일의 30일 전까지 이를 가입자에게 통보하고 블록체인시스템에 등록된 각 참가기관과 결제원에 통보합니다.

3.6.2. 인증업무 폐지

참가기관이 자연재해 또는 천재지변이 아닌 불가피한 사정으로 인증업무를 폐지하고자 하는 때에는 폐지 예정일의 60일 전까지 이를 가입자에게 통보하고 블록체인시스템에 등록된 각 참가기관과 결제원에 통보합니다.

4. 인증업무 관련정보의 공고

4.1. 공고 설비

참가기관은 인증서 발급 및 관리에 관한 정보와 폐기정보 등의 인증서 상태정보에 관한 공고 설비는 블록체인시스템으로 합니다. 참가기관 및 결제원은 인증업무 시설 및 장비 보호조치 기준에 따라 블록체인시스템을 운영하며, 이를 준수하지 않아 가입자 또는 이용기관에게 손해를 입힌 때에는 그에 따른 책임을 집니다.

4.2. 공고 방법

4.2.1. 주요정보 공고위치

인증서 정보 등 인증업무에 관한 정보는 블록체인시스템을 통해 참가기관 상호간 정보 공유 방식으로 공고합니다.

4.2.2. 공고 빈도

인증서 발급, 관리 및 폐기 등에 관한 정보는 생성 및 변경 즉시 공고합니다.

폐기된 인증서의 공고 누락에 따라 가입자 또는 이용기관에게 손해를 입힌 때에는 그에 따른 책임을 집니다.

5. 인증업무 시설 및 장비 보호조치

5.1. 물리적 보호조치

참가기관 및 결제원은 전자서명생성정보 생성·관리시스템, 인증서 생성·발급·관리시스템 등 블록체인시스템의 보안성 제고를 위해 세부사항을 정합니다.

5.1.1. 블록체인시스템 접근통제

참가기관 및 결제원은 다음의 블록체인시스템을 독립된 보안캐비넷에 설치합니다.

※ 보안캐비넷이란 시건장치가 있는 철제 랙캐비넷을 말함

- 참가기관 전자서명생성정보 관리, 인증서 생성·발급 기능을 제공하는 시스템은 동일 보안캐비넷에 설치할 수 있으나 다른 시스템과는 별도 보안캐비넷으로 분리
- 인증서 상태확인 기능을 제공하는 시스템은 동일 블록체인시스템 보안캐비넷에 설치할 수 있으나 다른 설비와는 별도 보안캐비넷으로 분리

5.1.2. 물리적 접근통제

참가기관 및 결제원은 외부인의 침입이나 불법적 접근 또는 화재 등의 물리적 위협으로부터 블록체인시스템이 설치된 장소를 다음과 같이 안전하게 보호합니다.

- 참가기관 및 결제원의 블록체인시스템은 통제구역 내에 설치·운영
- 참가기관 및 결제원의 출입통제시스템은 신원확인카드, 지문인식 등을 이용하여 통제구역에 대한 접근을 통제
- 참가기관 및 결제원은 하드웨어 보수 등의 업무수행을 위해 외부인이 블록체인시스템 보안캐비넷 등에 접근할 때에는 반드시 담당관리자가 동행
- 참가기관 및 결제원은 출입통제시스템과 연계하여 통제구역 출입내역을 기록하고 정기적으로 그 기록을 검토
- 참가기관 및 결제원은 다음의 감시통제시스템을 설치하며 이상상황 발생 시 경보 및 인접시설간 유·무선 연락기능을 확보
  - · CCTV 카메라 및 모니터링시스템
  - · 침입감지시스템

※ 침입감지시스템이 없는 경우, 건물 출입구는 경비원에 의하여 통제하고 출입통제 보안대책을 수립·운용할 것

5.1.3. 수해 방지

참가기관 및 결제원은 침수로부터 블록체인시스템을 안전하게 보호하기 위해 바닥으

로부터 최소 30cm이상의 위치에 설치하며 누수의 감지 및 신속한 대처를 위해 누수경보기를 이용합니다.

5.1.4. 화재 예방

참가기관 및 결제원은 화재로부터 블록체인시스템을 안전하게 보호하기 위해 화재탐지기, 휴대용소화기, 자동소화설비 등을 설치합니다.

5.1.5. 전원

참가기관 및 결제원은 갑작스러운 정전으로 블록체인시스템의 심각한 피해를 방지하기 위해 무정전 전원공급장치를 이용하고, 별도의 자가발전기를 설치하여 안정적으로 전원을 공급합니다.

5.1.6. 방호

참가기관 및 결제원은 인증업무의 안정적 제공을 위해 외부 침입으로부터 블록체인시스템을 보호할 수 있도록 설치장소를 다음과 같이 설계·운영합니다.

- 블록체인시스템이 설치된 장소 외벽 재질은 벽돌 또는 철근 콘크리트로 축조되어 있거나, 철골구조물에 3T 이상의 철판으로 용접(선택)
- 블록체인시스템이 설치된 장소 외벽은 천장, 바닥까지 완벽하게 마감(선택)
- 블록체인시스템이 설치된 장소에 창문이 있는 경우 강화유리 또는 강화필름으로 코팅한 유리를 사용(선택)

5.1.7. 항온항습, 통풍

블록체인시스템이 설치된 장소 및 블록체인시스템 보안캐비넷은 적정용량의 항온항습장치를 설치 운영하며, 통풍창은 사람이 통과할 수 있을 경우 차폐막을 설치합니다.

5.1.8. 기타 보호설비

블록체인시스템이 설치된 장소에 대한 물리적인 침입을 감지하고 이를 경보하여 주는 장치를 다음과 같이 설치·운영합니다.

- 침입감지장치에 이상이 생겼을 경우 이를 감지하는 기능
- 침입감지장치가 침입을 감지하였을 경우 관리자에게 즉각 알리는 기능

※ 침입감지시스템이 없는 경우, 경비원에 의하여 통제하고 출입통제 보안대책을 수립·운영할 것

5.1.9. 매체 저장

참가기관 및 결제원은 다음의 주요 매체를 접근이 제한된 장소의 내화금고에 보관하여 물리적으로 접근을 통제합니다.

- 참가기관 : 참가기관 전자서명생성정보 및 인증서를 담은 휴대용 저장매체
- 결제원 : 참가기관 전자서명생성정보 및 인증서 발급장비

5.1.10. 시설 및 장비의 폐기 처리

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

5.1.11. 원격지 백업설비 안전 운영

참가기관 및 결제원은 인증서 등 중요정보 보관을 위해 10km 이상 떨어진 곳에 원격지 백업설비를 운영하며, 출입통제시스템, 침입감지장치 등 보호설비를 구축·운영합니다.

5.2. 절차적 보호조치

5.2.1. 인증업무에 대한 업무 분장

참가기관 및 결제원은 인증업무의 안전성과 신뢰성을 확보하기 위해 소속직원으로 인증업무 수행인력을 역할별로 분리하여 운용하며, 해당 인력은 “5.4.1 인증업무 인력의 자격, 경력 등 요구사항”에서 정한 자격 및 경력을 갖추어야 합니다.

- 참가기관 및 결제원은 모든 보호조치를 계획, 감독, 통제하는 관리책임자를 지정
- 참가기관 및 결제원은 모든 보호조치의 실행을 담당하는 보안관리자를 지정
- 참가기관 및 결제원은 주요시설의 유지·관리를 위해 블록체인시스템 관리, 네트워크 관리 등을 담당하는 전문인력(관련분야 2년 이상 경력자)인 보안실무자를 확보
- 참가기관 및 결제원은 블록체인시스템의 설치운영 및 유지보수에 복수의 직원을 배치하여 공동으로 업무를 수행
- 참가기관 및 결제원은 인증서 생성·발급·관리 기능을 지원하는 블록체인시스템의 설치 운영 및 유지보수에 복수의 직원을 배치하여 공동으로 업무를 수행

5.2.2. 인증업무 담당자 인증 방법

참가기관 및 결제원의 인증업무 담당자는 신원확인카드, 지문인식 등으로 보호되는 통제구역을 통과한 후에 방화벽 및 서버보안 소프트웨어로 보호되는 시스템을 관리할

수 있습니다.

5.2.3. 동일인에 의해 동시 수행될 수 없는 인증업무

참가기관 및 결제원은 인증업무 운영시의 신뢰성 및 보안성 확보를 위해 다음과 같이 업무분리 원칙을 준수합니다.

- 참가기관 전자서명생성정보 및 인증서 생성 업무는 복수의 직원이 공동으로 수행
- 참가기관 인증서 발급 및 관리 업무는 복수의 직원이 공동으로 수행
- 동일 시스템에 대한 운영 및 감사업무는 동일하지 않은 자가 각각 수행

5.3. 기술적 보호조치

5.3.1. 전자서명정보 생성

- 참가기관 및 결제원은 인가된 자만이 참가기관 전자서명정보를 생성할 수 있도록 합니다.
- 참가기관 및 결제원은 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되는 안전한 키 생성시스템에서 전자서명정보를 생성합니다.
- 참가기관 및 결제원은 생성된 전자서명정보를 해당 참가기관에 안전한 방법으로 전달합니다.
- 참가기관은 전자서명정보를 안전한 방법으로 블록체인시스템에 주입합니다.

5.3.2. 전자서명정보의 크기 및 해시값

참가기관 및 결제원은 안전하고 신뢰할 수 있는 전자서명 알고리즘을 사용하기 위해 다음 크기의 정보 및 해시값을 이용합니다.

- RSA의 경우 : 참가기관 4096 비트 이상, 개인용 2048 비트 이상
- ECC의 경우 : P256 비트 이상
- SHA-256 경우 : 256 비트 이상

※ 근거 : NIST SP 800-57, Recommendation for Key Management Part I : General (revision 4), 2016.1
암호알고리즘 및 키길이이용안내서, KISA

5.3.3. 전자서명생성정보 저장장치

참가기관 및 결제원은 참가기관의 전자서명생성정보를 안전하게 저장하기 위해 다음 중 한 가지 방법으로 이중 암호화하여 저장합니다.

- 전자서명생성정보를 블록체인시스템 서버의 하드웨어 정보에서 유도된 키로 이중 암호화하여 저장
- 봉인, 접근권한 확인 및 전자서명생성정보 유출·변경 방지 기능을 갖춘 별도의 저장장치에 이중 암호화하여 저장(선택)

5.3.4. 전자서명생성정보 생성·사용 후 안전한 삭제 방법

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

5.3.5. 전자서명생성정보 파기 방법

참가기관은 참가기관 인증서의 유효기간이 만료되거나 전자서명생성정보가 훼손·유출되었을 경우 해당 전자서명생성정보의 저장매체를 물리적으로 완전히 파기합니다.

5.3.6. 전자서명생성정보 사용기간

참가기관 및 가입자의 전자서명생성정보는 해당 인증서가 유효한 기간 동안 사용할 수 있습니다.

5.3.7. 블록체인시스템 구성 및 관리 등 시스템 보호에 관한 사항

- 참가기관 및 결제원은 주센터의 블록체인시스템을 이중화로 구성·운영하며, 백업센터를 운영합니다.
- 참가기관 및 결제원은 인증업무와 관련된 주요 프로그램 또는 프로세스의 동작여부를 점검할 수 있는 시스템을 설치 운영합니다.
- 참가기관 및 결제원은 루트관리자의 권한을 제한할 수 있는 소프트웨어를 설치합니다.
- 참가기관 및 결제원은 블록체인시스템의 운영에 필요한 프로그램만을 설치합니다.
- 참가기관 및 결제원은 블록체인시스템의 운영체제에서 불필요한 사항은 삭제합니다.
- 참가기관 및 결제원은 블록체인시스템 운영체제의 문제점 해결을 위한 최신의 패치를 설치하여 운영합니다.
- 참가기관 및 결제원은 블록체인시스템을 잠금장치가 장착된 보안캐비넷에 보관하고, 잠금장치의 열쇠는 별도의 보관함을 마련하여 관리합니다.
- 참가기관 및 결제원은 블록체인시스템에 대한 논리적인 접근통제를 설정합니다.
- 참가기관 및 결제원은 블록체인시스템의 추가·폐기·변경(운영체제의 변경, 패치

등)에 관한 사항을 관리대장에 기록하고 유지합니다.

- 참가기관 및 결제원은 블록체인시스템의 추가·폐기·변경에 관한 사항을 내부 지침에 의거 관리합니다.
- 참가기관 및 결제원은 서비스 방해공격을 방지하기 위해 침입탐지시스템을 사용합니다.
- 참가기관 및 결제원은 네트워크 보안을 위해 국내·외 CC(국제 공통평가기준)인증을 획득한 침입차단시스템을 사용합니다.(선택)

5.3.8. 인증 S/W 형상관리 등 운영관리에 관한 사항

결제원은 인증 S/W의 형상관리 등 블록체인시스템의 운영에 대한 형상관리를 하고, 참가기관은 최신 버전의 S/W(솔루션 등)로 운영합니다.

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

5.3.9. 네트워크의 구성 및 운영 등 네트워크 보호에 관한 사항

- 참가기관 및 결제원은 주센터 블록체인시스템의 인증 네트워크를 이중화하여 구성하여 장애에 대비하고, 침입차단 및 침입탐지시스템을 사용하여 네트워크를 보호합니다.
- 참가기관 및 결제원은 침입차단 및 침입탐지시스템을 참가기관 내부 보안 규정에 따라 설치합니다.
- 결제원은 네트워크회선을 인증업무 제공을 위해 별도의 회선을 사용합니다.
- 참가기관 및 결제원은 침입차단 및 침입탐지시스템에 해당 기능의 소프트웨어만 설치합니다.
- 참가기관 및 결제원은 침입탐지시스템의 데이터베이스를 주기적으로 갱신하고, 네트워크관리시스템을 이용하여 블록체인시스템을 지속적으로 모니터링합니다.
- 참가기관 및 결제원은 로그 기록을 주기적으로 분석하여 침입시도, 네트워크 부하 등을 파악하고 이에 적절하게 대처합니다.
- 참가기관 및 결제원은 침입차단 및 침입탐지시스템에 대한 논리적인 접근통제를 설정합니다.
- 참가기관 및 결제원은 침입차단 및 침입탐지시스템에 대한 추가·폐기·변경에 관한 사항을 관리대장에 기록하고 유지합니다.
- 참가기관 및 결제원은 침입차단 및 침입탐지시스템의 추가·폐기·변경에 관한 사항

을 내부지침에 의거 관리합니다.

5.4. 인적 보안

참가기관 및 결제원은 블록체인시스템 운영인력의 자격과 자질을 주기적으로 조사하고 동 사항의 유지여부를 지속적으로 관리합니다.

5.4.1. 인증업무 인력의 자격, 경력 등 요구사항

참가기관 및 결제원은 인증업무에 필요한 시설 및 장비의 운영인력으로서 다음의 요건 중 하나 이상을 갖춘 자를 2인 이상 확보합니다.

- 정보통신기사, 정보처리기사 또는 전자계산기조직응용기사 이상의 국가기술자격 또는 이와 동등 이상의 자격을 갖출 것
- 정보보호 분야에서 2년 이상 근무한 경력이 있을 것
- 인증업무에 관한 시설 및 장비의 운영, 비상복구대책 및 침해사고의 대응 분야에서 2년 이상 근무한 경력이 있을 것

5.4.2. 인증업무 교육, 업무순환에 관한 사항

- 참가기관 및 결제원은 보호조치에 대해 소속직원이 관련 내용을 숙지할 수 있도록 내부교육 등의 필요한 조치를 취합니다.
- 참가기관 및 결제원은 보안관리자 및 보안실무자, 블록체인시스템을 관리하는 직원이 연 1회 이상 정보보호관련 내부 또는 외부교육을 이수하도록 합니다.
- 참가기관 및 결제원은 블록체인시스템을 관리하는 직원에 대해 업무상 지득한 기밀사항의 준수에 관한 서약서를 작성하여 날인하도록 합니다.
- 참가기관 및 결제원은 업무환경의 변화 등으로 인하여 보호조치의 수정·보완이 필요한 경우, 이를 지체 없이 보완합니다.
- 참가기관 및 결제원은 블록체인시스템을 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

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

5.5. 감사 기록

5.5.1. 감사기록의 유형 및 보존기간

참가기관 및 결제원은 블록체인시스템에서 발생한 다음의 사건에 대한 세부내역을 감사기록으로 저장하고 2년간 보존합니다.

- 가입자의 인증서 발급 및 폐기 (로그 기록)
- 참가기관의 전자서명생성정보 생성 (로그 기록)

감사기록에 대한 세부내역은 사건번호, 사건발생일시, 사건내용, 처리결과 등입니다.

※ 감사기록은 위변조가 불가능하도록 해야 하며 삭제여부를 탐지할 수 있어야 함

5.5.2. 감사기록 보호조치

감사기록은 블록체인시스템에서 자체 관리·보호됩니다.

참가기관 및 결제원의 감사관리자는 블록체인시스템의 감사기록을 총괄하여 조회·관리하고, 각 업무관리자는 각자의 업무에 대한 감사기록만을 열람할 수 있습니다.

5.5.3. 감사기록 백업주기 및 절차

참가기관 및 결제원은 감사기록을 블록체인시스템의 백업정책에 따라 저장매체에 보관합니다.

5.6. 기록 보관

5.6.1. 기록의 유형 및 보관기간

참가기관 및 결제원은 다음의 정보를 기록으로 관리합니다. 기록의 보관기간은 보존기간(2년)을 포함한 5년으로 합니다.

- 5.5.1에 명시된 감사기록

※ 현재 활용되어지고 있는 인증업무에 관한기록을 '보존기록'이라 하며, 보존기간이 지난 기록을 '보관기록'이라 함

※ 운영로그(접속 로그, AP 로그 등)는 참가기관의 관리 정책 절차에 따라 관리함

5.6.2. 기록의 보호조치

참가기관 및 결제원은 보존기록의 위·변조 및 훼손 등을 방지하기 위해 주기적으로 백업하고 관리합니다.

참가기관 및 결제원은 “5.6.1”의 기록을 인증업무를 수행하는 시설과 해당 시설로부

터 10km이상의 원격지 저장설비에 각 1부씩 보관합니다.

5.6.3. 기록의 백업주기 및 백업절차

참가기관 및 결제원은 정해진 정책(백업주기 및 절차)에 따라 블록체인시스템 관련 기록의 백업업무를 수행합니다.

5.7. 장애 및 재해복구

참가기관 및 결제원은 블록체인시스템 장애, 전자서명 생성정보 유출 등에 따른 인증업무의 중단 또는 그와 동등한 사고와 지진·홍수·화재 등 재해에 대비하여 신속한 대응 및 복구체제를 구축하고 있습니다.

5.7.1. 인증업무 장애 및 재해 유형별 신고·복구

참가기관 및 결제원은 「비상대응 실무 매뉴얼」에 의하여 장애 및 재해 유형별로 유관 기관에 신고합니다.

5.7.2. 인증업무 장애 유형

다음의 장애 유형은 “주의”의 비상상황 등급으로 분류합니다.

- 해킹 등 침해사고에 의한 일부 가입자 전자서명생성정보 유출
- 블록체인시스템의 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
- 인증서 발급서비스 장애

다음의 장애 유형은 “심각”의 비상상황 등급으로 분류합니다.

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

구분	주의	경계	심각
장애·재해	· 블록체인시스템 장애, 오작동	· 발급서비스 장애	· 발급서비스 정지
침해	· 일부 가입자 전자서명생성정보 유출 · 웜·바이러스, Dos 공격	· 전자서명생성정보(백업 포함) 손상 · 대량의 가입자 전자서명생성정보 유출	· 인증서 발급에 사용하는 전자서명생성정보 유출 · 가입자 전자서명생성정보가 대량 유출되어 부정 사용되는 사고 발생

5.7.3. 인증업무 장애 처리절차

참가기관 및 결제원은 “주의”, “경계”, “심각” 등급의 비상상황의 경우 내부규정에 따라 자체 비상대응조치를 취합니다.

5.7.4. 인증업무 장애 유형별 복구

- 웜·바이러스, Dos 공격 등으로 인한 장애의 경우, 관련 침입차단시스템을 이용하여 해당 IP 및 포트를 차단하고, 침입탐지시스템을 통한 모니터링 강화조치를 취합니다.
- 해킹으로 인한 인증서 유출의 경우, 유출된 인증서를 폐기하고 가입자에게 통보합니다.
- 웜·바이러스, Dos 공격 및 해킹 등에 대비하여 방화벽, 침입탐지시스템, 보안S/W 및 S/W의 최신패치로 방어하며, 피해 발생 시 백업데이터로 복구합니다.
- 블록체인시스템을 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.

5.7.5. 인증업무 장애방지 등 연속성 보장 대책

- 참가기관 및 결제원은 블록체인시스템을 이중화하여 무정지 운영체제를 구축하고 백업센터를 운영하여 장애의 방지에 최선의 노력을 다합니다.
- 참가기관 및 결제원은 인증서 등의 주요 데이터의 훼손·멸실이 발생하였을 경우, 백업된 자료를 이용하여 신속히 복구하여 서비스의 연속성을 보장합니다.
- 참가기관 및 결제원은 연중 무휴로 인증업무를 제공합니다.

6. 인증업무 보증 등 기타사항

6.1. 보증

6.1.1. 보증 책임

참가기관은 참가기관이 발급한 인증서와 관련하여 다음의 내용을 보증합니다.

- 인증서 내에 포함된 내용은 발급신청 당시를 기준으로 참가기관에 등록된 사실임
- 인증서는 준칙을 준수하며, 준칙에 따라 발급됨
- 폐기정보 내용의 정확함

6.1.2. 보증 제한

참가기관은 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

참가기관은 발급한 인증서 및 인증업무와 관련하여 가입자 또는 인증서를 신뢰한 이용기관에게 손해를 입힌 경우 전자금융거래법령 및 준칙 등에 따라 그 손해를 배상합니다.

6.2.2. 책임 제한

참가기관은 발급한 인증서 및 인증업무와 관련하여 발생하는 배상책임 이외의 것에 대해서는 책임을 지지 않습니다. 또한, 참가기관은 관련 손해에 대해 참가기관의 과실 없음을 입증한 경우에는 그 배상책임이 면제됩니다.

6.2.3. 배상 한도

참가기관은 인증서로 인해 발생되는 손해에 대해 인증서별로 연간 배상 한도 내에서 배상합니다. 연간 배상 한도는 전자금융감독규정 제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준)에서 정한 금액으로 합니다.

인증서로 인해 발생되는 손해배상액은 민법 제398조(배상액의 예정)에 따라 위 배상한도를 초과하지 않습니다.

6.3. 분쟁 해결

6.3.1. 준거법

본 준칙은 대한민국의 관계법령에 따라 해석되고 적용됩니다.

6.3.2. 재판 관할

인증업무 관련 분쟁이 발생할 경우 그 관할기관은 참가기관 본사 소재지를 관할하는 지방법원이 됩니다.

6.3.3. 분쟁을 해결하는 절차

인증업무와 관련하여 참가기관과 가입자 또는 참가기관간 분쟁이 발생한 경우, 참가기관은 관련법령의 절차에 따라 신속한 방법으로 분쟁을 해결할 수 있습니다. 이 경우 참가기관은 관련 당사자의 서면요청에 의해 관련 자료를 제공할 수 있습니다.

6.3.4. 전자서명인증체계 관련자에게 전달되는 전자문서가 법적효력을 갖기 위한 요건

전자서명인증체계 관련자에게 전달되는 전자문서가 법적효력을 갖기 위해서는 다음과 같은 요건을 만족해야 합니다.

- 인증서에 기초한 전자서명을 포함하며, 전자서명에 사용된 인증서가 유효한 상태이며, 폐기상태가 아닐 것

6.4. 개인정보보호

6.4.1. 인증업무 관련 정보의 보호범위 및 책임

참가기관은 인증업무 수행과정에서 얻게 되는 다음의 자료를 안전하게 보호해야 합니다. 그러나, 참가기관은 제3자가 법률에서 정한 요건 및 절차에 따라 정보공개를 요구하는 경우 이를 따를 수 있습니다.

- 가입자의 개인정보(본인의 동의가 있거나 공개된 내용은 제외)
- 인증업무 관련 전문 기록과 전문에 대한 로그
- 참가기관에서 생성 또는 보관하는 인증업무 관련 감사자료
- 재해복구대책

- 참가기관 인증업무 운영 관련 보안조치

6.4.2. 개인정보보호를 위한 조치

참가기관은 개인정보 접근·관리에 필요한 최소인원으로 사용자를 지정한 후 비밀번호를 통해 개인정보를 철저히 관리해야 하며, 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 다음과 같은 조치를 취해야 합니다.

- 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

참가기관은 인증서 발급 및 관리, 인증서비스 관련 각종 공고 및 통보, 본인확인용 VID생성, 인증서 중복발급 방지, PC인터넷뱅킹 이용 등의 목적을 위해 다음과 같이 최소한의 개인정보를 수집하고 있습니다.

- 수집하는 고유식별정보 : 주민등록번호(또는 외국인등록번호)
- 수집하는 개인정보 : 스마트폰등 식별정보(Android ID, Device ID, Random UUID), 휴대전화번호

6.4.4. 개인정보보호에 대한 처리방침

참가기관의 개인정보보호에 관한 사항은 개인정보처리방침을 수립하여 시행하고 있으며, 동 내용은 참가기관 홈페이지에서 확인하실 수 있습니다.

6.5. 보안성 심의 및 점검 등

6.5.1. 시설 및 장비에 대한 보안성 심의

참가기관은 의결기구에서 정한 일정 수준 이상의 시설 및 장비를 구비하고, 전자금융감독규정 및 참가기관 자체보안성심의 기준 등에 따라 시설 및 장비에 대한 자체 심의를 실시한 후 인증업무를 수행하고 있습니다.

참가기관은 인증업무 수행을 위한 시설 및 장비의 변경이 필요한 경우 이를 결제원과 협의하여 의결기구에 상정하고, 변경 내용의 적정성 등에 대해 의결기구의 의결을 거쳐 인증업무에 적용합니다. 단, 침해사고, 자연재해, 시스템 오류 등으로 인하여 긴급한 조치가 필요한 경우에는 변경 내용을 미리 적용할 수 있으며 적용 후 사후보고를

통해 확정합니다.

6.5.2. 정기점검

참가기관은 인증업무 수행을 위한 시설 및 장비의 안전운영 여부, 개인정보 관리 현황 등을 매년 정기적으로 점검하고 그 결과를 결제원에 통지합니다.

점검은 다음과 같은 사항에 대해 이루어집니다.

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

6.6. 관련 법·제도의 준수

인증업무 관련자가 준수해야 하는 법률규정 등은 다음과 같습니다.

- 전자금융거래법
- 전자금융거래법 시행령
- 전자금융감독규정

다음 사항에 대한 지식재산권은 저작권법 등 관련 법령에 따라 참가기관 및 결제원에 귀속됩니다.

- 참가기관 및 결제원이 공동 개발한 소프트웨어 및 하드웨어
- 인증업무 명칭(뱅크사인(Banksign) 공동인증서비스)
- 준칙

6.7. 준칙의 효력

준칙이 개정되면 개정전 내용은 개정 준칙의 효력발생일에 그 효력이 상실됩니다.

본 준칙은 2021년 1월 1일부터 효력이 발생하며, 이전 준칙은 2018년 8월 27일부터 효력이 발생하여 2020년 12월 31일 부로 효력이 종료합니다.