KB국민인증서 인증업무준칙
Version 1.0.11

2021. 7. 9 제정 2021. 8.19 개정 2021. 9. 8 개정 2021. 10. 1 개정 2021. 10. 8 개정 2021. 11. 1 개정 2021. 12. 1 개정 2022. 4. 22 개정 2022. 5. 20 개정 2022. 12. 8 개정 2023. 12. 29 개정 2024. 1. 24 개정

목 차

1. 소 개
2. 전자서명인증업무 관련 정보의 공고
3. 신원확인
4. 인증서 관리
5. 시설 및 운영관리
6. 기술적 보호조치
7. 인증서 형식
8. 감사 및 평가
9. 전자서명인증업무 보증 등 기타사항

부록 A. 프로파일

부록 B. 개정이력

KB국민은행

1. 소 개

1.1 개 요

1.1.1 배경 및 목적

KB국민인증서 인증업무준칙(CPS: Certification Practice Statement)은 전자서명법 및 동법 시행령, 동법 시행규칙에 의하여 주식회사 국민은행(이하 “국민은행”)이 KB국민인증서(이하 "인증서")의 발급, 관리 및 인증시스템을 운영함에 있어서 필요한 사항을 정하고, 국민은행과 가입자 등 인증 관련 당사자의 책임과 의무사항 규정을 목적으로 합니다.

1.1.2 전자서명인증체계

국민은행은 전자서명인증체계의 안전·신뢰성 있는 운영정책의 수립 및 시행기관으로서 최상위인증기관(ROOT CA), 인증기관(CA)으로 전자서명인증체계를 구성하여 관리합니다.

1. 국민은행 최상위 인증기관(KB ROOT CA)
   - 안전한 전자서명 인증관리체계 구축 및 운영
   - 전자서명 인증기술의 개발 및 보급
   - 인증기관(CA) 검사 및 안전한 운영지원
   - 인증기관 전자서명생성정보에 대한 인증 등 인증업무 수행
   - 오프라인으로 관리 운영

2. 국민은행 인증기관(KB CA)
   - 가입자의 신원 확인
   - 가입자 인증서 발급, 재발급, 폐지 업무
   - 인증서 유효성 확인 업무
   - 기타 인증기관으로서 수행해야 할 업무

1.2 문서의 명칭

본 문서의 명칭은 「KB국민인증서 인증업무준칙」(이하 “인증업무준칙”이라 한다)으로 전자서명법, 동법 시행령, 동법 시행규칙을 준수합니다.

1.3 전자서명인증체계 관련자

1.3.1 국민은행

1. 역할
   ⅰ. 인증서비스 제공과 관련된 가입자의 신원확인 업무
   ⅱ. 인증서 업무(발급/갱신/ 폐지 등)
   ⅲ. 인증서 관련 정보 공고

iv. 실시간 인증서 유효성 확인서비스(OCSP)

v. 기타 인증서비스와 관련된 업무

2. 책임 및 의무사항

ⅰ. 국민은행은 정당한 사유 없이 전자서명인증 서비스의 제공을 거부하거나, 가입자 또는 이용자를 부당하게 차별하지 않습니다.

ⅱ. 국민은행은 가입자 및 이용자에게 인증서의 신뢰성이나 유효성에 영향을 미칠 수 있는 다음의 정보를 당사 홈페이지에 공고하여 그 사실을 확인할 수 있도록 합니다.

- 전자서명인증업무 운영기준 준수사실 인정 또는 취소
- 전자서명인증업무 휴지·정지 또는 폐지
- 전자서명인증업무의 양도·양수·합병
- 준칙의 제·개정
- 기타 전자서명인증업무 수행 관련 정보 등

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

iv. 국민은행은 인증기관으로서 안전하게 생성한 전자서명생성정보로 발급한 가입자의 인증서에 대해 그 내용이 신청등록된 사실과 오차가 없다는 것을 확인합니다.

v. 국민은행 인증기관 자신의 전자서명생성정보의 분실·훼손 또는 도난·유출 등 인증서의 신뢰성이나 유효성에 영향을 미치는 사유가 발생한 사실을 인지하는 경우 해당 사실을 당사 홈페이지에 즉시 공고하며, 해당 전자서명생성정보로 발급한 가입자의 인증서를 폐지하고 이를 가입자에게 통보합니다. 또한 전자서명인증업무의 신뢰성·유효성을 확보할 수 있는 대책을 강구합니다.

vi. 국민은행은 신뢰할 수 있는 인증을 획득한 암호화 모듈 및 보안 기술규격을 적용하는 것을 원칙으로 하며, 암호알고리즘, 암호모듈 및 키 운영, 암호알고리즘이 적용되는 매커니즘 등과 같은 전자서명인증시스템 암호 운영 관련 전반에서 가입자 또는 이용자에게 손해가 발생하였을 때에도 책임을 부담합니다.

1.3.2 등록대행기관

국민은행은 별도의 등록대행기관을 운영 및 관리하지 않습니다.

1.3.3 가입자

1. 가입자란 전자서명생성정보에 대하여 국민은행으로부터 전자서명인증을 받은 고객을 말합니다.
2. 가입자는 다음과 같은 책임과 의무를 가집니다.

ⅰ. (정확한 정보 제공) 가입자는 다음 사항에 대하여 정확한 정보를 국민은행에 제공하여야 합니다. 또한 국민은행이 신원확인을 위하여 관련 서류를 요청하는 경우 가입자는 성실히 협조하여야 합니다.

- 인증서의 발급/재발급 신청

- 인증서의 폐지 신청
- 가입자 정보 변경 등

ii. (인증서의 용도 내 사용) 가입자는 정당한 이용범위 및 용도에 맞게 인증서를 사용하여야 합니다. 그리고 인증서를 사용하여 전자서명을 제공할 때에는, 당해 인증서에 포함된 전자서명검증정보에 합치하는 전자서명생성정보를 사용하여야 합니다.

iii. (전자서명생성정보의 보호) 가입자는 생성된 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 보관·관리하여야 합니다.

iv. (전자서명생성정보 안전조치) 가입자는 전자서명생성정보가 분실·훼손 또는 도난·유출되었거나 안전하지 않다고 인지하는 경우, 지체없이 국민은행에 관련사실을 통보하여 국민은행이 해당 인증서를 폐지할 수 있도록 협조하여야 합니다.

1.3.4 이용자(이용기관)

1. 이용자란 국민은행이 제공하는 인증서비스를 이용하려는 자를 말합니다.
2. 이용자는 다음과 같은 책임과 의무를 가집니다.

i. (인증서의 용도 내 사용) 이용자는 국민은행이 가입자에게 발급한 인증서의 이용목적 및 이용범위(제한 포함)를 확인 및 이해하여야 합니다.

ii. (인증서의 유효성 확인) 이용자는 인증서 기재사항 등에 의하여 전자서명의 진위여부를 확인하기 위하여 다음의 조치를 취하여야 합니다.

- 인증서 유효 여부의 확인
- 인증서의 만료 또는 폐지 여부의 확인
- 인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항의 확인

1.3.5 기타 참여자

해당 사항이 없습니다.

1.4 인증서 종류

1.4.1 인증서 이용범위 및 용도

인증서의 용도 및 유효기간은 다음과 같습니다.

구 분	용 도	유효기간
KB국민인증서	- 국민은행 및 이용자(이용기관)의 전자서명인증 - 가입자 신원확인을 위한 간편인증 - 기타 국민은행이 별도로 정하는 사항	발급일로부터 2년

1.4.2 인증서 이용제한

가입자에게 발급한 인증서는 발급 시의 이용범위 또는 용도 내에서만 이용하고 있으며, 누구든지 인증서를 이용범위 또는 용도에 벗어나 부정하게 사용할 수 없습니다. 또한 유효기간이 만료 또는

폐지된 인증서를 사용하여서는 안 됩니다.

1.5 준칙의 관리

1.5.1 준칙의 관리조직

국민은행은 인증업무준칙에 대한 수립 및 개정업무 등 전반적인 관리를 담당합니다.

1.5.2 준칙의 담당부서

국민은행 인증업무에 대한 담당부서 및 연락처는 다음과 같습니다.

1. 부서: 스타뱅킹영업부(P)(인증사업)
2. 이메일: kbg110350@kbfg.com
3. 주소: (07320)서울특별시 영등포구 여의대로 24, 32층(여의도동, 전국경제인연합회회관)

1.5.3 인증업무준칙 개정 관리

국민은행의 인증업무준칙의 제·개정은 국민은행 인증업무 관리책임자의 승인을 받아 개정하며, 아래 내용을 포함한 개정 관련 기록을 유지·관리 합니다.

1. 준칙의 버전
2. 적용 업무 및 범위의 개요
3. 준칙의 제·개정 기록(기존 준칙의 규정, 제·개정 내용 및 사유 등)

1.5.4 준칙의 승인 절차

국민은행이 인증업무준칙을 개정하면서 가입자에게 중대한 영향을 미칠 수 있다고 국민은행이 판단하는 경우에는 가입자에게 사전에 개정 사실을 알릴 수 있습니다. 변경된 준칙의 공고일을 포함하여 공고 후 1개월 내에 서면으로 이의를 제기하지 아니한 가입자는 변경된 준칙에 동의한 것으로 봅니다.

1.6 정의 및 약어

1. "전자문서"란 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말합니다.
2. "전자서명"이란 다음 각 목의 사항을 나타내는 데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말합니다.
   ⅰ. 서명자의 신원
   ⅱ. 서명자가 해당 전자문서에 서명하였다는 사실
3. "전자서명생성정보"란 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말합니다.
4. "전자서명수단"이란 전자서명을 하기 위하여 이용하는 전자적 수단을 말합니다.
5. "전자서명인증"이란 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말합니다.

6. "인증서"란 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말합니다.
7. "전자서명인증업무"란 전자서명인증, 전자서명인증 관련 기록의 관리 등 전자서명인증서비스를 제공하는 업무를 말합니다.
8. "전자서명인증사업자"란 전자서명인증업무를 하는 자를 말합니다.
9. "인정사업자"란 전자서명법 제8조에 따라 운영기준 준수사실의 인정을 받은 전자서명인증사업자를 말합니다.
10. "전자서명인증시스템"이란 인정사업자가 전자서명인증서비스를 제공하기 위해 운영하는 다음 각 호의 시스템을 말합니다.
    ⅰ. 가입자의 등록정보를 관리하기 위한 시스템
    ⅱ. 전자서명생성정보를 생성·관리하기 위한 시스템
    ⅲ. 인증서를 생성·발급·관리하기 위한 시스템
    ⅳ. 기타 전자서명인증업무의 수행과 관련된 시스템 및 설비
11. "등록대행기관"이란 인정사업자를 대신하여 전자서명인증서비스에 가입하려는 자의 신원을 확인하고 가입 신청을 접수·등록하는 등의 업무를 수행하는 자를 말합니다.
12. "암호화 모듈(Crypto-module)"이란 암호화 키를 안전하게 생성하고 관리하는 스마트 카드, 토큰 또는 하드웨어 보안 모듈과 같은 하드웨어 장치를 말합니다.
13. "키 쌍(Key Pair)"이란 전자서명생성정보(개인키)와 이에 대응하는 전자서명검증정보(공개키)를 말합니다.
    ⅰ. 전자서명검증정보(공개키)(Public Key): 해당 전자서명생성정보(개인키)의 소유자가 공개할 수 있는 키로서, 신뢰 당사자가 대응하는 전자서명생성정보(개인키)로 생성된 디지털 서명을 확인 또는 해당 전자서명생성정보(개인키) 소유자만 암호를 해독할 수 있도록 메시지를 암호화하는데 사용됩니다.
    ⅱ. 전자서명생성정보(개인키)(Private Key): 키 쌍의 소유자만 알고 있는 비밀키로서, 디지털 서명을 생성 및/또는 대응하는 전자서명검증정보(공개키)로 암호화된 전자기록이나 파일 암호를 해독하는 데 사용됩니다.
14. "신뢰 당사자(Relying Party)"란 인증서에 포함된 정보나 타임스탬프 토큰 중 하나를 사용하는 개인 및 법인을 말합니다.
15. “인증서 폐지”란 가입자의 신청에 의한 폐지, 국민은행 전자서명인증업무 수행의 안정성, 보안성, 신뢰성 등을 위하여 부득이한 사유로 인한 폐지 등 인증서의 효력을 강제로 종료하는 것을 말합니다.
16. “객체식별자(OID: Object Identifier)”란 인증서 내 가입자(DN), 버전 등 기본정보 외에 알고리즘, 인증서 정책, 키용도, 인증서 속성 등이 포함되며, 정보들이 표현하는 대상을 객체(Object)라 한다. 이러한 객체들이 유일하게 중복되지 않고 식별하기 위해서는 각 객체에 고유번호를 부여하는 방법이 사용되며, 이것을 객체식별자라 합니다.
17. "온라인 인증서 상태 프로토콜(OCSP)"이란 국민은행의 권한 하에 운영되고 인증서 상태 요청을 처리하기위한 저장소에 연결된 온라인 소프트웨어 응용프로그램을 말합니다.

2. 전자서명인증업무 관련 정보의 공고

2.1 공고설비

1. 국민은행은 인증업무준칙을 포함하여 전자서명인증서비스에 필요한 신청서 양식 등 누구든지 적시에 정확한 사실을 항상 확인할 수 있도록 홈페이지를 안전하게 운영 관리합니다.
2. 국민은행은 인증서, 인증서 유효성 확인 정보 등 인증업무와 관련된 정보 (이하 '인증업무관련정보')가 있는 공고설비를 이중화 구성(Active-Active)으로 안정적으로 운영하고 있습니다.
3. 국민은행의 전자서명인증업무와 관련된 책임사항은 업무준칙 1.3.1에 명시되어 있습니다.
4. 국민은행의 최상위인증기관 인증서와 인증서 지문값을 국민은행 인증센터 홈페이지에 게시하여 언제든지 인증서의 신뢰여부를 확인할 수 있도록 합니다.
   (https://obank.kbstar.com/quics?page=C105368)

2.2 공고방법

국민은행은 인증서 발급 및 관리 등에 관련된 정보를 누구든지 그 사실을 항상 확인할 수 있도록 웹사이트를 통해 공개합니다.

1. 웹 사이트
   ⅰ. 인증업무준칙: https://obank.kbstar.com/quics?page=C100993
   ⅱ. KB국민인증서 이용약관: https://obank.kbstar.com/quics?page=C020003
   ⅲ. 온라인 인증서 상태 프로토콜: http://mbank.kbstar.com/ocsp
   ⅳ. 사용자 인증서 폐지목록: http://mbank.kbstar.com/ca/crl/kb_ca/1(번호 지속증가)
   ※ 사용자 인증서 폐지목록이 방대하여 순차적으로 분할하여 관리함.
   ⅴ. CA 인증서 폐지목록: http://mbank.kbstar.com/ca/arl/kb_ca

2.3 공고주기

1. 국민은행은 인증업무준칙의 개정 승인일로부터 7일 이내에 개정된 준칙을 서비스 홈페이지에 게시합니다.
2. 국민은행은 인증서 유효성 상태 정보를 실시간으로 갱신합니다.
3. 국민은행은 사용자 인증서 폐지목록을 2일 주기로 갱신합니다.

2.4 공고된 정보에 대한 책임

국민은행은 인증업무준칙 및 서비스이용약관 등을 통해 전자서명인증업무와 관련된 정보를 공고하고 있으며, 공고 누락에 따라 가입자 또는 이용자에게 손해를 입힌 때에는 전자서명법 제20조(손해배상책임)에 따른 책임을 집니다.

3. 신원확인

3.1 가입자 이름 표시 방법

3.1.1 명칭의 종류

국민은행 가입자 인증서는 X.509 표준을 준수하며 아래와 같은 DN(Distinguished Name: 고유명) 체계를 가지고 가입자 이름을 CN(Common Name) 값에 기술하며, DN은 UID 값을 통해 유일성을 보장합니다.

- CN=가입자 이름
- UID=user ID
- SerialNumber=가입자 번호
- OU=Personal
- O=KB Kookmin Bank
- C=KR

3.1.2 유의미한 명칭의 필요성

국민은행은 인증서의 subjectDN에 의미 있는 가입자의 실명을 사용합니다.

3.1.3 가입자를 식별할 수 없는 익명성 또는 가명성

국민은행은 익명이나 가명 인증서를 발급하지 않습니다.

3.1.4 다양한 명칭 해석 규정

국민은행 인증서 내 DN은 X.500 표준 및 ASN.1 구문을 사용합니다.

3.1.5 명칭의 고유성

가입자의 Subject DN은 UID와 SerialNumber 값을 통해 유일성을 보장합니다.

3.1.6 상표의 인식, 인증 및 역할

가입자는 제3자의 지적 재산권을 침해하는 내용이 포함된 인증서를 요청할 수 없습니다.
국민은행은 상표를 사용할 수 있는 신청자의 권리를 확인하도록 요구하지 않으며, 분쟁과 관련된 모든 인증서를 취소할 권리를 보유합니다.

3.2 인증서 신규 발급 시 신원 확인

3.2.1 전자서명생성정보(개인키)의 소유 증명 방법

인증서 발급을 위해서는 국민은행에 인가코드, 참조번호를 포함한 CMP 검증을 수행하여 전자서명생성정보(개인키)의 소유권을 증명해야 합니다.

3.2.2 법인 신원 확인

국민은행에서는 법인에게 인증서를 발급하지 않습니다.

3.2.3 개인 신원 확인

국민은행 인증서는 개인을 대상으로 하여 발급됩니다. 개인이 국민은행 인증서를 신규 발급받는 경우 전자서명법 제14조 및 동법 시행령 제9조, 동법 시행규칙 제5조에 근거하여 다음과 같은 신원확인을 하고 있습니다.

1. 휴대폰 본인확인
   본인확인기관인 통신사를 통해 가입신청자의 본인명의 휴대폰을 이용하여 신원확인합니다.
2. 신분증 확인
   ⅰ. 가입신청자는 실명확인증표(주민등록증, 운전면허증, 여권 등)를 이용하여 비대면 실명확인(신분증 촬영)을 진행합니다.
   ⅱ. 신분증 촬영은 영업점 창구에서 대면으로 실명확인 후 발급받은 신청번호 입력으로 대체가 가능합니다.
3. 계좌 인증
   가입신청자의 본인명의 계좌를 이용하여 해당 계좌의 비밀번호를 입력하거나 소액을 이체하여 입금내역을 확인한 뒤 인증값을 입력하는 방식으로 신원확인합니다.

3.2.4 미확인 가입자 정보

국민은행은 가입자 정보가 확인되지 않은 경우 인증서를 발급하지 않습니다.

3.2.5 권한 검증

가입자는 인증서를 신청할 권한이 있으며 국민은행은 인증서가 가입자의 인증서 신청 내용과 정확한지 검증하여야 하고, 신청 과정이 성공적으로 완료되었는지 합리적 수준에서 검증할 수 있는 통제력을 유지합니다.

3.2.6 상호운용 기준

해당 사항이 없습니다.

3.3 인증서 갱신발급, 재발급 및 변경 시, 신원확인

3.3.1 갱신발급에 대한 신원 확인 및 인증

KB국민은행 인증서 갱신발급 시 가입자 신원확인을 인증서 갱신발급 신청에 대한 가입자의 전자서명으로 합니다. 갱신발급 대상 가입자 인증서는 유효해야 하며, 가입자는 해당 인증서에 합치하는 기존 전자서명생성정보를 소유하고 있어야 합니다. 가입자는 패턴 또는 생체정보 인증 등 전자서명생성정보 접근통제 수단을 이용하여 전자서명을 생성함으로써 기존 전자서명생성정보 소유를 증명할 수 있습니다. 신규 전자서명생성정보의 소유 증명 방법은 “3.2.1

전자서명생성정보의 소유 증명방법”을 준용합니다.

3.3.2 폐지 후 재발급에 대한 신원 확인 및 인증(재발급 및 변경 시)

3.2 인증서 신규 발급 시 신원 확인과 동일합니다.

3.4 인증서 효력정지·효력회복·폐지 시, 신원확인

가입자 및 국민은행은 인증서를 폐지하고자 할 경우 4.9.3 항목에 따라 신원확인 후 인증서를 폐지할 수 있으며, 인증서 효력정지 및 효력회복 서비스는 제공하지 않습니다.

4. 인증서 관리

4.1 인증서 발급신청

4.1.1 인증서 발급 신청 주체

개인, 개인사업자, 개인임의단체(단, 종교단체, 동창회 등 가입 시 단체 서류를 제출한 경우는 제외)가 인증서발급을 신청할 수 있습니다.

4.1.2 인증서 신청 절차 및 책임

신청자는 인증사업자의 소프트웨어(이하 'KB스타뱅킹앱')를 이용하여 인증서 발급 요청 기능을 실행함으로써 발급 신청 처리가 시작됩니다.

등록 절차에는 다음이 포함될 수 있습니다.

- 관련 프로그램의 필수 문서를 포함한 인증서 신청서 제출
- 키 쌍 생성
- 키 쌍의 공개 키를 국민은행에 전달
- 해당 신청자 약관에 동의

4.2 인증서 발급 신청 처리

4.2.1 신원 확인 및 인증 수행

개인이 국민은행 인증서를 신규 발급받는 경우 신원확인 방법은 다음과 같습니다.

1. 가입신청자는 이용약관 및 개인정보 수집이용에 동의합니다.
2. 국민은행이 정하는 방식으로 가입신청자의 신원을 확인합니다. 신원확인 방법은 “3.2.3 개인 신원 확인” 방법을 준용합니다.
3. 국민은행은 가입신청자가 제출한 전자서명검증정보의 유일성을 국민은행이 보유중인 전자서명검증정보와의 합치여부 확인을 통하여 합치되는 정보가 없을 경우 전자서명생성정보의 소유자가 가입신청자 본인임을 확인합니다.

4.2.2 인증서 발급 신청 승인 및 거절

다음에 해당하는 경우, 발급 신청이 제한됩니다.

1. 국민은행이 지정한 인증서 서비스 제공 대상이 아니거나, 기술상 인증서 서비스 제공이 불가능한 경우
2. 가입자가 입력한 명의가 실명이 아니거나, 허위 정보의 기재 또는 신청 내용을 정확히 기재하지 않거나 오기 등이 있는 경우
3. 제3자가 가입자 본인을 대리하여 신청하는 경우
4. 법인 고객이 신청하는 경우
5. 기타 법령 위반 등의 사유로 금융사고 발생의 우려가 있거나, 이용약관에 충족이 되지 않을 경우

4.2.3 인증서 신청 처리 소요시간

가입신청자의 발급 신청은 가입신청자가 필요한 절차를 완료한 즉시 처리됩니다.

4.3 인증서 발급 절차 및 보호조치

4.3.1 인증서 발급 절차

국민은행 가입자의 모든 정보는 암호화된 정보통신망을 통해 전송됩니다. 국민은행 서버는 유일성을 검증하고 인증서를 발급하여 가입자 단말기에 저장합니다. 이 과정은 모두 가입신청자의 개입 없이 시스템 간의 통신으로 이루어 집니다.

1. 가입자의 전자서명생성정보는 인증서 발급 신청 시 가입자의 단말기 내에서 생성되며, 안전한 보안 모듈을 이용하여 안전하게 관리됩니다. 발급 신청 시 부여받은 인가코드, 참조번호, 공개키가 포함된 발급신청내역을 전송합니다. 이때 공개키에 해당하는 개인키 소유를 증명하기 위해서 발급신청내역에 전자서명값을 포함합니다.
2. 인증기관은 발급신청내역에서 발급 신청시 부여한 인가코드, 참조번호를 확인하고 공개키를 이용하여 전자서명값을 검증한 후 인증서를 발급하여 전송합니다.
3. 가입자의 단말기에 전송받은 인증서를 저장합니다.

4.3.2 인증서 발급 사실 공지

CMP(인증서 관리 프로토콜)를 통해 인증서가 가입자에게 전달되면 SMS메시지를 통해 가입자에게 발급사실을 알립니다.

4.4 인증서 수령

4.4.1 인증서 수령 절차

가입자는 KB스타뱅킹앱을 이용하여 국민은행이 생성한 인증서를 수령 후 안전하게 저장합니다.

4.4.2 인증기관의 인증서 공개

국민은행 인증기관 인증서는 국민은행 인증센터 홈페이지에 게시합니다.

(https://obank.kbstar.com/quics?page=C105368)

4.4.3 다른 개인 또는 법인에 인증서 발급 공지

해당 사항이 없습니다.

4.5 인증서 이용

4.5.1 가입자 전자서명생성정보 및 인증서 사용

가. 발급된 인증서는 이용자가 거래정보에 대한 전자서명을 위해 이용될 수 있습니다.
나. 인증서가 만료되었거나 폐지된 경우 사용할 수 없습니다.
다. 국민은행은 가입자 키와 인증서의 무결성을 보장하고, 유효기간 동안 안전하게 보호합니다. 또한, 인증서의 이용범위, 용도 등 인증서 이용시 유의하여야 할 사항을 가입자가 확인할 수 있도록 합니다.
라. 가입자는 정확한 정보 제공, 인증서의 용도 내 사용, 전자서명생성정보의 보호, 전자서명생성정보 안전조치에 대해서 책임과 의무를 집니다.

4.5.2 이용자의 전자서명검증정보와 인증서 이용

이용자가 가입자의 전자서명 생성 요청 시, 가입자의 전자서명생성정보로 서명된 전자서명과 연계정보 등을 수신받습니다. 이용자는 인증서 내 확장필드에 정의된 용도로만 이용해야합니다. 또한, 인증서의 이용범위, 용도, 유효기간 확인 등 인증서 이용시 유의하여야 할 사항을 이용자가 확인할 수 있도록 합니다.

4.6 인증서 갱신발급

4.6.1 인증서 갱신 기준

가입자 인증서 발급 1년 경과 후 유효기간 이내에 갱신 가능합니다.

4.6.2 인증서 갱신 신청자

가입자 인증서 갱신 신청은 갱신 대상 인증서의 가입자가 합니다.

4.6.3 인증서 갱신 절차

가입자 본인명의 이용기기에서 인증서 발급 1년 경과 후 유효기간 이내에 가입자가 등록한 패턴 혹은 생체정보를 통해 인증서 인증에 성공하면 가입자의 전자서명으로 유효기간을 2년 갱신하며, 갱신된 인증서는 본 인증업무준칙 4.4.1 항목에 따라 수령합니다.

4.7 인증서 재발급

4.7.1 인증서 재발급 요건

인증서의 재발급은 가입자가 자신의 인증서를 폐지 또는 분실하였거나 유효기간이 경과한 경우, 유효기간이 남아있더라도 간편비밀번호를 분실한 경우 새로운 인증서를 다시 발급 받는 것을 말합니다.

4.7.2 인증서 재발급 절차

인증서는 가입자 본인명의의 이용기기 1개에만 재발급되며(1인 1기기), 인증서를 발급받은 가입자가 인증서를 재발급 받는 경우 기존 인증서는 자동 폐지됩니다. 인증서 재발급은 신규발급 절차와 동일하게 진행합니다.

4.8 인증서 변경

해당 사항이 없습니다.

4.9 인증서 효력정지·효력회복·폐지

4.9.1 가입자 인증서 폐지 사유

국민은행은 다음 사유 발생 시 당해 인증서를 폐지할 수 있습니다.

1. 가입자가 인증서 폐지를 신청한 경우
2. 가입자가 부정한 방법으로 인증서를 발급받은 사실 또는 이용한 사실을 인지하였거나, 그 가능성을 객관적으로 인지한 경우
3. 가입자의 전자서명생성정보 등 중요정보가 분실, 훼손, 도난 또는 유출된 사실을 인지한 경우
4. 가입자가 국민은행의 약관 및 운영정책 또는 본 전자서명인증 업무준칙을 위반한 경우
5. 가입자의 신원확인이 적법하게 이루어 지지 않았음을 국민은행이 인지한 경우
6. 가입자가 인증서 발급 후 1년 이상 사용하지 않는 경우
7. 인증서의 유효기간이 경과한 경우
8. 인증서 비밀번호 중 간편비밀번호를 5회 연속 잘못 입력하는 경우
9. 국민은행이 가입자의 키 쌍 훼손을 인지한 경우

4.9.2 인증서 폐지 신청인

전자서명 생성정보의 분실·훼손 또는 도난·유출 등 여타의 사유로 인증서 폐지 신청을 하고자 하는 경우 신청인은 사유확인 및 인증서 가입자와 동일인이라는 사실을 확인할 수 있는 신원확인을 거쳐 국민은행으로 인증서 폐지를 신청할 수 있습니다.

4.9.3 인증서 폐지 절차

1. 가입자의 신청에 따른 폐지

ⅰ. KB스타뱅킹앱 내 기능에 의한 폐지

1) 인증서 폐지 신청

- KB스타뱅킹앱 내 '인증서 폐기'버튼을 눌러 신청합니다.

2) 가입자 신원 확인

- 가입자가 등록한 간편비밀번호로 전자서명 후 패턴으로 신원을 확인합니다.

3) 인증서 폐지 사실의 확인 방법 제공

- 국민은행은 당해 인증서를 폐지 처리한 후, 인증서 폐지목록을 갱신하고 누구든지 그 사실을 항상 확인할 수 있도록 지체 없이 공고합니다. 공고 방법은 2.2를 참조합니다.

ⅱ. 고객센터 문의에 의한 폐지

1) 인증서 폐지 신청

- 가입자는 고객센터를 통해 인증서 폐지 신청 및 국민은행이 요구하는 신원확인 방법으로 인증서 폐지를 요청합니다.

2) 가입자 신원 확인

- 국민은행은 고객센터 본인확인 방법을 통하여 신청자의 신원을 확인합니다.

3) 인증서 폐지 사실의 확인 방법 제공

- 국민은행은 당해 인증서를 폐지 처리한 후, 인증서 폐지목록을 갱신하고 누구든지 그 사실을 항상 확인할 수 있도록 지체 없이 공고합니다. 공고 방법은 2.2를 참조합니다.

2. 국민은행의 직권에 따른 폐지

국민은행의 직권으로 4.9.1의 2호부터 8호까지 해당할 경우 당해 인증서를 폐지 처리하고, 인증서 폐지목록을 갱신하며 누구든지 그 사실을 항상 확인할 수 있도록 지체 없이 공고합니다.

4.9.4 인증서 폐지 유효기간

가입자는 개인키 손실 또는 침해가 의심되는 직후 즉시 인증서 폐지 신청을 해야 합니다.

4.9.5 인증서 폐지 처리기간

국민은행은 폐지 신청자의 신원을 확인한 후 즉시 인증서의 폐지 처리를 완료합니다.

4.9.6 이용자에 의한 인증서 폐지 확인 요건

이용자는 인증서를 신뢰하기 전에 관련된 인증서폐지목록(CRL) 또는 온라인 인증서 상태 프로토콜(OCSP) 응답자를 확인하여 인증서 체인에 있는 각 인증서의 유효성을 검증할 수 있습니다.

4.9.7 인증서 폐지 목록 발행 빈도

국민은행은 가입자 인증서폐지목록(CRL)을 2일 주기로 갱신합니다. 또한 인증서 유효성 확인 서비스를 통해 조회할 수 있도록 제공하고 있으며, 인증서 폐지 시 해당 정보는 실시간으로 갱신됩니다.

4.9.8 인증서 폐지 목록 발행 최대 소요 시간

인증서폐지목록(CRL) 생성 후 영업일 기준 1일 이내 공고설비에 게시됩니다.

4.9.9 온라인 인증서의 폐지 상태 확인

OCSP를 사용합니다.

4.9.10 온라인 인증서의 폐지 확인 요건

OCSP 응답 메시지는 실시간으로 갱신되며 유효기간은 지정되어있지 않습니다. 또한 OCSP 응답메시지 관련 모든 필드는 RFC6960을 준용합니다.

4.9.11 그 외 인증서 폐지 알림 수단

인증서 폐지 시 고객 이용기기에 폐지에 대한 알림을 즉시 전송합니다.

4.9.12 인증서 효력정지 기준

인증서 효력 정지를 지원하지 않습니다.

4.10 인증서 유효성 확인 서비스

4.10.1 서비스 운영 특징

국민은행은 인증서 유효성 확인 서비스(OCSP)를 제공받고자 하는 경우 이용자와의 계약에 의해 서비스를 제공할 수 있습니다. 이때 서비스 이용 수수료, 이용계약의 해지, 기타 제공 조건 등은 상호 협의된 계약의 내용에 따릅니다.

4.10.2 서비스 가용성

유지보수 또는 서비스 장애로 인해 일시적으로 사용할 수 없는 경우를 제외하고 인증서 상태 서비스를 연중무휴로 제공합니다.

4.11 서비스 가입 철회

가입자는 국민은행 계정을 탈퇴함으로써 전자서명인증서비스의 가입을 철회할 수 있습니다. 국민은행 계정을 탈퇴하는 방법 및 절차는 국민은행 약관이 정하는 바에 따릅니다. 가입 철회 시 인증서 및 인증서 관련 개인정보는 유관 법령에서 따로 정함이 없는 한 지체 없이 파기됩니다

4.12 기타 부가 서비스

4.12.1 키 위탁 및 복구 정책 절차

기타 부가 서비스를 지원하지 않습니다.

4.12.2 세션키 캡슐화 및 복구 정책 및 절차

기타 부가 서비스를 지원하지 않습니다.

5. 시설 및 운영관리

5.1 물리적 보호조치

5.1.1 장소 위치 및 구성

국민은행의 전자서명인증업무를 위한 인증서 발급 및 전자서명 처리 시스템은 두 곳의 데이터센터에 이중화 구성되어 있으며, 전자서명인증업무와 무관한 다른 시스템과는 물리적으로 분리되어 있습니다.

- 김포 IT센터(Main 센터) 위치 : 경기 김포시 태장로 769번길 35
- 여의도 전산센터(DR 센터) 위치 : 서울특별시 영등포구 의사당대로 13

5.1.2 물리적 접근 통제

1. 국민은행의 전자서명인증 업무 관련 설비가 위치한 데이터센터는 외부인의 침입이나 불법적 접근 등의 물리적 위협으로부터 안전하게 보호되고 있습니다.
2. 국민은행은 인증시스템을 별도의 통제구역 내에 설치, 운영하고, 랙별 시건장치를 통해 인가된 사용자에게만 물리적인 접근을 허용합니다.
3. 국민은행은 이상 상황 발생시 경보 기능을 갖는 CCTV 카메라 및 모니터링시스템과 침입감지 시스템 등 감시통제시스템을 설치, 운영하고 있습니다.
4. 국민은행은 출입통제 시스템의 신원확인카드, 생체인증 등을 결합하여 통제구역에 대한 접근을 통제합니다.

5.1.3 전원 및 공기조절 시스템

국민은행은 정전으로 인한 심각한 피해를 방지하기 위해 무정전 전원공급장치를 사용합니다. 또한, 온도 및 습도를 일정하게 유지하기 위해 공기조절시스템을 설치 및 운영합니다.

5.1.4 수해방지

국민은행은 침수로부터 인증시스템을 안전하게 보호하기 위해 바닥으로부터 이격하여 설치합니다.

5.1.5 화재 예방

국민은행은 인증시스템이 설치된 공간에 화재 탐지기, 휴대용 소화기 및 자동 소화설비를 사용합니다.

5.1.6 매체 저장

국민은행은 인증서비스에 사용되는 저장 및 기록매체를 내화금고에 저장하여 물리적 접근을 통제합니다.

5.1.7 폐기물 처리

국민은행은 키, 활성화 데이터 또는 중요 파일을 보관하는 모든 매체를 폐기할 때 내부절차에 따라 처리하거나 완전히 파기합니다.

5.1.8 원격지 백업

국민은행은 연속적인 인증서비스를 위해 백업을 수행합니다. 백업 장소는 주요 설비가 설치된 장소와 동등한 보안 단계 및 통제 수준을 유지하며, 물리적으로 분리된 원격 장소이어야 합니다. 국민은행은 김포 통합IT센터에 전자서명생성정보 저장 시스템을 운영하고 있으며, 약 24Km 떨어진 곳 여의도 전산센터를 백업 장소로 지정하여 전자서명생성정보에 대한 백업을 수행하고 있습니다.

5.2 절차적 보호조치

5.2.1 신뢰할 수 있는 역할(Trusted Roles)

국민은행은 인증업무의 안전성과 신뢰성을 확보하기 위하여 인증업무 수행인력을 역할별로 분리하여 운영합니다.

1. 인증업무 관리책임자는 인증 업무를 총괄하며, 인증서 정책 승인 및 주요사안의 의사결정과 책임 등을 이행합니다.
2. 인증정책 관리자는 인증서비스의 정책 수립 및 개정, 인증관리 담당자에 대한 정기적 교육을 수행합니다.
3. 보안관리자는 인증기관 시스템(CA, RA, OCSP, WEB 등)과 인증서비스에 대한 보안을 관리합니다.
4. 내부통제자는 스타뱅킹영업부(P)(인증사업) 인증서 관련 내부감사 대응 업무를 수행합니다.
5. 재해복구자는 연간 재해복구 훈련 및 키 검증 테스트를 수행합니다.
6. 키 생성 관리자는 하드웨어 보안 모듈(HSM) 운영 및 관리, 인증서 세레머니 절차 수립 및 이행 관리 등을 수행합니다.
7. 인증기관 인증서 관리자는 인증시스템(CA/RCA)에서 인증서 신규 발급/재발급/갱신/폐지를 수행하고 관리합니다.
8. 가입자 인증서 관리자는 등록관리시스템(RA)에서 인증서 신규 발급/재발급/갱신/폐지를 수행하고 하위 등록관리자를 생성 및 권한 부여합니다.
9. 가입자 신원확인 담당자는 가입자가 제출한 신청서 및 신원확인 자료를 수령하고 해당 내역을 확인하고 감시합니다.
10. 인증기관 웹사이트 관리자(WEB)는 인증기관(CA) 웹사이트를 운영하고 관리하고 인증서비스의 기획 등을 수행합니다.
11. 개발자는 인증 시스템 등 인증서비스에 필요한 개발을 수행합니다.

12. 운영자는 인증센터의 시설 및 장비, 인증시스템, 인증시스템 네트워크 등을 운영하고 관리합니다.
13. 보안관리자는 인증서 생성 세레모니의 보안 감독업무 및 전자서명생성정보 파기 절차 감독 등을 수행합니다.
14. 키 소유자는 키 쌍 생성에 필요한 암호화 장비 활성화에 필요한 다자인증 키의 소유자로 인증서 생성 세레모니 등 최상위인증기관 및 인증기관/OCSP 하드웨어 보안 모듈(HSM)내 전자서명생성정보 저장 영역의 접근 필요 시 다자인증을 수행합니다.
15. 감사자는 별도 구성된 감사 조직 인력으로 전자서명인증업무 규정 및 정책 감사업무와 IT감사 업무를 수행합니다.

5.2.2 업무별 수행 인원

인증기관 키 생성은 최소 3인 이상이 수행하며, 각 실은 최소 2인 이상의 신뢰된 역할 수행자가 참석합니다.

5.2.3 인증업무 담당자 인증방법

전자서명인증업무 담당자는 신원확인카드, 지문인식 등 다중으로 결합되어 보호되는 통제구역으로 출입을 통제하고, 인증업무시스템의 접근은 인증업무에 대한 업무분장표에 따라 업무 접근을 통제합니다.

5.2.4 동일인에 의해 동시 수행할 수 없는 인증업무

인증업무 운영 시 신뢰성 및 보안성 확보를 위하여 다음과 같이 업무분리원칙을 준수합니다.

1. 동일 시스템에 대한 운영자 및 보안감사자는 동일하지 않는 자가 각각 수행
2. Root CA실, CA실, RA실에 대한 운영자를 구분하고 접근통제 수행
3. 주요정보를 보관하고 있는 각실의 내화금고 키 관리자를 동일하지 않은 자가 각각 관리

5.3 인적보안

5.3.1 자격, 경력 및 기밀취급 요건

국민은행이 운영하는 인증센터의 주요업무 담당자는 인증업무준칙 요건에 따라 국가가 인정한 정보통신 관련 자격을 취득하거나 이에 준하는 업무 경력을 보유하여야 합니다. 또한, 직원의 역량 및 직무 적성을 합리적으로 확인할 수 있는 인사 관리 및 관리 정책을 수립하고 수행합니다. 신뢰역할은 국민은행 직원만이 수행할 수 있으나, 필요 시 국민은행이 허용하는 범위 내에서 외주인력에 일부 기능을 부여할 수 있습니다.

5.3.2 배경 확인 절차

국민은행의 정보보안정책 또는 인사관리정책에 따라 직원 채용 시 필요한 사항에 대해 검증합니다.

5.3.3 교육 및 훈련

국민은행이 운영하는 인증센터의 주요업무 담당자는 업무담당 시 또는 업무담당 후 1년 이내에 업무수행에 필요한 인증업무 법제, 정책 및 인증서 관리 교육을 이수합니다. 또한 인증센터의 주요업무 담당자는 업무상 취득한 기밀사항의 준수에 관한 서약서를 작성하여 날인하도록 합니다.

5.3.4 재교육 및 훈련

국민은행이 운영하는 인증센터 주요업무 담당자는 연 1회 이상 정보보호 관련 내부 또는 외부교육을 이수하도록 합니다.

5.3.5 직무 이동 및 순환

국민은행이 운영하는 인증센터 주요업무 담당자의 업무순환 및 업무환경의 변화 등으로 인하여 보호조치의 수정 및 보완이 필요한 경우 이를 지체 없이 보완합니다. 또한 인증센터의 주요업무 담당자가 인사이동 및 퇴직하는 경우에는 내부 규정에 따라 계정삭제 및 저장매체 반납 등의 적절한 조치를 취하도록 합니다.

5.3.6 비인가 행위 처벌

국민은행은 허가되지 않은 행위를 한 인증센터 담당자에 대해서 내부규정에 따라 업무중지 등의 제재 조치를 취할 수 있습니다.

5.4 감사기록

5.4.1 감사기록 대상 사건의 종류

국민은행은 인증업무 운영과 관련해 전자적으로 생성되는 로그와 수동으로 생성되는 로그에 대해서 다음과 같은 내용을 기록합니다.

1. 인증서 관리에 관한 기록(인증서 발급/재발급/삭제 등)
2. 인증서 사용에 관한 기록(전자서명 생성/이용/전달 등)
3. 인증기관 키에 관한 기록(키 생성/키 파기/키 운반/키 마이그레이션 등)
4. 기타 인증시스템 관리자의 주요 활동

5.4.2 감사 기록 처리 주기

국민은행은 필요에 따라 감사로그를 분기에 1회 주기적으로 검토합니다.

5.4.3 감사 기록 보존 기간

국민은행은 생성된 모든 감사로그를 최소 5 년 이상 보존하며, 필요시 보관된 감사로그를 내부 또는 외부 감사인에게 제공할 수 있습니다.

5.4.4 감사 기록 보호

각 시스템의 감사기록은 보안감사자에 의해 총괄 관리되며 시스템의 각 업무관리자는 당해 업무에 대한 감사기록만 열람할 수 있습니다. 단, 감사기록은 변경 및 삭제를 할 수 없습니다.

5.4.5 감사 기록 백업 절차

국민은행은 감사기록을 필요 시 관련 표준에 규정된 대로 사용할 수 있도록 주기적으로 백업하여 보관하는 공식 절차를 유지합니다.

5.4.6 감사 기록 취합 시스템

감사기록 시스템을 인증기관(CA)이 직접 운영하고 있습니다.

5.4.7 취약점 평가

국민은행은 인증서비스 업무를 수행함에 있어 효율적인 보안관리를 위해 보안담당부서 주체로 주요정보통신 기반시설, 전자금융기반 시설에 대한 정기적으로 취약점 분석평가를 실시하고 있으며, 신규 서비스 도입 시 보안성 심의를 통해 취약점 점검을 수행합니다.

5.5 기록보존

5.5.1 기록 보존 대상의 종류

국민은행이 보존하는 기록의 유형은 다음과 같습니다.

1. 5.4.1에 명시된 기록의 대상에 정의된 유형
2. 기타 인증 시스템 운영 및 관리의 중요 활동 등

5.5.2 보존 기록 보관 기간

국민은행은 보존기록의 보관기간을 저장 공간의 가용성과 관리의 효율성을 고려하여 인증서가 폐지 및 만료된 날로부터 5년간 보존합니다.

5.5.3 보존 기록 보호

국민은행은 보존기록에 대해 엄격한 물리적 접근통제 및 절차통제를 적용하여 보안을 유지합니다. 보존기록의 조회는 업무범위에 한해 조회가 가능하고, 권한이 없는 업무 담당자는 변경 및 삭제가 불가능 합니다. 또한, 보존장소는 항온 항습기를 설치하고 화재의 발생에 대비하여 화재경보가 등의 보호설비를 설치하여 운영합니다.

5.5.4 보존 기록 백업 절차

국민은행은 보존기록을 천재지변 및 기타 재난 발생시 보존기록의 손실 및 파괴에 대비하여 원격지 저장 설비에 주기적으로 백업하여 보존합니다. 백업 대상, 생성주기 및 보존기간 등의 세부사항은 국민은행 전산관리 업무매뉴얼에 의거하여 수행합니다.

5.5.5 보존 기록 취합 시스템

모든 보존기록 시스템은 인증기관(CA)이 직접 운영하고 있습니다.

5.5.6 보존 기록 확보 및 검증 절차

국민은행은 정기적으로 보관된 정보의 통계 샘플을 테스트하여 정보의 지속적인 무결성과 가독성을 확인합니다. 인증된 국민은행의 장비, 신뢰할 수 있는 역할 및 기타 인증된 사람 만 보존기록에 액세스 할 수 있습니다. 보존 기록 정보 획득 및 확인 요청은 신뢰할 수 있는 역할의 운영자에 의해 조정됩니다.

5.6 전자서명인증사업자의 전자서명생성정보 갱신

인증기관의 인증서(또는 전자서명생성정보)가 만료되는 날의 3년 전부터 새로운 전자서명생성정보를 생성하고, 이 때부터 생성되는 가입자 인증서는 새로운 인증사업자 전자서명생성정보로 발급합니다. 다만 이전의 인증사업자 인증서도 유지하여, 기존 가입자 인증서는 이전 인증사업자 인증서의 유효기간이 만료될 때까지 정상적으로 이용할 수 있도록 처리합니다. 이를 통해 가입자들이 인증사업자의 전자서명생성정보 갱신으로 인해 발생할 수 있는 불편을 최소화합니다. 또한, 갱신된 인증서는 4.4.2 항목에 따라 가입자 및 이용자에게 배포됩니다.

5.7 장애 및 재난 복구

5.7.1 사고 및 침해 처리 절차

전자서명인증업무 장애 및 재해 시, 업무지속성 확보방안 및 재난복구 비상대책과 관련된 "KB국민인증 BCP 운영 계획"에 따라 전파 및 복구를 진행합니다.

5.7.2 컴퓨팅 자원, 소프트웨어, 데이터 훼손에 대한 대책

국민은행은 가입자 인증서에 관련된 주요 데이터가 훼손되거나 파괴가 발생하는 경우에 보존 기록된 자료를 이용하여 복구합니다.

5.7.3 가입자 및 인증기관 전자서명생성정보(개인키) 손실에 대한 복구 절차

국민은행은 인증서비스에 사용되는 전자서명생성정보(개인키)가 안전하지 않다는 사실을 인지한 경우 전자서명검증정보(공개키)를 포함하는 인증기관 및 가입자 인증서를 폐지하고 신규 키 쌍을 생성하여 인증기관 인증서를 재발급합니다.

5.7.4 재해 발생 후 업무 연속성 계획 수립

국민은행은 인증서 발급, 갱신, 폐지 등 인증서 생명주기 업무와 인증기관 시설 및 설비 관리 등 인증서비스 주요 업무가 자연재해, 인적재해, 기술적 재해, 전자적 침해 등으로 업무가 중단되지 않도록 업무 연속성계획을 수립하고 아래와 같이 이행합니다.

1. 인증시스템 및 서비스 운영과 관련된 시스템은 이중화로 구성하여 주 시스템에 문제가 발생하여도 인증서비스가 가능하도록 구성합니다.
2. 연 1회 이상 비상대응훈련(자연재해, 인적재해, 기술적 재해 및 전자적 침해) 및 침해사고 대응훈련(전자적 침해)을 진행하고 결과에 따라 해당 절차의 변경을 검토합니다.

5.8 업무 휴지·폐지·종료

국민은행이 전자서명인증사업을 휴지, 폐지 또는 종료하는 경우 다음의 절차를 따릅니다.

1. 회사가 전자서명인증업무를 휴지, 폐지할 경우 관련 법과 규정에 따라 적절한 절차를 통하여 진행하여야 합니다.
2. 전자서명인증업무의 휴지 절차
   ⅰ. 자연재해 또는 천재지변이 아닌 불가피한 사정으로 회사가 전자서명인증업무의 전부, 또는 일부를 휴지하고자 할 때에는 휴지기간을 정하여 휴지하고자 하는 날의 30일전까지 이를 가입자에게 통보하고 발급 앱, 은행 홈페이지 등에 게시합니다.
3. 전자서명인증업무의 폐지 및 종료 절차
   ⅰ. 자연재해 또는 천재지변이 아닌 불가피한 사정으로 회사가 전자서명인증업무를 폐지하고자 할 때에는 폐지하고자 하는 날의 60일전까지 이를 가입자에게 통보하고 인증서 발급 앱, 은행 홈페이지 등에 게시합니다. 이때 회사는 가입자의 인증서와 그 폐지에 관한 기록을 다른 인증기관에 인계하여야 합니다.

6. 기술적 보호조치

6.1 전자서명생성정보 보호

국민은행은 인가된 자만이 전자서명생성정보를 생성할 수 있도록 합니다.

ⅰ. 국민은행은 물리적으로 안전한 환경에서 규정된 절차에 따라 FIPS140-2 레벨 3이상의 장비로 전자서명생성정보를 생성합니다.

ⅱ. 전자서명생성정보 생성 시 전용 장비를 사용하며, 전용 장비는 모든 네트워크 연결이 차단된 상태로 관리됩니다.

ⅲ. 전자서명 생성정보 생성 시 하드웨어 보안 모듈(HSM) 장비에 3인이상의 관리자가 함께 다자인증을 수행합니다.

ⅳ. 생성된 전자서명생성정보(개인키)는 국민은행에서 허용한 키 백업 용도를 제외하고는 하드웨어 보안 모듈 외부로 추출할 수 없습니다.

6.2 전자서명생성정보 보호조치

국민은행은 전자서명생성정보에 대한 비인가된 접속과 사용을 방지하기 위해 가입자에게 비밀번호 및 이에 상응하는 인증수단을 사용할 것을 강하게 권고하고 있습니다. 인증기관

전자서명생성정보(개인키)가 인증서 서명에 사용되는 경우는 다음과 같습니다.

6.2.1 암호화 모듈 표준 및 통제

인증기관의 키쌍은 FIPS 140-2 레벨 3 이상인 하드웨어 보안 모듈(HSM)에 보관하여 운영합니다.

6.2.2 전자서명생성정보(개인키) 다중 통제

국민은행은 내부 키 생성 절차에 의해 인증기관 키 쌍 생성을 수행합니다. 키 쌍 생성시 최소 3인 또는 그 이상 인원이 참여합니다.

6.2.3 전자서명생성정보(개인키) 위탁

국민은행은 인증기관 키쌍을 제3자에게 위탁하지 않습니다.

6.2.4 전자서명생성정보(개인키) 백업

인증기관 전자서명생성정보(개인키)는 국민은행의 백업 절차에 따라 암호문 형태로 안전한 위치에 보관됩니다. 백업된 전자서명생성정보(개인키)는 하드웨어 보안 모듈(HSM)과 내화금고 내에 안전하게 보관됩니다.

6.2.5 전자서명생성정보(개인키) 기록 보존

국민은행은 인증기관의 전자서명생성정보(개인키)를 6.2.4 전자서명생성정보 백업 항목에 명시된 용도 이외에 별도로 기록 보존하지 않습니다.

6.2.6 암호화 모듈 내부로 전자서명생성정보(개인키) 전송 또는 외부로 추출

인증기관 전자서명생성정보(개인키) 백업 목적으로 국민은행 승인 하에 키 생성절차서, 키 복구절차서, 키 운반절차서, 키 파기절차서에 따라 인증기관 전자서명생성정보(개인키)를 추출할 수 있습니다.

6.2.7 암호화 모듈에 전자서명생성정보(개인키) 저장

인증기관인 국민은행 전자서명생성정보(개인키)가 암호문 형태로 생성되면 본 인증업무준칙 6.2.1 항목의 요건을 충족하는 하드웨어 보안 모듈(HSM)에 저장됩니다.

6.2.8 전자서명생성정보(개인키) 활성화

국민은행 승인 하에 하드웨어 보안 모듈(HSM) 공급업체가 지정한 절차에 따라 인증기관 전자서명생성정보(개인키)가 저장된 하드웨어 보안 모듈을 활성화할 수 있습니다.

6.2.9 전자서명생성정보(개인키) 비활성화

국민은행 승인 하에 하드웨어 보안 모듈(HSM) 공급업체가 지정한 절차에 따라 인증기관

전자서명생성정보(개인키)가 저장된 하드웨어 보안 모듈을 비활성화할 수 있습니다.

6.2.10 전자서명생성정보(개인키) 파기

국민은행은 다음과 같은 사유로 인증기관 전자서명생성정보(개인키)를 복구 불가능하도록 파기할 수 있습니다.

1. 인증기관 인증서 유효기간의 만료
2. 인증기관 전자서명생성정보(개인키/백업 및 보관된 개인키 포함)의 분실·훼손 또는 도난·유출 등 인증서의 신뢰성이나 유효성에 영향을 미치는 사유가 발생한 사실을 인지하는 경우
3. 서버의 해킹으로 인한 키 손상이 우려되는 경우

6.2.11 암호화 모듈 등급

6.2.1 항목 요건을 충족하는 하드웨어 보안 모듈(HSM)을 사용합니다.

6.3 전자서명생성정보 및 전자서명검증정보의 관리

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

6.4 데이터 보호 조치

국민은행은 전자서명생성정보의 유출방지를 위하여 FIPS 140-2 Level 3 이상을 준수하는 하드웨어 보안 모듈(HSM) 장비 내에 전자서명생성 정보를 안전하게 생성 및 보관합니다.

6.5 시스템 보안 통제

국민은행의 인증기관 시스템 정보는 서버 및 OS 통제, 물리적 통제 및 네트워크 통제에 의해 보호되고 있습니다. 네트워크 보안 통제는 6.7 항목에 명시되어 있으며, 인증시스템에서 발급된 인증서 생명주기 관리 업무에 사용되는 모든 계정은 다중 인증(Multi Factor Authentication)이 구현되어 있습니다.

6.6 시스템 운영 관리

6.6.1 시스템 개발 통제

국민은행에서 사용되는 응용 소프트웨어는 회사의 시스템 개발 및 변경 정책 및 절차에 따라 개발, 테스트 및 운영됩니다. 서버를 포함한 하드웨어는 회사 조달 및 구매 절차에 의해 공급업체가 선정됩니다.

6.6.2 보안관리 통제

국민은행은 정보보호 조직을 운영하고 있으며 정보보호를 위해 관리적, 기술적, 물리적 보호대책에 대한 세부규정을 수립, 이행 하고 있습니다.

1. 전자서명인증업무와 관련된 프로그램, 프로세스의 동작 여부를 점검할 수 있는 시스템을 운영하고 있습니다.
2. 전자서명인증시스템의 운영에 필요한 프로그램만 설치하여 관리하고 있습니다.
3. 전자서명인증시스템의 접근을 최소화하고 제한된 인원에 한해 접근 권한을 부여합니다.
4. 전자서명생성정보를 생성하기 위한 단말기에 대한 보안통제를 수행합니다.
5. 전자서명시스템의 생성 및 변경사항에 따른 취약성 점검을 실시합니다.
6. 전자서명시스템의 소프트웨어에 개발, 도입, 폐지에 대한 형상관리를 진행하고 있습니다.

6.7 네트워크 보호조치

국민은행 네트워크 관리정책에 따라 다음과 같은 기준으로 보호하고 있습니다.

1. 전자서명 네트워크를 이중화 구성하여 장애에 대비하고, 침입차단 및 침입탐지시스템을 사용하여 네트워크를 보호합니다.
2. 로그기록을 주기적으로 분석하여 전자서명인증업무에 대한 침입시도, 네트워크 부하 등을 파악하고 이에 적절한 대응을 하고 있습니다.
3. 침입탐지시스템의 데이터베이스를 주기적으로 갱신하고, 네트워크관리시스템을 이용하여 전자서명인증시스템을 지속적으로 모니터링합니다.
4. 침입차단 및 침입탐지시스템에 대한 접근통제를 설정합니다.

7. 인증서 형식

7.1 인증서 형식

7.1.1 버전

국민은행에서 발급하는 가입자 인증서 버전은 X.509 버전 3 입니다.

7.1.2 인증서 확장

부록 A를 참조합니다.

7.1.3 알고리즘 개체 식별자

부록 A를 참조합니다.

7.1.4 명칭 양식

- 객체식별자(OID): 1.2.410.200101.2.1
- 가입자 인증서 정책(OID): 1.2.410.200101.5.1.1.1

7.1.5 명칭 제한

인증서는 재사용되지 않는 고유한 양의 정수로 할당된 일련번호를 포함합니다. 인증서 주체의 하위 필드 선택 사항은 국민은행에 의해 검증된 정보를 포함하거나 공백이어야 합니다. 또한 인증서는 마침표(.), 하이픈(-) 및 가운데점(·) 등의 메타데이터 또는 필드에 허용되지 않는 어떠한 표현도 포함할 수 없습니다.

7.1.6 정책 한정자 구문 및 의미

부록 A를 참조합니다.

7.1.7 주요 인증서 정책 확장에 대한 의미 처리

부록 A를 참조합니다.

7.2 인증서 유효성 확인 정보 형식

7.2.1 버전

국민은행 인증서폐지목록(CRL) 프로파일은 X.509 버전 2를 준수합니다.

7.2.2 CRL 및 CRL 확장 필드

7.2.2.1 기본필드

#	필드명	ASN.1 type	설명
1	Version	INTEGER	V2
2	Signature	OID	sha256ECDSA
3	Issuer		CN = 가입자 이름 OU = Personal O = KB Kookmin Bank C = KR
	type	OID	
	value	printableString 또는 utf8String	
4	This Update	UTCTime	발급 시점
5	Next Update	UTCTime	다음 발급 시점 (인증기관 정책에 따름)
6	Revoked Certificates		
	userCertificate	INTEGER	폐지된 인증서의 일련번호
	revocationDate	UTCTime	폐지된 날짜
	crlEntryExtensions	Extensions	CRL 엔트리 확장필드
7	CRL Extension	Extensions	CRL 확장필드

- 효력정지 및 폐지된 인증서가 없을 경우는 Revoked Certificates 필드를 생성하지 않음

- CRL 엔트리 확장필드, CRL 확장필드는 아래 표 참조

7.2.2.2 확장필드

#	필드명	ASN.1 type	설명
1	Authority Key Identifier		
	KeyIdentifier	OCTET STRING	최상위 인증기관 인증서의 Subject Key Identifier
2	CRL Number	INTEGER	CRL 일련번호

7.2.2.3 엔트리 확장필드

#	필드명	ASN.1 type	설명
1	Reason Code	ENUMERATED	폐지 사유

7.3 인증서 유효성 확인 서비스 형식

7.3.1 버전

국민은행 온라인 인증서 상태 프로토콜(OCSP) 응답자는 RFC 6960에 정의된 버전 1을 준수합니다. 국민은행 OCSP 응답자는 RFC6960를 준수하지 않는 메시지에 대한 응답을 거부할 수 있습니다.

7.3.2 OCSP 확장 필드

7.3.2.1 OCSP Response 기본필드

#	필드명	ASN.1 type	설명
1	responseStatus	ENUMERATED	OCSP 응답 결과
2	responseType	OID	id-pkix-ocsp-basic OID: 1.3.6.1.5.5.7.48.1.1
3	tbsResponseData		
	version	INTEGER	V1
	responderID	OCTET STRING	OCSP 서버 subject DN
	producedAt	UTC Time	OCSP응답에 서명한 시간
	responses		
	certID		
	hashAlgorithm	OID	hashAlgorithmIdentifier- sha1 OID: 1.3.14.3.2.26
	issuerNameHash	OCTET STRING	발급자 DN의 해시값

	issuerKeyHash	OCTET STRING	발급자 공개키 해시 값
	serialNumber	INTEGER	인증서 일련번호
	certStatus		인증서 상태
	thisUpdate	UTC Time	OCSP 갱신시간
	responseExtensions		OCSP Response 확장필드
4	signatureAlgorithm	OID	ecdsaWithSHA256 OID: 1.2.840.10045.4.3.2
5	signature	BIT STRING	OCSP 응답 서명 값
6	certs		OCSP 서버 인증서 정보

7.3.2.2 OCSP Response 확장필드

#	필드명	ASN.1 type	설명
1	responseExtensions	ENUMERATED	폐지 사유
	extnId	OID	id-pkix-ocsp-nonce OID: 1.3.6.1.5.5.7.48.1.2
	extnValue	OCTET STRING	

8. 감사 및 평가

8.1 감사 및 평가 현황

1. 국민은행은 운영기준 준수 사실의 인정을 받기 위해 매년 평가기관의 평가를 받습니다.
2. 평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대해 평가를 하고, 그 결과를 인정기관에 제출 합니다.
3. 과학기술정보통신부 장관은 운영기준에 부합한다고 인정하는 국제적으로 통용되는 평가를 정하여 고시할 수 있으며, 전자서명인증사업자가 국제통용평가를 받으면 평가기관의 평가를 받은 것으로 봅니다.
4. 운영기준 준수 사실에 대한 인정의 유효기간은 인정받은 날로부터 1년으로 합니다.
5. 평가와 별도로 국민은행은 연 1회 전자서명인증업무에 대한 내부감사를 실시합니다.

8.2 평가자의 신원, 자격

1. 평가자의 신원 및 자격은 전자서명법 시행령 제 5조(평가기관의 선정기준 및 절차 등)에 따라 선정됩니다.
2. 평가기관의 전문인력 요건은 전자서명법 시행령 [별표1]에 따릅니다.
3. 내부감사는 전문성을 갖춘 인력으로 구성하여 평가를 실시합니다.

8.3 평가 대상과 평가자의 관계

1. 평가기관은 전자서명법령상 과학기술정보통신부에 의해 '피 평가기관에 대한 공정성, 객관성, 신뢰성, 독립성을 확보'한 것으로 인정받은 기관으로 평가자와 평가대상과는 독립성 등이 유지되고 있습니다.
2. 내부감사는 독립성을 확보하여 사업부서와 독립적인 조직에서 실시합니다.

8.4 평가 목적 및 내용

1. 국민은행은 인정기관으로부터 운영기준의 준수 사실에 대한 인정을 받기 위해 평가기관으로부터 평가를 받습니다.
2. 평가내용은 전자서명인증사업자의 운영기준 준수 여부에 대해 평가하며, 세부사항은 평가기관이 정한 세부평가 기준에 따릅니다.
3. 감사 목적은 전자서명인증업무 관련 통제 및 위험 관리 절차가 목적을 달성하고 있음을 확인합니다.

8.5 부적합 사항에 대한 조치

1. 과학기술정보통신부 장관은 운영기준 준수 사실의 인정을 받은 전자서명인증사업자가 전자서명법 제17조(시정명령) 각호의 어느 하나에 해당하는 경우에는 기간을 정하여 시정을 명할 수 있으며, 운영기준 준수 사실의 인정을 받은 전자서명인증사업자는 기간 내에 시정명령을 이행하여야 합니다.
2. 인증심사의 부적합사항에 대해서는 조치가 취해지며 합리적인 기간 내에 보완하고 있습니다.
3. 감사를 통한 부적합 사항 발견 시 이에 대한 조치를 적극적으로 실시합니다.

8.6 결과 보고

1. 평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수여부에 대해 평가를 하고 그 결과를 인정기관에 제출하여야 합니다.
2. 감사진행 결과는 총괄책임자 보고 및 이해관계자 등에게 공유를 합니다.

9. 전자서명인증업무 보증 등 기타사항

9.1 수수료

9.1.1 인증서 발급 또는 갱신 수수료

1. 가입자가 전자서명인증서비스를 이용하는 데 있어서, 가입자에게는 별도의 발급 또는 갱신 수수료가 부과되지 않습니다.
2. 이용자가 전자서명인증서비스를 이용하는 데 있어서 이용자가 지불하는 수수료는 이용자와의

별도 계약에 따릅니다.

9.1.2 인증서 접근 수수료

해당 사항이 없습니다.

9.1.3 인증서 효력정지 및 폐지목록 접근 수수료

해당 사항이 없습니다.

9.1.4 기타 서비스에 대한 수수료

해당 사항이 없습니다.

9.1.5 환불 정책

해당 사항이 없습니다.

9.2 배상

국민은행은 전자서명인증업무와 관련하여 가입자 또는 이용자에게 손해를 입힌 경우 전자서명법 제20조(손해배상책임)에 따라 그 손해를 배상합니다.

9.3 영업비밀

9.3.1 기밀 정보의 범위

국민은행 인증업무와 관련되어 합리적인 수준에서 공개되지 않도록 보호하는 기밀 정보는 다음과 같습니다.

1. 전자서명생성정보(개인키)
2. 인증기관 시스템에 접근할 때 사용되는 활성화 데이터
3. 업무연속성 장애대응 비상대책 및 재해복구 계획
4. 정보의 기밀성 무결성 또는 가용성을 보호하는 데 사용되는 보안준칙
5. 개인정보로 보유하는 정보
6. 감사로그 및 보존 기록

9.3.2 기밀 정보 범위에 속하지 않는 정보

인증서 및 인증서 폐지 데이터는 기밀 정보로 간주되지 않습니다. 또한 본 인증업무준칙에 따라 공개가 의무화된 정보는 기밀 정보로 간주되지 않습니다.

9.3.3 기밀 정보 보호 책임

국민은행은 이용자와 가입자의 정보를 보호하기 위하여 합리적인 수준에서 기밀 정보를 처리하고

보호합니다.

9.4 개인정보 보호

9.4.1 개인정보 보호 계획

국민은행은 다음 웹사이트에 게시된 개인정보 정책에 따라 개인정보를 처리합니다.

- https://obank.kbstar.com/quics?page=C109072

9.4.2 개인정보로 간주되는 정보

국민은행은 인증서비스에서 다음 웹사이트에 게시된 전자서명인증업무 개인정보처리방침상의 개인정보를 처리하고 있습니다.

- https://obank.kbstar.com/quics?page=C109072

9.4.3 개인정보 보호의 책임

국민은행은 개인정보보호법 등 관계 규정을 준수하여 홈페이지에 게시된 개인정보처리방침에 따라 개인정보를 수집·보유·처리합니다.

9.4.4 개인정보 사용에 대한 통지 및 동의

국민은행은 개인정보보호법 등 관계 규정을 준수하며, 인증서 발급 시 개인정보 사용에 대한 이용 동의를 받습니다.

9.4.5 사법 또는 행정 절차에 따른 공개

해당 사항이 없습니다.

9.4.6 기타 정보 공개 기준

해당 사항이 없습니다.

9.5 지식 재산권

다음 사항에 대한 지식재산권은 저작권법 등 관련법률에 따라 국민은행 귀속됩니다.

1. 국민은행 인증시스템을 위해 개발된 소프트웨어 및 하드웨어
2. 본 전자서명인증업무준칙 및 국민은행 서비스 이용 약관과 운영 정책
3. 기타 관련 법령에 따라 국민은행에게 권리가 귀속되는 일체의 저작물

9.6 보증

1. 국민은행 KB국민인증서는 본 준칙에 따라 발급됨을 보증합니다.
2. 국민은행은 KB국민인증서 내에 포함된 내용이 발급신청 당시 기준으로 국민은행 CA에 등록된 사실임을 보증합니다.

9.7 보증 예외 사항

국민은행은 전자서명법, 동법 시행령 및 시행규칙, 국민은행의 약관 또는 운영정책과 본 전자서명인증 업무준칙에서 정한 사항 이외의 사항 즉, 가입자 신용 및 가입자 관련 정보의 불변성 등을 보증하지 않습니다.

9.8 보험의 보상 범위

국민은행은 전자서명인증업무의 수행과 관련하여 전자서명법 제20조에 따라 연간 총 보상한도가 10억 원 이상인 보험에 가입하고 있습니다.

9.9 배상 한계

전자서명법 제20조(손해배상책임)에 의거하여 은행의 고의 또는 과실이 없음을 입증하면 그 배상책임이 면제됩니다.

9.10 준칙의 효력

9.10.1 준칙의 유효기간

인증업무준칙은 홈페이지에 게시되고 본 문서에 명시된 기간 이후에 효력이 발생합니다. 또한, 개정사항은 홈페이지에 게시된 이후에 적용됩니다. 다만 각 호의 사유가 발생한 때에 효력이 소멸합니다.

1. 국민은행의 전자서명인증업무가 정지된 경우 해당 정지 기간
2. 국민은행이 전자서명인증업무의 전부를 휴지한 경우 해당 휴지 기간
3. 국민은행이 전자서명인증업무를 폐지한 경우 폐지시점 이후
4. 기타 전자서명인증 업무준칙의 효력이 소멸하는 경우로 과학기술정보통신부 장관이 인정하는 경우

9.10.2 준칙의 종료

인증업무준칙 및 관련된 정책 문서는 신규 버전으로 개정되기 전까지 효력을 유지합니다.

9.10.3 준칙의 경과 조치

본 인증업무준칙 효력이 종료된 시점을 기준으로 발급된 모든 인증서의 남은 유효기간 동안 본 인증업무준칙 효력이 적용됩니다.

9.11 통지 및 의사소통

국민은행은 전자서명생성정보에 대한 손상, 노출, 파손, 분실, 도난 등 인증서의 신뢰도 및 유효성에 중대한 영향을 미치는 사실이 발생할 때 해당 사실을 홈페이지에 공고합니다.

9.12 이력 관리

국민은행은 다음 웹사이트에서 전자서명인증업무준칙의 변경 이력을 관리합니다.

- https://obank.kbstar.com/quics?page=C100993

9.12.1 개정 절차

국민은행은 전자서명인증업무준칙의 변경이 필요하다고 판단한 경우에 이를 개정합니다. 또한 국민은행은 다음의 내용을 포함한 전자서명인증업무준칙의 개정 관련 기록을 유지·관리합니다.

1. 전자서명인증업무준칙 버전
2. 적용 업무 및 범위의 개요
3. 전자서명인증업무준칙의 개정 기록
   ⅰ. 개정된 기존 전자서명인증업무준칙의 규정
   ⅱ. 개정 내용
   ⅲ. 개정 사유 등

9.12.2 개정 게시

국민은행은 제·개정된 전자서명인증업무준칙을 다음 웹사이트에 게시합니다.

- https://obank.kbstar.com/quics?page=C100993

9.12.3 인증체계식별명(OID)를 변경해야 하는 상황

해당 사항이 없습니다.

9.13 분쟁 해결

1. 전자서명인증체계 관련자에게 전달되는 문서(또는 전자문서)가 법적 효력을 갖기 위해서는 다음과 같은 요건을 만족해야 합니다.
   ⅰ. 전자서명은 전자적 형태라는 이유만으로 서명, 서명날인 또는 기명날인으로서의 효력이 부인되지 아니한다.
   ⅱ. 전자문서는 전자적 형태로 되어 있다는 이유만으로 법적 효력이 부인되지 아니한다.
   ⅲ. 법령의 규정 또는 당사자 간의 약정에 따라 서명, 서명날인 또는 기명날인의 방식으로 전자서명을 선택한 경우 그 전자서명은 서명, 서명날인 또는 기명날인으로서의 효력을 가진다.
2. 전자서명인증인증업무와 관련하여 국민은행과 가입자 또는 이용자간 분쟁이 발생한 경우 전자서명법 제22조(분쟁의 조정)에 따라 전자문서 · 전자거래분쟁조정위원회에 조정을 신청하여 관련 절차에 따라 신속한 방법으로 분쟁을 해결할 수 있습니다.

9.14 관할법원

전자서명인증서비스 관련 소송 발생시, 관할 법원은 민사소송법이 정한 바에 따릅니다

9.15 관련 법률 준수

1. 전자서명인증업무와 관련된 전자서명인증체계 관련자들은 전자서명법 및 관계 법령을 준수하여야 합니다.
2. 본 인증업무준칙의 해석과 적용은 전자서명법 등 대한민국 관련 법률에 따릅니다.
3. 인증서비스와 관련한 소송의 관할 법원은 민사소송법이 정한 바에 따릅니다.

9.16 기타 규정

해당 사항이 없습니다.

부칙

이 준칙은 2021 년 7 월 9 일부터 시작합니다.

부칙

이 준칙은 2021 년 8 월 19 일부터 시행합니다.

부칙

이 준칙은 2021 년 9 월 8 일부터 시행합니다.

부칙

이 준칙은 2021 년 10 월 1 일부터 시행합니다.

부칙

이 준칙은 2021 년 10 월 8 일부터 시행합니다.

부칙

이 준칙은 2021 년 11 월 1 일부터 시행합니다.

부칙

이 준칙은 2021 년 12 월 1 일부터 시행합니다.

부칙

이 준칙은 2022 년 4 월 22 일부터 시행합니다.

부칙

이 준칙은 2022 년 5 월 20 일부터 시행합니다.

부칙

이 준칙은 2022 년 12 월 8 일부터 시행합니다.

부칙

이 준칙은 2023 년 12 월 29 일부터 시행합니다.

부칙

이 준칙은 2024 년 1 월 24 일부터 시행합니다.

부록 A. 프로파일

A.1 최상위 인증기관 인증서 프로파일

A.1.1 기본필드

#	필드명	ASN.1 type	설명
1	Version	INTEGER	V3
2	Serial Number	INTEGER	고유일련번호
3	Signature	OID	sha384ECDSA
4	Issuer		CN = KB Root CA 1 O = KB Kookmin Bank C = KR
	type	OID	
	value	printableString 또는 utf8String	
5	Validity		유효기간
6	Subject		CN = KB Root CA 1 O = KB Kookmin Bank C = KR
	type	OID	
	value	printableString 또는 utf8String	
7	Subject Public Key Info		
	algorithm	OID	ecPublicKey(384 Bits)
	subjectPublicKey	BIT STRING	
8	Extensions	Extensions	확장필드 참고

A.1.2 확장필드

#	필드명	ASN.1 type	설명
1	Subject Key Identifier	OCTET STRING	subjectPublicKey의 hash 값
2	Key Usage	BIT STRING	Certificate Signing, Off-line CRL Signing, CRL Signing
3	Basic Constraints		Subject Type=CA
	cA	TRUE	

A.2 인증기관 인증서 프로파일

A.2.1 기본필드

#	필드명	ASN.1 type	설명
1	Version	INTEGER	V3
2	Serial Number	INTEGER	고유일련번호
3	Signature	OID	sha384ECDSA

4	Issuer		CN = KB Root CA 1 O = KB Kookmin Bank C = KR
	type	OID	
	value	printableString 또는 utf8String	
5	Validity		유효기간
6	Subject		CN = KB CA 2 O = KB Kookmin Bank C = KR
	type	OID	
	value	printableString 또는 utf8String	
7	Subject Public Key Info		
	algorithm	OID	ecPublicKey(256Bits)
	subjectPublicKey	BIT STRING	
8	Extensions	Extensions	확장필드 참고

A.2.2 확장필드

#	필드명	ASN.1 type	설명
1	Authority Key Identifier	INTEGER	V3
	KeyIdentifier	OCTET STRING	최상위 인증기관 인증서의 Subject Key Identifier
	authorityCertIssuer	GeneralNames	최상위 인증기관 인증서의 Subject
	authorityCertSerialNumber	INTEGER	최상위 인증기관 인증서의 Serial Number
2	Subject Key Identifier	OCTET STRING	subjectPublicKey의 hash 값
3	Key Usage	BIT STRING	Certificate Signing, Off-line CRL Signing, CRL Signing
4	Basic Constraints		Subject Type=CA Path Length Constraint=
	cA	TRUE	
	pathLenConstraint	INTEGER	
5	CrlDistributionPoint		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://mbank.kbstar.com/ca/crl/kb_ca
	distributionPoint	DistributionPoint Name	
	reasons	ReasongFlags	
	cRLIssuer	GeneralNames	

A.3 가입자 인증서 프로파일

A.3.1 기본필드

#	필드명	ASN.1 type	설명
1	Version	INTEGER	V3
2	Serial Number	INTEGER	고유일련번호
3	Signature	OID	sha256ECDSA
4	Issuer		CN = KB CA 2 OU = Personal O = KB Kookmin Bank C = KR
	type	OID	
	value	printableString 또는 utf8String	
5	Validity		유효기간
6	Subject		CN = 가입자 이름 UID = user ID SerialNumber = 동일 가입자에게 발행된 인증서의 유일성 식별자 OU = Personal O = KB Kookmin Bank C = KR
	type	OID	
	value	printableString 또는 utf8String	
7	Subject Public Key Info		
	algorithm	OID	ecPublicKey(256Bits)
	subjectPublicKey	BIT STRING	
8	Extensions	Extensions	확장필드 참고

A.3.2 확장필드

#	필드명	ASN.1 type	설명
1	Authority Key Identifier		
	KeyIdentifier	OCTET STRING	인증기관 인증서의 Subject Key Identifier
	authorityCertIssuer	GeneralNames	인증기관 인증서의 Subject
	authorityCertSerial Number	INTEGER	인증기관 인증서의 Serial Number
2	Subject Key Identifier	OCTET STRING	subjectPublicKey의 hash 값

3	Key Usage	BIT STRING	Digital Signature, Non-Repudiation
4	Certificate Policy		[1]Certificate Policy: Policy Identifier=1.2.410.200101.5.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://obank.kbstar.com/quics?page=C100993
	policyIdentifier	OID	
	policyQualifiers		
	PolicyQualifierId	OID	
	Qualifier		
	CPSuri	IA5String	
	UserNotice		
	SEQUENCE		
	ExplicitText	BMPString	
5	CrlDistributionPoint		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://mbank.kbstar.com/ca/crl/kb_ca
	distributionPoint	DistributionPointName	
	reasons	ReasongFlags	
	cRLIssuer	GeneralNames	
6	Authority Information Access		[1]Authority Info Access Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://mbank.kbstar.com/ocsp
	accessMethod	OID	
	accessLocation	GeneralName	
7	Basic Constraints		Subject Type=Not CA
	cA	False	
8	Subject Alternative Name		CN=실명
	directoryName	Name	

부록 B. 개정이력

Version	내용	일자
1.0.0	인증업무준칙 제정	2021.07.09
1.0.1	주요내용 업데이트 - 2.1 최상위인증기관 인증서 게시 URL 추가 - 3.1.1 DN값 내 SerialNumber 추가 - 4.3.1 인증서 발급절차 세분화 - 4.4.2 인증기관 인증서 게시 URL 추가 - 4.9.12 고객 통지방법 추가 - 5.4.8 취약성 점검 주체 등 세부사항 추가 - 5.5.4 백업 수행관련 내부지침 명시 - 5.5.6 국민은행 역할 추가 - 5.7.1 BCP-DRP 지침 문서명 명시 - 6.1.2 인증기관 가입자 개인키 생성 여부 추가 - 6.1.4 외부기관 사용방법 추가 - 6.1.5 키 길이 내용 변경 및 일부내용 삭제 - 6.2.5 기록보존 내용 명확화 - 6.2.7 일부내용 삭제 - 6.2.10 개인키 파기사유 상세화, 키 파기절차 운용내용 명시 - 6.4.1 문구 일부수정 - 7.1.6 가입자 인증서 정책(OID) 추가 - 7.2.2.2 #3 Issuing Distribution Point 항목 삭제 - 7.3.2.1 #3 responderID 설명 항목 내용변경 (OCSP 서버 공개키의 해시값 → OCSP 서버 subject DN) - 7.3.2 #3 hashAlgorithm 설명 항목 내용변경 (sha256 → sha1, OID: 2.16.840.1.101.3.4.2.1 → OID: 1.3.14.3.2.26) - A.1.1 #3 Signature 설명 항목 내용변경 (Sha384ECDSA → sha384ECDSA) - A.1.1 #5 Validity 유효기간 변경 및 표시시간 삭제 - A.1.2 #2 Key Usage 설명 항목 내용삭제 (Didital Signature, Non-Repudiation 삭제, c6 삭제) - A.2.1 #3 Signature 설명 항목 내용변경 (ecdsaWithSHA256 → sha384ECDSA) - A.2.1 #5 Validity 유효기간 변경 및 표시시간 삭제 - A.2.1 #6 설명 항목 CN값 변경(KB CA 1 → KB CA 2) - A.2.2 #3 Key Usage 설명 항목 내용삭제	2021.08.19

	(Didital Signature, Non-Repudiation 삭제, c6 삭제) - A.2.2 #4 항목 삭제(Certificate policy) - A.3.1 #4 설명 항목 CN값 변경(KB CA 1 → KB CA 2) - A.3.1 #5 Validity 유효기간 변경 및 표시시간 삭제 - A.3.1 #7 Algorithm 설명 항목 내용변경 (ECDSA(256Bits) → ecPublicKey(256Bits)) - A.3.2 #3 - A.2.2 Key Usage 설명 항목 내용삭제 (c6 삭제) - 부록B 개정이력 추가	
1.0.2	전자서명인증사업자 평가내용 업데이트 - 1.1 대상 인증서 명확화 - 1.4.2 인증서 용도 세분화 - 1.5.4 공고기간 변경, 단어수정 - 2.1 참조항목 변경 - 2.3 게시기간 변경, 공고주기대상 추가 - 3.2.3 대상고객 및 프로세스 세분화 - 3.3.1 항목명 명확화 - 3.4 내용 명확화 - 4.3.1 정보보안 내용 추가, 일부내용 삭제 - 4.5.2 이용기관에 식별정보 전달내용 추가 - 4.6.1 인증서 수령 및 갱신알림 내용 추가 - 4.6.2 참조항목 추가(4.6.1) - 4.6.3 참조항목 추가(4.6.1) - 4.6.4 참조항목 삭제 - 4.6.5 참조항목 추가(4.6.1) - 4.6.6 참조항목 삭제 - 4.7.2 참조항목 변경(4.1.1→4.1.2) - 4.7.3 참조항목 변경(4.2→4.3.2) - 4.7.4 참조항목 변경(4.3.2→4.2.2) - 4.7.5 참조항목 삭제 - 4.7.6 참조항목 변경(4.4.2→4.4.3) - 4.7.7 항목 삭제 - 4.9 정보보안 내용 추가 - 4.9.3 단어수정(이용자→가입자), 내용 일부 추가 - 4.9.7 일부내용 변경 - 4.11 일부내용 추가 - 5.1.8 원격지 기준 명시	2021.09.08

	- 5.2.2 키 생성 인력 수정 - 5.6 갱신된 인증서 배포내용 추가 - 5.8 일부내용 삭제 - 6.1.1 하드웨어 보안 모듈(HSM) 수행인력 수정 - 6.2.2 키 생성 인력 수정 - 9.4.2 개인정보 내용 추가 - 9.4.3 항목 삭제 - 9.4.4 개인정보 보호책임 내용 추가, 항목번호 변경 - 9.4.5 항목번호 변경 - 9.4.6 항목번호 변경 - 9.4.7 항목번호 변경 - 9.11 인증업무준칙 공지기간 변경 - A.3.2 일부내용 삭제, 항목 추가	
1.0.3	- 1.5.1 팀명 삭제 - 1.5.2 팀명 삭제 - 3.2.3 항목 조정 및 일부내용 수정 - 4.9.3 일부내용 삭제 - 5.2.1 업무분장에 따른 역할 세분화 및 중복삭제 - 8.1 평가 변경으로 인한 내용 변경 - 8.2 평가 변경으로 인한 내용 변경 - 8.3 기존문구 삭제 및 법령, 제도요건 추가 - 8.4 평가 변경으로 인한 내용 변경 - 9.2.3 일부내용 삭제 - 9.9 책임보험 종류 변경 - 9.11 팀명 삭제	2021.10.01
1.0.4	- 1.1.1 조항신설 - 1.1.2 조항신설 - 1.2 명칭 수정 및 근거법령 작성 - 1.3.1 관련자 조항 신설 - 1.3.2 기존조항 삭제 및 관련자 조항 신설 - 1.3.3 관련자 조항 신설 - 1.3.4 관련자 조항 신설 - 1.3.5 관련자 조항 일부변경 - 1.3.6 기존조항 삭제 및 조 체하 - 1.4.1 조항 내용 조정(1.4.2 내용 반영) - 1.4.2 조항 내용 조정(1.4.1로 내용 이동) - 1.5.3 항목내용 명확화	2021.10.08

	- 1.6 미제공 서비스 및 불필요 정의 삭제, 신규항목 정의 추가 - 3.2.3 신원인증 내용 보완 - 3.2.6 불필요 조항 삭제 - 4.1.1 중복내용 삭제 및 조 체상 - 4.2.1 신원인증 내용 보완 - 4.2.2 일부 내용 수정 - 4.3.1 내용 추가 및 일부 수정 - 4.3.2 용어 수정 - 4.4.1 용어 수정 - 4.5.1 이해하기 쉬운 문구로 변경 - 4.6.1 문구 간소화 - 4.6.3 내용 수정 - 4.6.2 ~ 4.6.7 불필요 조항 삭제 - 4.7.1 하위조항 삭제 - 4.7.2 ~ 4.7.6 불필요 조항 삭제 - 4.8.1 하위조항 삭제 - 4.8.2 ~ 4.8.7 불필요 조항 삭제 - 4.9.11 오기재사항 수정 - 4.9.12 ~ 4.9.13 불필요 조항 삭제 - 4.9.15 ~ 4.9.16 불필요 조항 삭제 - 4.12.1 ~ 4.12.2 불필요 조항 삭제 - 5.2.3 내용 상세화 - 5.2.4 내용 상세화 - 5.3.3 내용 보완 및 상세화 - 5.3.4 ~ 5.3.5 불필요 조항 삭제 - 5.3.7 ~ 5.3.8 불필요 조항 삭제 - 5.7.1 개정문서와 용어 매칭 - 5.7.4 불필요 단어 삭제 - 6.1 용어 수정 - 6.5.1 하위조항 삭제 - 6.5.2 불필요 조항 삭제 - 7.1.5 불필요 조항 삭제 - 7.1.7 ~ 7.1.9 불필요 조항 삭제 - 9.1.2 ~ 9.1.5 불필요 조항 삭제 - 9.2.2 불필요 조항 삭제 - 9.4.1 URL 변경 - 9.4.2 개인정보항목 추가	

	- 9.4.5 조항내용 보완 - 9.4.6 불필요 조항 삭제 - 9.6 이해하기 쉬운 문구로 변경 - 9.6.1 ~ 9.6.4 불필요 조항 삭제 - 9.11 중복내용 삭제 및 일부내용 수정 - 9.12 이해하기 쉬운 문구로 변경 - 9.14 약관 및 타 조항과 내용 일치	
1.0.5	- 1.3.5 부적합 단어 수정 - 1.4.1 오기 삭제 - 1.6 폐기에 대한 대상명시로 표현 명확화 - 4.7 모바일인증서 서비스 이용약관 내용 반영 - 4.9.1 모바일인증서 서비스 이용약관 내용 반영 - 5.2 내부감사 기간 변경 - 5.8 부적합 단어 수정 - 8.5 부적합 단어 수정 - 9.2.2 전자서명법 내용반영 수정 - 9.5 용어 수정 - 9.11 오타 수정 - 9.13 일부내용 변경 및 내용추가	2021.11.01
1.0.6	- 4.7 간편 재발급 내용 삭제	2021.12.01
1.0.7	- 1.1.2 3 삭제 - 1.3 불필요 목차 삭제 - 1.5 관리 조직 명확화 - 1.5.4 중복내용 삭제 - 2.2 웹 사이트 주소 정비 - 3.2.3 발급 대상 명확화 - 3.2.6 항목 신설 - 4.1.1 항목 신설 - 4.2.2 발급 대상 명확화 - 4.5 항목 내용 구체화 및 용어 통일 - 4.6 항목 구체화 - 4.7 항목/내용 신설 및 항목 변경, 내용 추가 - 4.8 내용 삭제 - 4.9 항목/내용 추가 - 4.12 항목 구체화 - 5.2.1 내용 추가 - 5.2.2 내용 수정	2022.04.22

	- 5.3.3 항목 구체화 - 5.3.4 항목 신설 - 5.3.5 항목 신설 - 5.3.7 요건 신설 - 5.4 세부 내용 추가 - 5.5.5 기준 명확화 - 5.5.6 불필요 내용 삭제 - 5.7.4 잘못 기술된 내용 수정 - 6.1.1 내용 기술 명확화 - 6.1.3 용어 상세 기술 - 6.1.4 용어 상세 기술 - 6.1.6 용어 상세 기술 - 6.2 설명 추가 - 6.2.1 잘못 기술된 내용 삭제 - 6.2.4 형태 정보 기술 - 6.2.6 형태 정보 기술 및 절차 수정 - 6.2.7 형태 정보 기술 및 용어 통일 - 6.2.10 작업 담당자 내용 기술 - 6.3.1 문장 삭제 및 용어 상세 기술 - 6.4.1 내용 추가 및 삭제 - 6.6.2 오탈자 수정 - 7.1 항목 구체화 - 9.1 기준 및 내용 구체화 - 9.2.2 내용 추가 - 9.4 정보 명확화 및 목차 이동 - 9.5 오탈자 수정 - 9.12 상세 내용 추가 - 9.17 항목 신설	
1.0.8	- 3.2.3 내용 변경 - 4.2.1 내용 변경	2022.05.20
1.0.9	- 1.1.1 인증서 명칭 변경 - 1.1.2 일부 내용 삭제 - 1.3.2 명칭 변경 - 1.3.3 일부 내용 삭제 및 단어 수정 - 1.3.4 일부 내용 삭제 - 1.4.1 일부 내용 변경 - 1.6 내용 현행화 및 일부 삭제	2022.12.8

	- 2.1 오탈자 수정 - 2.3 오탈자 수정 - 3.2.1 일부 내용 수정 - 3.2.2 단어 수정 - 3.2.3 일부 내용 수정 - 3.3.1 내용 수정 - 4.2.1 일부 내용 수정 - 4.2.2 일부 내용 수정 - 4.3.1 일부 내용 수정 - 4.3.2 용어 수정 - 4.4.1 일부 내용 수정 - 4.5.2 일부 내용 수정 - 4.6.1 일부 내용 수정 - 4.6.3 일부 내용 현행화 - 4.6.4 ~ 4.6.7 항목 삭제 - 4.7.1 ~ 4.7.3 일부 내용 수정/삭제 및 조 체하 - 4.7.4 ~ 4.7.7 항목 삭제 - 4.9.1 일부 내용 삭제 및 내용 추가 - 4.9.3 단어 수정 및 일부 내용 수정 - 4.9.4 일부 내용 수정 - 4.9.5 단어 수정 - 4.9.6 내용 수정 - 4.9.7 용어 수정 - 4.9.11 용어 명확화 - 4.10.2 오탈자 수정 - 5.1.1 주소 추가 - 5.2.1 내용 일부 삭제 및 수정 - 5.4.1 일부 내용 삭제 - 5.4.3 내용 현행화 - 5.4.5 내용 명확화 - 5.5.5 내용 수정 - 5.5.7 내용 일부 삭제 - 5.6 용어 수정 - 5.7.1 인증서 명칭 변경 - 5.7.3 내용 일부 삭제 - 5.7.4 내용 수정 - 5.8 내용 일부 수정	

	- 6.1 내용 수정 및 조항 삭제 - 6.2 내용 일부 수정 - 6.3 내용 일부 수정 및 조항 삭제 - 6.4 내용 일부 수정 및 조항 삭제 - 6.6.2 오탈자 수정 - 6.7 내용 일부 수정 - 6.8 일부 내용 삭제 - 8.1 오탈자 수정 - 8.5 일부 내용 삭제 - 8.6 일부 내용 수정 - 9.2 내용 일부 수정 - 9.4 일부 내용 수정 - 9.6 인증서 명칭 변경 - 9.8 내용 일부 수정 - 9.9 내용 일부 수정 - 9.13 내용 일부 수정 - A.2.2 주소 현행화 - A.3.2 주소 현행화	
1.0.10	- 1.1.1 인증업무준칙 명칭 변경 - 1.1.2 일부 내용 수정 - 1.2 인증업무준칙 명칭 변경 - 1.3.1 내용 일부 수정 - 1.3.3 내용 일부 수정 - 1.3.4 내용 일부 수정 - 1.4.1 내용 일부 수정 - 1.4.2 내용 일부 수정 - 1.6 내용 일부 수정 - 2.2 내용 일부 수정 - 2.3 내용 일부 수정 - 2.4 내용 일부 수정 - 3.2.2 내용 일부 수정 - 3.2.3 내용 일부 수정 - 3.3 내용 일부 수정 - 3.4 내용 일부 수정 - 4.2 내용 일부 수정 - 4.3 내용 일부 수정 - 4.5 내용 일부 수정	2023.12.29

	- 4.7 내용 일부 수정 - 4.9 내용 일부 수정 - 4.9.1 내용 일부 수정 - 4.9.2 내용 일부 수정 - 4.9.3 내용 일부 수정 - 4.9.4 내용 일부 수정 - 4.9.5 내용 일부 수정 - 4.9.6 내용 일부 수정 - 4.9.7 내용 일부 수정 - 4.9.8 내용 일부 수정 - 4.9.9 내용 일부 수정 - 4.9.10 내용 일부 수정 - 4.9.11 내용 일부 수정 - 4.9.12 내용 삭제 - 4.9.14 내용 삭제 - 4.9.15 내용 삭제 - 4.9.16 내용 삭제 - 4.10.3 내용 삭제 - 5.2.1 내용 일부 수정 - 5.3.7 내용 삭제 - 5.4.7 내용 삭제 - 5.4.8 5.4.7 항목으로 이동 - 5.5.2 내용 일부 수정 - 5.7.3 내용 일부 수정 - 5.7.4 내용 일부 수정 - 6.4 내용 일부 수정 - 6.6.2 내용 일부 수정 - 6.6.3 내용 삭제 - 7.1.6 내용 삭제 및 7.1.8 조 체하 - 7.1.7 내용 삭제 및 7.1.9 조 체하 - 7.2.1 내용 일부 수정 - 7.2.2.1 내용 일부 수정 - 7.2.2.3 내용 일부 수정 - 7.3.2.2 내용 일부 수정 - 8.1 내용 일부 추가 - 8.2 내용 일부 추가 - 8.3 내용 일부 추가	

	- 8.4 내용 일부 추가 - 8.5 내용 일부 추가 - 8.6 내용 일부 추가 - 9.2 내용 일부 수정 - 9.3.2 내용 일부 수정 - 9.5 내용 일부 삭제 및 수정 - 9.9 내용 일부 수정 - 9.13 내용 일부 수정 - 9.17 내용 삭제	
1.0.11	- 1.5.2 내용 일부 수정 - 5.2.1 내용 일부 수정	2024.01.24