본인확인인증업무준칙

본인확인인증업무준칙 버전번호 : Ver 1.0

본인확인인증업무준칙 시행일자 : 2023.03.06

1. 소개

1.1 개요

1.1.1 배경 및 목적

주식회사 카카오뱅크(이하 "카카오뱅크") 본인확인인증업무준칙(CPS : Certification Practice Statement)은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의2 제2항에 따른 주민등록번호 대체수단에 해당하는 카카오뱅크 인증서(이하 "인증서")의 발급, 관리 및 인증시스템 운영함에 있어서 필요한 사항을 정하고, 카카오뱅크와 가입자 등 인증 관련 당사자의 책임과 의무사항 규정을 목적으로 합니다.

※ 전자서명법 제8조 운영기준 준수사실의 인정과 관련된 사항은 전자서명인증업무준칙에 명시하고 있습니다.

1.1.2 전자서명인증체계

카카오뱅크는 전자서명인증체계의 안전하고, 신뢰성 있는 운영을 위한 정책의 수립, 시행 및 감독하는 기관으로서 최상위 인증기관(Root CA), 인증기관(CA)으로 전자서명인증체계를 구성하여 관리 감독합니다.

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

2. 카카오뱅크 인증기관(KakaoBank CA)
 - 가입자의 신원확인
 - 가입자 인증서 발급, 재발급, 폐지 업무

- 인증서 유효성 확인 업무
- 기타 인증기관으로서 수행해야 할 업무

1.2 문서의 명칭

본 문서의 명칭은 「카카오뱅크 본인확인인증업무준칙」(이하 “준칙”)으로 전자서명법, 동법 시행령, 동법 시행규칙을 준수합니다.

1.2.1 개정 이력

본 문서의 개정 이력은 다음과 같습니다.

버전	시행일	주요 변경 내역
1.0	2023.03.06.	- 본인확인인증업무준칙 제정

1.3 전자서명인증체계 관련자

1.3.1 전자서명인증사업자

카카오뱅크는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제23조의3 제1항에 따라
방송통신위원회로부터 지정받은 본인확인기관이자 전자서명인증사업자로서 본인확인업무를 수행합니다.

1.3.1.1 카카오뱅크의 역할

1. 카카오뱅크는 전자서명인증사업자로서 최상위 인증기관 및 인증기관을 직접 운영하며, 다음의 업무를 수행합니다.
- 안전한 전자서명인증체계의 구축 및 운영
- 서비스 제공과 관련된 가입자의 신원확인 업무
- 인증서 발급, 재발급 및 폐지 등의 업무
- 준칙, 카카오뱅크 인증서 서비스 이용약관(이하 “이용약관”) 및 인증서 유효성 확인 정보 등의 공고
- 인증서 유효성 확인 서비스
- 기타 본인확인기관 및 전자서명인증사업자로서 필요하다고 인정되는 업무

2. 카카오뱅크의 최상위 인증기관은 다음과 같은 업무를 수행합니다.
- 인증기관의 전자서명생성정보에 대한 인증 등 인증업무 수행
- 인증기관 인증서 유효성 확인 정보 등의 공고
- 기타 최상위 인증기관으로서 수행해야 할 업무

1.3.1.2 카카오뱅크의 책임 및 의무사항

1. 카카오뱅크는 정당한 사유 없이 본인확인서비스의 제공을 거부하거나, 가입자 또는 이용자를 부당하게 차별하지 않습니다.

2. 카카오뱅크는 가입자 및 이용자가 인증서의 신뢰성이나 유효성에 영향을 미칠 수 있는 아래의 정보를 확인할 수 있도록, 이를 카카오뱅크의 홈페이지 또는 앱에 공고합니다.
- 본인확인업무 휴지·정지 또는 폐지
- 준칙의 제·개정
- 기타 본인확인업무 수행 관련 정보 등

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

4. 카카오뱅크는 외부 등록대행기관(RA)을 운영하지 않고, 서비스에 가입하려는 자의 신원을 확인하고 가입 신청을 접수·등록하는 등의 업무를 직접 수행합니다.

5. 카카오뱅크는 가입자가 본인의 전자서명생성정보를 안전하게 생성·저장할 수 있도록 신뢰할 수 있는 암호화 모듈 및 보안 기술 규격 등을 적용하여 본인확인서비스를 제공합니다. 카카오뱅크는 신뢰할 수 있는 인증을 획득한 암호화 모듈 및 보안 기술 규격을 적용하여 본인확인서비스를 제공하는 것을 원칙으로 합니다. 만약 인증이 없는 암호화 모듈 또는 기술 규격을 적용하는 경우, 카카오뱅크는 안전성을 확보하기 위해 충분한 기술적 검증 또는 조치를 취하며, 이에 대해 책임을 부담합니다.

6. 카카오뱅크는 인증기관으로서 안전하게 생성한 전자서명생성정보로 발급한 가입자의 가입자 인증서에 대해 그 내용이 신청등록된 사실과 오차가 없다는 것을 확인합니다.

7. 카카오뱅크는 카카오뱅크의 전자서명생성정보의 분실·훼손 또는 도난·유출 등 인증서의 신뢰성이나 유효성에 영향을 미치는 사유가 발생한 사실을 인지하는 경우 해당 사실을 카카오뱅크 홈페이지 또는 앱에

즉시 공고하며, 해당 전자서명생성정보로 발급한 가입자 인증서를 폐지하고 이를 가입자에게 통보합니다. 또한, 본인확인업무의 신뢰성·유효성을 확보할 수 있는 대책을 강구합니다.

1.3.2 등록대행기관

카카오뱅크는 인증서 발급, 신원확인 업무를 등록대행기관에 위임하지 않고 직접 수행합니다.

1.3.3 가입자

가입자는 본인확인서비스 가입을 위해 전자서명생성정보에 대하여 카카오뱅크로부터 전자서명인증을 받은 자를 말합니다.

1.3.3.1 정확한 정보제공

가입자는 다음 사항에 대하여는 정확한 정보를 카카오뱅크에 제공하여야 합니다. 또한 카카오뱅크가 신원확인을 위하여 관련 서류를 요청하는 경우 가입자는 성실히 협조하여야 합니다.
- 인증서의 발급/재발급 신청
- 인증서의 폐지 신청

1.3.3.2 인증서의 합목적적 사용

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

1.3.3.3 전자서명생성정보의 보호

가입자는 신뢰할 수 있는 소프트웨어나 하드웨어를 이용하여 전자서명정보를 생성하며, 생성된 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 보관·관리하여야 합니다. 가입자의 전자서명생성정보 보호의무 위반으로 인한 결과의 책임은 전적으로 가입자에게 있습니다.

1.3.3.4 전자서명생성정보 안전조치

가입자는 전자서명생성정보가 분실·훼손 또는 도난·유출되었거나 안전하지 않다고 인지하는 경우 지체 없이 카카오뱅크에 관련사실을 통보하여 인증서를 폐지할 수 있도록 협조하여야 합니다.

1.3.3.5 카카오뱅크의 면책보장

가입자는 인증서 사용과 공개에 있어 다음의 사유로 인하여 발생되는 모든 책임과 비용에 대하여는 카카오뱅크의 면책을 보장합니다.
- 가입자가 사실과 다르게 제공한 정보
- 가입자가 태만 또는 고의로 제공하지 않은 변경된 정보
- 가입자의 전자서명생성정보 관리 부주의(정보 노출, 분실, 변조 등)

1.3.3.6 배상책임

가입자는 인증서 사용과 관련하여 가입자의 고의 또는 과실로 카카오뱅크 또는 이용자에게 손해를 입힌 경우 그 손해를 배상해야 합니다.

1.3.4 이용자(이용기관)

이용자란 전자서명인증사업자가 제공하는 본인확인서비스를 이용하는 자를 말합니다.

1.3.4.1 이용자의 책임과 의무

1. 인증서의 용도 내 사용
이용자는 카카오뱅크가 가입자에게 발급한 인증서의 이용 목적 및 이용가능 범위(제한 포함)를 확인 및 이해해야 하며, 이용자의 과실로 인한 손해는 이용자가 책임져야 합니다.

2. 인증서의 유효성 확인
이용자는 인증서 기재사항 등에 의하여 전자서명의 진위여부를 확인하기 위하여 다음의 조치를 취해야 합니다.
- 인증서 유효 여부의 확인
- 인증서의 만료 또는 폐지 여부의 확인
- 인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항의 확인

3. 배상책임

이용자는 인증서 사용과 관련하여 이용자의 고의 또는 과실로 카카오뱅크 또는 가입자에게 손해를 입힌 경우 카카오뱅크 또는 가입자에게 그 손해를 배상해야 합니다. 상세한 내용은 "9. 본인확인업무 보증 등 기타사항"에 고시합니다.

1.3.5 방송통신위원회

방송통신위원회는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제23조의3 및 같은 법 시행령(이하 "영"이라 한다) 제9조의3부터 제9조의5까지의 본인확인기관의 지정에 필요한 세부심사기준 및 평가방법과 본인확인업무의 휴지 또는 폐지의 통보 및 신고의 절차를 운영하고, 심사위원을 구성하여 본인확인기관에 대해 심사를 수행합니다.

1.4 인증서 종류(인증서 종류 및 유효기간)

1.4.1 인증서 이용범위 및 용도

카카오뱅크는 개인을 대상으로 신원확인 후 인증서를 발급합니다.

1. 용도
본인확인서비스 및 전자서명이 필요한 일반 전자거래 및 전자계약 업무
- 금융기관이 제공하는 서비스 이용
- 정부민원 및 공공기관이 제공하는 서비스 이용
- 기타 이용기관이 제공하는 서비스 이용
※ 단, 카카오뱅크와 본인확인서비스 이용 계약이 된 이용기관에서만 사용 가능

2. 유효기간: 발급일로부터 3년

1.4.2 인증서 이용제한

가입자에게 발급한 인증서는 발급 시의 이용범위 또는 용도 내에서만 이용 가능하며, 누구든지 인증서를 이용범위 또는 용도에 벗어나 부정하게 사용할 수 없습니다. 또한 유효기간이 만료 또는 폐지된 인증서를 사용하여서는 안됩니다.

1.5 준칙의 관리

1.5.1 준칙의 관리조직

카카오뱅크 본인확인업무 관리조직은 준칙에 대한 수립 및 개정업무 등의 관리업무를 수행합니다.

1.5.2 준칙의 담당부서

카카오뱅크의 인증업무에 대한 담당부서 연락처는 다음과 같습니다.

- 관리부서 : 카카오뱅크 고객인증캠프 인증사업팀
- 전자우편 : auth@kakaobank.com
- 주소 : 경기도 성남시 분당구 분당내곡로 131, 판교테크원 11층
- 전화 : 1599-3333

1.5.3 준칙 개정 관리

카카오뱅크의 인증정책 담당자가 준칙의 변경이 필요하다고 판단한 경우 인증업무 책임자의 승인을 받아 이를 개정할 수 있습니다. 또한 카카오뱅크 준칙이 제·개정된 경우 아래 항목을 포함한 준칙의 제·개정 관련 기록을 유지·관리 하여야 합니다.

- 준칙의 버전
- 적용 업무 및 범위의 개요
- 준칙의 제·개정 기록 (기존 준칙의 규정, 제·개정 내용 및 사유 등)

1.5.4 준칙의 승인 절차

카카오뱅크는 개정된 준칙을 카카오뱅크 홈페이지에 즉시 공고합니다. 변경된 준칙의 공고일을 포함하여 공고 후 30일 내에 서면으로 이의를 제기하지 아니한 경우 카카오뱅크는 가입자 및 이용자가 변경된 준칙에 동의한 것으로 봅니다.

1.6 정의 및 약어

1.6.1.1 법 용어 정의

본 준칙에서 사용되는 주요 용어들은 전자서명법 및 그 하위 법령, 본인확인기관 지정 등에 관한 기준에 정의되어 있습니다.

1. 전자문서: 정보처리시스템에 의하여 전자적 형태로 작성 · 변환되거나 송신 · 수신 또는 저장된 정보를 말합니다.
2. 전자서명: 다음 각 목의 사항을 나타내는 데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말합니다.
  가. 서명자의 신원
  나. 서명자가 해당 전자문서에 서명하였다는 사실
3. 전자서명생성정보: 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말합니다.
4. 전자서명수단: 전자서명을 하기 위하여 이용하는 전자적 수단을 말합니다.
5. 전자서명인증: 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말합니다.
6. 인증서: 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보로서, 본 준칙에서는 카카오뱅크가 발급하는 인증서를 말합니다.
7. 전자서명인증업무: 전자서명인증, 전자서명인증 관련 기록의 관리 등 전자서명인증서비스를 제공하는 업무를 말합니다.
8. 전자서명인증사업자: 전자서명인증업무를 하는 자를 말합니다.
9. 가입자: 전자서명생성정보에 대하여 전자서명인증사업자로부터 전자서명인증을 받은 자를 말합니다. 본 준칙에서는 카카오뱅크 인증서를 발급받은 자를 말합니다.
10. 본인확인기관: 가입자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하는 자로서 법 제23조의3제1항에 따라 방송통신위원회로부터 본인확인기관의 지정을 받은 자를 말합니다.
11. 본인확인입력정보: 본인확인을 위하여 가입자에게 발급된 대체수단(본 준칙에서는 카카오뱅크 인증서) 및 가입자가 입력하는 부가정보(인증 비밀번호 등)를 말합니다.
12. 본인확인서비스: 본인확인입력정보를 이용하여 가입자를 안전하게 식별 · 인증하기 위해 본인확인기관이 제공하는 서비스를 말하며, 본 준칙에서는 전자서명인증을 통해 가입자를 안전하게 식별 · 인증하는 것을 말합니다.

1.6.1.2 준칙 용어의 정의

본 준칙을 위하여 다음과 같이 용어를 정의합니다.

1. 카카오뱅크 인증서비스: 카카오뱅크가 제공하는 본인확인서비스를 말합니다.
2. 이용자: 본인확인기관이 제공하는 본인확인서비스를 이용하는 자를 말합니다.
3. 본인확인업무: 본인확인서비스를 위해 수행하는 전자서명인증업무를 말합니다.

4. 실명 가입자: 카카오뱅크가 금융실명거래 및 비밀보장에 관한 법률 제2조제4호에 따른 실지명의를 확인한 가입자를 말합니다.
5. 인증서 폐기: 인증서 폐지와 동일한 표현입니다.
6. 사용자관리번호: 가입자를 식별하기 위하여 카카오뱅크에서 랜덤하게 부여한 식별자를 말합니다.
7. 인증기관 인증서 폐지목록(Authority Revocation List, ARL): 인증기관의 인증서 폐지목록을 말합니다.
8. 가입자 인증서 폐지목록(Certificate Revocation List, CRL): 가입자의 인증서 폐지목록을 말합니다.
9. 객체식별자(Object Identifier, OID): 인증서 내에는 버전, 발급자 고유명, 가입자 고유명, 공개키 등 기본정보 외에 알고리즘, 인증서 정책, 키용도, 인증서 속성 등이 포함되며, 정보들이 표현하는 대상을 객체 (Object)라 합니다. 이러한 객체들을 유일하게 중복되지 않고 식별하기 위해서는 각 객체에 고유번호를 부여하는 방법이 사용되며, 이것을 객체식별자라 합니다.
10. 고유명(Distinguished Name, DN): 가입자 객체를 명확히 구별할 수 있도록 부여하는 고유한 이름으로 , 유일한 인증서를 소유하는것을 식별하기 위한 표준화된 식별 명칭을 말합니다.
11. 인증서 발급 신청서(Certification Request Syntax, CSR): 인증서 발급 신청자가 인증서 발급 신청을 위해 생성하는 정보로서 인증서 발급 신청자의 고유명(DN), 전자서명검증정보, 전자서명으로 구성 되어 있습니다.
12. 인증 비밀번호: 가입자가 등록한 6자리 숫자로 구성된 비밀번호(PIN)를 말합니다.
11. 기기인증정보: 가입자 소유의 실지명의 확인 후 등록된 기기임을 증명하는 정보를 말합니다.
12. 온라인 신원확인: 실명 가입자에 대해 정보통신망을 통하여 신원을 확인하는 방법을 말합니다.

2. 본인확인업무관련 정보의 공고

2.1 공고 설비

1. 본 준칙을 포함하여 본인확인서비스에 필요한 내용은 카카오뱅크 홈페이지를 통해 관리합니다.
2. 카카오뱅크는 본인확인업무와 관련된 정보를 적시에 정확하게 제공하기 위해 공고 설비를 안전하게 운영하고 관리합니다.
3. 카카오뱅크의 본인확인업무와 관련된 책임사항은 본 준칙 1.3.1.2 에 명시되어 있습니다.

2.2 주요정보 공고위치

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

- 준칙: https://www.kakaobank.com/Corp/Policy/Cert/CertCps

- 이용약관: https://www.kakaobank.com/Corp/Policy/Cert/CertTerms
- 개인정보처리방침 : https://www.kakaobank.com/Corp/Policy/Cert/CertPmp
- 가입자 인증서 폐지목록(CRL): http://crl.kakaobank.com/user
- 인증기관 인증서 폐지목록(ARL): http://arl.kakaobank.com/rca2_arl.crl
- 인증서 유효성 확인 서비스(OCSP): http://ocsp.kakaobank.com/

2.3 공고 주기

1. 카카오뱅크는 준칙의 개정일로부터 7일 이내에 개정된 준칙을 홈페이지에 게시합니다.
2. 가입자 인증서 폐지목록(CRL)은 24시간을 주기로 갱신·공고 합니다.
3. 인증기관 인증서 폐지목록(ARL)은 3개월을 주기로 갱신·공고 합니다.

위 주기는 변경될 수 있으며, 변경이 발생하는 경우 해당 사실을 카카오뱅크 홈페이지에 공고합니다.

2.4 공고된 정보에 대한 책임

카카오뱅크는 준칙 및 이용약관 등에 관련된 정보를 누구든지 그 사실을 홈페이지에서 항상 확인할 수 있도록 게시하고, 기밀정보가 공개되거나 변경되지 않도록 보호해야 합니다.

3. 신원확인

3.1 가입자 이름 표기 방법

3.1.1 명칭의 종류

인증서는 고유명(DN)으로 서로 구분 될 수 있습니다. 고유명(DN)은 가입자의 실명과 가입자의 식별정보를 포함하고 있습니다. 가입자의 식별정보는 카카오뱅크의 생성 규칙에 유일하게 부여되고 있습니다.
인증서의 고유명(DN)의 구성방식은 국제 표준 규격(X.509)을 준용 합니다.

- CN=가입자 실명(사용자관리번호)
- O=KakaoBank CA Class 2
- OU=개인
- C=KR

3.1.2 유의미한 명칭의 필요성

인증서 내의 고유명(DN)에는 가입자의 실명이름을 사용합니다.

3.1.3 가입자를 식별할 수 없는 익명성 또는 가명성

카카오뱅크는 익명이나 가명 인증서를 발급하지 않습니다

3.1.4 다양한 명칭 해석 규정

카카오뱅크는 인증서 내 고유명(DN)은 X.500 표준 및 ASN.1 구문을 사용합니다.

3.1.5 명칭의 고유성

인증서는 고유명(DN)으로 서로 구분 될 수 있습니다. 고유명(DN) 내 가입자의 실명과 가입자를 식별할 수 있는 식별정보를 포함하고 있습니다.

3.1.6 상표의 인식, 인증 및 역할

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

3.2 인증서 발급 시 신원확인

3.2.1 전자서명생성정보의 소유 증명 방법

인증서 발급을 위해서는 카카오뱅크에 PKCS#10 형식의 인증서 서명 요청(Certificate Signing Request) 또는 이와 암호학적으로 동등한 수준의 증거를 제공하여 전자서명생성정보(개인키)의 소유권을 증명해야 합니다.

3.2.2 기관 신원확인

카카오뱅크에서는 기관에게 인증서를 발급하지 않습니다.

3.2.3 신규발급 시 신원확인

카카오뱅크는 가입신청자의 신원을 확인합니다. 또한, 인증서를 발급하기 전에 인증서의 이용범위, 전자서명의 효력, 가입자 전자서명생성정보 및 인증서의 생성·보관 등에 관한 이용약관을 앱 을 통해 안내하고 이에 대한 동의 절차를 거칩니다.

3.2.3.1 대면에 준하는 비대면 신원확인에 의한 발급

카카오뱅크는 금융위원회의 「비대면 실명확인 가이드라인」에 의해 대면에 준하는 비대면 실명확인 방법으로 가입신청자의 신원을 확인할 수 있습니다.
다만, 카카오뱅크 실명 가입자에 대해서는 '온라인 신원확인'에 의하여 신원을 확인할 수 있으며, '온라인 신원확인'은 아래 사항을 확인함으로써 수행합니다.
- 전자금융거래 가입자의 계정(ID)과 로그인 인증 수단(패턴 또는 생체) 또는 계좌번호와 그 비밀번호
- 전자금융거래 가입자의 고유식별정보(주민등록번호 또는 CI(연계정보))
- 카카오뱅크가 전자금융거래를 위하여 가입자에게 제공한 일회용비밀번호 또는 가입자 본인만이 알 수 있거나 소유하고 있는 두 가지 이상의 정보(인증 비밀번호, 기기인증정보 등)
- 기타 전자금융거래 가입자의 신원을 확인할 수 있는 정보(예 : 휴대폰 본인확인 등)

3.2.3.2 접근매체(인증서)에 의한 대체발급

가입신청자가 카카오뱅크 전자금융거래 기본약관 제2조제1항제6호에 따른 접근매체(인증서)를 보유한 경우 전자금융거래법 시행령 제6조에 따라 해당 인증서에 의해 생성된 전자서명을 통해 해당 인증서를 카카오뱅크 인증서로 대체발급 신청할 수 있습니다.

3.2.3.3 기타 신원확인에 의한 발급

가입신청자가 상기 신원확인을 수행할 수 없을 경우, 카카오뱅크 고객센터 창구를 통해 신원확인을 수행할 수 있고, 이 과정에서 가입신청자의 실명확인증표 외 법정 대리인의 서류가 필요할 수 있습니다.
- 가입신청자의 실명확인증표 : 주민등록증, 운전면허증, 여권 및 여권정보증명서(여권에 주민등록번호가 없는 경우, 3개월 내 발급분)
- 법정 대리인의 서류 : 법정대리인 동의서, 법정 대리인의 실명확인증표, 가입신청자 기준 기본증명서 및 가족관계증명원(3개월 내 발급분)

3.2.4 미확인 가입자 정보

카카오뱅크는 가입자 정보가 확인되지 않은 경우 인증서를 발급하지 않습니다.

3.2.5 권한 검증

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

3.2.6 상호운영 기준

해당 사항 없습니다.

3.3 인증서 갱신발급, 재발급 및 변경 시 신원확인

3.3.1 갱신발급에 대한 신원확인 및 인증

갱신 대상 인증서의 전자서명으로 신원확인 및 인증을 수행합니다.

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

3.2 인증서 신규 발급 시 신원확인과 동일합니다.

3.4 인증서 폐지 시 신원확인

인증서 폐지는 가입자가 카카오뱅크 앱을 통해 직접 폐지 신청할 수 있으며, 가입자 인증 수단 검증이 성공적으로 수행될 경우 폐지 처리가 완료됩니다. 부득이하게 카카오뱅크 앱을 통한 폐지 신청이 불가능한 경우에는 카카오뱅크 고객센터(1599-3333)으로 폐지 신청이 가능합니다. 이때 카카오뱅크는 사전에 등록된 두가지 이상의 개인정보를 확인하는 등 신뢰할 수 있는 방법을 통하여 신원확인을 합니다.

4. 인증서 관리

4.1 인증서 발급 신청

4.1.1 인증서 신청 절차

가입신청자가 카카오뱅크 앱을 이용해 인증서 발급 요청 기능을 실행함으로써 발급 신청 처리가 시작됩니다. 신청 절차는 다음과 같습니다.

1. 이용약관 동의 및 신원확인 (신원확인 절차는 "3.2.3 신규발급 시 신원확인" 항목을 참조합니다.)
2. 키 쌍(개인키(전자서명생성정보)와 공개키(전자서명검증정보)) 생성
3. 키 쌍의 공개키(전자서명검증정보)를 포함한 인증서 발급 신청서(CSR) 생성 및 제출

4.2 인증서 발급 신청 처리

4.2.1 신원확인 및 인증 수행

카카오뱅크는 가입신청자의 신원확인을 마친 후 가입신청자가 제출한 전자서명검증정보의 유일성과 정보의 합치여부를 확인하여 전자서명생성정보의 소유자가 가입신청자 본인임을 확인하고 인증서 발급 신청에 대해 승인합니다.

4.2.2 인증서 발급 신청 승인 및 거절

다음에 해당하는 경우 발급이 제한될 수 있습니다.

1. 본인의 명의가 아닌 제3자의 명의로 신청한 경우
2. 카카오뱅크가 정한 절차를 완료하지 못한 경우
3. 신청시 제공한 정보에 허위, 누락이나 오류가 있거나 카카오뱅크가 요구하는 기준을 충족하지 못하는 경우
4. 서비스를 이용할 수 없는 모바일 디바이스 환경에 해당하는 경우
5. 법정대리인(친권, 미성년후견, 성년후견, 한정후견)의 동의가 필요한 신청인임에도 법정대리인의 동의 없이 가입하려는 경우
6. 그 외 부정한 방법으로 가입자 인증서를 발급한 사실이 드러나거나 본 항 각 호의 사유가 있는 것으로 의심되는 경우

7. 기타 가입신청자의 귀책사유로 인하여 승낙이 불가능하거나 해당 신청이 법령, 서비스 약관 및 기타 카카오뱅크가 정한 제반 사항에 배치되는 경우

4.2.3 인증서 신청 처리 소요시간

가입신청자의 발급 신청은 가입신청자가 필요한 절차를 완료한 즉시 처리됩니다.

4.3 인증서 발급 절차 및 보호 조치

4.3.1 인증서 발급 절차

인증서 발급신청을 받은 카카오뱅크는 인증서를 발급하기 전에 인증서 발급신청 내용에 대해 다음의 검증을 실시함으로써 전자서명생성정보가 가입자에게 유일하게 속함을 확인합니다.
가. 인증서 발급 신청서(CSR), 등록정보 등을 포함한 가입신청 전문 위변조 확인
나. 가입자가 제출한 인증서 발급 신청서(CSR) 내의 전자서명검증정보의 유일성 확인
 - 카카오뱅크가 발급한 유효한 인증서 중에 동일한 전자서명검증정보가 없음을 확인
다. 가입자가 제출한 전자서명검증정보에 합치하는 전자서명생성정보의 소유 여부 확인

카카오뱅크는 인증서 발급신청 내용에 대한 검증 후, 가입자에게 다음의 사항이 포함된 인증서를 발급 및 전송합니다.
- 일련번호
- 가입자 정보(실명 및 가입자 식별정보)
- 발급자 정보 (인증기관의 고유명(DN))
- 전자서명 알고리즘
- 전자서명검증정보(공개키)
- 인증서의 유효기간
- 인증서의 이용범위 또는 용도를 제한하는 경우에 이에 관한 사항 등

카카오뱅크가 발급하는 인증서는 고유명(DN)으로 서로 구분될 수 있습니다. 카카오뱅크는 인증서 신청등록 시 가입자가 등록한 명칭으로 인증서, 인증서 내의 기본영역에 사용될 명칭을 구성하며, 해당 명칭의 구성방식은 국내외 표준을 따릅니다. 가입자가 신청등록 시 등록 가능한 명칭은 실명을 원칙으로 합니다.

4.3.2 인증서 발급 사실 공지

인증서가 가입자에게 전달되면 휴대폰 문자메시지 또는 카카오 알림톡을 통해 가입자에게 발급사실을 알립니다.

4.4 인증서 수령

4.4.1 인증서 수령 절차

가입자는 카카오뱅크 앱을 통해 발급 된 인증서를 수령한 후 안전하게 저장합니다.

4.4.2 인증기관의 인증서 공개

최상위 인증기관과 인증기관의 인증서는 홈페이지에 게시합니다.
- RootCA 인증서: http://cert.kakaobank.com/cert/rca2.der
- CA 인증서: http://cert.kakaobank.com/cert/ca2.der

4.4.3 다른 개인 또는 법인에 인증서 발급 공지

해당 사항이 없습니다.

4.5 인증서 이용

4.5.1 가입자 전자서명생성정보(개인키) 및 인증서 사용

- 카카오뱅크가 발급하는 가입자 인증서는 인증서를 필요로 하는 전자거래의 모든 분야에서 사용 가능합니다.
- 인증서의 유효기간은 3년입니다. 가입자는 정당한 이용범위 및 용도에 맞게 인증서를 사용해야 하며, 인증서를 사용하여 전자서명을 제공할 때에는 해당 인증서에 포함된 전자서명검증정보에 합치하는 전자서명생성정보를 사용해야 합니다.
- 가입자는 신뢰할 수 있는 소프트웨어나 하드웨어를 이용하여 전자서명생성정보를 생성하며, 생성된 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 보관·관리해야 합니다.
- 가입자 전자서명생성정보는 가입자 인증서가 발행되어 가입자가 수령한 후부터 사용 가능합니다. 가입자 인증서가 만료되거나 폐지된 후에는 전자서명생성정보의 사용을 중단해야 합니다.
- 가입자는 전자서명생성정보가 분실·훼손 또는 도난·유출되었거나 안전하지 않다고 인지하는 경우, 지체 없이 카카오뱅크에 관련사실을 통보하여 카카오뱅크가 해당 인증서를 폐지할 수 있도록 협조해야 합니다.

4.5.2 이용자의 공개키와 인증서 이용

- 이용자는 본 준칙에서 명시한 인증 체계 및 어플리케이션에서 인증서 내 확장필드에 정의된 용도로 전자서명검증정보를 사용할 수 있습니다.
- 이용자는 본 준칙 및 이용약관에 명시한 인증서의 이용범위, 용도, 유효기간 등 인증서 이용시 유의하여야 할 사항을 확인할 수 있습니다.

4.6 인증서 갱신 발급

4.6.1 인증서 갱신 기준

카카오뱅크 앱 내 유효한 인증서가 있는 상태에서, 가입자는 인증서 만료일 60일 전부터 만료일 까지 동일한 종류의 인증서에 대한 유효기간 갱신을 신청할 수 있습니다.

4.6.2 인증서 갱신 신청자

인증서 갱신 기준에 해당하는 가입자만이 인증서 갱신을 신청할 수 있습니다.

4.6.3 인증서 갱신 신청 절차

가입자는 인증서 갱신 대상이 되었을 때 카카오뱅크 앱 내 인증서 갱신 요청 기능을 실행함으로써 인증서 갱신 신청을 할 수 있으며, 신청 절차는 다음과 같습니다.

1. 이용약관 동의
2. 갱신 대상 인증서 소유자 인증(전자서명생성정보 활성화를 위한 인증 비밀번호 입력 등)
3. 기존 키 쌍의 공개키(전자서명검증정보)를 포함 한 인증서 발급 신청서(CSR) 생성 및 제출

카카오뱅크는 인증서 갱신 신청서의 전자서명을 검증 하고, 인증서 신청서 내 공개키와 갱신 대상 인증서의 공개키가 동일하면, 유효기간이 갱신된 인증서를 발급하고, 기존 인증서는 폐지합니다.

4.6.4 인증서 갱신 발급 공지

인증서가 가입자에게 전달되면 휴대폰 문자메시지 또는 카카오 알림톡을 통해 가입자에게 갱신 사실을 알립니다.

4.6.5 인증서 갱신 수락 행위

“4.4.1 인증서 수령 절차" 항목을 참조합니다.

4.6.6 갱신된 인증서 공고

"4.4.2 인증기관의 인증서 공개" 항목을 참조합니다.

4.6.7 다른 개인 및 법인에 인증서 갱신 공지

해당 사항이 없습니다.

4.7 인증서 재발급

4.7.1 인증서 재발급 기준

가입자당 1개의 인증서 발급을 원칙으로 하며, 카카오뱅크 앱 내 유효한 인증서가 있는 상태에서 앱 재설치, 기기변경, 가입자의 키손상 및 인증서 개인키 유출 등을 통해 인증서 발급을 신청을 하는 경우 재발급으로 처리 됩니다.

4.7.2 인증서 재발급 신청자

인증서 재발급 기준에 해당하는 가입자만이 인증서 재발급을 신청할 수 있습니다.

4.7.3 인증서 재발급 신청 절차

"4.1.1 인증서 신청 절차", "4.2 인증서 발급 신청 처리" 항목을 참조합니다.
재발급 처리 시 기존 인증서가 폐지되고 신규 인증서가 발급됩니다.

4.7.4 가입자에게 인증서 재발급 공지

인증서가 가입자에게 전달되면 휴대폰 문자메시지 또는 카카오 알림톡을 통해 가입자에게 재발급사실을 알립니다.

4.7.5 인증서 재발급 수락 행위

"4.4.1 인증서 수령 절차" 항목을 참조합니다.

4.7.6 발급된 인증서 공고

"4.4.2 인증기관의 인증서 공개" 항목을 참조합니다.

4.7.7 다른 개인 및 법인에 인증서 발급 공지

해당 사항이 없습니다.

4.8 인증서 변경

4.8.1 인증서 변경 기준

인증서 변경 기능은 별도로 제공되지 않으며, 가입자 정보가 변경되는 경우에는 인증서 재발급을 통해 기존 인증서를 폐지하고 신규 인증서를 발급받을 수 있습니다.

4.8.2 인증서 변경 신청

해당 사항이 없습니다.

4.8.3 인증서 변경 수정 절차

해당 사항이 없습니다.

4.8.4 가입자에게 인증서 변경 공지

해당 사항이 없습니다.

4.8.5 인증서 변경 수락 행위

해당 사항이 없습니다.

4.8.6 변경된 인증서 공고

해당 사항이 없습니다.

4.8.7 다른 개인 또는 법인에 인증서 변경 공지

해당 사항이 없습니다.

4.9 인증서 효력 정지, 효력 회복, 폐지

인증서 효력 정지, 효력 회복 기능은 제공하지 않습니다. 인증서 폐지는 인증서 유효기간 만료 전에 가입자의 신청 또는 카카오뱅크 인증업무 수행의 안전성, 보안성, 신뢰성 등을 위한 부득이한 사유로 인해 인증서의 효력을 영구히 종료하는 것을 말합니다. 가입자의 인증서를 폐지시키는 경우, 인증서의 유효기간에 상관없이 그 효력이 즉시 상실됩니다.

4.9.1 가입자 인증서 폐지 사유

카카오뱅크는 다음의 사유가 발생한 경우 해당 인증서를 폐지합니다.

- 가입자가 인증서의 폐지를 신청한 경우
- 가입자의 사망·실종선고 사실을 인지한 경우
- 가입자가 개명 또는 주민등록번호 변경을 한 경우
- 가입자가 카카오뱅크를 탈퇴한 경우
- 가입자가 부정한 방법으로 인증서를 발급받은 사실 또는 이용한 사실을 인지하였거나, 그 가능성을 객관적으로 인지한 경우
- 가입자 또는 인증기관의 전자서명생성정보가 분실·훼손 또는 도난·유출되었거나 그렇다고 의심되는 경우
- 가입자가 본 준칙의 주요 의무나 주요 사항을 준수하지 않은 경우
- 기타 인증서 서비스 방식이 변경 되어 기존 방식을 지원하지 못하게 되는 경우 등

4.9.2 인증서 폐지 신청자

가입자는 인증서를 폐지하는 경우 본인이 직접 신청하여야 합니다.

4.9.2.1 분실신고 접수 시 처리

카카오뱅크는 인증서를 카카오뱅크 앱에 저장하므로, 휴대폰 분실 시 가입자 본인이 고객센터를 통해 신고를 할 수 있으며, 신고가 접수된 경우 카카오뱅크 앱의 거래를 제한하거나, 인증서 폐지를 수행할 수 있습니다.

4.9.2.2 강제 폐지에 따른 공지

카카오뱅크는 "4.9.1 가입자 인증서 폐지 사유" 에 따라 가입자의 동의 없이 인증서를 폐지한 경우 해당 가입자에게 휴대폰 문자메시지 또는 카카오 알림톡을 이용하여 해당 사실을 통지합니다.

4.9.3 인증서 폐지 절차

1. 가입자의 신청에 따른 폐지
가입자는 카카오뱅크 앱내의 인증서 폐지 버튼을 눌러 폐지 합니다. 이때, 가입자의 전자서명을 통해 신원을 확인 한 후 인증서를 폐지 합니다.
2. 고객센터를 통한 폐지
가입자는 카카오뱅크 고객센터를 통해 인증서 폐지 신청을 합니다. 이때, 카카오뱅크 고객센터는 가입자 본인만이 아는 2 가지 정보 이상을 확인하여 신청자의 신원을 확인 후에 가입자의 인증서를 폐지합니다.
3. 카카오뱅크 직권에 따른 폐지
카카오뱅크가 아래 사항을 확인한 경우 직권에 따라 가입자의 인증서를 폐지 합니다.
  - 가입자가 부정한 방법으로 인증서를 발급받은 사실 또는 이용한 사실을 인지하였거나, 그 가능성을 객관적으로 인지한 경우
  - 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출된 경우
  - 가입자가 본 준칙의 주요 의무나 주요 사항을 준수하지 않은 경우

4.9.4 인증서 폐지 요청 유예 기간

개인키 손실 또는 침해가 의심되는 직후 즉시 인증서 폐지 신청을 해야 합니다. 이외 요인에 대해서는 가능한 빨리 폐지 신청을 해야 합니다.

4.9.5 인증서 폐지 요청 처리 시간

카카오뱅크는 신청자의 신원을 확인한 후 즉시 인증서의 폐지 처리를 완료합니다.

4.9.6 인증서 폐지 확인 요구사항

이용자는 인증서를 신뢰하기 전에 인증서 경로 검증을 통해 인증서의 유효성을 확인해야하고, 각 계층의 인증서가 폐지 되었는지 확인해야 합니다.
이용자는 인증서 폐지 여부 조회 방법으로 인증서 폐지목록(CRL 및 ARL) 또는 인증서 유효성 확인 서비스(OCSP) 응답 또는 카카오뱅크와 계약된 별도 방법을 사용할 수 있습니다.

4.9.7 인증서 폐지목록의 갱신과 공고

카카오뱅크는 가입자 인증서의 폐지 결과를 반영하여 24시간 주기로 CRL을 갱신하고, 갱신 즉시 카카오뱅크 공고설비에 공고합니다.

- 가입자 인증서 폐지목록(CRL) : http://crl.kakaobank.com/user
- 인증기관 인증서 폐지목록(ARL) : http://arl.kakaobank.com/rca2_arl.crl

4.9.8 인증서 폐지목록 발행 최대 소요 시간

인증서폐지목록(CRL) 생성 후 영업일 기준 24시간 이내 공고설비에 게시됩니다.

4.9.9 온라인 인증서의 폐지 상태 확인

인증서 유효성 확인 서비스(OCSP)를 사용합니다.

4.9.10 온라인 인증서의 폐지 확인 요건

OCSP 응답 메시지는 실시간으로 갱신되며 유효기간은 지정되어 있지 않습니다. 또한 OCSP 응답 메시지 관련 모든 필드는 RFC 6960을 준용합니다

4.9.11 그 외 인증서 폐지 알림 수단

인증서 폐지 시 휴대폰 문자메시지 또는 카카오 알림톡을 통해 가입자에게 인증서 폐지사실을 알립니다.

4.9.12 키 교체 또는 키 손상의 특수 요구 사항

해당 사항 없습니다.

4.9.13 인증서 효력 정지 기준

해당 사항 없습니다.

4.9.14 인증서 효력 정지 대상

해당 사항 없습니다.

4.9.15 인증서 효력 정지 절차

해당 사항 없습니다.

4.9.16인증서 효력 정지 기간

해당 사항 없습니다.

4.10 인증서 유효성 확인 서비스(OCSP)

인증서 유효성 확인 서비스(OCSP)란 가입자의 인증서의 이용 가능 상태를 확인하는 서비스입니다.
가입자가 이용자의 서비스에 접속하여 자신의 인증서를 제출하면 이용자는 인증서 일련번호를 카카오뱅크 OCSP(Online Certificate Status Protocol) 시스템에 전송, 카카오뱅크는 가입자가 제출한 인증서의 유효성을 실시간으로 검증하여 검증결과를 이용자에 회신합니다.

4.10.1 서비스 운영 특징

카카오뱅크는 인증서 유효성 확인 서비스(OCSP)를 제공받고자 하는 경우 이용자의 요청에 의해 서비스를 제공 할 수 있습니다.

4.10.2 서비스 가용성

유지보수 및 서비스 장애로 인하여 일시적으로 사용할 수 없는 경우를 제외하고 인증서 상태 서비스를 연중무휴로 제공합니다.

4.10.3 서비스 운영 기능 및 기타사항

해당 사항 없습니다.

4.11 서비스 가입 철회

가입자는 서비스 가입 철회를 원할 경우 인증서를 폐지 및 삭제 하거나 카카오뱅크를 탈퇴하여 서비스 이용을 중단할 수 있습니다. 이 경우 가입자의 개인정보는 "5.5.2 보존 기록 보관 기간"에 준하여 처리 됩니다.

4.12 기타 부가 서비스

기타 부가 서비스를 지원하지 않습니다.

4.12.1 키 위탁 및 복구 정책 및 실행

해당 사항 없습니다.

4.12.2 세션 키 캡슐화 및 복구 정책 및 실행

해당 사항 없습니다.

5. 시설 및 운영관리

5.1 물리적 보호조치

5.1.1 인증시스템 운영실의 격실 분리에 관한 사항

카카오뱅크는 다음의 인증시스템을 별도의 운영실로 분리합니다.

1. 최상위 인증기관 전자서명생성정보, 인증기관 인증서 발급 기능을 제공하는 시스템
2. 가입자정보 관리 기능을 제공하는 시스템, 인증기관 전자서명키 관리, 가입자 인증서 생성·발급 기능을 제공하는 시스템
3. 인증서 공고 기능을 제공하는 시스템, 인증서 상태확인 기능을 제공하는 시스템

5.1.2 물리적 접근 통제

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

1. 카카오뱅크는 외부인의 침입이나 불법적 접근 등의 물리적 위협으로부터 본인확인업무 시스템을 안전하게 보호합니다.
2. 카카오뱅크는 본인확인업무 시스템을 통제구역 내에 설치하여 운영하고, 허가된 사용자에게만 물리적인 접근을 허용합니다.
3. 카카오뱅크의 출입통제 시스템은 금속탐지기, 신원확인카드, 생체인증 등을 다중으로 결합하여 통제구역에 대한 접근을 통제합니다.
4. 카카오뱅크는 CCTV 및 모니터링 시스템을 설치하여 이상상황을 항상 감시하고 통제합니다.

5.1.3 수해 방지

카카오뱅크는 침수로부터 본인확인업무 시스템을 안전하게 보호하기 위해 외벽과 바닥으로부터 이격설치 되었으며, 누수 감지 및 신속한 대처를 위한 누수감지기를 설치하고 있습니다.

5.1.4 화재 예방

카카오뱅크는 화재로부터 본인확인업무 시스템을 안전하게 보호하기 위해 감지설비, 경보설비, 자동 소화설비 등을 설치하고 있습니다.

5.1.5 정전 방지

카카오뱅크는 정전으로부터 본인확인업무 시스템을 안전하게 보호하기 위해 전원공급을 이중화하고, 무정전 전원장치(UPS), 자가발전기를 설치하여 전원을 안정적으로 공급하고 있습니다.

5.1.6 방호

본인확인업무 시스템이 운영되는 시스템실의 외벽은 본인확인업무의 제공에 필수적으로 요구되는 인증시스템을 외부 침입으로부터 보호할 수 있도록 설계합니다.
1. 외벽 재질은 벽돌 또는 철근 콘크리트로 축조되어 있거나, 철골구조물에 3T 이상의 철판으로 용접
2. 외벽은 천장, 바닥까지 완벽하게 마감

3. 인증시스템과 타 시스템을 분리할 수 있도록 시스템실내 케이지 설계

5.1.7 항온 항습, 통풍

카카오뱅크는 본인확인업무 시스템이 운영되는 시스템실의 항온을 위해 냉방기기를 이중화하여 설치하였고, 항습은 해당층의 공조기를 통해 자동조절되며, 통풍창은 사람이 통과할 수 있는 경우 차폐막을 설치하고 있습니다. 온습도 이상감지를 위해 온습도센서를 설치하였고, 비상대응을 위한 별도의 항온항습기를 설치하고 있습니다.

5.1.8 매체 저장

카카오뱅크는 인증서비스에 사용되는 저장 및 기록매체를 별도의 금고실에 있는 내화금고에 저장하여 물리적 접근을 통제합니다.

5.1.9 시설 및 장비의 폐기 처리

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

5.1.10 원격지 백업설비 안전운영

카카오뱅크는 인증서 등 중요정보 보관을 위해 20km 이상 떨어진 곳에 원격지 백업설비를 운영하고 있으며, 출입통제시스템, 침입감지장치 등 보호설비를 구축 · 운영하고 있습니다.

5.2 절차적 보호조치

5.2.1 본인확인업무에 대한 업무 분장

카카오뱅크 본인확인업무의 안전성과 신뢰성을 확보하기 위하여 본인확인업무 수행 인력을 역할별로 분리하여 운용합니다.
- 책임자: 인증업무 정책, 사업연속성계획, 재해복구계획 등을 승인합니다.
- 정책관리자: 인증업무 정책 수립, 등록, 유지 및 개정을 합니다.
- 내부 감사자: 인증시스템과 인증서비스에 대한 감사를 진행합니다.
- 보안관리자: 보안이슈 발생 시 침해사고 등의 유형과 영향도를 파악하고, 책임자에게 보고 합니다.

- 암호 모듈 장치 담당자: 암호 모듈 장비(Hardware Security Module)를 관리하고, 암호화 모듈 활성화에 필요한 접근권한 담당자에게 필요한 물품 및 정보를 제공하고 관리합니다.
- 시스템 운영자: 시스템/네트워크/정보보안 시설에 대한 운영 관리 및 유지보수를 수행합니다.
- 시스템 관리자 : 시스템에서 사용되는 인증서를 관리하고, 시스템의 환경 설정 및 서비스 기동 등을 관리합니다.

5.2.2 업무별 수행 인원

카카오뱅크의 전자서명생정보(개인키) 생성 및 최상위 인증기관 전자서명생성정보(개인키) 활성화는 최소 3인 이상이 수행합니다. 각 실의 출입은 2인 이상이 수행합니다.

5.2.3 업무 담당자 신원확인 및 인증

카카오뱅크는 본인확인업무 수행인력이 본인확인업무 시스템을 통해 신원이 확인될 수 있도록 직접 생성했거나 할당된 고유한 자격증명을 사용하도록 요구합니다.

5.2.4 직무 분리가 필요한 역할

카카오뱅크는 할당된 책임 및 업무를 문서화하여 관리합니다. 또한 책임 범위 및 보안 관점에서 분리되어야 하는 직무는 동일인이 겸업할 수 없습니다.

5.3 인적 보안

카카오뱅크는 직원 채용 시 신원조사를 실시하고 있으며, 인증시스템 운영인력의 자격과 자질을 주기적으로 조사하고 동 사항의 유지 여부를 지속적으로 관리합니다.

5.3.1 자격, 경력 및 기밀취급 요건

카카오뱅크가 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. 본인확인업무는 카카오뱅크 직원만이 수행할 수 있으나, 필요 시 카카오뱅크가 허용하는 범위 내에서 외주인력에 일부 기능을 부여할 수 있습니다.

5.3.2 배경 확인 절차

카카오뱅크의 정보보호규정 또는 인사규정에 따라 직원 채용 시 필요한 사항에 대해 검증합니다.

5.3.3 교육 및 업무순환

1. 인증시스템을 관리하는 직원은 정보보호 관련 내부 또는 외부 교육을 이수하도록 합니다.
2. 인증시스템을 관리하는 직원은 업무상 취득한 기밀사항의 준수에 관한 서약서를 작성하여 날인하도록 합니다.
3. 업무순환 및 업무환경의 변화 등으로 인하여 보호조치의 수정 및 보완이 필요한 경우 이를 지체없이 보완합니다.
4. 인증시스템을 관리하는 직원이 인사이동 및 퇴직하는 경우에는 내부 규정에 따라 계정삭제 및 저장매체 반납 등의 적절한 조치를 취하도록 합니다.

5.3.4 재교육 주기 및 요건

연 1회 이상 정보보호 관련 내부 또는 외부 교육을 실시합니다.

5.3.5 직무순환 주기 및 순서

해당 사항 없습니다.

5.3.6 비인가 행위 처벌

비인가 행위를 한 직원에 대해서는 내부 규정에서 정하는 바에 따라 해당 직원들 징계합니다.

5.3.7 독립적 계약자 요건

해당 사항 없습니다.

5.3.8 직원에게 제공되는 문서

해당 사항 없습니다.

5.4 감사 기록

5.4.1 감사 기록의 유형

카카오뱅크는 인증업무 운영과 관련해 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. 인증서 발급에 사용되는 개인정보 등

5.4.2 감사 기록 검토 주기

카카오뱅크는 필요에 따라 감사기록을 분기에 1회 검토합니다.

5.4.3 감사 기록 보존 기간

카카오뱅크는 생성된 모든 감사 기록을 최소 2년 이상 보존하며, 필요시 보관된 감사기록을 내부 또는 외부 감사인에게 제공할 수 있습니다.

5.4.4 감사기록 보호조치

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

5.4.5 감사 기록 백업 절차

카카오뱅크는 감사기록을 필요할 때 관련 표준에 규정된 대로 사용할 수 있도록 실시간 또는 주기적으로 백업합니다.

5.4.6 감사 기록 취합 시스템

카카오뱅크는 감사기록시스템을 직접 운영합니다.

5.4.7 감사 기록 대상에 대한 통보

해당 사항 없습니다.

5.4.8 취약점 평가

카카오뱅크는 인증서비스 업무를 수행함에 있어 효율적인 보안관리를 위해 정기적으로 취약점 점검을 수행합니다.

5.5 기록 보존

5.5.1 기록 보존 대상의 종류

카카오뱅크가 보존하는 기록의 유형은 다음과 같습니다.
1. '5.4.1 감사 기록의 유형'에 정의된 유형
2. 기타 인증 시스템 운영 및 관리의 중요 활동 등

5.5.2 보존 기록 보관 기간

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

5.5.3 보존 기록 보호

카카오뱅크는 보존기록에 대해 엄격한 물리적, 논리적, 인적 접근통제를 적용합니다. 보존기록은 허용된 업무범위에 한하여 조회 가능하며, 변경 및 삭제가 불가능합니다. 또한, 보존장소는 항온항습기를 설치하고, 화재 발생에 대비하여 화재경보기 등의 설비로 보호합니다.

5.5.4 보존기록의 백업주기 및 백업절차

카카오뱅크는 보존기록의 손실 및 파괴에 대비하여 독립된 저장설비에 주기적으로 백업하여 보존합니다.

5.5.5 기록의 시간 기준

정확한 기록 유지를 위해 GPS 위성기반 한국 표준시 기반의 NTP(Network Time Protocol) 서버와 동기화합니다.

5.5.6 보존기록 취합 시스템

카카오뱅크는 보존기록시스템을 직접 운영합니다

5.5.7 보존기록 확보 및 검증 절차

카카오뱅크는 정기적으로 보관된 정보의 통계 샘플을 테스트하여 정보의 지속적인 무결성과 가독성을 확인합니다. 인증된 카카오뱅크의 장비 및 본인확인업무담당자만 보존기록에 접근할 수 있으며, 보존기록 정보 획득 및 확인 요청은 본인확인업무 운영자(내부 감사자, 정책관리자 및 보안 담당자)에 의해 수행됩니다.

5.6 전자서명인증사업자의 전자서명생성정보 갱신

인증서(또는 전자서명생성정보)는 만료되는 날의 3년전부터 새로운 전자서명생성정보를 생성하고, 이때부터 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.

5.7 장애 및 재해복구

5.7.1 인증업무 장애 및 재해 유형별 신고 및 복구 절차

1. 인증업무 장애 및 IDC재해 시 서비스 지속성을 보장하고자 내부지침에 유형별 대응 절차를 마련합니다.
2. 년 1회 인증 위기대응훈련을 통해 내부지침을 검증하고 개선사항을 도출하여 지속 개선 및 현행화를 통해 유사 시 최선의 대응 준비합니다.

5.7.2 컴퓨팅 자원, 소프트웨어, 데이터 훼손에 대한 대책

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

5.7.3 개인 및 법인 전자서명생성정보(개인키) 손실에 대한 복구 절차

카카오뱅크는 가입자의 전자서명생성정보(개인키)가 안전하지 않다는 사실을 인지한 경우 가입자 인증서를 폐지하고 신규 키 쌍을 생성하여 가입자 인증서를 재발급합니다.

5.7.4 인증업무 장애방지 등 연속성 보장 대책

1. 인증시스템을 이중화하여 무정지 운영체제를 구축하고 백업센터를 운영하여 장애 방지에 최선을 다합니다.
2. 인증관련 주요 데이터가 훼손되거나 파괴가 발생하는 경우에 백업된 자료를 이용하여 복구합니다.
3. 내부지침을 통해 오류를 관리하고 발생된 오류가 재발되지 않도록 최선을 다합니다.

5.8 업무 휴지, 폐지, 종료

5.8.1 업무 휴지

1. 자연재해 또는 천재지변이 아닌 불가피한 사정으로 카카오뱅크가 본인확인업무의 전부 또는 일부를 휴지하려는 경우 휴지기간을 정하여 휴지하려는 날의 30일 전까지 그 사실을 가입자에게 통보하고 카카오뱅크 홈페이지 또는 앱에 게시합니다.
2. 통보 및 게시 내용에는 가입자의 개인정보 폐지 등 가입자 보호조치를 포함합니다.

5.8.2 업무 폐지 및 종료

1. 자연재해 또는 천재지변이 아닌 불가피한 사정으로 카카오뱅크가 본인확인업무를 폐지 및 종료하려는 경우 폐지하려는 날의 60일 전까지 그 사실을 가입자에게 통보하고 카카오뱅크 홈페이지 또는 어플리케이션에 게시합니다.
2. 통보 및 게시 내용에는 가입자의 개인정보 폐지 등 가입자 보호조치를 포함합니다.

6. 기술적 보호조치

6.1 전자서명생성정보 보호

6.1.1 전자서명생성정보 생성 시 보호

6.1.1.1 최상위 인증기관 및 인증기관 전자서명생성정보 생성 시 보호

1. 카카오뱅크는 물리적으로 안전한 환경에서 규정된 절차에 따라 FIPS 140-2 레벨 3 이상의 장비로 전자서명생성정보를 생성합니다.
2. 전자서명생성정보 생성 시 전용 장비를 사용하며, 최상위 인증기관의 전자서명생성정보 생성 시 전용 장비는 모든 네트워크 연결이 차단된 상태로 관리됩니다.
3. 전자서명생성정보 생성 시 하드웨어 보안 모듈 장비에 3인 이상의 관리자가 함께 다자인증을 수행합니다.
4. 생성된 전자서명생성정보는 카카오뱅크에서 허용한 키 백업 용도를 제외하고는 하드웨어 보안 모듈 외부로 추출할 수 없습니다.

6.1.1.2 가입자 전자서명생성정보 생성 시 보호

1. 카카오뱅크는 가입자의 전자서명생성정보를 생성하지 않으며 전자서명생성정보는 가입자의 단말 내에서 생성됩니다.
2. 카카오뱅크는 가입자가 본인의 전자서명생성정보를 안전하게 생성할 수 있도록 신뢰할 수 있는 암호화 모듈 및 보안 기술 규격 등을 적용합니다.

6.1.2 가입자에게 전자서명생성정보 전달

카카오뱅크는 가입자의 전자서명생성정보를 생성하지 않으며 전자서명생성정보는 가입자의 단말 내에서 생성됩니다.

6.1.3 인증서 발급자에게 전자서명검증정보 전달

가입자는 전자서명검증정보를 PKCS #10 형식의 인증서 서명 요청에 포함해 카카오뱅크로 전송하며 카카오뱅크는 이를 검증하고 인증서를 발급하여 가입자 단말에 저장합니다. 이 과정은 모두 가입자의 개입 없이 시스템 간 통신으로 이루어집니다. 전자서명검증정보의 보호를 위해 가입자와 카카오뱅크 시스템 간 통신은 암호화 통신(HTTPS)을 이용합니다.

6.1.4 가입자 및 이용자에게 인증기관 전자서명검증정보 전달

카카오뱅크는 카카오뱅크가 운영하는 모든 인증기관의 전자서명검증정보를 "2.1 공고설비" 항목에 명시된 공고설비를 통해 공개합니다.

6.1.5 키 길이

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

1. 최상위 인증기관
   가. ECDSA: 256 비트
   나. AES: 128 비트 이상
   다. SHA-256: 256 비트
2. 인증기관
   가. ECDSA: 256 비트
   나. AES: 128 비트 이상
   다. SHA-256: 256 비트
3. 가입자
   가. ECDSA: 256 비트
   나. AES: 128 비트 이상
   다. SHA-256: 256 비트

6.1.6 전자서명검증정보 매개변수 생성 및 품질검사

카카오뱅크는 전자서명검증정보 매개변수를 생성합니다. 카카오뱅크 인증기관 키는 FIPS 140-2 레벨 3 이상을 준수하는 하드웨어 보안모듈(HSM)에서 생성합니다.

6.1.7 키 사용 용도(X.509 V3 키 사용 필드 기준)

1. 최상위 인증기관 전자서명생성정보가 사용되는 경우는 다음과 같습니다.
   가. 최상위 인증기관임을 스스로 보증하기 위한 자체 서명 인증서 발급
   나. 인증기관용 인증서 발급
   다. 인프라 목적용 인증서(예: 관리용 인증서, 운영장치용 인증서 및 OCSP 응답확인용 인증서) 발급

라. 인증기관 인증서 폐지목록(ARL) 생성

2. 인증기관 전자서명생성정보가 사용되는 경우는 다음과 같습니다.
   가. 가입자 인증서 발급
   나. 서버 인증서 발급(예 : RA 서버 인증서)
   다. 가입자 인증서 폐지목록(CRL) 생성

3. 가입자의 전자서명생성정보가 사용되는 경우는 다음과 같습니다.
   가. 가입자 인증서 발급 절차에서 인증서 발급 신청서(CSR) 생성 시
   나. 이용자의 요청에 따라 전자서명 수행 시
   다. 가입자 인증서 폐지 절차에서 폐지 요청하는 인증서의 전자서명생성정보 소유를 확인하기 위한 전자서명 생성 시

6.2 전자서명생성정보 보호 조치

6.2.1 전자서명생성정보 저장장치

카카오뱅크 인증기관의 전자서명생성정보는 FIPS 140-2 레벨3 인증을 받은 하드웨어 보안 모듈(HSM)을 사용합니다.

6.2.2 전자서명생성정보(개인키) 다중 통제

카카오뱅크는 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

해당 사항 없습니다.

6.2.4 전자서명생성정보(개인키) 백업

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

6.2.5 전자서명생성정보 기록 보존

카카오뱅크는 인증기관의 전자서명생성정보를 "6.2.4 전자서명생성정보 백업" 항목에 명시된 용도 이외에 별도로 기록 보존하지 않습니다.

6.2.6 암호화 모듈 내부로 전자서명생성정보 전송 또는 외부로 추출

카카오뱅크의 전자서명생성정보 백업 목적으로 책임자의 승인 하에 하드웨어 보안 모듈 공급업체가 지정한 절차에 따라 인증기관 전자서명생성정보를 추출할 수 있습니다.

6.2.7 암호화 모듈에 전자서명생성정보 저장

카카오뱅크 인증기관의 전자서명생성정보가 생성되면 "6.2.1 전자서명생성정보 저장장치" 항목의 요건을 충족하는 하드웨어 보안 모듈에 저장됩니다.

6.2.8 전자서명생성정보 활성화

카카오뱅크 승인 하에 하드웨어 보안 모듈 공급업체가 지정한 절차에 따라 인증기관의 전자서명생성정보가 저장된 하드웨어 보안 모듈을 활성화할 수 있습니다.

6.2.9 전자서명생성정보 비활성화

카카오뱅크 승인 하에 하드웨어 보안 모듈 공급업체가 지정한 절차에 따라 인증기관의 전자서명생성정보가 저장된 하드웨어 보안 모듈을 비활성화할 수 있습니다.

6.2.10 전자서명생성정보 파기

1. 카카오뱅크는 다음과 같은 사유로 인증기관의 전자서명생성정보를 파기할 수 있습니다.
 - 인증기관 인증서의 유효기간이 만료된 경우
 - 인증기관의 전자서명생성정보가 훼손, 유출 및 손상되었거나 그럴 가능성이 있는 경우

2. 가입자의 전자서명생성정보는 다음의 경우에 가입자의 단말기에서 파기됩니다.
 - 가입자 인증서가 폐지된 경우
 - 가입자 인증서의 유효기간이 만료된 경우

6.2.11 암호화 모듈 등급

"6.2.1 전자서명생성정보 저장장치" 항목 요건을 충족하는 하드웨어 보안 모듈을 사용합니다.

6.3 전자서명생성정보 및 전자서명검증정보의 관리

6.3.1 공개 키 보관

인증기관, 가입자 인증서는 카카오뱅크 백업 절차에 따라 보관됩니다. 또한, 전자서명검증정보와 전자서명생성정보는 분실, 훼손 도난, 유출 방지를 위해 관리적 기술적 보호조치를 하여 안전하게 보관됩니다.

6.3.2 인증서 운영기간 및 키쌍 유효기간

인증서 유효기간은 인증서 필드에 명시된 유효기간 종료시점에 만료됩니다. 가입자 인증서 유효기간은 가입자가 인증서 신청 시 3년입니다.

6.4 데이터 보호 조치

6.4.1 활성화 데이터 생성 및 설치

카카오뱅크 인증기관 활성화 데이터는 하드웨어 보안 모듈로 생성하며, IC 칩 또는 토큰 형태로 설치되어 보관합니다. 활성화 데이터는 인증기관 전자서명생성정보를 생성하거나 전자서명 기능 및 하드웨어 보안 모듈의 세션을 활성화할 때 사용됩니다.

6.4.2 활성화 데이터 보호

1. 최상위 인증기관 및 인증기관 활성화 데이터는 인증기관 전자서명생성정보와 동일한 수준의 물리적 보호조치를 적용한 공간에 위치하며 내화금고 등의 안전한 장소에 보관합니다.
2. 인증기관 키 관리자는 활성화 장치를 안전하게 보관 관리하며, 필요 시 지정된 키 소유자에게 할당될 수 있도록 배분합니다.

6.4.3 활성화 데이터 추가 고려 사항

해당 사항 없습니다.

6.5 시스템 보안 통제

1. 카카오뱅크는 인증시스템을 이중화하여 관리합니다
2. 카카오뱅크는 인증업무와 관련된 주요 프로그램 또는 프로세스 동작여부를 점검할 수 있는 시스템을 설치 운영합니다.
3. 카카오뱅크는 인증시스템 운영에 필요한 프로그램 및 기능만 설치합니다.
4. 카카오뱅크는 인증시스템 운영체제의 문제점 해결을 위한 최신 패치를 설치하여 운영합니다.
5. 카카오뱅크는 인증시스템에 대한 접근을 최소화하고 제한된 인원에 한하여 권한을 부여합니다.
6. 카카오뱅크는 인증시스템에서 인증서 생명주기 관리에 관한 업무에 사용되는 모든 계정은 접근 시 다중인증(Multi-Factor Authentication)을 적용합니다.
7. 카카오뱅크는 인증시스템의 추가·폐지·변경에 관한 사항을 내부 지침에 의거 관리합니다.
8. 카카오뱅크는 인증시스템의 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위해 정보보호시스템을 설치 및 운영합니다.

6.5.1 특정 컴퓨터 보안 기술 요구 사항

해당 사항 없습니다.

6.5.2 컴퓨터 보안 등급

해당 사항 없습니다.

6.6 시스템 운영 관리

카카오뱅크는 본인확인업무 시스템의 S/W 형상관리 및 운영을 합니다.
- 본인확인업무 시스템의 S/W 등록에 대한 형상관리
- 본인확인업무 시스템의 변경사항 등 운영관리에 대한 형상관리

6.6.1 시스템 개발 통제

카카오뱅크에서 사용되는 본인확인업무 시스템의 S/W는 시스템 개발, 변경 정책 및 절차에 따라 개발·테스트·운영합니다.
- 본인확인업무 시스템의 S/W 소스 코드는 형상관리 됨

6.6.2 보안관리 통제

카카오뱅크는 정보보호 조직을 운영하고 있으며, 정보보호 및 정보 자산에 대한 기밀성, 무결성, 가용성을 위해 정보보호 원칙에 따라 업무를 수행할 수 있도록 관리 및 통제하고 있습니다.

1. 본인확인업무와 관련된 프로세스의 동작 여부를 점검할 수 있도록 시스템을 운영하고 있습니다.
2. 본인확인업무 시스템 운영에 필요한 최소한의 프로그램만 설치하여 관리하고 있습니다.
3. 본인확인업무 시스템의 접근을 최소화하고 제한된 인원에 한해 접근 권한을 부여하고 있습니다.
4. 전자서명시스템의 S/W 개발,도입,폐지에 대한 적절한 형상 관리를 진행하고 있습니다.

6.6.3 생명주기 보안 통제

해당 사항 없습니다.

6.7 네트워크 보호조치

1. 카카오뱅크는 인증시스템 관련 네트워크를 이중화하여 장애 발생에 대비하고 안정적인 서비스를 제공합니다.
2. 카카오뱅크는 네트워크관리시스템을 통하여 네트워크 부하 등 이상징후를 모니터링합니다.
3. 카카오뱅크는 침입탐지 및 침입차단시스템을 운영하여 네트워크를 보호하며, 침입탐지시스템의 데이터베이스를 주기적으로 갱신합니다.
4. 카카오뱅크는 관련 로그를 분석하여 인증시스템에 대한 해킹 등 전자적 침해행위를 모니터링합니다.
5. 카카오뱅크는 침입차단 및 침입탐지시스템에 대한 논리적인 접근통제를 설정합니다.

6.8 시점확인서비스 보호조치

해당 사항 없습니다.

7. 인증서 형식

7.1 인증서 형식

7.1.1 최상위 인증기관 전자서명 인증서 프로파일

- 기본필드

NO	필드명	입력 값
1	version	V3
2	serial Number	일련번호
3	signature Algorithm	SHA256 with ECDSA
4	issuer	C = KR, O = KakaoBank Corp., OU = KakaoBank Certification Authority, CN = KakaoBank Root CA Class 2
5	subject	C = KR, O = KakaoBank Corp., OU = KakaoBank Certification Authority, CN = KakaoBank Root CA Class 2
6	validity	인증서의 유효기간
7	subject Public Key Info	공개키 정보

- 확장필드

NO	필드명	입력 값
1	authority Key Identifier	최상위 인증기관의 subjectKeyIdentifier
2	subject Key Identifier	공개키에 대한 해쉬 값
3	key Usage	digitalSignature (0), keyCertSign (5), cRLSign (6)
4	basic Constraints	CA = true, pathLenConstraint=None

7.1.2 인증기관 전자서명 인증서 프로파일

- 기본 필드

NO	필드명	입력 값
1	version	V3
2	serial Number	일련번호
3	signature Algorithm	SHA256 with ECDSA
4	issuer	C = KR, O = KakaoBank Corp., OU = KakaoBank Certification Authority, CN = KakaoBank Root CA Class 2
5	subject	C = KR, O = KakaoBank Corp., OU = KakaoBank Certification Authority, CN = KakaoBank CA Class 2
6	validity	인증서의 유효기간
7	subject Public Key Info	공개키 정보

- 확장 필드

NO	필드명	입력 값
1	authority Key Identifier	- 최상위 인증기관의 subjectKeyIdentifier - 최상위 인증기관의 subject - 최상위 인증기관의 serialNumber
2	subject Key Identifier	공개키에 대한 해쉬 값
3	key Usage	digitalSignature (0), keyCertSign (5), cRLSign (6)
4	basic Constraints	CA = true, pathLenConstraint=0
5	certificate Policies	OID = 1.2.410.200088.2 CPS =https://www.kakaobank.com/Corp/Policy/Cert/CertCps unotice = "이 인증서는 카카오뱅크 CA 인증서 입니다."
6	CRL Distribution Points	http://arl.kakaobank.com/rca2_arl.crl
7	authority Info Access	http://ocsp.kakaobank.com/ca

7.1.3 가입자

- 기본필드

NO	필드명	입력 값
1	version	V3
2	serial Number	일련번호
3	signature Algorithm	SHA256 with ECDSA
4	issuer	CN=KakaoBank CA Class 2, OU=KakaoBank Certification Authority, O=KakaoBank Corp., C=KR
5	subject	CN=한글실명(사용자관리번호), O=KakaoBank CA Class 2, OU=개인, C=KR
6	validity	인증서의 유효기간
7	subject Public Key Info	공개키 정보

- 확장필드

NO	필드명	입력 값
1	authority Key Identifier	- 인증기관의 subjectKeyIdentifier - 최상위 인증기관의 subject - 인증기관의 serialNumber
2	subject Key Identifier	공개키에 대한 해쉬 값
3	key Usage	digitalSignature (0), nonRepudiation(contentCommitment) (1)
4	extKey Usage	id-kp-clientAuth {1.3.6.1.5.5.7.3.2}
5	basic Constraints	CA = false
6	certificate Policies	OID = 1.2.410.200088.2.1.2 또는 1.2.410.200088.2.1.3 CPS =https://www.kakaobank.com/Corp/Policy/Cert/CertCps unotice = "이 인증서는 카카오뱅크 개인 인증서 입니다."
7	CRL Distribution Points	http://crl.kakaobank.com/user
8	authority Info Access	http://ocsp.kakaobank.com/user

7.1.4 이름 양식

해당 사항 없습니다.

7.1.5 이름 제한

해당 사항 없습니다.

7.1.6 인증서 정책 개체 식별자

실명 가입자에게 발급하는 인증서의 정책 개체 식별자(Object Identifier)는 신원확인 방식에 따라 구분됩니다.
- 대면 또는 비대면 실명확인 : 1.2.410.200088.2.1.3
- 온라인 신원확인 또는 접근매체(인증서)에 의한 대체발급 : 1.2.410.200088.2.1.2

7.1.7 정책 제한 확장의 사용

해당 사항 없습니다.

7.1.8 정책 한정자 구분 및 의미

해당 사항 없습니다.

7.1.9 주요 인증서 정책 확장에 대한 의미 처리

해당 사항 없습니다.

7.2 가입자 전자서명 인증서 폐지목록(CRL) 프로파일

7.2.1 버전

가입자 인증서 폐지목록(CRL) 프로파일은 X.509 버전 2를 준수합니다.

7.2.2 CRL 및 CRL 확장 필드

7.2.2.1 기본필드

NO	필드명	입력 값
1	signature Algorithm	SHA256withECDSA
2	issuer	CN=KakaoBank CA Class 2, OU=KakaoBank Certification Authority, O=KakaoBank Corp., C=KR
3	this Update	발행일시

4	next Update	다음 발행일시
5	revoked Certificates	폐지된 인증서 목록(인증서 시리얼, 폐지 일시)

7.2.2.2 확장필드

NO	필드명	입력 값
1	authority Key Identifier	- Root CA 의 subjectKeyIdentifier - Root CA 의 subject - Root CA 의 serialNumber
2	crl Number	CRL 발행 번호
3	issuing Distribution Point	http://crl.kakaobank.com

7.2.2.3 엔트리 확장필드

NO	필드명	입력 값	비고
1	Reason Code	폐지 사유	

7.3. OCSP 서버용 인증서 프로파일

7.3.1 버전

카카오뱅크 인증서 유효성 확인 서비스(OCSP) 응답자는 RFC 6960에 정의된 버전 1을 준수합니다.

카카오뱅크는 OCSP 요청 메시지가 RFC 6960를 준수하지 않는 경우 응답을 거부할 수 있습니다.

7.3.2 OCSP 확장 필드

7.3.2.1 OCSP Response 기본필드

NO	필드명	입력 값
1	responseStatus	v1
2	responseType	id-pkix-ocsp-basic {1.3.6.1.5.5.7.48.1.1}
3	ResponseData	
	/ version	V1
	/ responderID	OCSP 서버의 SubjectDN
	/ producedAt	OCSP 응답을 생성한 시간
	ResponseData/ responses	요청한 가입자 인증서 정보

		(OCSP Request 의 CertID 와 동일)
	/../ certID	
	/../ certStatus	인증서 상태
	/../ thisUpdate	OCSP 갱신 시간
4	signatureAlgorithm	SHA256 with ECDSA
5	signature	OCSP 서버의 전자서명 값
6	certs	OCSP 서버의 인증서 정보

7.3.2.2 OCSP Response 확장필드

NO	필드명	입력 값
1	responseExtensions	폐지 사유
2	extnId	ocsp-nonce OID
3	extnValue	OCTET STRING

8. 감사 및 평가

카카오뱅크는 웹 트러스트 원칙 및 기준(WebTrust Principles and Criteria)을 준수하고 있습니다.

8.1 감사 및 평가 현황

카카오뱅크는 본인확인업무를 수행함에 있어 효율적인 보안관리를 위하여 매년 1회 이상 웹트러스트 감사 또는 평가를 실시 합니다.

8.2 감사 및 평가자의 신원, 자격

카카오뱅크는 웹 트러스트 감사를 받기 위해 웹 트러스트 감사를 수행할 수 있는 회계법인을 선임합니다.

8.3 감사 및 평가 대상과 평가자의 관계

감사자는 피감사 대상자와 금전적으로나 사업 등으로 이해관계가 없어야 합니다.

8.4 감사 및 평가 목적 및 내용

감사의 범위는 준칙의 준수여부, 인증기관 키 관리, 인증서 관리, 인증기관 및 최상위인증기관 시스템 관리를 포함합니다.

8.5 부적합 사항에 대한 조치

부적합 사항에 대해서는 조치가 취해지며 합리적인 기간 내 보완하고 있습니다.

8.6 결과 보고

해당 사항 없습니다.

9. 본인확인업무 보증 등 기타사항

9.1 수수료

9.1.1 인증서 발급 또는 갱신 수수료

1. 가입자가 서비스를 이용하는데 있어서, 가입자에게는 별도의 발급 수수료가 부과되지 않습니다.
2. 이용자가 서비스를 이용하는데 있어서, 이용자가 지불하는 수수료는 이용자와의 별도 계약에 따릅니다.

9.1.2 인증서 접근 수수료

별도의 인증서 접근 수수료가 부과되지 않습니다.

9.1.3 인증서 폐지목록 정보 확인 수수료

별도의 인증서 폐지목록(CRL 및 ARL) 정보 확인 수수료가 부과되지 않습니다.

9.1.4 기타 서비스 수수료

별도의 기타 서비스 수수료가 부과되지 않습니다.

9.1.5 환불 정책

1. 가입자가 서비스를 이용하는데 있어서 수수료가 부과되지 않기에 별도의 환불 정책은 없습니다.
2. 이용자에 대한 환불 정책은 이용자와의 별도 계약에 따릅니다.

9.2 배상

카카오뱅크는 카카오뱅크가 본 준칙, 이용약관 등의 관련 규정을 위반하였거나, 안전하지 않은 알고리즘 등에 따른 기술적 내용의 결함으로 인해 가입자 또는 이용자에게 손해를 입힌 경우 그 손해를 배상합니다.

9.3 영업비밀

카카오뱅크는 카카오뱅크 본인확인서비스와 관련된 영업비밀을 보호합니다.

9.3.1 기밀 정보의 범위

카카오뱅크 본인확인서비스와 관련되어 기밀 정보는 다음과 같습니다.
1. 전자서명생성정보(개인키)
2. 인증기관 시스템에 접근 시 사용되는 정보
3. 개인정보로 보유하는 정보
4. 감사로그 및 보존 기록

9.3.2 기밀 정보의 범위를 벗어난 정보

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

9.3.3 기밀 정보 보호의 책임

카카오뱅크는 이용자와 가입자의 정보를 보호하기 위하여 기밀 정보를 처리하고 보호합니다.

9.4 개인정보 보호

9.4.1 개인정보 보호 계획

카카오뱅크는 개인정보의 안전성 확보에 필요한 관리적·기술적·물리적 조치를 하고 있습니다.

1. 관리적 조치

가. 내부 관리계획 수립 및 시행

나. 개인정보 취급 직원의 최소화 및 교육: 개인정보를 취급하는 직원을 지정하고 담당자에 한정시켜 최소화하여 개인정보를 관리하는 대책을 시행하고 있습니다.

2. 기술적 조치

가. 개인정보처리시스템 접근권한 관리 및 접근통제: 개인정보를 처리하는 데이터베이스시스템에 대한 접근권한의 부여, 변경, 말소를 통하여 개인정보에 대한 접근을 통제하고 있으며, 침입차단시스템을 이용하여 외부로부터 무단 접근을 통제하고 있습니다.

나. 개인정보의 암호화: 고객의 개인정보를 보관 또는 네트워크 송수신 시 안전하게 암호화여 관리 하고 있습니다.

다. 해킹 등에 대비한 기술적 대책: 해킹이나 바이러스 등에 의한 개인정보 유출 및 훼손을 막기 위하여 보안 프로그램을 설치하여 주기적인 갱신·점검을 하며 외부로부터의 접근이 통제된 구역에 시스템을 설치하는 등 기술적·물리적으로 감시 및 차단하고 있습니다.

3. 물리적 조치: 전산실, 자료 보관실 등의 접근 통제

9.4.2 개인정보 기준

카카오뱅크는 이용 목적을 위해 개인정보보호법 및 정보통신망 이용촉진 및 정보보호 등에 관한 법, 시행령 및 시행규칙에서 정한 방식에 따라 필요한 최소한의 개인정보를 수집하고 있습니다.

1. 이용 목적: 인증서 발급 및 관리, 인증서비스 관련 각종 공고 및 통보, 인증서 부정 발급 및 부정 사용 방지, 비인가 사용방지

2. 개인정보 항목: 이름, 생년월일, 성별, 내/외국인여부, 이메일 주소, 휴대폰번호, CI(연계정보), DI(중복가입확인정보), 고유식별정보(주민등록번호, 운전면허번호, 외국인등록번호), 실명확인증표(주민등록증, 운전면허증, 여권/여권정보증명서, 외국인등록증) 사본, 타행계좌 확인을 위한 정보(은행명, 계좌번호), 얼굴사진 및 얼굴의 특징정보(민감정보)

3. 기기정보: 단말기 식별정보

9.4.3 개인정보 제외 기준

해당 사항 없습니다.

9.4.4 인증업무 관련 정보의 보호범위 및 책임

카카오뱅크는 인증업무수행 과정에서 취득한 자료에 대하여 안전하게 보호하고 관리합니다.

9.4.5 개인정보 사용에 대한 이용 동의

카카오뱅크는 개인정보를 수집하는 경우 본인확인서비스 제공에 필요한 최소한의 정보를 수집하며 가입신청자 및 가입자의 동의를 얻어야합니다.

9.4.6 사법 또는 행정 절차에 따른 공개

카카오뱅크는 고객의 개인정보를 9.4.2 에서 명시한 목적 범위 내에서 처리하며, 고객의 사전 동의없이는 본래의 범위를 초과하여 처리하거나 제 3자에게 제공하지 않습니다. 다만, 다음 각 항의 경우에는 고객 또는 제 3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적외의 용도로 이용하거나 제 3자에게 제공할 수 있습니다.

1. 본인확인서비스의 제공에 따른 요금정산을 위하여 필요한 경우
2. 통계·학술연구 또는 시장조사를 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우
3. 전자서명법 또는 관련 법령에 규정이 있는 경우

9.4.7 기타 정보 공개 기준

카카오뱅크는 개인정보보호법 등 관계 규정을 준수하며 홈페이지에 게시된 카카오뱅크 인증서 서비스 개인정보처리방침에 따라 개인정보를 처리합니다.

9.5 지식재산권

다음 사항에 대한 지식재산권은 저작권법 등 관련법률에 따라 카카오뱅크에 귀속됩니다.

1. 카카오뱅크 인증시스템을 위해 개발된 소프트웨어 및 하드웨어
2. 본 준칙 및 이용약관과 운영 정책
3. 카카오뱅크가 생성한 전자서명 정보
4. 기타 관련 법령에 따라 카카오뱅크에게 권리가 귀속되는 일체의 저작물

9.6 보증

1. 인증서는 본 준칙에 따라 발급됨을 보증합니다.
2. 인증서 내에 포함된 내용이 발급신청 당시 기준으로 카카오뱅크 CA에 등록된 사실임을 보증합니다.

9.7 보증 예외 사항

카카오뱅크는 전자서명법, 동법 시행령 및 시행규칙, 이용약관 또는 운영정책과 본 준칙에서 정한 사항 이외의 사항 즉, 가입자 신용 및 가입자 관련 정보의 불변성 등을 보증하지 않습니다.

9.8 보험의 보상 범위

카카오뱅크는 본인확인업무의 수행과 관련하여 가입자 또는 이용자에게 손해를 입힌 경우에는 그 손해를 배상합니다. 다만, 카카오뱅크의 고의 또는 과실이 없는 경우에는 배상책임을 부담하지 않습니다.

9.9 배상 한계

카카오뱅크는 가입자 또는 이용자에 대한 손해배상을 담보하기 위하여 전자서명 및 인증업무용 책임보험에 가입하고 있으며, 해당 보험계약에서 정한 배상 한도는 본인확인용 책임보험 보상한도 10억원 범위 내에서 본인확인인증업무와 관련하여 카카오뱅크의 고의 또는 과실로 발생한 사고로 인한 가입자 및 이용자의 손해를 배상합니다.
보험계약 상의 배상한도를 초과하여 손해가 발생한 경우, 당사자간의 합의에 따라 초과 분에 대한 손해를 배상하며 합의가 이루어지지 않을 경우 관련 법령 및 법원 등 유권기관의 판단에 따라 배상을 합니다.

9.10 준칙의 효력

9.10.1 준칙의 유효기간

준칙은 홈페이지에 게시되고 본 문서에 명시된 기간 이후에 효력이 발생합니다. 또한, 개정사항은 홈페이지에 게시된 이후에 적용됩니다. 다만 각 호의 사유가 발생한 때에 효력이 소멸합니다.
- 카카오뱅크의 본인확인업무가 정지된 경우 해당 정지 기간
- 카카오뱅크가 본인확인업무의 전부를 휴지한 경우 해당 휴지 기간
- 카카오뱅크가 본인확인업무를 폐지한 경우 폐지시점 이후
- 기타 준칙의 효력이 소멸하는 경우로 과학기술정보통신부 장관이 인정하는 경우

9.10.2 준칙의 종료

본 준칙 및 관련된 정책 문서는 신규 버전으로 개정되기 전까지 효력을 유지합니다.

9.10.3 준칙의 경과 조치

본 준칙의 효력이 종료되더라도 종료된 시점을 기준으로 발급된 모든 인증서의 남은 유효기간 동안에는 본 준칙 효력이 적용됩니다.

9.11 통지 및 의사소통

카카오뱅크는 인증서의 신뢰도 및 유효성에 중대한 영향을 미치는 사실이 발생하거나 중요한 변경사항이 생겼을때 해당 사실을 홈페이지에 공고합니다.

9.12 이력 관리

카카오뱅크는 준칙의 변경 이력을 관리하며, 최신 준칙은 카카오뱅크 홈페이지(https://www.kakaobank.com/Corp/Policy/Cert/CertCps)에서 열람할 수 있습니다.

9.13 분쟁 해결

9.13.1 법적 효력 요건

1. 전자서명인증체계 관련자에게 전달되는 문서(또는 전자문서)는 아래와 같이 법적 효력을 갖습니다.
- 전자문서법 제4조(전자문서의 효력)의 각 항에 따른 사항
- 전자서명법 제3조(전자서명의 효력)의 각 항에 따른 사항
2. 전자서명에 관한 분쟁의 조정을 받으려는 전자서명인증체계 관련자는 전자서명법 제22조에 따라 전자문서 및 전자거래 기본법 제32조에 따른 전자문서 · 전자거래분쟁조정위원회에 조정을 신청할 수 있습니다.

9.13.2 분쟁 해결 절차

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

9.14 관할 법원

본인확인서비스 관련 소송 발생시, 관할 법원은 민사소송법이 정한 바에 따릅니다

9.15 관련 법률 준수

1. 전자서명인증체계 관련자가 준수하여야 하는 법률규정은 다음과 같습니다.
- 정보통신망법, 동법 시행령 및 시행규칙, 본인확인기관 지정 등에 관한 기준
- 전자서명법, 동법 시행령 및 시행규칙
2. 본 준칙은 대한민국의 관계법령에 따라 해석되고 적용됩니다.

9.16 기타 규정

해당 사항 없습니다.

9.17 기타 조항

해당 사항 없습니다.