# 전자서명 인증업무준칙

Ver 1.2

# 제·개정 이력

| 버전 | 변경일 | 변경사유 | 변 경 내 용 | 작성자 | 승인자 |
|---|---|---|---|---|---|
| 1.0 | 2021.10.29 | - | 신규제정 | 이주원 | 박형진 |
| 1.1 | 2021.11.22 | 내용수정 | 신원확인강화 | 이주원 | 박형진 |
| 1.2 | 2021.12.15 | 내용수정 | OCSP 내용 현행화 및 오타 수정 | 이주원 | 박형진 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

* 문서 버전 : 최초 버전은 1.0으로 시작하되, 변경 사항이 오류수정 등 미비할 경우 소수점 자리, 내용 추가 등 중대한 변경이 발생한 경우는 정수 자리의 버전번호 증가로 구분

* 변경 사유 : 최초작성/내용수정/내용추가/내용삭제로 구분하여 기입

# SK텔레콤 전자서명 인증업무준칙

## 1.소개

### 1.1 개요

#### 1.1.1 배경 및 목적

본 전자서명 인증업무준칙(이하 '준칙'이라 함)은, 전자서명법(이하 '법'이라 함), 전자서명법시행령(이하 '시행령'이라 함) 및 전자서명법시행규칙(이하 '시행규칙'이라 함)과 전자서명인증업무 운영기준(이하 '운영기준'이라 함)에 의하여 SK텔레콤 주식회사(이하 'SK텔레콤'이라 함)가 SK텔레콤 PASS 인증서(이하 '인증서'라 함)의 발급, 관리, 신원확인 및 인증시스템을 운영함에 있어서 필요한 사항을 정하며, 이용자 및 가입자 등 인증 관련 당사자의 책임과 의무사항의 규정을 목적으로 합니다.

#### 1.1.2 전자서명인증체계 소개

SK텔레콤은 본 준칙에 따라 인증서의 발급 및 인증관련 기록의 관리, 인증서를 이용한 인증업무 등을 제공하기 위한 전자서명인증체계를 구성하여 관리 감독합니다.

[SK텔레콤의 전자서명인증체계]

- 가입자의 신원확인
- 인증서의 발급, 폐지 및 재발급
- 전자서명 인증관리 시스템의 구축 및 운영

### 1.2. 문서의 명칭

본 준칙의 명칭은 "SK텔레콤 전자서명 인증업무준칙'으로 합니다.

### 1.3 전자서명인증체계 관련자

#### 1.3.1 과학기술정보통신부

과학기술정보통신부는 전자문서의 안정성, 신뢰성 및 전자서명수단의 다양성을 확보하고 그 이용을 활성화하는 등 전자서명의 발전을 위하여 다음과 같은 업무를 수행합니다.

- 전자서명의 신뢰성 제고, 전자서명수단의 다양성 확보 및 전자서명의 이용 활성화
- 전자서명 제도의 개선 및 관계 법령의 정비
- 가입자와 이용자의 권익 보호
- 전자서명의 상호연동 촉진
- 전자서명법 제 9조에 따른 인정기관 지정 및 제 10조에 따른 평가기관의 선정 및 고시
- 그 밖에 전자서명의 발전을 위하여 필요한 사항

#### 1.3.2 인정기관(한국인터넷진흥원)

전자서명법 제9조에 의해 인정기관은 다음의 역할을 합니다.

- 평가 결과와 운영기준 준수사실의 인정을 받으려는 전자서명인증사업자가 제8조에 따른 자격을 갖추었는지 여부를 확인하여 운영기준 준수사실의 인정 여부를 결정
- 운영기준 준수사실을 인정하는 경우 그 인정내용 및 유효기간이 기재된 증명서를 해당 전자서명인증사업자에게 발급하며, 증명서 발급사실을 공고

**1.3.3 평가기관**

평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대해 평가를 하고, 그 결과를 인정기관에 제출하는 업무를 수행합니다.

**1.3.4 SK텔레콤 (전자서명인증사업자)**

**1.3.4.1 역할**

SK텔레콤은 전자서명인증사업자로서 가입자에게 다음과 같은 인증서비스를 제공합니다.
- 인증서비스 제공과 관련한 가입자 신원확인 업무
- 인증서 발급(신규, 재발급, 갱신 등)
- 인증서 관련 정보 공고
- 실시간 인증서 유효성 확인서비스(OCSP)
- 인증서 폐지 목록(CRL) 관리
- 기타 인증서비스와 관련된 업무

**1.3.4.2 책임과 의무사항**

① 정확한 정보 제공

SK텔레콤은 가입자와 이용자에게 인증서의 신뢰성이나 유효성에 영향을 미칠 수 있는 다음의 정보를 당사 홈페이지에 공고하고 있습니다.
- 인증업무 휴지·정지 또는 폐지
- SK텔레콤 전자서명 인증업무준칙(CPS)
- 기타 인증업무 수행 관련 정보 등

② 전자서명생성정보의 보호

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

③ 전자서명생성정보 안전조치

SK텔레콤은 전자서명생성정보의 분실·훼손, 도난·유출 등 인증서의 신뢰성이나 유효성에 영향을 미치는 사유가 발생한 사실을 인지하는 경우 가입자에게 이를 통보하며 필요한 경우 당해 전자서명생성정보로 발급한 가입자의 인증서를 폐지합니다.

④ 신원확인 및 발급정책

SK텔레콤은 사전에 가입자의 신원확인을 실지명의를 기준으로 확인한 본인확인기관으로서, 인증서를 발급받고자 하는 자에 대하여 휴대폰 본인확인과 본인 명의로 개설된 계좌를 통한 인증 및 이동통신사에 등록된 명의자에 대한 정보를 확인합니다. 또한 본인명의의 1인 1디바이스에 설치

된 SK텔레콤 PASS 어플리케이션을 기준으로 인증서를 발급하며 다른 기기로 이동 및 복사는 불가능합니다.
⑤ 가입자 개인정보보호
SK텔레콤은 인증서비스 중 취득한 개인정보를 보호하여야 하며, 수집한 개인정보를 적법한 범위 내에서 업무 목적으로만 사용하여야 합니다.
⑥ 관련 법령 및 규정 준수
SK텔레콤은 인증서비스를 수행할 때 전자서명법령, 개인정보 보호법령 등 관련 규정을 준수합니다.

### 1.3.5 가입자

#### 1.3.5.1 정의
SK텔레콤 PASS 인증서를 발급 받았거나 받으려는 SK텔레콤의 PASS(SK텔레콤의 이동통신 서비스를 이용하는 고객에 대하여 제공하는 인증서비스, 본인확인서비스, 모바일 운전면허 확인서비스, 기타 부가서비스를 통칭한 서비스) 회원을 의미 합니다.

#### 1.3.5.2 책임과 의무사항
① 신뢰할 수 있는 단말기를 이용하여 안전한 방법으로 본인의 전자서명생성정보를 생성하여야 합니다.
② SK텔레콤이 인증업무를 위하여 신원확인 정보를 요청하는 경우 가입자는 정확한 정보를 제공하여야 하며 제공한 정보가 완전하게 유지되도록 하여야 합니다.
③ 정당한 용도 및 제한에 맞게 인증서를 사용 하여야 하며 인증서에 포함된 전자서명검증정보에 합치하는 전자서명생성정보를 사용하여야 합니다.
④ 생성된 인증서 정보가 분실·훼손 또는 유출되지 않도록 잘 관리하여야 합니다.
⑤ 스마트폰을 분실하였거나, 스마트폰 내 인증서가 안전하지 않다고 인지하는 경우 지체없이 관련사실을 통보하고, 해당 인증서를 폐지할 수 있도록 협조 하거나 SK텔레콤 PASS 어플리케이션에서 인증서 삭제 메뉴를 통해 인증서를 삭제하여야 합니다.
⑥ 인증서 사용에 있어 다음의 사유로 발생되는 모든 책임과 비용에 대하여는 SK텔레콤의 면책을 보장합니다.
- 가입자가 사실과 다르게 제공한 정보
- 가입자가 태만 또는 고의로 제공하지 않은 변경된 정보
- 가입자의 전자서명생성정보 관리 부주의(정보 노출, 분실, 변조 등)

⑦ 본 사항은 인증서를 발급할 때부터 시작됩니다.

### 1.3.6 이용자(이용기관)

#### 1.3.6.1 정의
SK텔레콤이 제공하는 인증서비스를 이용하여 가입자의 전자서명생성정보와 전자서명검증정보의 합치성을 확인하려는 자(개인, 법인, 단체, 개인사업자 등)를 말합니다.

#### 1.3.6.2 책임과 의무사항

① 이용자는 SK텔레콤이 제공하는 인증서비스의 이용 목적 및 이용가능범위를 이해하여야 하고, 가입자가 제공한 인증서가 이용자의 목적과 적합한지(또는 목적에 부합하는지) 판단하여야 합니다.
② 이용자는 인증서 폐지 목록을 통해 인증서가 유효한 인증서인지 확인해야 합니다.
③ 이용자는 SK텔레콤이 제공한 인증데이터의 진위여부를 확인하여야 합니다.
④ 이용자는 사기 또는 위조된 전자서명의 이용 등 고의 및 중과실 또는 악의적 방법으로 SK텔레콤의 가입자에게 손해를 입히면 SK텔레콤 가입자에게 그 손해를 배상해야 합니다.

### 1.3.7 등록대행기관

#### 1.3.7.1 역할

SK텔레콤은 SK텔레콤을 대신하여 가입자에 대한 신원확인을 수행하고 인증서 발급 또는 폐지 등의 신청을 접수 및 등록하는 외부기관을 지정하여 운영할 수 있습니다. 등록대행기관의 업무는 다음과 같습니다.

#### 1.3.7.2 책임 및 의무사항

① 가입자의 신원확인
등록대행기관은 인증서를 발급받고자 하는 자에 대하여 전자서명관련법에서 정하는 신원확인의 기준 및 방법에 따라 신원을 확인하여야 하며 신청내용의 무결성을 확인하여야 합니다.
② 배상 및 책임
등록대행기관은 본 인증업무준칙상 의무사항을 위반함으로써 SK텔레콤, 가입자 또는 이용자에게 손해를 입힌 경우 그 손해에 대해 배상할 책임이 있습니다.
③ 인증업무준칙의 준수
등록대행기관은 PASS 인증서 서비스 제공과 관련하여 본 인증업무준칙에서 정한 등록대행기관의 업무를 성실히 수행할 의무를 가집니다.
④ 가입자의 개인정보보호
등록대행기관은 등록대행업무 수행 중 취득한 가입자의 개인정보를 보호하고 자료에 대한 보안을 유지할 의무가 있습니다.

## 1.4 인증서 종류

### 1.4.1 인증서의 발급 대상

SK텔레콤은 개인에게 인증서를 발급합니다.

### 1.4.2 인증서의 용도와 유효기간

인증서의 유효기간은 원칙적으로 3년으로 하며 유효기간은 SK텔레콤의 정책에 따라 변경될 수 있습니다. 또한 해당 유효기간 내 다음과 같은 인증서를 발급 할 수 있습니다.

| 구분 | 용도 | 유효기간 |
|---|---|---|

| | | |
|---|---|---|
| 개인용 | 본인인증 및 전자서명이 필요한 전자적 업무<br>- 금융기관업무<br>- 정부 및 공공기관업무<br>- 사업자간 계약 또는 합의된 업무 | 발급일로부터 3년 |

#### 1.4.3 인증서의 이용 제한

SK텔레콤이 발급하는 모든 인증서는 발급 시의 용도 및 사업자간 계약 또는 합의된 업무 내에서만 이용되어야 합니다. 발급 받은 목적과 용도에 벗어나 부정하게 사용하는 것을 금지합니다. 또한 유효기간이 만료 또는 폐지된 인증서를 사용하여서는 안 됩니다.

### 1.5 인증업무준칙의 관리

#### 1.5.1 인증업무준칙 제정 및 개정 기관

SK텔레콤은 인증업무준칙을 제정하고 인증 정책의 일관성을 유지하기 위한 개정을 관리합니다.

#### 1.5.2 인증업무준칙 개정 관리

본 인증업무준칙의 변경이 필요하다고 판단한 경우에 이를 개정합니다. 또한, 본 인증업무준칙이 개정된 경우 다음의 내용을 포함한 인증업무준칙의 개정 관련 기록을 유지/관리하여야 합니다.

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

#### 1.5.3 인증업무준칙 수립 및 개정 담당자

본 준칙의 제·개정 최종 승인은 인증업무 관리책임자에게 있으며, 기술적 또는 절차적인 변경 등의 사유가 발생할 경우 인증업무 관리책임자의 승인을 받아 개정합니다.

- 관리부서 : SK텔레콤 인증사업팀
- 전자우편 : pass@sk.com
- 주소 : 서울특별시 중구 을지로65 SK T-타워

#### 1.5.4 인증업무준칙의 공지

SK텔레콤은 개정된 준칙을 홈페이지에 즉시 공고합니다.

- 준칙 공지 위치 : SK텔레콤 홈페이지 및 SK텔레콤 PASS 어플리케이션 내 공지

#### 1.5.5 인증업무준칙에 대한 가입자동의

가입자가 개정된 준칙이 공고된 후 30일(공고일 포함) 내에 서면으로 이의를 제기하지 아니한 경우 SK텔레콤은 가입자가 개정된 준칙에 동의한 것으로 간주합니다.

### 1.6 정의 및 약어

본 준칙에서 사용하는 용어 및 약어는 전자서명법 및 그 하위 법령에 의거하여 해석 및 적

용됩니다.

## 2. 전자서명인증업무 관련 정보의 공고

### 2.1 공고설비

① SK텔레콤은 인증서, 인증서 효력 정지 및 폐지 목록 등 전자서명인증업무와 관련된 정보를 인증관리체계에 의하여 이중화 구성(Active-standby)으로 안정적으로 운영하고 있으며, 누구든지 그 사실을 항상 확인할 수 있도록 공고합니다.
② SK텔레콤은 전자서명인증업무 관련 정보를 적시에 정확한 제공을 위해 공고설비를 안전하게 운영 관리합니다.

### 2.2 공고방법

① SK텔레콤은 인증업무준칙을 포함하여 전자서명인증서비스에 필요한 신청서 양식과 관련규칙을 홈페이지를 통해 관리합니다.
② SK텔레콤은 인증서 효력 정지 및 폐지 목록에 대해서는 변경 사유가 없더라도 매일 1회 이상 정기적으로 갱신한 후 공고합니다.
- 공고 위치 : https://sktpass.com/pass_terms_02.html

### 2.3 공고주기

① SK텔레콤은 인증업무준칙 및 이용약관의 개정 승인 날로부터 15일 이내에 전자서명인증업무 관련 정보를 홈페이지 및 SK텔레콤 PASS 어플리케이션에 게시합니다.
② SK텔레콤은 인증서 폐지 목록을 12시간 주기로 갱신합니다.

### 2.4 공고된 정보에 대한 책임

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

## 3. 신원확인

### 3.1 가입자 이름 표시 방법

가입자 이름(DN) 표현 및 유일성 보장은 인증서 발급 시 가입자 이름을 CN(Common Name) 값에 기술하며, DN은 이름과 가입자의 전화번호 등을 통해 생성된 고유값을 통해 유일성을 보장합니다.

### 3.2 인증서 신규 발급 시 신원확인

SK텔레콤 PASS 인증서는 개인만을 대상으로 하여 발급하며 아래의 방법으로 신원을 확인합니다.
① 인증서 발급을 위한 SK텔레콤 PASS 어플리케이션 접속 시 가입자의 사용자인증(PIN, 생체인증)을 통해 PASS 서비스 가입자 정보를 확인합니다.

② 가입 신청자는 본인명의 휴대폰을 이용하여 신청자의 SK텔레콤 PASS 어플리케이션에 등록된 정보(이름, 생년월일, 휴대전화번호 등)를 통해 이동통신사의 휴대폰 본인인증을 수행합니다.
③ 가입 신청자는 본인명의로 개설된 계좌 정보를 입력합니다. 해당 정보의 계좌정보가 유효하며 송금 가능한지 확인한 후 입력된 계좌에 소액의 금액을 이체하며 송금에 따른 고객계좌의 적요에 생성된 인증코드(숫자)를 입력하여 계좌점유인증을 수행합니다.
④ SK텔레콤 PASS 인증서 발급 시 가입자의 2차 사용자인증(PIN, 생체인증)을 통해 재검증합니다

### 3.3 인증서 재발급 시 신원확인

인증서 재발급 시 [3.2 인증서 신규발급 시 신원확인]과 동일한 절차로 신원을 확인합니다.

#### 3.3.1 가입자 신원확인

인증서의 재발급 시 신원확인 방법은 다음과 같습니다.
①휴대폰 본인인증
- 신규 가입과 동일하게 휴대폰 본인인증을 통하여 신원확인을 진행합니다.
②계좌점유인증
- 신규 가입과 동일하게 본인 명의의 계좌를 통하여 계좌점유인증을 진행합니다.
③PIN코드 또는 생체인증 입력
- 휴대폰 본인인증에 성공한 경우, 가입자가 최초 인증서를 생성하면서 단말 내 SK텔레콤 PASS 어플리케이션에 설정한 PIN코드 또는 생체인증 정보를 입력하여 본인 여부를 한 차례 더 검증합니다.

### 3.4 인증서 폐지 시 신원확인

#### 3.4.1 가입자 신원확인

인증서는 가입자가 SK텔레콤 PASS 어플리케이션에 로그인하고 인증서 메뉴에서 직접 삭제하거나, 고객센터를 통해 가입자의 신원을 별도로 확인 후 관리자에 의하여 인증서를 삭제 할 수 있습니다.

## 4. 인증서 관리

### 4.1 인증서 발급 신청

가입자는 인증사업자 소프트웨어(SK텔레콤 PASS 어플리케이션)를 이용하여 인증서 발급 요청 기능을 실행함으로써 발급 신청 처리가 시작됩니다.

### 4.2 인증서 발급 신청 처리

#### 4.2.1 가입 신청자 식별 및 신원확인

개인이 인증서를 신규 발급받는 경우 신원확인 방법은 다음과 같습니다.

①가입자는 이용약관 및 개인정보 수집·이용에 동의합니다.
②SK텔레콤이 정하는 방식으로 가입자의 신원을 확인합니다. 휴대폰 본인인증 단계를 거쳐 신원 확인이 진행됩니다.
③본인명의의 계좌를 통해 계좌점유인증을 진행합니다. 만약 이상거래자로 판단될 경우 SK텔레콤은 추가 인증을 요구할 수 있습니다.
④SK텔레콤은 가입자가 제출한 전자서명검증정보의 유일성과 정보의 합치여부 확인을 통하여 전자서명생성정보의 소유자가 가입자 본인임을 확인합니다.

#### 4.2.2 인증서 발급 제한

다음에 해당하는 경우, 인증서 발급 신청이 제한됩니다.
①만14세 미만의 가입자
②타인의 명의를 도용하여 신청하였거나 그렇다고 의심되는 경우
③신청서에 허위 사실을 기재 또는 허위서류를 첨부하였거나 그렇다고 의심되는 경우
④업무상 또는 기술상 문제로 인증서를 발급하지 못하는 경우
⑤사고정보를 이용하여 신청 또는 발급하였거나 그렇다고 의심되는 경우
⑥단말기 또는 추가인증 등에 실패한 경우

### 4.3 인증서 발급 절차 및 보호조치

#### 4.3.1 인증서 발급 절차

가입자의 단말 내에서 key 쌍이 생성되고, 이 중 전자서명검증정보를 SK텔레콤 서버로 전송하면 SK텔레콤 서버는 이를 검증하고 인증서를 발급하여 가입자 단말 내 안전하게 저장합니다. 이 과정은 모두 가입자의 개입 없이 시스템 간의 통신으로 이루어집니다.

#### 4.3.2 정보통신망을 통해 전송되는 가입자 정보의 전송 방법

SK텔레콤은 정보통신망을 통해 가입자정보를 전송하는 경우 기밀성, 무결성 보장을 위해 HTTPS 암호통신망 또는 전용선을 통해 전송합니다.

### 4.4 인증서 수령

가입자는 SK텔레콤이 제공하는 SK텔레콤 PASS 어플리케이션을 이용하여 SK텔레콤이 생성한 인증서를 HTTPS 암호통신망을 통해 수령한 후 안전하게 저장합니다.

### 4.5 인증서 이용

SK텔레콤이 발급하는 인증서는 인증서를 필요로 하는 일반 전자거래의 모든 분야 및 기타 전자서명관련 제반 분야에서 사용 가능합니다. 인증서의 유효기간은 3년입니다. 가입자는 정당한 이용범위 및 용도에 맞게 인증서를 사용하여야 하며, 인증서를 사용하여 전자서명을 제공할 때에는 당해 인증서에 포함된 전자서명검증정보에 합치하는 전자서명생성정보를 사용하여야 합니다. 가입자는 신뢰할 수 있는 소프트웨어나 하드웨어를 이용하여 전자서명정보를 생성하며, 생성된 전

자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 보관·관리하여야 합니다.
또한 가입자는 전자서명생성정보가 분실·훼손 또는 도난·유출되었거나 안전하지 않다고 인지하는 경우, 지체없이 SK텔레콤에 관련사실을 통보하여 SK텔레콤이 해당 인증서를 폐지할 수 있도록 협조하여야 합니다.

### 4.6 인증서 갱신발급

SK텔레콤은 만료되지 않은 인증서의 유효기간을 연장하는 갱신발급 기능을 제공하지 않습니다.

### 4.7 인증서 재발급

인증서의 재발급은 인증서의 유효기간이 경과한 경우, 이용자가 자신의 인증서를 삭제(폐지)하였거나 스마트폰을 분실한 경우, 기기를 변경한 경우, 휴대전화번호가 변경된 경우, SK텔레콤 PASS 어플리케이션을 삭제하거나, SK텔레콤 PASS 어플리케이션 내 데이터를 삭제하는 경우, PASS 내 PIN번호 입력 오류로 초기화되는 경우, 전자서명생성정보의 노출, 손상 등이 우려되는 경우에 새로운 인증서를 다시 발급받는 것을 말합니다. 재발급된 인증서의 유효기간은 PASS 인증서 재발급일로부터 3년입니다.

#### 4.7.1 유효기간 만료 혹은 이용자 요청에 의한 재발급

인증서의 유효기간이 경과한 경우나, 유효기간이 남아있더라도 이용자의 요청(인증서 삭제, 데이터 삭제, 전자서명생성정보의 노출, 손상 등)에 의한 재발급 절차는 다음과 같습니다.
①재발급 요청한 가입자의 신원확인을 위해 휴대폰 본인확인을 다시 한 번 거칩니다. 휴대폰 본인확인 결과로 확인한 연계정보 값이 현재 로그인된 가입자의 계정에 등록된 연계정보와 일치하는 경우에만 다음 단계로 진행합니다.
②본인명의의 계좌를 통해 계좌점유인증을 진행합니다. 만약 이상거래자로 판단될 경우 SK텔레콤은 추가 인증을 요구할 수 있습니다.
③가입자가 등록한 PIN 코드를 입력합니다. PIN코드를 올바르게 입력한 경우에는 인증서가 재발급되고 프로세스를 종료하며, PIN코드 입력에 실패하면 기존 인증서가 폐지됩니다. PIN코드 재설정 후 인증서를 재발급할 수 있습니다.

#### 4.7.2 PIN코드 입력 실패에 의한 재발급

PIN코드 및 생체정보 입력을 5회 이상 실패한 경우의 재발급 절차는 다음과 같습니다.
①가입자의 신원확인을 위해 휴대폰 본인확인을 다시 한번 거칩니다. 휴대폰 본인확인 결과로 확인한 연계정보 값이 현재 로그인된 가입자의 계정에 등록된 연계정보와 일치하는 경우에만 다음 단계로 진행합니다.
②본인명의의 계좌를 통해 계좌점유인증을 진행합니다. 만약 이상거래자로 판단될 경우 SK텔레콤은 추가 인증을 요구할 수 있습니다.
③PIN코드를 재설정합니다. PIN코드 재설정에 성공하면, 신규 인증서를 재발급합니다.

#### 4.7.3 기기변경, 번호변경, 명의변경에 의한 재발급

기기변경, 번호변경, 명의변경하는 경우, 재발급절차는 신규발급과 동일한 절차로 합니다.

단, 기존 발급된 인증서는 폐지됩니다.

### 4.8 인증서 변경

SK텔레콤은 인증서 변경 기능을 제공하지 않습니다. 가입자의 등록 정보가 변경된 경우, 해당 가입자는 현재 인증서를 폐지하고 재발급 받아야 합니다.

### 4.9 인증서 효력정지/효력회복/폐지

#### 4.9.1 인증서 효력회복

SK텔레콤은 인증서 효력 회복 기능을 제공하지 않습니다.

#### 4.9.2 인증서 폐지

##### 4.9.2.1 인증서 폐지 사유

SK텔레콤은 다음 사유 발생 시 당해 인증서를 폐지할 수 있습니다.
①가입자 또는 그 대리인이 인증서 폐지를 신청한 경우
②가입자가 부정한 방법으로 인증서를 발급 받은 사실 또는 이용한 사실을 인지하였거나, 그 가능성을 객관적으로 인지한 경우
③가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출된 사실을 인지한 경우
④가입자가 SK텔레콤의 약관 및 운영정책 또는 본 전자서명 인증업무준칙을 위반한 경우
⑤가입자의 신원확인이 적법하게 이루어지지 않았음을 SK텔레콤이 인지한 경우

##### 4.9.2.2 인증서 폐지신청 방법

① SK텔레콤 PASS 어플리케이션을 삭제하거나 모바일 기기를 변경했을 경우 자동으로 삭제(폐지)됩니다.
② 가입자는 SK텔레콤 PASS 어플리케이션 내 인증서 > 설정 메뉴에서 인증서 삭제를 눌러 직접 삭제(폐지)를 신청할 수 있습니다.
③ 가입자 또는 대리인은 SK텔레콤 고객센터를 통하여 첨부서류와 함께 인증서 폐지를 신청할 수 있습니다.

| 신청자 | 신청사유 | 신청시 필요서류 |
|---|---|---|
| 가입자 본인 | 전자서명생성정보의 분실,훼손 또는 도난,유출 등 기타사유로 인증서를 폐지하고자 하는 경우 | 마스킹 처리된 본인 신분증 사본 |
| 법정대리인 | 가입자의 사망,실종,파산,한정치산,금치산 등 | 사망,실종,파산,한정치산,금치산을 입증할 수 있는 서류, 법정대리인 증명서류 |

##### 4.9.2.3 인증서 폐지 절차

가. SK텔레콤 PASS 어플리케이션 내 인증서 삭제 메뉴를 통한 신청

①인증서 폐지 신청
SK텔레콤 PASS 어플리케이션 내 인증서 > 설정 메뉴에서 인증서 삭제를 눌러 직접 폐지를 요청합니다.
②가입자 신원확인
가입자가 등록한 PIN 코드를 입력 또는 생체인증을 수행하여 본인 여부를 검증합니다.
③인증서 폐지 사실의 확인 방법 제공
인증서는 요청과 본인 여부 검증 즉시 폐지 처리한 후, 인증서 폐지 목록을 갱신합니다.

나. SK텔레콤 고객센터 문의하기를 통한 신청
①인증서 폐지 신청서 제출
가입자는 인증서 폐지 신청서와 SK텔레콤 요구하는 첨부서류를 첨부하여 고객센터를 통해 폐지를 요청합니다.
②가입자 신원확인
SK텔레콤은 신청자가 제출한 첨부서류를 검토하여 신청자의 신원을 확인합니다.
③인증서 폐지 사실의 확인 방법 제공
SK텔레콤은 당해 인증서를 폐지 처리한 후, 인증서 폐지 목록을 갱신하고 누구든지 그 사실을 항상 확인할 수 있도록 지체 없이 공고합니다. 공고 방법은 [2.2 공고방법]에 기술한 바에 따릅니다.

다. SK텔레콤의 직권에 따른 폐지
SK텔레콤은 가입자가 부정한 방법으로 인증서를 발급 받은 사실 또는 이용한 사실을 인지하였거나, 그 가능성을 객관적으로 인지한 경우 등 SK텔레콤의 약관 및 운영정책 또는 본 전자서명 인증업무준칙을 가입자가 위반한 사실을 객관적으로 인지한 경우 당해 인증서를 폐지 처리한 후, 인증서 폐지목록을 갱신하고 누구든지 그 사실을 항상 확인 할 수 있도록 지체 없이 공고합니다. 공고방법은 [2.2 공고방법]에 기술한 바에 따릅니다.

#### 4.9.2.4 인증서 폐지 목록의 갱신 빈도
SK텔레콤은 인증서 효력정지 및 폐지 목록을 12시간마다 갱신합니다. 또한 SK텔레콤은 인증서 유효성 확인 서비스를 통해 조회할 수 있도록 제공하고 있으며, 인증서 폐지 시 해당 정보는 실시간으로 갱신됩니다.

#### 4.9.2.5 인증서 폐지 신청의 처리 소요시간
SK텔레콤 PASS 어플리케이션 내 인증서 삭제 메뉴에서 신청한 경우 가입자가 등록한 PIN 코드 입력 또는 생체인증을 통해 본인 여부를 검증한 후 즉시 폐지 처리합니다. SK텔레콤 고객센터에서 신청한 경우 신청자의 신청서와 첨부서류를 통해 신원을 확인한 후 3영업일 이내에 인증서의 폐지 처리를 완료합니다.

### 4.10 인증서 유효성 확인 서비스
SK텔레콤은 인증서 유효성 확인 서비스(OCSP)를 제공받고자 하는 경우 서비스제공기관과의 계약에 의해 서비스를 제공할 수 있습니다. 이때 서비스 이용 수수료, 이용계약의 해지, 기타 제공 조

건 등은 상호 협의된 계약의 내용에 따릅니다

### 4.11 서비스 가입 철회

가입자는 SK텔레콤 PASS 어플리케이션 계정을 탈퇴함으로써 전자서명인증서비스의 가입을 철회할 수 있습니다. SK텔레콤 계정을 탈퇴하는 방법 및 절차는 SK텔레콤 계정 약관이 정하는 바에 따릅니다. 가입 철회 시 인증서 및 관련 정보는 유관 법령에서 따로 정함이 없는 한 지체없이 파기됩니다.

### 4.12 기타 부가 서비스

기타 부가 서비스는 제공되지 않습니다.

## 5. 시설 및 운영 관련

### 5.1 물리적 보호조치

#### 5.1.1 시설 위치와 구조

SK텔레콤의 전자서명인증업무를 위한 인증서 발급 및 전자서명 처리 시스템은 총 2곳의 데이터센터에 이중화 구성되어 있으며, 다른 시스템과 물리적으로 분리되어 있습니다.

#### 5.1.2 물리적 보호조치

SK텔레콤의 인증시스템 데이터센터는 철저한 통제에 따라 승인된 외부인과 관련자의 출입 및 접근만을 허용하며 다음과 같이 안전하게 보호합니다.

① SK텔레콤은 외부인의 침입이나 불법적 접근 등의 물리적 위협으로부터 인증시스템 등이 설치된 장소를 보호합니다.
② SK텔레콤의 인증시스템은 데이터센터 내의 별도의 통제구역 내에 설치, 운영하고, 랙별 시건장치를 통해 인가된 사용자에게만 물리적인 접근을 허용합니다.
③ SK텔레콤은 CCTV 카메라 및 모니터링 시스템과 침입감지 시스템 등 철저한 감시통제시스템을 설치하고 운영합니다.
④ SK텔레콤의 출입통제 시스템은 신원확인카드, 안면인식 장치 등을 다중으로 결합하여 통제구역에 대한 접근을 통제합니다.
⑤ SK텔레콤은 24시간 관제실을 통해 인증시스템을 모니터링하며 보안요원의 상시 점검을 시행하고 통제구역 내 출입내역을 관리합니다.

#### 5.1.3 화재, 수재, 정전방지 및 방호

##### 5.1.3.1 화재예방

SK텔레콤은 인증시스템실 등에 화재 탐지기, 휴대용 소화기 및 자동소화설비를 설치합니다.

#### 5.1.3.2 수재방지

SK텔레콤은 침수로부터 인증시스템을 안전하게 보호하기 위하여 바닥으로부터 이격하여 설치합니다.

#### 5.1.3.3 정전방지

SK텔레콤은 갑작스러운 정전으로 인한 피해를 방지하기 위하여 다음과 같은 조건을 준수합니다.

- 전원 공급의 이중화
- 비상발전기 운용 및 비상발전기 전환까지 유지되는 UPS 보유

### 5.1.4 항온/항습, 통풍 및 기타 보호설비

SK텔레콤은 인증시스템의 항온을 위한 냉방기기를 이중화하여 설치 및 운영하고 항습은 공조기를 통해 자동조절되며, 통풍창은 사람이 통과할 수 있는 경우 차폐막을 설치하고 있습니다.

### 5.1.5 시설 및 장비의 폐지처리

SK텔레콤은 문서 및 장비 등을 폐지하는 경우 물리적으로 완전히 파기 처리하며 폐지처리에 대한 사항은 내부지침에 따라 안전하게 폐지합니다.

### 5.1.6 원격지 백업설비 안전운영

백업된 전자서명생성정보는 전자서명인증업무 수행시설과는 떨어진 별도의 원격지의 저장설비를 마련하여 별도로 보관하며 안전한 운영을 위해 비인가자의 접근을 철저히 차단하고 이를 CCTV를 설치하여 모니터링 합니다.

## 5.2 절차적 보호조치

### 5.2.1 업무의 종류와 그 업무 분장

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

① 인증업무관리책임자(CA Head, CAH)는 인증업무 정책, 사업연속성계획, 재해복구계획 등을 승인합니다.
② 인증정책관리자(Policy Administrator, PA)는 인증업무 정책 수립, 등록, 유지 및 개정합니다.
③ 보안관리자(Security Manager, SM)는 인증시스템과 인증서비스에 대한 보안을 관리합니다.
④ 내부감사자(Internal Auditor, IA)는 인증서 발급 및 관리에 대한 정기적인 내부감사를 수행합니다.
⑤ 키 관리자(CA Key Manager, CKM)는 암호화 모듈 장비를 입고하고 적절한 장소에 보관합니다. 암호화 모듈 장비 관련된 키 생성 데이터를 내화금고에 안전하게 보관하며, 해당 데이터 사용이 적절하게 수행되었는지 확인합니다. 암호화 모듈 활성화에 필요한 접근권한(m of n) 담당자에게 필요한 물품 및 정보를 제공하고 관리합니다.
⑥ 보안 금고 관리자는 인증 시스템실 내 금고 및 금고 내 물품을 관리·보관합니다.
⑦ 키 소유자는 인증시스템 주요 key를 관리 및 보관하며, MofN 인증 시 보유한 key를 통해 인

증을 수행합니다.

⑧ 인증서 신규발급 관리자(CA System Administrator, SA)는 인증시스템의 인증서 신규 발급/재발급/갱신/폐지를 수행하고 관리합니다.

⑨ 인증기관 웹사이트 관리자는 인증업무준칙(CPS)을 웹사이트에 게시하고 관리합니다. 개인정보보호지침 등 공개가 필요한 규정 및 규칙을 공개하고 관리합니다. 이 외 필요하다고 판단되는 정보에 대해 내부 승인을 득한 후 공개하고 관리합니다.

⑩ 개발자(Developer, DEV)는 인증업무에 필요한 개발을 수행하고 관리합니다. 국내외 국제 기술표준 및 필요에 의한 기술요건을 분석하고, 시스템 및 어플리케이션에 적용합니다. 테스트용 인증서를 발급하고 관리합니다. 인증시스템 감사로그에 해당업무가 기록되는지 확인합니다.

⑪ 운영자(Operator, OP)는 인증센터의 시설 및 장비를 운영하고 관리합니다. 인증시스템에 사용되는 네트워크를 관리합니다. 시설 및 장비에 필요한 유지보수 업무를 관리합니다.

#### 5.2.2 전자서명 인증업무 주요 업무별 수행인력

SK텔레콤은 인증업무 운영 시의 신뢰성 및 보안성 확보를 위하여 다음과 같이 업무분리 원칙을 준수합니다.

①3인 이상의 권한이 있는 직원에 의해 SK텔레콤의 전자서명생성정보를 생성합니다..

②동일 시스템에 대한 운영관리자 및 보안감사자에 대한 역할을 구분하고, 접근통제를 시행합니다.

#### 5.2.3 인증업무 담당자 인증방법

SK텔레콤 인증시스템 업무 담당자는 소지기반 및 안면인식 등의 인증방법을 통하여 출입을 통제하고, 인증업무시스템의 접근은 업무 권한에 따라 접근을 통제합니다.

### 5.3 인적 보안

#### 5.3.1 자격 요건

SK텔레콤 인증시스템의 운영인력은 국가가 인정한 정보통신 관련 자격을 취득하거나 이에 준하는 업무 경력을 보유 하여야 합니다.

#### 5.3.2 교육 및 업무 순환

① 인증시스템을 관리하는 직원은 연1회 이상 정보보호 관련 내부 또는 외부교육을 이수하도록 합니다.

② 인증시스템을 관리하는 직원에 대하여 업무상 취득한 기밀사항의 준수에 관한 서약서를 작성하여 날인하도록 합니다.

③ 업무순환 및 업무환경의 변화 등으로 인하여 보호조치의 수정·보완이 필요한 경우, 이를 지체없이 보완합니다.

④ 인증시스템을 관리하는 직원이 인사이동 또는 퇴직하는 경우에는 내부규정에 따라 계정삭제 및 저장매체 반납 등의 적절한 조치를 취합니다.

#### 5.3.3 비인가된 행위에 대한 처벌
비인가된 행위에 대하여 SK텔레콤은 내부 규정에 정하는 바에 따라 해당 직원을 징계합니다.

### 5.4 감사 기록

#### 5.4.1 감사 기록의 유형 및 보존기간
SK텔레콤은 인증업무 운영과 관련해 다음과 같은 내용을 기록하며 이를 5년간 보관합니다.
①인증서 관리에 관한 기록(인증서 발급/재발급/삭제 등)
②인증서 사용에 관한 기록(전자서명 생성/이용/전달 등)
③인증서 발급에 사용되는 개인정보 등

#### 5.4.2 감사기록의 보호조치
각 시스템의 감사기록은 보안감사자에 의해 총괄 관리되며 시스템의 각 업무관리자는 해당하는 업무에 대한 감사기록만 열람할 수 있습니다.

#### 5.4.3 감사기록의 백업주기 및 절차
SK텔레콤은 각 인증시스템의 감사기록을 주기적으로 백업하여 원격지 시설 내 저장장치에 보존합니다.

### 5.5 기록 보존

#### 5.5.1 보존기록의 유형 및 보존기간
SK텔레콤이 보존하는 기록의 유형은 다음과 같으며 보존기록의 보관기간을 저장 공간의 가용성과 관리의 효율성을 고려하여 인증서가 폐지된 날로부터 5년간 보관합니다
①"5.4.1 감사기록의 유형 및 보존기간"에 정의된 유형
②기타 인증 시스템 운영 및 관리의 중요 활동 등

#### 5.5.2 보존기록의 보호조치
SK텔레콤은 보존기록에 대해 엄격한 물리적 접근통제 및 절차통제를 적용하여 보안을 유지합니다. 보존기록의 조회는 업무범위에 한해 조회가 가능합니다. 보존장소는 항원, 항습기를 설치하고 화재의 발생에 대비하여 화재경보기등의 보호설비를 설치하여 운영합니다.

#### 5.5.3 보존기록의 백업주기 및 백업절차
SK텔레콤은 보존기록을 천재지변 및 기타 재난 발생시 보존기록의 손실 및 파괴에 대비하여 원격지 저장 설비에 주기적으로 백업하여 보존합니다.

### 5.6 전자서명인증사업자의 전자서명생성정보 갱신
인증사업자의 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.

### 5.7 장애 및 재해 복구

#### 5.7.1 장애 및 재해 유형별 처리 및 복구 절차
전자서명인증업무 장애 및 재해 시, 내부 규정인 "재해복구 관리지침"에 따라 전파 및 복구를 진행합니다.

#### 5.7.2 업무 장애방지 등 연속성 보장 대책
① 핵심인증시스템 및 서비스 운영과 관련된 시스템은 이중화로 구성하여 주 시스템에 문제가 발생하여도 인증서비스가 가능하도록 구성합니다.
② 주기적인 재해복구 모의훈련 절차서에 따라 재해복구 모의훈련을 진행하고 재해복구 모의훈련 평가서를 통해 효과성을 확인합니다.
③ 인증서 가입자의 주요 데이터가 훼손되었을 경우 백업된 자료를 이용하여 신속히 복구하여 서비스의 연속성을 보장합니다.

### 5.8 업무 휴지, 폐지, 종료
① SK텔레콤이 부득이한 사유로 전자서명인증사업을 휴지, 폐지 또는 종료하는 경우 휴지기간을 정하여 휴지하고자 하는 날의 30일전까지 홈페이지 공지 및 이를 이용자에게 전자우편, SK텔레콤 PASS 어플리케이션 및 기타 방법으로 통보합니다.
② SK텔레콤이 부득이한 사유로 인증업무를 폐지하는 때에는 폐지하고자 하는 날의 60일 전까지 홈페이지 및 이를 이용자에게 전자우편 및 SK텔레콤 PASS 어플리케이션 및 기타 방법으로 통보합니다.

## 6. 기술적 보호조치

### 6.1 전자서명생성정보 보호

#### 6.1.1 전자서명생성정보 생성
① 내부 규정에 따라 인가된 자만이 전자서명생성정보를 생성할 수 있습니다.
② SK텔레콤은 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되며 FIPS 140-2 level 3를 충족하는 안전한 하드웨어보안장치(HSM)를 사용하여 전자서명생성정보를 생성합니다.
③ 전자서명생성정보 생성 작업은 다자인증 통제(최소 3명 이상) 하에서 전자서명생성정보를 생성합니다.

#### 6.1.2 전자서명생성정보의 크기 및 해시값

SK텔레콤은 안전하고 신뢰할 수 있는 전자서명 알고리즘을 사용하기 위하여 다음과 같은 크기의 키 및 해시값을 이용합니다.

① RSA : 2,048bit 이상

② SHA-256 : 256bit

### 6.2 전자서명생성정보 보호조치

#### 6.2.1 전자서명생성정보의 저장 시 보호조치

SK텔레콤은 전자서명생성정보를 안전하게 저장하기 위하여 전자서명생성정보가 분실, 훼손 또는 도난, 유출되지 않도록 하드웨어보안장치(HSM)에 안전하게 관리합니다.

#### 6.2.2 전자서명생성정보의 이용 시 보호조치

SK텔레콤은 전자서명생성정보를 이용할 경우 안전하게 이용하기 위하여 하드웨어보안장치(HSM) 내에서 전자서명 업무를 수행합니다..

#### 6.2.3 전자서명생성정보의 백업 보관 시 보호조치

① SK텔레콤은 백업된 전자서명생성정보 중 1부를 전자서명인증업무 수행 시설과는 별도의 원격지 저장설비에 안전하게 보관합니다.

② SK텔레콤은 전자서명생성정보를 백업 보관하는 경우, 2인 이상의 권한 있는 직원이 공동으로 이를 수행합니다.

#### 6.2.4 전자서명생성정보의 삭제 및 파기 시 보호조치

① SK텔레콤은 인증서 유효기간이 만료되거나 전자서명생성정보가 훼손, 유출되었을 때 해당 전자서명생성정보 저장매체를 물리적으로 완전히 파기하거나, 전자서명생성정보를 삭제합니다.

② SK텔레콤은 인증업무관리책임자와 보안관리자의 승인 하에 백업된 전자서명생성정보와 그 원본을 안전하게 파기합니다.

### 6.3 전자서명생성정보 및 전자서명검증정보의 관리

SK텔레콤은 신뢰할 수 있는 소프트웨어나 하드웨어보안장치(HSM) 등을 이용하여 안전한 방법으로 전자서명생성정보를 생성하며 생성된 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리합니다

### 6.4 데이터 보호조치

SK 텔레콤은 권한이 있는 관리자만 데이터에 접근할 수 있습니다.

① 접근 권한 최소화 및 사전승인으로 접근 권한을 통제합니다.

② 데이터 접근 권한의 적정성을 주기적으로 점검합니다.

③ 부적절한 접근 권한일 경우 회수 및 철회합니다.

### 6.5 시스템 보안 통제

① SK 텔레콤은 전자서명시스템을 이중화하여 구성하고 있습니다.
② SK 텔레콤은 전자서명인증업무와 관련된 프로그램, 프로세스의 동작 여부를 점검할 수 있는 시스템을 설치하여 운영하고 있습니다.
③ SK 텔레콤은 전자서명인증시스템의 운영에 필요한 프로그램만 설치하여 관리하고 있습니다.
④ SK 텔레콤은 전자서명인증시스템의 접근을 최소화하고 제한된 인원에 한해 접근 권한을 부여합니다.
⑤SK 텔레콤은 전자서명생성정보를 생성하기 위한 단말기에 대한 보안통제를 수행합니다.

### 6.6 시스템 운영 관리

① SK 텔레콤은 전자서명시스템의 소프트웨어 개발/도입/폐지 절차에 따라 안전하게 운영합니다.
② SK 텔레콤은 전자서명시스템의 생성 및 변경사항에 따른 취약성 점검을 실시합니다.
③ SK 텔레콤은 전자서명시스템의 소프트웨어에 대한 형상관리를 진행하고 있습니다.

### 6.7 네트워크 보호조치

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

### 6.8 시점확인서비스 보호조치

해당사항 없습니다.

## 7. 인증서 형식

### 7.1 인증서 형식

#### 7.1.1 최상위 인증기관 인증서 프로파일

| 기본 필드 명 | 선택여부 | | 입력 값 |
|---|---|---|---|
| | 생성 | 처리 | |
| 버전(Version) | m | m | V3 |
| 일련 번호(Serial Number) | m | m | 고유일련번호(up to 20Byte) |

| 서명 알고리즘(Signature) | m | m | sha256RSA |
|---|---|---|---|
| 발급자<br>(Issuer) | m | m | CN = **sktrootca**<br>OU = sktpassca<br>O = SK TELECOM<br>C = KR |
| 유효기간(Validity) | m | m | 인증서 유효기간 |
| 주체(Subject) | m | m | CN = **sktrootca**<br>OU = sktpassca<br>O = SK TELECOM<br>C = KR |
| 공개 키(Subject Public Key Info) | m | m | 사용자 공개키에 대한 정보 |
| 확장필드(Extensions) | m | m | 아래참조 |

| 확장필드(Extensions) | Critical | 선택여부 | | 입력값 |
|---|---|---|---|---|
| | | 생성 | 처리 | |
| 주체 키 식별자<br>(Subject Key Identifier) | n | m | m | 사용자의 공개키 hash값 |
| 키 사용<br>(Key Usage) | c | m | m | Certificate Signing<br>Off-line CRL Signing<br>CRL Signing (06) |
| 기본 제한<br>(Basic Constraints) | c | m | m | Subject Type=CA<br>Path Length Constraint=None |
| 정책 제약 조건<br>(Policy Constraints) | c | o | m | Required Explicit Policy Skip Certs=0 |

c : critical, n : non-critical, m : 생성, o : 선택 , x : 생성하지 않음

### 7.1.2 인증기관 인증서 프로파일

| 기본 필드 명 | 선택여부 | | 입력 값 |
|---|---|---|---|
| | 생성 | 처리 | |
| 버전(Version) | m | m | V3 |
| 일련 번호(Serial Number) | m | m | 고유일련번호(up to 20Byte) |
| 서명 알고리즘(Signature) | m | m | sha256RSA |
| 발급자<br>(Issuer) | m | m | CN = **sktrootca**<br>OU = sktpassca<br>O = SK TELECOM |

| | | | | |
|---|---|---|---|---|
| | | | | C = KR |
| 유효기간(Validity) | m | m | | 인증서 유효기간 |
| 주체(Subject) | m | m | | CN = **sktca**<br>OU = sktpassca<br>O = SK TELECOM<br>C = KR |
| 공개 키(Subject Public Key Info) | m | m | | 사용자 공개키에 대한 정보 |
| 확장필드(Extensions) | m | m | | 아래참조 |
| 확장필드(Extensions) | Critical | 선택여부 | | 입력값 |
| | | 생성 | 처리 | |
| 기관 키 식별자<br>(Authority Key Identifier) | n | m | m | 발급기관의 공개키 hash값<br>인증기관 인증서의 발급자 DN<br>인증기관 인증서의 일련번호 |
| 주체 키 식별자<br>(Subject Key Identifier) | n | m | m | 사용자의 공개키 hash값 |
| 키 사용<br>(Key Usage) | c | m | m | Certificate Signing<br>Off-line CRL Signing<br>CRL Signing (06) |
| 인증서 정책<br>(Certificate Policies) | c | m | m | [1]Certificate Policy:<br>Policy Identifier=모든 발급 정책<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>https://www.sktelecom.com/customer/notice_detail.do?page.index=358&page.page=1&page.type=all&page.keyword=<br>[1,2]Policy Qualifier Info:<br>Policy Qualifier Id=사용자 알림<br>Qualifier:<br>Notice Text:=This certificate is issued from SK Telecom.(sktrootca) |
| 기본 제한<br>(Basic Constraints) | c | m | m | Subject Type=CA<br>Path Length Constraint=0 |
| 정책 제약 조건<br>(Policy Constraints) | c | m | m | Required Explicit Policy Skip Certs=0 |

| | | | | |
|---|---|---|---|---|
| CRL 배포 지점<br>(CRL Distribution Points) | n | m | m | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=ldap://sktca.sktpass.com:389/cn=sktrootca,ou=sktpassca,o=SK TELECOM,c=KR?authorityRevocationList |
| 기관 정보 액세스<br>(Authority Information Access) | n | o | m | [1]Authority Info Access<br>Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.sktpass.com:9020/OCSPServer |

### 7.1.3 가입자 인증서 프로파일

| 기본 필드 명 | 선택여부 | | 입력 값 |
|---|---|---|---|
| | 생성 | 처리 | |
| 버전(Version) | m | m | V3 |
| 일련 번호(Serial Number) | m | m | 고유일련번호(up to 20Byte) |
| 서명 알고리즘(Signature) | m | m | sha256RSA |
| 발급자<br>(Issuer) | m | m | CN = sktca<br>OU = sktpassca<br>O = SK TELECOM<br>C = KR |
| 유효기간(Validity) | m | m | 인증서 유효기간 |
| 주체(Subject) | m | m | CN = 사용자명-UniqueValue<br>OU = sktpassca<br>O = SK TELECOM<br>C = KR |
| 공개 키(Subject Public Key Info) | m | m | 사용자 공개키에 대한 정보 |
| 확장필드(Extensions) | m | m | 아래참조 |

| 확장필드(Extensions) | Critical | 선택여부 | | 입력값 |
|---|---|---|---|---|
| | | 생성 | 처리 | |
| 기관 키 식별자<br>(Authority Key Identifier) | n | m | m | 발급기관의 공개키 hash값<br>인증기관 인증서의 발급자 DN<br>인증기관 인증서의 일련번호 |
| 주체 키 식별자 | n | m | m | 사용자의 공개키 hash값 |

| | | | | |
|---|---|---|---|---|
| (Subject Key Identifier) | | | | |
| 키 사용<br>(Key Usage) | c | m | m | Digital Signature<br>Non-Repudiation |
| 인증서 정책<br>(Certificate Policies) | c | m | m | [1]Certificate Policy:<br>Policy Identifier=1.2.410.200106.4 |
| 기본 제한<br>(Basic Constraints) | n | x | x | Subject Type=End Entity<br>Path Length Constraint=None |
| CRL 배포 지점<br>(CRL Distribution Points) | n | m | m | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=ldap://sktca.sktpass.com:389/ou=해당dp,ou=crl,ou=sktpassca,o=SK TELECOM,c=KR |
| 기관 정보 액세스<br>(Authority Information Access) | n | m | m | [1]Authority Info Access<br>Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.sktpass.com:9020/OCSPServer |

### 7.2.1 인증기관 인증서 폐지목록(ARL) 프로파일

| 기본 필드 명 | 생성 | 처리 | 입력 값 |
|---|---|---|---|
| 버전 | m | m | V2 |
| 서명 알고리즘 | m | m | sha256RSA |
| 서명 해시 알고리즘 | m | m | sha256 |
| 발급자 | m | m | CN = **sktrootca**<br>OU = sktpassca<br>O = SK TELECOM<br>C = KR |
| 개시 날짜 | m | m | 게시 날짜 |
| 다음 업데이트 | m | m | 만료 날짜 (유효기간: 100일) |
| 해지된 인증서<br>-일련번호<br>-해지 날짜<br>-CRL 엔트리 확장필드 | -<br>m<br>m<br>m | -<br>m<br>m<br>m | 제공됨 (목록이 없는 경우 값이 없음)<br>폐지된 인증서의 일련번호 입력<br>폐지날짜 입력<br>아래 참고 |
| CRL 확장필드 | m | m | 아래 참고 |

| 인증서 효력정지 및 폐지 목록 확 | critical | 선택여부 | 입력 값 |
|---|---|---|---|

| 장필드명 | | 생성 | 처리 | |
|---|---|---|---|---|
| 기관 키 식별자 | n | m | m | 발급기관의 공개키 hash값<br>인증기관 인증서의 발급자 DN<br>인증기관 인증서의 일련번호 |
| CRL 숫자 | n | m | m | CRL 일련번호 |

### 7.2.2 가입자 인증서 폐지목록(CRL) 프로파일

| 1. 기본 필드 명 | 생성 | 처리 | 입력 값 |
|---|---|---|---|
| 버전(Version) | m | m | V2 |
| 서명 알고리즘(Signature) | m | m | sha256RSA |
| 발급자<br>(Issuer Name) | m | m | CN = **sktca**<br>OU = sktpassca<br>O = SK TELECOM<br>C = KR |
| 개시 날자(This Update) | m | m | 게시 날짜 |
| 다음 업데이트(Next Update) | m | m | 만료 날짜 (유효기간: 24시간) |
| 해지된 인증서<br>-일련번호<br>-해지 날짜<br>-CRL 엔트리 확장필드 | -<br>m<br>m<br>m | -<br>m<br>m<br>m | 제공됨 (목록이 없는 경우 값이 없음)<br>폐지된 인증서의 일련번호 입력<br>폐지날짜 입력<br>아래 참고 |
| CRL 확장필드(CRL Extensions) | m | m | 아래 참고 |

| 인증서 효력정지 및 폐지 목록 확장필드명 | critical | 선택여부 | | 입력 값 |
|---|---|---|---|---|
| | | 생성 | 처리 | |
| 기관 키 식별자(Authority Key Identifier) | n | m | m | 발급기관의 공개키 hash값<br>인증기관 인증서의 발급자 DN<br>인증기관 인증서의 일련번호 |
| CRL 숫자(CRL Number) | n | m | m | CRL 일련번호 |
| 배포 지점 발급 중<br>(Issuing Distribution Point) | c | o | m | Distribution Point Name:<br>Full Name:<br>URL=ldap://sktca.sktpass.com:389/ou=해당 dp,ou=crl,ou=sktpassca,o=SK TELECOM,c=KR<br>Only Contains User Certs=예<br>Only Contains CA Certs=아니요<br>Indirect CRL=아니요 |

### 7.3 OCSP 인증서 형식

| 기본 필드 명 | 선택여부 | | 입력 값 |
|---|---|---|---|
| | 생성 | 처리 | |
| 버전(Version) | m | m | V3 |
| 일련 번호(Serial Number) | m | m | 고유일련번호(up to 20Byte) |
| 서명 알고리즘(Signature) | m | m | sha256RSA |
| 발급자<br>(Issuer) | m | m | CN = sktrootca<br>OU = sktpassca<br>O = SK TELECOM<br>C = KR |
| 유효기간(Validity) | m | m | 인증서 유효기간 |
| 주체(Subject) | m | m | CN = sktocsp<br>OU = sktpassca<br>O = SK TELECOM<br>C = KR |
| 공개 키(Subject Public Key Info) | m | m | 공개키에 대한 정보 |
| 확장필드(Extensions) | m | m | 아래참조 |

| 확장필드(Extensions) | Critical | 선택여부 | | 입력값 |
|---|---|---|---|---|
| | | 생성 | 처리 | |
| 기관 키 식별자<br>(Authority Key Identifier) | n | m | m | 발급기관의 공개키 hash값<br>인증기관 인증서의 발급자 DN<br>인증기관 인증서의 일련번호 |
| 주체 키 식별자<br>(Subject Key Identifier) | n | m | m | 사용자의 공개키 hash값 |
| 키 사용<br>(Key Usage) | c | m | m | Certificate Signing<br>Off-line CRL Signing<br>CRL Signing (06) |
| 인증서 정책<br>(Certificate Policies) | c | m | m | [1]Certificate Policy:<br>Policy Identifier=1.2.410.200106.3<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>https://www.sktelecom.com/customer/notice_deta |

| | | | | |
|---|---|---|---|---|
| | | | | il.do?page.index=358&page.page=1&page.type=all&page.keyword=<br>[1,2]Policy Qualifier Info:<br>Policy Qualifier Id=사용자 알림<br>Qualifier:<br>Notice Text=This certificate is issued from SK Telecom.(sktrootca) |
| 기본 제한<br>(Basic Constraints) | c | m | m | Subject Type=CA<br>Path Length Constraint=0 |
| 정책 제약 조건<br>(Policy Constraints) | c | m | m | Required Explicit Policy Skip Certs=0 |
| 확장된 키 사용<br>(Extended Key Usage) | c | o | m | OCSP 서명 (1.3.6.1.5.5.7.3.9) |
| CRL 배포 지점<br>(CRL Distribution Points) | n | m | m | [1]CRL Distribution Point<br>Distribution Point Name:<br>Full Name:<br>URL=ldap://sktca.sktpass.com:389/cn=sktrootca,ou=sktpassca,o= SK TELECOM,c=kr?authorityRevocationList |
| 기관 정보 액세스<br>(Authority Information Access) | n | o | m | [1]Authority Info Access<br>Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.sktpass.com:9020/OCSPServer |

## 8. 감사 및 평가

### 8.1 감사 및 평가 현황

① SK텔레콤은 운영기준 준수 사실의 인증을 받기 위해서 매년 평가기관에 평가를 받습니다.

② 평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대해 평가를 하고, 그 결과를 인정기관에 제출합니다.

③ 과학기술정보통신부 장관은 운영기준에 부합한다고 인정하는 국제적으로 통용되는 평가를 정하여 고시할 수 있으며, 전자서명인증사업자가 국제통용 평가를 받으면 평가기관의 평가를 받은 것으로 봅니다.

④ 운영기준 준수 사실의 인정의 유효기간은 인정받은 날로부터 1년으로 합니다.

### 8.2 평가자의 신원, 자격

① 평가자의 신원 및 자격은 전자서명법 시행령 제 6조(평가기관의 선정기준 및 절차 등)에 따라

선정됩니다.
② 평가기관의 전문인력 요건은 전자서명법 시행령 [별표1] 에 따릅니다.

### 8.3 평가 대상과 평가자의 관계
평가기관은 전자서명 법령상 과기부에 의해 '피 평가기관에 대한 공정성, 객관성, 신뢰성, 을 인정받은 기관으로 평가자와 평가 대상과는 독립성 등이 유지되고 있습니다.

### 8.4 평가목적 및 내용
① SK텔레콤은 인정기관으로부터 전자서명 인증서비스의 운영기준 준수 사실에 대해 인정받기 위해 평가기관으로부터 평가를 받습니다.
② 평가내용은 전자서명인증사업자의 운영기준 준수 여부에 대하여 평가를 하며, 자세한 사항은 평가기관이 정한 세부평가 기준에 따릅니다.

### 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 있습니다.
② SK텔레콤은 기간 내에 위 시정명령을 이행하여야 합니다.
③ SK텔레콤은 매년 정보보호 및 개인정보보호 등의 감사, 심사를 진행하며 결과에 따라 관리적, 물리적, 기술적 보완조치를 진행합니다.

### 8.6 결과 보고
평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대해 평가를 하고 그 결과를 인정기관에 제출하여야 합니다.

## 9. 전자서명인증업무 보증 등 기타사항

### 9.1 인증서비스 수수료
① 가입자가 전자서명인증서비스를 이용하는 데 있어서, 가입자에게는 별도의 수수료가 부과되지 않습니다.
② 이용자가 전자서명인증서비스를 이용하는 데 있어서 이용자가 지불하는 수수료와 환불 정책은 이용자와의 별도 계약에 따릅니다.

### 9.2 배상

#### 9.2.1 배상책임
SK텔레콤은 인증업무 수행과 관련하여 가입자 또는 인증서를 신뢰한 이용자에게 손해를 입힌 때에는 배상의 타당성이 인정된 가입자 또는 이용자에 한해 그 손해를 배상합니다. 다만, 그 손해가

불가항력으로 인하여 발생하였거나, SK텔레콤의 고의 또는 과실이 없는 경우에는 그 배상책임을 부담하지 않습니다.

#### 9.2.2 배상책임의 면책

SK텔레콤은 다음의 경우 배상책임을 지지 않습니다.

① SK텔레콤이 본 준칙에서 정한 인증서별 발급대상, 용도를 가입자 또는 이용자가 임의로 변경, 사용하여 발생한 손해

② 인증서 발급(신규, 재발급) 및 인증서 폐지 목록의 공고 등과 같은 인증서비스 제공과정에서 통신경로 장애 또는 가입자 및 이용자의 시스템 장애 등 SK텔레콤의 귀책사유가 아닌 원인으로 인하여 발생한 손해

③ 이용자 또는 이용기관의 고의 또는 과실로 인하여 발생한 손해

④ 가입자의 고의 또는 과실로 인하여 발생한 손해

⑤ 이용자 또는 이용기관이 변경된 정보를 제공하지 아니하여 발생한 손해

⑥ 본 준칙에서 정하지 아니한 방법으로 인증서가 사용 또는 임의로 변경되어 발생한 손해

⑦ 천재지변, 디도스(DDOS)공격, IDC장애, 회선장애, 폭동, 전쟁, 정부(지방자치단체포함)의 규제 또는 사회통념상 이에 준하는 불가항력적인 사유 등으로 인하여 발생한 손해

⑧ 이용자 시스템 장애, 통신경로 장애 및 예상치 못한 기술적 장애 등으로 발생한 손해

⑨ 인증서 업무와 관련하여 직접적으로 발생하지 아니한 손해

⑩ 효력이 정지된 인증서를 이용하여 발생한 손해

⑪ 전자우편용, 법적인 효력이 없는 시험용 인증서를 목적 외의 용도로 사용함으로써 발생한 손해

⑫ 전자서명법, 전자서명법시행령, 전자서명법시행규칙 및 본 준칙에서 정한 사항 이외의 사유로 발생한 손해

#### 9.2.3 가입자의 배상책임

가입자는 가입자의 고의 또는 과실로 전자서명법, 전자서명법시행령, 전자서명법시행규칙 및 SK텔레콤의 약관에 따라본 전자서명 인증업무준칙의 의무사항을 위반하거나, 인증서비스를 이용함에 있어 SK텔레콤 및 기타 관련자(다른 가입자, 다른 이용자 등)에게 손해를 입힌 경우에는 당해 손해를 배상하여야 합니다.

#### 9.2.4 이용자의 배상책임

이용자는 이용자의 고의 또는 과실로 전자서명법, 전자서명법시행령, 전자서명법시행규칙 및 SK텔레콤의 약관 또는 운영정책과 본 전자서명 인증업무준칙의 의무사항을 위반하거나, 이용자가 인증서비스를 이용함에 있어서 SK텔레콤 및 기타 관련자(가입자, 다른 이용자 등)에게 손해를 입힌 경우에는 당해 손해를 배상하여야 합니다.

### 9.3 영업비밀

해당 사항 없습니다.

### 9.4 개인정보 보호

① SK텔레콤은 가입 신청자 및 가입자의 개인정보를 수집하는 경우 전자서명인증서비스 제공에 필요한 최소한의 정보를 수집하여야 하며 당해 가입자 및 가입자의 동의를 얻어야 합니다. 다만, 다음 각호의 경우에는 그러하지 아니합니다.

- 전자서명인증서비스 이용계약의 이행을 위하여 불가피하게 필요한 경우
- 전자서명인증서비스 제공에 따른 요금정산을 위하여 필요한 경우
- 전자서명법 또는 다른 법률에 특별한 규정이 있는 경우

② SK텔레콤은 본인의 동의가 있거나 아래에 해당하는 경우를 제외하고는 전자서명인증업무 수행 과정에서 획득한 가입자 및 가입자에 관한 개인정보를 전자서명인증업무 이외의 타 목적으로 이용하거나 제3자에게 공개하지 않습니다. 다만, 인증서상의 기재 내용 및 이미 공개된 내용은 제외합니다.

- 전자서명인증서비스의 제공에 따른 요금정산을 위하여 필요한 경우
- 전자서명법 또는 다른 법률에 특별한 규정이 있는 경우

③ SK텔레콤은 개인정보보호법 등 관계규정을 준수하며 인증서 발급 시 개인정보 사용에 대한 이용동의를 받습니다.

④ SK텔레콤은 개인정보보호법 등 관계규정을 준수하며 홈페이지에 게시된 개인정보처리방침에 따라 개인정보를 수집,보유,처리합니다.

### 9.5 지식 재산권

다음 사항에 대한 지식재산권은 저작권법 등 관련 법률에 따라 SK텔레콤에 귀속됩니다.

① SK텔레콤 인증시스템을 위해 개발된 소프트웨어 및 하드웨어

② 본 전자서명 인증업무준칙 및 SK텔레콤의 서비스 이용 약관과 운영정책

③ SK텔레콤이 생성한 전자서명정보

④ 기타 관련 법령에 따라 SK텔레콤에게 권리가 귀속되는 일체의 저작물

### 9.6 보증

① 인증서는 본 준칙에 따라 발급됨을 보증합니다.

② SK텔레콤은 가입자가 제출한 정보 중 전자서명인증서비스를 제공하기 위해 필요한 최소한의 정보에 대해서만 사실여부를 확인하며, 해당정보에 대한 사실성을 이용자에게 보증합니다.

### 9.7 보증 예외 사항

SK텔레콤은 전자서명법, 전자서명법시행령, 전자서명법시행규칙 및 SK텔레콤 PASS 인증서의 약관 또는 운영정책과 본 전자서명 인증업무준칙에서 정한 사항 이외의 사항 즉, 가입자 신용 및 가입자 관련 정보의 불변성 등을 보증하지 않습니다.

### 9.8 보험의 보상 범위

SK텔레콤은 전자서명인증업무의 수행과 관련하여 가입자 또는 이용자에게 손해를 입힌 경우에는 그 손해를 배상합니다. 다만, SK텔레콤의 고의 또는 과실이 없는 경우에는 배상책임을 부담하지 않습니다.

### 9.9 배상 한계

① SK텔레콤은 가입자 또는 인증서를 신뢰한 이용자에게 발생하는 손해를 담보하기 위하여 보험에 가입하고 있으며, 당해 보험계약에서 정한 배상 한도 내에서 가입자 또는 이용자의 정당한 손해를 배상합니다.

② 보험계약 상의 배상한도를 초과하여 손해가 발생한 경우에는 당사자간의 합의에 의하여 초과분에 대한 손해를 배상하며, 합의가 이루어지지 않을 경우에는 법원의 판결에 따릅니다.

### 9.10 준칙의 효력

① 본 준칙은 2021년 9월 30일부터 시행하며 준칙이 개정되면 개정 전 내용은 개정 준칙의 효력 발생일에 그 효력이 종료됩니다.

② 본 준칙은 다음 각 호의 사유가 발생한 때에 효력이 소멸합니다.

- SK텔레콤의 전자서명인증업무가 정지된 경우 해당 정지 기간
- SK텔레콤이 전자서명인증업무의 전부를 휴지한 경우 해당 휴지 기간
- SK텔레콤이 전자서명인증업무를 폐지한 경우 폐지시험 이후
- 기타 전자서명 인증업무준칙의 효력이 소멸하는 경우로 과학기술정보통신부 장관이 인정하는 경우

### 9.11 통지 및 의사소통

SK텔레콤은 본 전자서명인증업무 운영준칙을 개정하는 경우 개정된 준칙을 서비스 홈페이지 및 SK텔레콤 PASS 어플리케이션에 공지합니다.

### 9.12 이력관리

SK텔레콤은 전자서명인증업무 운영준칙의 변경 이력을 관리합니다.

### 9.13 분쟁 해결

SK텔레콤은 이용자와 가입자 간 SK텔레콤 PASS 인증서와 관련한 분쟁 발생시, 전자서명법 및 관련 법령에 따라 이를 원만히 해결하도록 성실히 협의합니다.

### 9.14 준거법

① 본 준칙은 대한민국의 관계법령에 따라 해석되고 적용됩니다.

② 인증서 서비스와 관련한 소송의 관할법원은 서울중앙지방법원으로 합니다.

### 9.15 관련 법률 준수

SK텔레콤은 전자서명법 및 관계법령과 개인정보 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 관련 법령을 준수하여야 합니다.

### 9.16 기타 규정

해당사항  없습니다.