전자서명인증업무준칙

[버전 25.1]

2022. 11

KICA
한국정보인증

NO	버 전	개정일	결재자	개정의 주요내용	시행일
00/01	v0.1	2000. . .	이정욱	제정	2000. . .
01/01	v1.1	2001.6.13	이정욱	개정	2001.8.8
02/01	v2.1	2002.6.11.	강영철	- 전자서명법 개정사항 반영 - 무선공인인증서비스 개시 - 기타 정책 변경 등	2002.6.19.
02/02	v2.2	2002.8.7	강영철	- 무선공인인증서비스 정책 반영	2002.9.9
03/01	v3.1	2003.3.17	강영철	- 상호연동 정책 반영 - 손해배상의 한계 조항 신설 - 공인인증서 종류 개정 - "변경발급" 삭제 등	2003.4.1
04/01	v4.1	2004.4.30	강영철	- 행정안전부고시 제2003-51호 - 전자서명인증업무지침 개정내용 반영 - 개인인증서(상호연동용) 요금 반영 - 기타 정책 변경 반영	2004.6.12
04/02	v4.2	2004.9.7	강영철	- 시행일 변경	2004.9.11
05/01	v5.1	2005.12.19	강영철	- 환불규정 개정	2006.1.2
06/01	v6.1	2006.8.1	강영철	- 공인인증서비스 종류 규정 개정	2006.9.1
07/01	v7.1	2007.5.17	강영철	- 행정안전부 고시 제2007-6호 "공인인증업무준칙 작성표준"에 따른 개정	2007.7.23
11/01	v11.1	2011.3.21	고성학	- 행정안전부 권고에 따른 개정 - 공인인증업무준칙 작성표준에 따른 보완 - 기관명칭 등 변경 - 118분실신고센터 운영 - 정기점검 보완 사항	2011.12.26
12/01	V12.1	2012.10.12	고성학	- 정기점검에 따른 수정 - 프로파일 - 개인정보보호방침 -〉 개인정보처리방침으로 수정 - 준칙 3.6.7 118 신고센터 처리 절차 수정 - 준칙 4.2 공고방법 용어 정리 - 기타 자구 수정 - 준칙 1.3.8.3 가입자의 의무, 준칙 2.1 "공인인증서의 종류"에 용도제한용 이용에 관한 내용 포함	2012.11.1

14/01	V14.1	2014.3.31.	고성학	- 주관부서 변경에 따른 수정 - 행정안전부 -〉 미래창조과학부로 수정(17건) - 행정안전부 -〉 안정행정부로 수정(1건) - 다년간 인증서 관련 근거 규정 보완 - 공인인증서 종류/ 갱신발급/ 가입자 등록정보변경 등 관련 규정 보완	2014.4.7.
16/01	V16.1	2016.6.	김상준	- 전자서명법 시행규칙 개정에 따른 내용반영 - 온라인신원확인에 의한 발급관련 내용 - 재외국민 신원확인 증표로 주민등록증 추가	2016.7.1.
17/01	V17.1	2017.2.	김상준	- 은행용 인증서의 용도범위 변경	2017. 2.
17/2	V17.2	2017.5.	김상준	- 공인인증업무준칙 변경신고기간의 수정	2017.5.
19/1	V19.1	2019.2	김상준	- 공인인증업무준칙 개정사유 근거 규정 수정 - 감사기록 보존 절차 변경 - 정부기관 명칭 변경 반영	2019.2
21/1	V20.0	2021.1	김상준	- 전자서명법 개정에 따른 전자서명인증업무준칙 전면 개정	2021.01.15
21/2	V21.0	2021.7	김상준	- 전자서명인증사업자 평가기관 의견 반영 - 준칙 1.5.3 준칙의 제•개정 절차에 사전 협의 기관 추가 - 준칙 5.1.7 원격지 백업 보관 기준 변경	2021.7.22
21/3	V22.0	2021.8	김상준	- 한국인터넷진흥원의 의견 반영 - 준칙 1.3.3 최상위인증기관 추가 - 준칙 1.5.3 준칙의 제·개정 절차에 인정기관을 최상위인증기관으로 수정 - 준칙 5.1.7 원격지 백업 기준 변경 - 준칙 5.5.2 기록의 보존기관에 전자서명법 개정전 기록에 대한 조항 추가	2021.8.9
21/4	V23.0	2021.9.	김상준	- 한국인터넷진흥원 의견 반영 - 준칙 3.2.1.2 온라인 신원확인 방법 근거조항 추가 - 준칙 4.1.2 신청절차에 대면과 온라인 신청방법 구문	2021.9.22

21/5	V24.0	2021.10	김상준	- 전자서명인증업무준칙 현행화를 위한 전면개정	2021.10.26
22/9	V25.0	2022.9	김상준	- 1.5 준칙의 관리 내용 추가 - 1.5.3 준칙의 개정권자 내용 추가 - 3.1 가입자 이름 표시 방법 수정 - 3.2 DN의 유일성 보장 방법 추가 - 3.2.2 신원확인절차의 신분확인증표 진위확인 방법 삭제 - 3.2.3 가입자의 전자서명생성정보소유 증명방법 수정 - 3.4 인증서 효력정지, 효력회복, 폐지 신청서 용어 변경 - 4.3.1 인증서의 발급절차 수정 - 4.3.2 인증서 발급 조치 수정 - 4.9.1.3 인증서 효력정지 방법 및 절차 추가 - 4.12.2 기타부가서비스에 클라우드 공동인증서비스 추가 - 5.1.7 원격지 물리적 기준 수정 - 5.8.1 전자서명인증업무 휴지 수정 - 8.1 감사 및 평가 현황에 본인확인기관 정기점검 내용 추가 - 9.13 분쟁해결 절차 추가 - 9.14 준거법 및 관할법원 내용 추가 - 9.3 영업비밀 내용 수정	2022.9.6
22/11	V25.1	2022.11	김상준	- 4.12.2 클라우드 공동인증서비스 수정 - 9.2.1 배상책임 수정 - 9.2.2 배상책임 면책 수정 - 9.8 보험의 보상범위 수정 - 9.9 배상 한계 수정 - 9.13 분쟁해결 수정	2022.11.24

목차

1. 총칙

1.1 목적

1.1.1 준칙의 배경 및 목적

본 전자서명인증업무준칙(CPS:Certification Practice Statement)은 전자서명법, 전자서명법시행령, 전자서명법시행규칙 및 전자서명인증업무운영기준에 따라 한국정보인증 주식회사(이하 "정보인증" 이라 한다.)가 인증서의 발급·관리 및 인증시스템을 운영함에 있어 필요한 사항을 정하며, "정보인증"과 가입자 등 전자서명인증업무 관련 당사자의 책임과 의무사항의 규정을 목적으로 합니다.

1.1.2 전자서명인증체계 소개

"전자서명인증체계"라 함은 인증서의 발급 및 인증 관련 기록의 관리, 인증서를 이용한 부가업무 등을 제공하기 위한 체계를 말합니다.

1.2 문서의 명칭

본 준칙의 명칭은 "정보인증" 전자서명인증업무준칙 버전 25.1입니다.

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 다음과 같은 업무를 수행합니다.

- 전자서명인증사업자가 전자서명법 제8조(운영기준 준수 사실의 인정)에 따른 자격을 갖추었는지 인정 여부 결정
- 전자서명인증사업자에 운영기준 준수 사실을 인정하는 경우 증명서 발급

1.3.3 최상위인증기관

인증체계의 최상위인증기관(RootCA)은 한국인터넷진흥원으로 (구)공인전자서명 인증관리체계 및 운영하는 업무를 수행합니다.

- (구)공인인증기관에 대한 (구)공인인증서 발급·관리 등 전자서명인증업무
- 전자서명인증 관련 기술 개발/보급

1.3.4 평가기관

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

1.3.5 전자서명인증사업자

전자서명인증사업자는 전자서명인증업무를 하는 자를 말합니다.

1.3.6 “정보인증”

1.3.6.1 역할

가. “정보인증”은 전자서명인증사업자로서 다음과 같은 역할을 합니다.

- 인증서비스 관련 신청서 접수 및 처리
- 인증서비스 제공과 관련한 가입자 신원확인 업무
- 기타 인증서비스와 관련된 업무

나. “정보인증”은 전자서명인증사업자로서 가입자에게 다음과 같은 인증서비스를 제공합니다.

- 인증서 발급(신규, 재발급, 갱신 등)
- 인증서 효력정지, 효력회복 및 폐지
- 인증서에 대한 폐지 목록 공고(CRL)
- 시점확인서비스(TSA)
- 인증서 유효성 확인 서비스(OCSP)
- 본인확인 서비스 (UCPID)

1.3.6.2 책임 및 의무사항

가. 정확한 정보 제공

“정보인증”은 가입자와 이용자에게 인증서의 신뢰성이나 유효성에 영향을 미칠 수 있는 다음의 정보를 당사 홈페이지 또는 디렉터리시스템에 공고하여 그 사실을 확인할 수 있도록 합니다.

- 전자서명인증업무 휴지·정지 또는 폐지
- 준칙
- 인증서에 대한 폐지 목록
- 기타 전자서명인증업무 수행 관련 정보 등

나. 전자서명생성정보의 보호

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

다. 전자서명생성정보 안전조치

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

라. 신원확인

“정보인증”은 인증서를 발급받고자 하는 자에 대하여 전자서명법 시행규칙 제5조(실지 명의 기준의 신원확인 방법)에서 정하는 신원확인의 기준 및 방법에 따라 신원을 확인합니다.

마. 가입자 개인정보보호

“정보인증”은 인증서비스 중 취득한 개인정보를 보호하며, 수집한 개인정보를 업무 목적으로만 사용합니다.

바. 관련 법령 및 규정 준수

“정보인증”은 인증서비스를 수행할 때 전자서명법령, 개인정보 보호법령 등 관련 규정을 준수합니다.

1.3.7 등록대행기관

1.3.7.1 역할

가. 등록대행기관은 “정보인증”을 대신하여 가입자에 대한 신원확인을 수행하고 인증서 발급, 효력정지, 효력회복 또는 폐지 등의 신청을 접수·등록하는 가입자 등록 업무를 위탁받은 외부기관을 의미합니다.

나. 등록대행기관은 가입자에 대한 신원확인, 인증서 발급, 효력정지, 효력회복 또는 폐지 등의 신청을 접수 및 등록하는 업무를 수행합니다. 가입자등록정보(인증서 신청서, 신원확인 서류 및 제시한 증명서)의 보관 및 관리에 따른 책임이 있습니다.

1.3.7.2 책임 및 의무사항

가. 인증서 가입 신청자의 신청서류 접수 등 등록 업무

등록대행기관은 정당한 사유 없이 인증서 발급, 재발급, 갱신 발급, 효력정지, 효력회복, 폐지 등의 인증서 관련 신청접수를 거부할 수 없습니다.

나. 신원확인

등록대행기관은 인증서를 발급받고자 하는 자에 대하여 전자서명법 시행규칙 제5조(실지명의 기준의 신원확인 방법)에서 정하는 신원확인의 기준 및 방법에 따라 신원을 확인합니다.

다. 준칙 및 계약 이행

등록대행기관은 "정보인증"의 준칙과 "정보인증"과 체결한 계약서 내용을 준수하여야 하며 가입자 신원확인의 정확성에 대한 책임이 있습니다.

라. 배상책임

등록대행기관이 전자서명법령 및 준칙 그리고 "정보인증"과의 계약을 위반하거나 가입자의 신원확인 오류 등으로 인하여 "정보인증", 가입자 또는 이용자에게 발생한 손해에 대하여 배상할 책임이 있습니다.

마. 가입자 개인정보보호

등록대행기관은 등록대행업무 수행 중 취득한 개인정보를 보호하여야 하며, 수집한 개인정보를 업무 목적으로만 사용하여야 합니다.

1.3.8 가입자

1.3.8.1 정의

전자서명생성정보에 대하여 "정보인증"으로부터 전자서명인증을 받은 자를 말합니다.

1.3.8.2 책임과 의무사항.

가. 가입자는 자신의 목적에 맞는 인증서를 선택하여 신청해야 하며, 인증서비스의 신청과 관련하여 정확한 정보 및 사실만을 "정보인증"에 제공 할 의무가 있습니다.

나. 가입자는 가입자의 중요한 신상정보가 변경되거나 인증서 비밀번호 유출, 가입자의 전자서명생성정보가 유출되었다고 생각되는 경우 가입자는 "정보인증" 또는 등록대행기관에 해당 인증서의 폐지 또는 재발급을 요청하여 새로운 인증서를 발급받아야 합니다.

다. "정보인증"은 가입자가 조치를 이행하지 않아 가입자에게 발생하는 문제에 대해서는 책임을 지지 않습니다.

라. 가입자는 사기 또는 위조된 전자서명의 이용 등 고의·중과실 또는 악의적 방법으로 "정보인증"과 이용자에게 손해를 입히면 "정보인증"과 이용자에게 손해를 배상해야 합니다.

1.3.9 대리인

대리인은 법인/단체가 인증서비스 관련 업무의 대리를 위해 지정한 자를 말합니다. 대리인은 가입자의 위임장 같은 증명서를 지참한 때에만 가입자를 대리하여 인증서를 신청할 수 있습니다.

1.3.10 이용자

1.3.10.1 정의

"정보인증"이 제공하는 전자서명인증서비스를 이용하는 자를 말합니다.

1.3.10.2 책임과 의무사항

가. 이용자는 가입자의 인증서에 대해 이용목적과 이용 가능 범위에 대해 정확하게 이해해야 하며, 가입자가 보내온 인증서가 이용자의 목적에 적합한가를 판단하여야 합니다.

나. 이용자는 인증서 폐지 목록 또는 인증서 유효성 확인 서비스를 통해 인증서가 유효한 인증서인지 확인해야 합니다.

다. 이용자는 사기 또는 위조된 전자서명의 이용 등 고의·중과실 또는 악의적 방법으로 "정보인증"과 가입자에게 손해를 입히면 "정보인증"과 가입자에게 그 손해를 배상해야 합니다.

1.4 인증서 종류

1.4.1 인증서의 발급대상

"정보인증"은 개인과 법인/단체/개인사업자에게 인증서를 발급합니다.

1.4.2 인증서 이용범위 및 용도

가. "정보인증"의 범용인증서는 인증서가 필요한 모든 분야에서 사용 가능한 인증서입니다. 용도제한용인증서는 정해진 용도 외에 사용할 수 없습니다.

구 분			용도	유효기간
개인	범용		인증서를 필요로 하는 일반 전자거래의 모든 분야에서 사용 가능	3년이내
	용도제한용	은행용	은행 업무 정부 민원 업무(단, 전자입찰 등 제외)	3년이내
		기타	개별 계약에 따름	3년이내
법인, 단체, 개인사업자	범용		인증서를 필요로 하는 일반 전자거래의 모든 분야에서 사용 가능	3년이내
	용도제한용		개별 계약에 따름	3년이내
서버			인터넷상에서 서비스를 제공하는 서버를 인증	3년이내

1.5 준칙의 관리

"정보인증"은 준칙이 제정 또는 개정할 경우 버전, 사유, 내용 등 개정내역에 대한 기록을 유지·관리합니다. 다음의 내용을 포함한 준칙의 제·개정 관련 기록을 유지 및 관리합니다.

1.5.1 준칙 관리부서 및 연락처

- 관리부서 : "정보인증" 인증기획팀
- 전자우편 : webmaster@signgate.com

- 주소 : 13487, 경기도 성남시 분당구 판교로 242 판교디지털센터 C동 5층
- 전화 : 1577-8787
- FAX : 02-360-3001

1.5.2 준칙의 제·개정 사유

"정보인증"은 다음의 경우에 준칙을 개정합니다.

가. 새로운 업무를 반영하거나 인증서비스를 개선하기 위해 준칙의 내용에 대하여 보완·수정이 필요하다고 판단한 경우

나. 준칙에 포함하여야 하는 전자서명법 제15조(전자서명인증업무준칙의 준수 등) 제1항 각호 또는 전자서명법시행규칙 제6조, 전자서명인증업무준칙 작성방법(과학기술정보통신부 고시 제2020-70호)에 변동이 생긴 경우

1.5.3 준칙의 제·개정 절차

"정보인증"은 다음 각 호의 사항이 포함된 준칙을 작성하여 내부 결재 후 인터넷 홈페이지 등에 공지함을 원칙으로 합니다. 준칙 중 다음 각 목의 내용을 변경한 때도 또한 같습니다.

가. 인증서비스의 종류

나. 인증서비스의 요금, 이용범위 및 유효기간 등 이용조건

다. 전자서명인증업무의 수행방법 및 절차

라. 그 밖에 전자서명인증업무의 수행에 필요한 사항

준칙 제·개정 사항이 관련기관 또는 최상위인증기관(한국인터넷진흥원)등에 중대한 영향을 미치거나 협의가 필요한 사항의 경우 관련자들과 사전 협의 후 진행하여야 합니다.

"정보인증"은 전자서명인증업무 개선을 위하여 준칙의 변경이 필요하다고 판단한 경우 이를 개정할 수 있으며, 제·개정권자는 "정보인증"의 대표이사 이며, 경미한 개정의 경우 인증업무 관리 책임자가 권한을 대행할 수 있습니다.

1.5.4 준칙의 공지

"정보인증"은 제·개정된 준칙을 다음의 절차에 따라 공지합니다.

가. 개정된 준칙은 새로운 버전이 부여됩니다.

나. 개정된 준칙의 공지 위치는 아래와 같습니다.

- 준칙 공지 위치 : https://www.signgate.com/policy/certRule/pyCertRule.sg

1.5.5 가입자 동의방법

가입자는 변경된 준칙이 공고된 후 7일(공고일 포함) 이내에 서면 또는 전자서명생성정보로 전자서명 한 전자문서 등의 수단으로 이의를 제기할 수 있으며, 이의를 제기하지 아니한 경우 "정보인증"은 가입자가 변경된 준칙에 동의한 것으로 봅니다.

1.6 정의 및 약어

가. "전자문서"란 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말합니다.

나. "전자서명"이란 다음 각 목의 사항을 나타내는 데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합한 전자적 형태의 정보를 말합니다.

1) 서명자의 신원

2) 서명자가 해당 전자문서에 서명하였다는 사실

다. "전자서명생성정보"란 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말합니다.

라. "전자서명검증정보"란 전자서명을 검증하기 위하여 이용하는 전자적 정보를 말합니다.

마. "인증서비스"란 "정보인증"이 제공하는 전자서명인증서비스를 말합니다.

바. "인증시스템"이란 인증서비스를 제공하기 위해 운영하는 시스템을 말합니다.

사. "가입자등록정보"란 인증서비스에 가입하려는 자가 인정사업자에게 제출한 신청서, 신원확인을 위해 제출한 서류 및 증명서 등의 사본 그리고 기타 신청에 필요한 전자적 기록 등을 말합니다.

아. "인증서"란 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말합니다.

자. "전자서명인증업무"란 전자서명인증, 전자서명인증 관련 기록의 관리 등 인증서비스를 제공하는 업무를 말합니다.

차. "DN"이란 인증서 발급자 및 인증서 소유자를 확인하기 위해 사용되는 이름 형식을 말합니다.

2. 전자서명인증업무 관련 정보의 공고

2.1 공고설비

가. "정보인증"은 전자서명인증업무와 관련된 정보를 인증관리체계에 의하여 이중화 구성(Active-Active)으로 안정적으로 운영합니다.

나. "정보인증"은 전자서명인증업무 관련 정보를 적시에 정확한 제공을 위해 공고설비를 안전하게 운영관리합니다.

2.2 공고방법

가. "정보인증"은 전자서명인증업무 관련 정보를 처리한 즉시 공고합니다.

나. "정보인증"은 인증서 효력정지 및 폐지 목록에 대해서는 변경 사유가 없더라도 매일 1회 이상 정기적으로 갱신한 후 공고합니다. 현재 운영되고 있는 공고의 내용은 아래와 같습니다.

- 공고 위치 : ldap://ldap.signgate.com:389

다. 인증서 유효성 상태를 확인할 수 있는 인증서 유효성 확인 서비스를 이용자에게 제공합니다.

2.3 공고주기

- 공고 시점 : 0시, 12시
- 공고주기 : 12시간 주기

2.4 공고된 정보에 대한 책임

"정보인증"은 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

가. "정보인증"은 가입자를 구별하기 위해 ITU-T X.500에서 정한 DN(Distinguished Name) 을 이용합니다.

나. "정보인증"은 가입자의 인증서 발급함에 있어 DN 구성 시 다음과 같은 가입자 이름을 CN(Common Name)값으로 허용합니다.

- 실명, 법인명 등 법적 이름
- 특허청 또는 국제적으로 이와 동등한 기관으로부터 받은 상표권 등(증명서 필요)
- 인터넷 도메인명
- 인터넷 IP 주소
- WWW용 URL
- 전자우편 주소 등

3.2 DN의 유일성 보장방법

가. "정보인증"은 가입자가 제출한 이름 및 기타 정보 등을 DN으로 구성하여 인증서에 저장합니다. DN은 이용자가 인증서를 확인할 때 기준정보가 되므로 신규 가입자의 DN과 기존 가입자의 DN의 중복성을 확인하여 중복되지 않는 경우에만 인증서를 발급합니다.

나. "정보인증"은 가입자가 제출한 이름 및 등록대행기관 정보, "정보인증"의 정보등을 조합하여 DN을구성하며, 구성하려는 신규 가입자의 DN을 기 가입자의 DN과 중복여부를 확인하여 중복되는 경우 CN값에 순차번호를 연접하여 DN의 유일성을 보장합니다. "정보인증"은 다양한 이름을 수용하기 위해 특별한 해석규칙을 적용하지 않습니다.

다. "정보인증"은 기존의 가입자가 신규 가입자의 법적 이름 등을 DN에 이용하고 있어 소송이나 분쟁과 같은 문제가 발생하더라도 문제해결에 대한 책임을 지지 않습니다.

3.3 인증서 신규 발급 시 신원확인

3.3.1 신원확인 방법

"정보인증" 또는 등록대행기관은 신원확인증표 등을 통해 가입 신청자의 신원을 대면으로 확인합니다.

가. 개인 신원확인 방법

1) 개인 본인이 “정보인증” 또는 등록대행기관을 방문하여 인증서를 신청할 경우

① 개인(성인), 재외국민, 외국인

- 인증서비스 신청서
- 신원확인증표 사본 앞면(원본지참)

② 개인(미성년자)

- 인증서비스 신청서
- 신원확인증표 사본 앞면(원본지참)
- 법정대리인 신원확인증표 사본 앞면(원본지참)
- 법정대리인과의 관계를 증명할 수 있는 서류(주민등록등본, 가족관계증명서 등)

나. 법인 또는 단체 신원확인 방법

1) 대표자 본인이 “정보인증” 또는 등록대행기관을 방문하여 인증서를 신청할 경우

① 법인

- 인증서비스 신청서
- 법인의 신원확인증표
- 대표자의 신원확인증표 사본 앞면(원본지참)

② 단체

- 인증서비스 신청서
- 단체의 신원확인 증표
- 대표자 또는 국가기관 또는 지방자치단체장의 신원확인증표 사본 앞면(원본지참)

③ 개인사업자

- 인증서비스 신청서
- 개인사업자 등록증 사본
- 대표자의 신원확인증표 사본 앞면(원본지참)

2) 대리인이 신청하는 경우

법인인증서 신청 시 대표자에 대한 신원확인은 대표자의 위임을 받은 법인의 임직원에 대한 신원확인으로 갈음할 수 있으며, 이때 추가로 확인해야 할 서류는 다음과 같습니다.

- 인증서비스 신청서

- 법인(단체)의 신원확인증표
- 위임장(인감 날인)
- 법인 인감증명서(개인사업자는 대표자의 인감증명서)
- 대리인의 신원확인증표 사본 앞면(원본지참)

다. 실지명의가 확인된 전자금융거래 가입자가 정보통신망을 통한 신원확인 방법

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

- 전자금융거래 가입자의 계정(ID)과 그 비밀번호 또는 계좌번호와 그 비밀번호
- 전자금융거래 가입자의 주민등록번호
- 금융기관이 전자금융거래를 위하여 가입자에게 제공한 일회용비밀번호(보안카드의 비밀번호 포함) 또는 가입자 본인만이 알 수 있는 두 가지 이상의 정보

3.3.2 신원확인 절차

가. 개인 신원확인 절차

“정보인증” 또는 등록대행기관은 개인에 대한 신원확인을 위해 제출된 인증서비스 신청서와 개인 신원확인증표의 성명과 주민등록번호 또는 첨부된 사진 등을 통해 신원확인을 합니다.

나. 법인 또는 단체 신원확인 절차

“정보인증” 또는 등록대행기관은 법인(단체)에 대한 신원확인을 위해 제출된 인증서비스 신청서와 법인 및 단체의 신원확인증표 및 추가 서류의 법인 명, 대표자 성명, 사업자등록번호 등을 통해 신원확인을 합니다.

대리인을 통하여 신청할 경우 대표자의 위임장, 법인인감증명서, 대리인의 신원확인증표 등 추가 서류를 통해 신원확인을 합니다.

3.3.3 가입자의 전자서명생성정보 소유증명 방법

가입자는 자신의 전자서명생성정보로 전자서명한 정보를 “정보인증”에 제출하고 “정보인증”은 그 전자서명한 정보를 가입자의 전자서명검증정보로 검증하는 절차를 거쳐 가입자가 전자서명생성정보를 소유하고 있음을 확인합니다.

3.4 갱신 및 재발급시 신원확인

3.4.1 갱신 발급

3.4.1.1 신원확인 방법 및 절차

"정보인증"은 가입자가 보유한 전자서명생성정보로 전자서명한 정보를 "정보인증"에 제출하고 "정보인증"은 그 전자서명한 정보를 가입자의 전자서명검증정보로 검증하는 과정을 통해서 가입자의 신원을 확인합니다.

3.4.1.2 가입자의 전자서명생성정보 소유증명 방법

본 준칙 "3.3.3가입자의 전자서명생성정보 소유증명 방법"을 준용하여 소유증명 합니다.

3.4.2 재발급

3.4.2.1 신원확인 방법 및 절차

인증서의 재발급은 본 준칙 "3.3.1신원확인 방법"과 "3.3.2신원확인 절차"에 따라 신원확인을 합니다.

3.4.2.2 가입자의 전자서명생성정보 소유증명 방법

본 준칙 "3.3.3가입자의 전자서명생성정보 소유증명 방법"을 준용하여 소유증명 합니다.

3.4.3 가입자 등록정보 변경

3.4.3.1 신원확인 방법과 절차

"정보인증"은 가입자가 등록정보를 변경하고자 하는 때에는 보유한 인증서 또는 본 준칙 "3.3.1신원확인 방법"과 "3.3.2신원확인 절차" 에 따라 신원확인을 합니다. 그 외 가입자 등록정보(주소, 전화번호, 전자우편주소 등) 변경 요청 시에는 가입자의 전자서명에 대한 검증으로 신원확인을 대체하여 "정보인증"에 등록된 해당 정보를 변경할 수 있습니다.

3.5 인증서 효력정지·효력회복·폐지 시, 신원확인

3.5.1 효력정지 신원확인 방법 및 절차

가. "정보인증"을 방문하여 정지하는 경우

1) 인증서관리요청서 제출

가입자는 "정보인증"이 제공하는 "인증서관리요청서"에 필요한 사항을 기재한 후 "정보인증"을 방문하여 제출합니다.

2) 신원확인

"정보인증"은 본 준칙 "3.3.1신원확인 방법"과 "3.3.2신원확인 절차" 에 따라 신원확인을 합니다.

나. 가입자가 정보통신망을 이용하여 직접 정지하는 경우

가입자는 인증서의 효력을 정지하고자 하면 정보통신망을 이용하여 "인증서효력정지"를 선택한 후, 안내에 따라 인증서 효력정지 절차를 진행합니다. 이때 신원확인은 본 준칙 "3.4.1.1신원확인 방법 및 절차"을 준용합니다.

3.5.2 효력회복 신원확인 방법 및 절차

가. 인증서관리요청서 제출

가입자는 "정보인증"이 제공하는 "인증서관리요청서"에 필요한 사항을 작성한 후 "정보인증"을 방문하여 제출하여야 합니다.

나. 신원확인

"정보인증"은 본 준칙 "3.3.1신원확인 방법"과 "3.3.2신원확인 절차" 에 따라 신원확인을 합니다.

3.5.3 폐지 신원확인 방법 및 절차

가. "정보인증"을 방문하여 폐지하는 경우

1) 인증서관리요청서 제출

가입자는 "정보인증"이 제공하는 "인증서관리요청서"에 필요한 사항을 작성한 후 "정보인증"을 방문하여 제출합니다.

2) 신원확인

"정보인증"은 본 준칙 "3.3.1신원확인 방법"과 "3.3.2신원확인 절차" 에 따라 신원확인을 합니다.

나. 가입자가 정보통신망을 이용하여 직접 폐지하는 방법

가입자는 인증서를 폐지하고자 하면 정보통신망을 이용하여 “인증서 폐지하기”를 선택한 후, 안내에 따라 인증서의 폐지 절차를 진행합니다. 이때 신원확인은 본 준칙 “3.4.1.1신원확인 방법 및 절차”을 준용합니다.

4. 인증서 관리

4.1 인증서 발급 신청

4.1.1 신청 주체

개인이 인증서를 발급받고자 할 때는 본인이 직접 신청하여야 하며, 법인의 경우에는 해당 법인의 임원 또는 직원이 법인을 대리하여 신청할 수 있습니다.

4.1.2 신청 절차

가. 가입 신청자는 “정보인증” 또는 등록대행기관에 방문하여 인증서비스 신청서와 신원확인증표 및 추가서류를 제출하여 신원확인을 받아야 합니다.

나. “정보인증” 또는 등록대행기관은 인증서비스 신청서와 신원확인증표를 비교하여, 개인의 경우에는 성명 및 주민등록번호를, 법인(단체)의 경우에는 법인(단체)명 및 사업자등록번호를 확인합니다.

4.2 인증서 발급 신청 처리

가. “정보인증” 또는 등록대행기관은 인증서 발급 신청정보 및 신청서류를 확인하고 가입신청자의 신원확인을 마친 후 가입자 등록번호(참조번호와 인가코드)를 가입신청자에게 전달합니다. 다만, 타인 명의 신청, 허위사실의 기재 및 허위서류 첨부, 수수료 미납 기타 가입 신청자의 귀책 사유로 인하여 인증서의 발급이 곤란한 경우에는 발급을 거절할 수 있습니다.

나. 인증서의 발급 소요기간은 가입 신청자가 발급요청을 한 날로부터 1~3일입니다. 다음의 경우에는 발급이 지연될 수 있습니다.

1) 가입 신청자의 정보가 정확성에 문제가 있는 경우

2) 가입 신청자가 요금을 미납한 경우

3) 단체가입 등 가입 신청자의 규모가 큰 경우 등

4.3 인증서 발급 절차 및 보호조치

4.3.1 인증서 발급 절차

가입 신청자는 "정보인증" 또는 등록대행기관으로부터 전달받은 가입자 등록번호(인가코드-참조번호) 또는 발급용 임시번호를 이용하여 인증서를 발급합니다.

4.3.2 인증서 발급 보호조치

가. 가입자는 가입자 소프트웨어를 이용하여 "정보인증"이 생성한 인증서를 안전하게 받습니다.

나. "정보인증"은 등록대행기관 등과 정보통신망을 이용하여 가입 신청자 정보를 전송하는 경우 모든 정보는 전자서명을 통해 위·변조 여부를 확인하며 암호화하여 안전하게 전송함으로써 가입자 정보의 기밀성, 무결성 등을 보장합니다

4.4 인증서 수령

가입 신청자는 가입자 소프트웨어를 통해 "정보인증"이 발급한 인증서를 전달받아, 인증서와 자신의 전자서명생성정보를 저장할 매체를 선택하고 인증서 비밀번호를 입력하여 수령합니다.

4.5 인증서 이용

"정보인증"이 발급한 인증서는 전자거래 등의 업무에 사용할 수 있습니다. 앞의 전자거래에서의 인증서 사용은 정당한 권한을 가진 가입자가 인증서의 이용범위 및 발급 용도에 맞게 인증서를 사용하는 것을 말합니다. 그러하지 아니한 경우 "정보인증"은 기발급된 인증서의 사용을 제한할 수 있습니다.

4.6 인증서 갱신 발급

4.6.1 갱신 발급 요건

가입자는 기존에 사용하던 인증서의 유효기간이 만료되기 60일 전부터 유효기간 만료일까지 갱신 발급 가능합니다.

4.6.2 갱신 신청 주체

개인이 인증서를 갱신 발급받고자 할 때는 본인이 직접 신청하여야 하며, 법인의 경우에는 해당 법인의 임원 또는 직원이 법인을 대리하여 신청할 수 있습니다.

4.6.3 갱신 절차

가. 인증서 갱신은 인증서를 보유한 가입자가 정보통신망으로 신청합니다.

나. “정보인증”은 가입자가 보유한 전자서명생성정보로 전자서명한 정보를 “정보인증”에 제출하고 “정보인증”은 그 전자서명한 정보를 가입자의 전자서명검증정보로 검증하는 과정을 통해서 가입자의 신원을 확인합니다.

다. 가입자는 자신의 전자서명생성정보로 전자서명한 정보를 “정보인증”에 제출하고 “정보인증”은 그 전자서명한 정보를 가입자의 전자서명검증정보로 검증하는 과정을 통해서 가입자의 전자서명생성정보와 가입자의 전자서명검증정보가 합치하는가를 확인함으로써 가입자가 전자서명생성정보를 소유한다는 사실을 확인하고 인증서를 갱신 발급합니다.

4.6.4 가입자가 갱신 발급된 인증서를 수령하는 방법

가입자가 온라인으로 인증서 갱신 신청을 하면 “정보인증”은 갱신 여부를 검토 후 갱신이 허용되면 새로운 유효기간의 인증서를 새로 발급함으로써 가입자는 갱신 발급된 인증서를 가입자 소프트웨어를 통해 수령합니다.

4.7 인증서 재발급

4.7.1 재발급 요건

“정보인증”은 가입자가 다음과 같은 경우 현재 이용 중인 인증서를 폐지하고 새로운 인증서를 발급 신청할

수 있습니다. 재발급된 인증서의 유효기간은 인증서 재발급일로부터 재발급 이전 인증서의 유효기간 만료일까지입니다.

가. 가입자가 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출 되었다고 판단되어 재발급을 신청한 경우

나. 가입자의 성명 또는 상호가 변경되어 재발급을 신청한 경우

4.7.2 재발급 신청 주체

개인이 인증서를 재발급 받고자 할 때는 본인이 직접 신청하여야 하며, 법인의 경우에는 해당 법인의 임원 또는 직원이 법인을 대리하여 신청할 수 있습니다.

4.7.3 재발급 신청 절차

가. 가입자는 인증서비스 신청서를 작성한 후 "정보인증" 또는 등록대행기관에 방문하여 신청서와 신원확인증표, 추가서류를 제출하여 신원확인을 받아야 합니다.

나. "정보인증" 또는 등록대행기관은 신원확인 절차를 수행한 후에 인증서를 재발급합니다.

4.7.4 가입자가 재발급된 인증서를 수령하는 방법

가입자는 가입자 소프트웨어를 통해 "정보인증"이 발급한 인증서를 전달받아, 인증서와 자신의 전자서명생성정보를 저장할 매체를 선택하고 수령합니다.

4.8 등록정보 변경

4.8.1 가입자 등록정보 변경 요건

인증서 내에 반영된 가입자 정보 변경의 경우는 인증서 신규 발급 절차를 따르며, 그 외의 가입자 등록정보(주소, 전화번호 등)가 변경된 경우에는 가입자가 등록정보 변경을 요청하여 "정보인증"에 등록된 정보를 변경할 수 있습니다.

4.8.2 가입자 등록정보 변경 신청 절차

4.8.2.1 가입자 등록정보 변경 신청 절차(인증서 내에 반영된 가입자 정보 변경)

가. 가입자는 인증서비스 신청서를 작성한 후 “정보인증” 또는 등록대행기관에 방문하여 신청서와 신원확인증표, 추가서류를 제출하여 신원확인을 받아야 합니다.

나. “정보인증” 또는 등록대행기관은 신원확인 절차를 수행한 후에 가입자 등록정보를 변경 하여 인증서를 재발급 합니다.

4.8.2.2 가입자 등록정보 변경 신청 절차(그 외 가입자 등록정보 변경)

가입자는 정보통신망을 이용하여 가입자 등록정보 변경 신청을 할 수 있으며, 이때 신원확인은 본 준칙 “3.4.1.1신원확인 방법 및 절차”을 준용합니다.

4.8.3 가입자 등록정보가 변경된 인증서를 수령하는 방법

인증서 내에 반영된 가입자 정보 변경을 요청한 가입자는 가입자 소프트웨어를 통해 "정보인증"이 발급한 인증서를 전달받아, 인증서와 자신의 전자서명생성정보를 저장할 매체를 선택하고 수령합니다.

4.9 인증서 효력정지·효력회복·폐지

4.9.1 인증서 효력정지

4.9.1.1 인증서 효력정지 요건

인증서 효력정지 사유는 다음과 같습니다.

가. 가입자 또는 그 대리인이 효력정지를 신청한 경우

나. 가입자가 준칙을 위반한 경우

다. 가입자의 전자서명생성정보에 대한 분실·훼손 또는 도난·유출이 의심되는 경우

4.9.1.2 인증서 효력정지 주체

개인이 인증서를 효력정지 할 때에는 본인이 직접 신청하여야 하며, 법인의 경우에는 해당 법인의 임원

또는 직원이 법인을 대리하여 효력정지 할 수 있습니다.

4.9.1.3 인증서 효력정지 방법 및 절차

가. "정보인증"을 방문하여 정지하는 방법 및 절차

1) 가입자는 효력정지 신청서를 작성한 후 "정보인증" 또는 등록대행기관에 방문하여 신청서와 신원확인증표, 추가서류를 제출하여 신원확인을 받아야 합니다.

2) "정보인증" 또는 등록대행기관은 신청서와 신원확인증표를 비교하여, 개인의 경우에는 성명 및 주민등록번호를, 법인(단체)의 경우에는 법인(단체)명 및 사업자등록번호를 확인 후 효력정지 합니다.

나. 가입자가 정보통신망을 이용하여 직접 정지하는 방법 및 절차

가입자는 인증서의 효력을 정지하고자 할 때 정보통신망을 이용하여 "인증서 효력정지"를 선택한 후 효력정지 합니다. 이때 신원확인은 본 준칙 "3.4.1.1신원확인 방법 및 절차"을 준용합니다.

4.9.2 인증서 효력회복

4.9.2.1 인증서 효력회복 요건

가입자는 인증서의 효력이 정지된 날로부터 6개월 이내에 그 회복을 신청하여야 합니다. 이 기간 내에 신청하지 않으면 현재 효력정지된 인증서는 자동 폐지됩니다.

4.9.2.2 인증서 효력회복 주체

개인이 인증서를 효력회복 할 때는 본인이 직접 신청하여야 하며, 법인의 경우에는 해당 법인의 임원 또는 직원이 법인을 대리하여 효력회복 할 수 있습니다.

4.9.2.3 인증서 효력회복 방법 및 절차

가. 가입자는 효력회복 신청서를 작성한 후 "정보인증" 또는 등록대행기관에 방문하여 신청서와 신원확인증표, 추가서류를 제출하여 신원확인을 받아야 합니다.

나. "정보인증" 또는 등록대행기관은 신청서와 신원확인증표를 비교하여, 개인의 경우에는 성명 및 주민등록번호를, 법인(단체)의 경우에는 법인(단체)명 및 사업자등록번호를 확인 후 효력회복 합니다.

4.9.2.4 효력회복까지 처리되는 소요 시간

"정보인증"은 가입자가 인증서의 효력을 회복시키는 경우에 유효기간 및 종류에 상관없이 1일 이내로 조치합니다.

4.9.3 인증서 폐지

4.9.3.1 인증서 폐지 요건

"정보인증"은 다음 사유 발생 시 해당 인증서를 폐지합니다.

1) 가입자 또는 그 대리인이 인증서 폐지를 신청한 경우
2) 가입자 또는 그 대리인이 인증서 가입취소를 요청한 경우
3) 가입자가 사위 기타 부정한 방법으로 인증서를 발급받은 사실 또는 이용한 사실을 인지하였거나, 그 가능성을 객관적으로 인지한 경우
4) 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출된 사실을 인지한 경우
5) 가입자가 본 준칙을 위반한 경우
6) 가입자가 인증서 효력회복 신청기한 내에 효력회복을 신청하지 아니한 경우
7) 가입자의 신원확인이 적법하게 이루어지지 않았음을 "정보인증"이 인지한 경우
8) 가입자의 사망·실종선고 또는 파산·청산·해산 사실을 인지한 경우
9) "정보인증"의 전자서명생성정보가 분실, 훼손, 도난, 유출되었음을 인지한 경우 또는 알고리즘의 취약성을 인지한 경우

4.9.3.2 인증서 폐지 주체

개인이 인증서를 폐지하는 경우에는 본인이 직접 신청하여야 하며, 법인의 경우에는 해당 법인의 임원 또는 직원이 법인을 대리하여 폐지할 수 있습니다.

"정보인증"은 가입자 또는 그 대리인의 신청이 없는 경우라 하더라도 본 준칙 "4.9.3.1인증서 폐지 요건" 중 3호 내지 9호를 충족한 경우, 직권으로 폐지할 수 있습니다.

4.9.3.3 인증서 폐지 방법 및 절차

가. "정보인증"을 방문하여 폐지하는 방법

1) 가입자는 폐지신청서를 작성한 후 "정보인증" 또는 등록대행기관을 방문하여 신청서와 신원확인증표,

추가서류를 제출하여 신원확인을 받아야 합니다.

2) “정보인증” 또는 등록대행기관은 신청서와 신원확인증표를 비교하여, 개인의 경우에는 성명 및 주민등록번호를, 법인(단체)의 경우에는 법인(단체)명 및 사업자등록번호를 확인 후 폐지합니다.

나. 가입자가 정보통신망을 이용하여 직접 폐지하는 방법

가입자는 인증서를 폐지하고자 할 때 정보통신망을 이용하여 “인증서 폐지하기”를 선택한 후 인증서의 폐지 절차를 진행합니다. 이때 신원확인은 본 준칙 “3.4.1.1신원확인 방법 및 절차”을 준용합니다.

다. 가입자의 긴급 폐지 요청

가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출 등의 긴급한 사유로 공동인증서의 폐지를 요청하는 때에는 사전에 등록된 2개 이상의 개인정보를 확인하는 등의 신뢰할 수 있는 방법을 통하여 당해 가입자의 본인여부를 확인하고 해당 인증서를 폐지합니다.

4.9.4 가입자 정보의 전송방법 및 가입자 정보의 기밀성, 무결성 등에 대한 정보 보안 방법

“정보인증”은 등록대행기관 등과 정보통신망을 이용하여 가입 신청자 정보를 전송하는 경우 모든 정보는 전자서명을 통해 위·변조 여부를 확인하며 암호화하여 안전하게 전송함으로써 가입자 정보의 기밀성, 무결성 등을 보장합니다.

4.9.5 인증서 효력정지 및 폐지 목록의 발행주기

“정보인증”은 인증서 효력정지 및 폐지 목록을 적어도 매일 1회 이상 갱신합니다.

4.9.6 인증서 효력정지 및 폐지 목록 발행 시점부터 해당 인증서 효력정지 및 폐지 목록을 공고하는 데까지 소요 시간

인증서 효력정지, 폐지 시 공고 하는 데까지 소요시간은 최대 24시간 이내입니다.

4.9.7 인증서 효력정지 상태 유지 가능 기간

가입자는 인증서의 효력이 정지된 날로부터 6개월 이내에 그 회복을 신청하여야 합니다. 이 기간 내에 신청하지 않으면 해당 인증서는 자동 폐지됩니다.

4.10 인증서 유효성 확인 서비스

4.10.1 인증서 유효성 확인 서비스 이용 방법

인증서 유효성 확인 서비스(OCSP) 신청자 또는 그 대리인은 서비스 가입을 위해 "정보인증"에 등록 신청을 하여야 합니다. OCSP 서비스 가입자는 "정보인증"에서 받은 OCSP 클라이언트 소프트웨어 또는 자신이 보유하고 있는 소프트웨어를 이용하여 유효성 확인 요청을 합니다.

4.10.2 이용조건

"정보인증"은 인증서 유효성 확인 서비스(OCSP)를 받고자 하는 경우 서비스가입자 및 이용자와의 계약으로 서비스를 제공할 수 있습니다. 이때 서비스 이용 수수료, 기타 제공 조건 등은 상호 협의한 계약의 내용에 따릅니다.

4.10.3 이용계약 해지

OCSP 서비스 가입자 또는 이용자는 "정보인증"에 해지 의사를 통보할 수 있으며, "정보인증"은 계약의 내용에 따라 계약해지를 진행합니다.

4.11 서비스 가입 철회

4.11.1 인증서비스 가입 철회 절차

가입자가 서비스 가입 철회를 원하면 인증서를 폐지함으로써 서비스 중단을 할 수 있습니다.
이 경우 가입자가 기 납부한 발급 수수료가 있을 경우 이의 환불 가능 여부와 환불 절차는 본 준칙 "9.1.2 환불정책"을 준용합니다.

4.11.2 인증서비스 가입 철회 시 인증서 폐지와 개인정보 파기

가입자가 서비스 가입 철회 시 가입자의 개인정보는 본 준칙 "5.5기록 보존"을 준용하여 파기합니다.

4.12 기타 부가서비스

4.12.1 시점확인서비스(TSA)

"정보인증"은 시점확인서비스 신청자와의 계약으로 시점확인서비스를 제공할 수 있습니다. 이때 서비스 이용 수수료, 이용계약의 해지, 기타 제공 조건 등은 상호 협의한 계약의 내용에 따릅니다.

4.12.2 클라우드 서비스

클라우드 서비스라 함은 가입자의 인증서를 클라우드에 보관하여 PC, 모바일 등 다양한 매체에서 인증서를 편리하게 사용할 수 있게 하는 서비스입니다. 클라우드 서비스는 "코스콤"과 "정보인증"이 함께 제공하는 서비스이며 "코스콤"의 등록서버에서 인증서가 등록되지만, "정보인증" 가입자의 인증서는 "정보인증" 저장서버에 저장 됩니다. 이때 서비스 이용 수수료, 이용계약의 해지, 기타 제공 조건 등은 상호 협의한 계약의 내용에 따릅니다.

5. 시설 및 운영 관리

5.1 물리적 보호조치

5.1.1 물리적 접근통제

5.1.1.1 인증시스템 위치

"정보인증"의 인증시스템을 위한 시설의 위치는 아래와 같습니다.

- 서울시 서초구 서초동 1421-1번지 LGU+ 서초 2센터 5층

5.1.1.2 인증시스템 구조

"정보인증"은 인증시스템을 보호하기 위하여 인증시스템별로 분리된 별도의 통제구역 내에 설치하여 운영합니다.

5.1.1.3 물리적 보호조치에 관한 사항

가. "정보인증" 인증시스템은 권한 있는 자만이 출입이 허가됩니다.

나. "정보인증"은 이상 상황 발생 시 경보 기능을 갖는 CCTV 카메라 및 모니터링시스템과 침입 감지 시스템 등 감시통제시스템을 설치, 운영합니다.

다. "정보인증"의 출입통제 시스템은 신원확인카드, 지문인식 및 무게 감지 장치 등을 다중으로 결합하여 통제구역에 대한 접근을 통제합니다.

라. "정보인증"은 보안 경비요원을 배치하여 보안경비업무를 수행합니다.

5.1.1.4 물리적 잠금장치에 관한 사항

"정보인증"은 인증시스템을 별도의 통제구역 내에 설치, 운영하고, 해당 시스템을 물리적 접근통제를 위하여 보안캐비닛 내에 설치합니다.

5.1.2 전원

"정보인증"은 갑작스러운 정전으로 인한 심각한 피해를 방지하기 위하여 무정전 전원 공급장치를 사용합니다.

5.1.3 수해방지

"정보인증"은 침수로부터 인증시스템 및 중요장비를 안전하게 보호하기 위하여 바닥으로부터 떨어져 설치합니다.

5.1.4 화재 예방

"정보인증"은 인증시스템실 등에 화재 탐지기, 휴대용 소화기 및 자동 소화설비를 설치합니다.

5.1.5 방호

"정보인증"은 인증시스템 운영실의 외벽을 외부침입으로부터 보호할 수 있도록 설계합니다.

가. 외벽 재질은 벽돌 또는 철근 콘크리트로 축조되어 있거나, 철골 구조물에 3T 이상의 철판으로 용접

나. 외벽은 천장, 바닥까지 완벽하게 마감

다. 운영실을 분리할 수 있도록 인증시스템 운영실의 내벽을 설계

라. 창문이 있는 경우 강화유리 또는 강화 필름으로 코팅한 유리를 사용

5.1.6 매체 저장

"정보인증"은 주요 저장, 기록매체를 금고에 저장하여 물리적으로 접근을 통제합니다.

5.1.7 원격지 백업

가. "정보인증"은 "정보인증"이 발급한 인증서, 인증서 효력정지 및 폐지 목록 등을 물리적으로 10KM이상 격리된 원격지에 백업하여 5년간 보관합니다.

나. "정보인증"은 원격지 백업설비의 안전한 운영을 위하여 CCTV 카메라 설치와 출입자의 신원을 확인할 수 있는 신원확인용 정맥 인식장치 설치 등을 통해 접근통제 합니다.

5.1.8 항온/항습, 통풍설비에 관한 사항

가. "정보인증"은 인증시스템의 안정적인 운영을 위한 온도 및 습도를 일정하게 유지하기 위해 항온 항습장치를 설치합니다.

나. "정보인증"은 통풍창을 통한 외부침입을 방지하기 위하여 차폐막과 감지기를 설치합니다.

5.1.9 폐기물 처리

가. "정보인증"은 문서, 디스켓 등을 폐기하는 경우 물리적으로 이를 파기합니다.

나. "정보인증"은 시설과 장비의 폐기처리에 관한 사항은 내부지침인 '정보자산관리지침'에 따라 안전하게 폐기합니다.

5.2 절차적 보호조치

5.2.1 전자서명인증업무 수행을 위해 필요한 업무 종류와 업무 분장

가. "정보인증"은 전자서명인증업무의 안전성 및 신뢰성을 확보하기 위하여 업무를 역할별로 분리하여 수행합니다.

나. "정보인증"은 전자서명인증업무의 수행에 필요한 인력 및 운영절차에 관하여 내부지침인 '데이터센터 운영매뉴얼'에 따라 수행합니다.

다. 전자서명인증업무 수행을 위한 업무의 종류와 업무 분장은 내부지침인 '인증업무운영자' 에 따라 수행합니다.

5.2.2 동일인에 의해 동시 수행될 수 없는 전자서명인증업무

"정보인증"은 전자서명인증업무 운영 시 신뢰성 및 보안성 확보를 위하여 다음과 같이 업무 분리 원칙을 준수합니다.

가. 인증기관 전자서명생성정보 생성·백업·이용·삭제·파기업무는 3인 이상이 공동으로 수행합니다.

나. 기타의 전자서명인증업무는 2인 이상이 공동으로 수행합니다.

다. 동일인에 의해 수행될 수 없는 전자서명인증업무는 내부지침인 '인증업무운영자' 규정을 두어 별도로 규정하고 있습니다.

5.2.3 업무 담당자 현황 및 담당자 인증방법

가. "정보인증"은 업무 권한에 따라 출입통제시스템에 등록된 소지 기반의 신원확인카드와 생체기반의 지문인식을 통해 신원을 확인합니다.

나. "정보인증"의 업무 담당자는 내부지침인 '인증업무운영자'에 규정을 두어 별도로 규정하고 있습니다.

5.3 인적 보안

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

"정보인증"은 인증시스템 운영 인력에 대하여 내부규정인 '취업규칙'에 따라 신원확인을 하고 있으며 이상이

없는 임직원만 관련 업무를 수행하도록 하고 있습니다.

5.3.2 업무 수행 인력의 교육 및 업무순환

가. "정보인증"은 인증시스템 보호조치 및 비상복구 대응 등에 대하여 소속직원이 관련 내용을 숙지할 수 있도록 내부교육 등의 필요한 조치를 합니다.

나. "정보인증"은 전자서명인증업무 수행 인력이 연 1회 이상 정보보호 교육을 이수하도록 합니다.

다. "정보인증"은 인증시스템의 안전한 운영을 위해 업무를 역할별로 분장하여 수행하고 있으며, 동일인에 의해 수행될 수 없는 업무는 당사 '인증업무운영자'규정에 따라 공동으로 수행하고 있습니다.

5.3.3 비인가 된 행위에 대한 처벌

"정보인증"은 전자서명법령 및 준칙에 인가되지 않는 행위를 한 경우에는 내부규정인 '상벌지침' 에 따라 해당 직원을 징계합니다.

5.4 감사 기록

5.4.1 감사 기록의 유형 및 보존 기간

"정보인증"은 다음을 내용으로 하는 인증시스템 감사기록을 정기적으로 백업하여 관리하고 있으며, 감사기록은 5년간 보관합니다.

① 가입자 등록정보를 입력·접근·변경·삭제 등에 관한 내역

② "정보인증"의 전자서명생성정보를 생성·접근·파기한 내역

③ 인증서를 생성·발급·갱신·효력정지 또는 폐지한 내역

④ 가입자인증서 등을 등록 및 관리한 사실

⑤ 인증시스템의 시작과 종료 사실

⑥ 로그인(Login) 및 로그오프(Logoff) 사실

⑦ 기타 인증 시스템 관리자의 주요 활동 사실

5.4.2 감사 기록 검토 등 보호조치

감사관리자는 사건 발생 시 감사 기록을 세밀히 검토하고 보존합니다. 각 시스템의 감사 기록은 감사관리자에 의해 총괄 관리되며 시스템의 각 운영권리자는 해당 업무에 대한 감사 기록만 열람할 수 있습니다.

5.4.3 감사 기록 백업 주기 및 절차

가. ""정보인증""은 변경된 내역에 대해 매일 백업하고 있으며, 전체 데이터에 대해서는 주 단위로 백업합니다.

나. 백업과 관련한 상세한 절차는 내부 지침 '데이터센터 운영매뉴얼'에 따라 실시합니다.

5.5 기록 보존

5.5.1 보존되는 기록의 유형

"정보인증"은 다음 업무와 관련된 내역을 기록, 보존합니다.

가. 가입자의 인증서 발급 및 관리 등 전자서명인증업무

나. "정보인증" 인증시스템 등의 운영 업무

5.5.2 기록의 보존 기간

"정보인증"은 5.5.1의 보존 대상 기록을 인증서 유효기간 만료일로부터 5년간 보존합니다. 단, 전자서명법(법률 제17354호) 부칙 제2조(공인인증서에 관한 경과조치)에 의거 전자서명법 개정전 법 제15조에 따라 발급된 유효한 공인인증서에 대해서는 유효기간 만료일로부터 10년간 보관합니다.

5.5.3 보존기록 보호조치

"정보인증"은 보존기록에 대해 물리적 및 절차적, 인적 통제를 통해 보안을 유지하고 조회가 필요한 경우 인적 통제를 통한 인가된 관리자 업무 범위에 한정시키며 잠금장치가 구비된 캐비넷에 보관하여 보존기록의 위·변조 및 훼손을 방지하도록 보호합니다.

5.5.4 보존기록의 백업주기 및 백업절차

가. "정보인증"은 변경된 내역에 대해 매일 백업하고 있으며, 전체 데이터에 대해서는 주 단위로 백업합니다.

나. 백업과 관련한 상세한 절차는 내부지침 '데이터센터 운영매뉴얼'에 따라 실시합니다.

5.6 전자서명인증사업자의 전자서명생성정보 갱신

"정보인증"은 "정보인증"의 전자서명생성정보를 갱신하지 않고 본 준칙 "6.1.1전자서명생성정보 생성"을 준용하여 신규 생성하고 최상위기관으로부터 신규 인증서를 수령 받습니다.

5.7 장애 및 재해 복구

5.7.1 전자서명인증업무 장애 및 재해 유형별 처리 및 복구 절차

"정보인증"은 전자서명인증업무와 관련하여 발생하는 장애 또는 재해에 대해 다음과 같이 유형별로 나누어 내부지침 '데이터센터 운영매뉴얼'에 규정하여 신고 및 복구 절차를 진행합니다.

가. 센터 내 외부침입 경보 발생

나. 센터 내 화재 발생

다. 센터 내 수재 발생

라. 하드웨어 장애 발생

마. 시스템 자원 및 소프트웨어 장애 발생

바. 데이터 손상 발생

사. 이중화 시스템 장애 발생

아. 기타 비상반출

5.7.2 업무 장애방지 등 연속성 보장 대책

가. "정보인증"은 시스템 자원 및 소프트웨어 등에 장애가 발생한 경우에 이중으로 설치한 시스템 자원 및 소프트웨어를 이용하여 복구합니다.

나. "정보인증"은 인증서 등의 주요 데이터에 훼손·멸실이 발생하였을 때 기록 보존된 자료를 이용하여

복구합니다.

다. "정보인증"은 전자서명인증업무 운영 인력을 주·야간으로 운영하여 연중무휴로 인증서비스를 제공합니다.

5.8 업무 휴지, 폐지, 종료

5.8.1 전자서명인증업무 휴지

자연재해 또는 천재지변이 아닌 불가피한 사정으로 "정보인증"이 전자서명인증업무의 전부 또는 일부를 휴지하는 경우 휴지 기간을 정하여 휴지하려는 날의 30일전까지 그 사실을 가입자에게 통보하고 인터넷 홈페이지에 요금의 반환 등 가입자 보호조치 내용을 게시합니다.

5.8.2 전자서명인증업무 폐지 및 종료

자연재해 또는 천재지변이 아닌 불가피한 사정으로 "정보인증"이 전자서명인증업무를 폐지 및 종료하려는 경우 폐지 및 종료하려는 날의 60일 전까지 그 사실을 가입자에게 통보하고 인터넷 홈페이지에 요금의 반환, 가입자의 개인정보 폐기 등 가입자 보호조치 내용을 게시합니다.

6. 기술적 보호조치

6.1 전자서명생성정보 보호

6.1.1 전자서명생성정보 생성

가. "정보인증"은 인가된 자만이 전자서명생성정보를 생성할 수 있습니다.

나. "정보인증"은 물리적 침해 등으로부터 보호되는 FIPS 140-2 Level 3 인증을 받은 HSM을 사용하여 전자서명생성정보를 생성합니다.

다. 전자서명생성정보 생성 작업은 다자인증 통제(최소 3명 이상) 하에서 전자서명생성정보를 생성합니다.

6.1.2 전자서명생성정보의 크기 및 해쉬 값

"정보인증"은 안전하고 신뢰할 수 있는 전자서명 알고리즘을 사용하기 위하여 다음과 같은 크기의 키 및 해쉬 값을 이용합니다.

가. RSA : 2,048bit 이상

나. SHA-256 : 256bit

6.2 전자서명생성정보 보호조치

6.2.1 전자서명생성정보의 저장 시 보호조치

"정보인증"은 "정보인증"의 전자서명생성정보를 전자서명생성정보가 분실, 훼손 또는 도난, 유출되지 않도록 하드웨어보안장치(HSM)에 안전하게 저장합니다.

6.2.2 전자서명생성정보의 이용 시 보호조치

"정보인증"은 "정보인증"의 전자서명생성정보 활성화 작업을 다자인증 통제(최소 3명 이상) 하에서 합니다.

6.2.3 전자서명생성정보의 백업 보관 시 보호조치

가. "정보인증"은 "정보인증"의 전자서명생성정보 백업 작업을 다자인증 통제(최소 3명 이상) 하에서 합니다.

나. "정보인증"은 백업된 전자서명생성정보 중 1부를 전자서명인증업무 수행 시설과는 원격지 저장설비에 안전하게 보관합니다.

다. "정보인증"은 전자서명생성정보를 백업 보관하는 경우, 2인 이상의 권한 있는 직원이 공동으로 이를 수행합니다.

6.2.4 전자서명생성정보의 삭제 및 파기 시 보호조치

가. "정보인증"은 인가된 자만이 전자서명생성정보를 삭제 및 파기할 수 있습니다.

나. 전자서명생성정보 삭제 및 파기 작업은 다자인증 통제(최소 3명 이상) 하에서 전자서명생성정보를 삭제 및 파기합니다.

다. "정보인증"은 관리책임자와 보안관리자의 입회 하에 백업된 전자서명생성정보와 그 원본을 시스템 메모리에서 전자서명정보를 안전하게 파기합니다.

6.3 전자서명생성정보 및 전자서명검증정보의 관리

"정보인증"은 신뢰할 수 있는 소프트웨어나 하드웨어 등을 이용하여 안전한 방법으로 전자서명생성정보를 생성하며 생성된 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리 합니다.

6.4 데이터 보호조치

가. "정보인증"은 "정보인증"의 전자서명생성정보가 분실, 훼손 또는 도난, 유출되지 않도록 하드웨어보안장치(HSM)에 안전하게 저장합니다.

나. 전자서명생성정보 생성 작업은 다자인증 통제(최소 3명 이상) 하에서 전자서명생성정보를 생성합니다.

다. "정보인증"은 전자서명생성정보를 백업 보관하는 경우, 2인 이상의 권한 있는 직원이 공동으로 이를 수행합니다.

6.5 시스템 보안 통제

가. "정보인증"은 인증시스템의 보안 소프트웨어를 설치하여 운영하고 보안 장비를 운영합니다.

나. "정보인증"은 인증시스템에 대한 물리적 접근통제 목록을 문서화하여 접근통제 현황에 대한 주기적인 모니터링을 합니다.

다. "정보인증"은 인증시스템에 설치되는 프로그램의 사용을 제한하고 통제합니다.

6.6 시스템 운영 관리

"정보인증"은 전자서명인증 인증시스템의 운영에 대한 형상관리를 다음과 같이 합니다.

- 인증시스템의 소프트웨어 등록에 대한 형상관리
- 인증시스템의 변경사항 등 운영관리에 대한 형상관리

6.7 네트워크 보호조치

가. "정보인증"은 물리적으로 분리된 두 개의 서로 다른 ISP로부터 회선을 공급받아 이중화 구성하여, 한 개의 회선이 장애가 발생하여도 서비스 제공을 중단하지 않고 안전하게 서비스를 제공합니다.

나. "정보인증"은 침입 차단시스템 및 침입 방지시스템을 운영하여 불법적인 접근을 차단하여 안전하게 서비스를 제공합니다.

6.8 시점확인서비스 보호조치

"정보인증"은 본 준칙 "5.1물리적 보호조치"에 따라 시점확인 기능을 제공하는 시스템은 인증시스템실과 별도로 운영실을 분리하는 보호조치를 마련하여 시행하고 있습니다.

7. 인증서 형식

7.1 인증서 형식

"정보인증"이 발급하는 인증서의 구성 및 내용은 아래와 같습니다.

기본 필드 명	선택 여부		입력값
	생성	처리	
Version	m	m	V3
Serial Number	m	m	고유일련번호(up to 20Byte)
Signature	m	m	sha256 with RSA (256byte)
Issuer	m	m	C(Country)는 printableString 그 외의 속성값은 utf8String
Validity	m	m	인증서 유효기간
Subject	m	m	C(Country)는 printableString 그 외의 속성값은 utf8String
Subject Public Key Info	m	m	가입자 공개키에 대한 정보
Issuer Unique ID	x	x	-
Subject Unique ID	x	x	-

Extensions	m	m		아래참조
확장필드	Critical	선택여부		입력값
		생성	처리	
Authority Key Identifier	n	m	m	- 발급기관의 공개키 hash값 - 인증기관 인증서의 발급자 DN - 인증기관 인증서의 일련번호
Subject Key Identifier	n	m	m	- 가입자의 공개키 hash값
Key Usage	c	m	m	- 전자서명: Digital Signature, Non-Repudiation - 유선용 키 분배: KeyEncipherment - 무선용 키 분배: KeyAgreement
Certificate Policies	c	m	m	[1]Certificate Policy: Policy Identifier=CPS에 있는 정책 OID [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.signgate.com/cps.html [1,2]Policy Qualifier Info: Policy Qualifier Id=가입자 알림 Qualifier: Notice Text=이 인증서는 공동 인증서입니다
Policy Mappings	-	-	-	-
Subject Alternative Names	n	o	m	RFC822 Name=email
		m	m	Other Name = VID
Issuer Alternative Names	n	o	m	-
Basic Constraints	-	x	x	Subject Type=End Entity Path Length Constraint=None
Name Constraints	-	-	-	-
Policy Constraints	-	-	-	-
Extended Key Usage	n	o	o	-
CRL Distribution Points	n	m	m	[1]CRL Distribution Point Distribution Point Name: FullName: URL=ldap://ldap.signgate.com:389/ou=해당 dp,ou=crldp,ou=AccreditedCA,o=KICA,c=KR
Authority Information Access	n	m	m	http://ocsp.signgate.com:9020/OcspServer

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

7.2 인증서 유효성 확인 정보 형식

"정보인증"의 가입자 인증서를 효력정지 및 폐지하는 경우, 인증서 효력정지 및 폐지 목록(CRL)을 생성하여 게시하고 있으며 프로파일은 다음과 같습니다.

인증서 효력정지 및 폐지 목록 확장필드명	critical	선택여부		입력 값
		생성	처리	
Authority Key Identifier	n	m	m	- 발급기관의 공개키 hash값 - 인증기관 인증서의 발급자 DN - 인증기관 인증서의 일련번호
Issuer Alternative Name	n	o	m	-
CRL Number	n	m	m	CRL 일련번호
Issuing Distribution Point	c	o	m	해당 CRL의 DP 입력 FullName: URL=ldap://ldap.signgate.com:389/ ou=해당dp,ou=crldp,ou=AccreditedCA, o=KICA,c=KR

엔트리 확장필드명	critical	선택여부		입력 값
		생성	처리	
Reason Code	n	m	m	폐지 사유 입력
Hold Instruction Code	n	o	m	-
Invalidity Date	n	o	m	폐지일 입력
Certificate Issuer	c	o	m	-

c: critical n : non-critical – : not defined m: mandatory o: optional

7.3 인증서 유효성 확인 서비스 형식

인증서 유효성 확인(OCSP) 서비스용 인증서 프로파일 다음과 같습니다.

기본 필드 명	선택여부		입력 값
	생성	처리	
Version	m	m	V3
Serial Number	m	m	고유일련번호(up to 20Byte)
Signature	m	m	sha256 with RSA (256byte)
Issuer	m	m	C(Country)는 printableString 그 외의 속성값은 utf8String
Validity	m	m	인증서 유효기간
Subject	m	m	C(Country)는 printableString 그 외의 속성값은 utf8String
Subject Public Key Info	m	m	가입자 공개키에 대한 정보
Issuer Unique ID	x	x	-
Subject Unique ID	x	x	-
Extensions	m	m	아래참조

확장필드	Critical	선택여부		입력값
		생성	처리	
Authority Key Identifier	n	m	m	- 발급기관의 공개키 hash값 - 인증기관 인증서의 발급자 DN - 인증기관 인증서의 일련번호
Subject Key Identifier	n	m	m	- 가입자의 공개키 hash값
Key Usage	c	m	m	- 전자서명: Digital Signature, Non-Repudiation - 유선용 키 분배: KeyEncipherment - 무선용 키 분배: KeyAgreement
Certificate Policies	c	m	m	[1]Certificate Policy: Policy Identifier=CPS에 있는 정책 OID [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.signgate.com/cps.html [1,2]Policy Qualifier Info: Policy Qualifier Id=가입자 알림 Qualifier: Notice Text=이 인증서는 공동 인증서입니다
Policy Mappings	-	-	-	-
Subject Alternative Names	n	m	m	Other Name = VID
Issuer Alternative Names	n	o	m	-
Subject Directory Attributes	n	x	x	-
Basic Constraints	-	x	x	Subject Type=End Entity Path Length Constraint=None
Name Constraints	-	-	-	-
Policy Constraints	-	-	-	-
Extended Key Usage	c	m	m	-
CRL Distribution Points	n	m	m	[1]CRL Distribution Point Distribution Point Name: FullName: URL=ldap://ldap.signgate.com:389/ou=해당 dp,ou=crldp,ou=AccreditedCA,o=KICA,c=KR
Authority Information Access	n	o	m	http://ocsp.signgate.com:9020/OcspServer

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

8. 감사 및 평가

8.1 감사 및 평가 현황

가. "정보인증"은 운영기준 준수 사실의 인정을 받기 위해서는 매년 평가기관에 평가를 받습니다.

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

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

라. 운영기준 준수 사실 인정의 유효기간은 인정받은 날로부터 1년으로 합니다.

마. "정보인증"은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 동법 시행령에 따라 방송통신위원회로부터 본인확인기관으로 심사·지정받았으며, 본인확인기관 지위 유지를 위하여 필요시 사후관리를 위한 심사를 정기적 또는 비정기적으로 받을 수 있습니다.

8.2 평가자의 신원, 자격

평가자의 신원 및 자격은 전자서명법 시행령 제 5조(평가기관의 선정기준 및 절차 등)에 따라 선정됩니다.

8.3 평가 대상과 평가자의 관계

평가기관은 전자서명 법령상 과학기술정보통신부에 의해 '피 평가기관에 대한 공정성, 객관성, 신뢰성, 독립성의 확보'한 것으로 인정받은 기관으로 평가자와 평가 대상과는 독립성 등이 유지되고 있습니다.

8.4 평가 목적 및 내용

가. "정보인증"은 인정기관으로부터 운영기준의 준수 사실에 대해 인정받기 위해 평가기관으로부터 평가를 받습니다.

나. 평가내용은 전자서명인증사업자의 운영기준 준수 여부에 대하여 평가를 하며, 자세한 사항은 평가기관이 정한 세부평가 기준에 따릅니다.

8.5 부적합 사항에 대한 조치

"정보인증"은 전자서명인증업무 운영기준 준수사실에 대한 인정을 받을 수 있도록, 평가

결과 발생한 부적합 사항에 대해 조치합니다.

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 이용요금

9.1.1 인증서비스 이용요금

가. "정보인증"은 가입자와 이용자에게 인증서 발급 및 이용 등에 대해 이용요금을 부과할 수 있습니다. "정보인증"의 인증서 이용요금은 신규 발급과 갱신 발급을 대상으로 합니다. "정보인증"은 인증서의 발급대상, 등급, 용도 등에 따라 발급 수수료의 기준을 아래 표와 같이 정합니다.

(단위 : 원, 부가세 포함)

<table>
<tr><th colspan="3">구 분</th><th>요금</th></tr>
<tr><td rowspan="3">개인</td><td colspan="2">범용</td><td>4,400원</td></tr>
<tr><td rowspan="2">용도제한용</td><td>은행/신용카드/보험용</td><td rowspan="2">인증서 이용자 혹은 가입자와의 계약 관계에 따름</td></tr>
<tr><td>기타</td></tr>
<tr><td rowspan="2">법인, 단체,
개인사업자</td><td colspan="2">범용</td><td>110,000원</td></tr>
<tr><td colspan="2">용도제한용</td><td>인증서 이용자 혹은 가입자와의 계약 관계에 따름</td></tr>
<tr><td colspan="3">서버</td><td>550,000</td></tr>
</table>

나. "정보인증"은 정책에 따라 인증서 이용요금을 면제하거나 할인할 수 있으며, 가입자 및 이용자와의 계약 또는 협약에 따라 부과방법이나 납부 시기 등을 변경할 수 있습니다.

다. "정보인증"은 이용요금 정책을 변경할 경우 홈페이지(www.signgate.com)를 통해 이를 공지합니다.

라. "정보인증"은 가입 신청 시 이용요금을 청구하며, 가입자는 이용요금을 선납하여야 합니다. 다만, 예외적인 때에만 후납할 수 있습니다.

마. 인증서비스 이용요금 부과 방식은 "정보인증"의 정책에 따릅니다.

바. "정보인증"은 인증서와 관련한 인증서 유효성 확인 서비스(OCSP), 시점확인서비스(TSA), 본인확인서비스(UCPID) 등의 부가서비스를 제공할 수 있으며, 부가서비스 이용요금은 이용자 혹은 가입자와 개별 계약에 따릅니다.

9.1.2 환불정책

가. 가입자는 인증서비스 이용요금을 결제한 날부터 10일 이내에 가입취소 및 이용요금의 환불을 요구할 수 있습니다.

나. "정보인증"은 가입자가 정해진 기간 내에 인증서비스 가입취소 및 이용요금의 환불을 요구할 경우, "정보인증"이 정한 필요경비(송금수수료, 방문 설치 설치수수료, 우체국 등기 수수료)를 공제한 후 잔액을 지급합니다. 이때 가입자의 인증서는 자동 폐지합니다.

9.2 배상

9.2.1 배상책임

가. "정보인증"은 전자서명인증업무 수행과 관련하여 가입자 또는 인증서를 신뢰한 이용자에게 손해를 입힌 때에는 배상의 타당성이 인정된 가입자 또는 이용자만 그 손해를 배상합니다.

나. "정보인증"은 신뢰할 수 있는 암호화 모듈 및 보안 기술 규격을 적용하는 것을 원칙으로 합니다. 만약 신뢰할 수 없는 암호화 모듈 또는 기술 규격을 적용하는 경우, "정보인증"은 안전성을 확보하기 위한 충분한 기술적 검증 또는 조치를 취하며, 이에 대한 책임을 부담합니다.

9.2.2 배상책임 면책

"정보인증"은 "정보인증"이 발급한 인증서 및 인증업무와 관련하여 발생하는 배상책임 이외의 것에 대해서

는 책임을 지지 않습니다. 또한 불가항력적 사유로 발생한 손해, 이용자 또는 가입자가 관련 법령이나 본 준칙을 준수하지 아니하여 발생한 손해 등 "정보인증"의 고의 또는 과실 없이 발생한 손해에 대해서는 전자서명법 제20조(손해배상책임)에 따라 그 배상책임이 면제됩니다.

9.2.3 등록대행기관의 배상책임

등록대행기관은 "정보인증"으로부터 위탁받은 업무를 수행하면서 전자서명법, 전자서명법시행령, 전자서명법시행규칙, 준칙 및 "정보인증"과 체결한 계약을 위반하여 "정보인증", 가입자와 이용자에게 손해를 입히면 그 손해를 배상하여야 합니다.

9.2.4 가입자의 배상책임

가입자는 가입자의 고의 또는 과실로 전자서명법, 전자서명법시행령, 전자서명법시행규칙 및 본 준칙의 의무사항을 위반하거나, 인증서비스를 이용하면서 "정보인증" 및 기타 관련자(다른 가입자, 다른 이용자 등)에게 손해를 입히면 해당 손해를 배상하여야 합니다.

9.2.5 이용자의 배상책임

이용자는 이용자의 고의 또는 과실로 전자서명법, 전자서명법시행령, 전자서명법시행규칙 및 본 준칙의 의무사항을 위반하거나, 이용자가 인증서비스를 이용하면서 "정보인증" 및 기타 관련자(가입자, 다른 이용자 등)에게 손해를 입히면 해당 손해를 배상하여야 합니다.

9.3 영업비밀

"정보인증"은 "부정경쟁방지 및 영업비밀보호에 관한 법률"을 준수하고 있으며, 전자서명인증체계 관계자는 "정보인증"의 인증서비스 이용과정에서 취득한 "정보인증"의 영업비밀에 대해 누설하거나 이를 부정하게 사용한 경우 그 손해에 대해 배상하여야 합니다.

9.4 개인정보보호

가. "정보인증"은 인증서 발급과정에서 취득한 가입자 정보를 가입자의 동의나 법에 정한 경우를 제외하고는 유출할 수 없으며, 이러한 의무 위반 시 "정보인증"은 가입자에 대해 손해배상 책임을 집니다.

나. "정보인증"은 가입자의 개인정보를 보호하기 위하여, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「개인정보 보호법」 등 관계 법규를 준수하고 있습니다.

다. "정보인증"은 개인정보보호와 관련하여 별도의 '개인정보처리방침'을 정하여 운영하고 있으며, 자세한 사항은 홈페이지에서 확인할 수 있습니다.

- 개인정보처리방침 정보저장 위치
- https://www.signgate.com/policy/personalInfo/pyPersonalInfo.sg

9.5 지식재산권

다음 사항에 대한 지식재산권은 저작권법 등 관련 법률에 따라 "정보인증"에 귀속됩니다.

가. 인증시스템을 위해 개발된 소프트웨어 및 하드웨어

나. 준칙 및 서비스 이용 약관

9.6 보증

가. "정보인증"은 전자서명 관계법령 및 준칙의 규정을 준수하여 인증서가 발급되었다는 사실을 보증합니다.

나. "정보인증"은 인증서 내에 포함된 내용이 발급신청 당시 기준으로 "정보인증" 인증시스템에 등록된 사실임을 보증합니다.

9.7 보증 예외 사항

"정보인증"은 전자서명법, 전자서명법시행령, 전자서명법시행규칙 및 본 준칙에서 정한 사항 이외의 사항 즉, 가입자 신용 또는 가입자 관련 정보의 불변성 등을 보증하지 않습니다.

9.8 보험의 보상 범위

"정보인증"은 가입자 또는 인증서를 신뢰한 이용자에게 발생하는 손해를 담보하기 위하여 보험에 가입하고 있으며, 해당 보험계약에서 정한 배상 한도인 연간 20억, 건당 5억의 범위 내에서 가입자 또는 이용자의 정당한 손해를 배상합니다.

9.9 배상 한계

"정보인증"은 전자서명법 제20조(손해배상책임)에 따라 전자인증업무 수행과 관련하여 "정보인증"의 과실로 가입자 또는 이용자에게 손해를 입힌 경우에는 그 손해를 배상합니다. 다만, "정보인증"의 고의 또는 과실없음을 입증하면 그 배상책임이 면제 됩니다.

9.10 준칙의 효력

준칙이 개정되면 개정 전 내용은 개정 준칙의 효력 발생일에 그 효력이 종료됩니다. 제•개정된 준칙은 "정보인증"이 준칙 정보저장위치에 공고하는 날로부터 시행합니다.

9.11 통지 및 의사소통

"정보인증"은 "정보인증"의 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

"정보인증"은 준칙의 변경 이력을 관리하여야 합니다.

9.13 분쟁 해결

가. 전자서명인증업무와 관련하여 "정보인증"과 가입자 또는 이용자 간 분쟁이 발생한 경우 상호 협의하여 이를 원만히 해결하도록 노력해야 합니다.

나. 본 인증체계 관련자에게 전달되는 문서(전자문서 포함)가 법적 효력을 갖기 위해서는 아래의 요건을 만족해야 합니다.

- 인증서에 기초한 전자서명을 포함하며, 전자서명은 전자서명법 제2조 제2호상의 요건을 갖출 것
- 전자서명이 가입자가 전자서명생성정보를 지배·관리하는 상황에서 이루어질 것
- 전자서명에 사용된 인증서가 유효한 상태이며 정지 또는 폐지 상태가 아닐 것

다. 전자서명인증업무와 관련하여 정보 인증과 가입자 또는 이용자간 분쟁이 발생한 경우에는 전자서명법 제22조상의 전자문서·전자거래분쟁조정위원회에 조정을 신청하여 관련 절차에 따라 분쟁을 해결할 수 있습니다.

9.14 준거법 및 관할법원

가. 본 준칙은 대한민국의 법 및 관계 법령에 따라서 해석되고 적용됩니다.

나. "정보인증"과 가입자 또는 이용자와의 인증업무와 관련한 분쟁이 발생한 경우 분쟁의 해결을 위하여 "정보인증" 본사 소재지 또는 가입자 또는 이용자의 소재지를 관할하는 법원을 관할법원으로 합니다.

9.15 관련 법률 준수

"정보인증"은 전자서명법, 전자서명법시행령, 전자서명법시행규칙 및 개인정보 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 관련 법령을 준수하여야 합니다.

9.16 기타 규정

해당 사항 없습니다.