전자서명인증업무준칙

(V 20.0)

2021. 1.

한국정보인증

- 목 차 -

[전자서명인증업무준칙]

1. 소개

1.1 개요

1.1.1 준칙의 배경 및 목적

본 전자서명인증업무준칙(CPS:Certification Practice Statement)은 전자서명법, 전자서명법시행령 및 전자서명법시행규칙에 따라 한국정보인증주식회사(이하 "정보인증"이라 한다.)가 인증서의 발급·관리 및 인증시스템을 운영함에 있어 필요한 사항을 정하며, "정보인증"과 가입자 등 인증업무 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

당 준칙의 명칭은 한국정보인증 전자서명인증업무준칙 Ver 20.0입니다.

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)

과학기술정보통신부 장관은「정보통신망 이용촉진 및 정보보호 등에 관한 법률」52조에 따른 한국인터넷진흥원을 운영기준 준수 사실의 인정에 관한 업무를 수행하는 기관으로 지정할 수 있으며, 다음과 같은 업무를 수행합니다.

- 전자서명인증사업자가 전자서명법 제 8조(운영기준 준수 사실의 인정)에 따른 자격을 갖추었는지 인정 여부 결정
- 전자서명인증사업자에 운영기준 준수 사실을 인정하는 경우 증명서 발급

1.3.3 평가기관

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

1.3.4 전자서명인증사업자

전자서명인증사업자는 전자서명인증업무를 하는 자를 말합니다.

1.3.5 (운영기준의 준수 사실에 대해) 인정받은 전자서명인증사업자

전자서명인증사업자는 전자서명법 제 10조(평가기관)에 따른 평가기관으로부터 운영기준의 준수 여부에 대한 평가를 받아 인정기관으로부터 운영기준의 준수 사실에 대한 인정을 받을 수 있습니다.

1.3.6 정보인증

1.3.6.1 역할

"정보인증"은 전자서명인증사업자로서 가입자에게 다음과 같은 인증서비스를 제공합니다.

- 인증서비스 관련 신청서 접수 및 처리
- 인증서비스 제공과 관련한 가입자 신원확인 업무
- 인증서 발급(신규, 재발급, 갱신 등)
- 인증서 효력 정지, 효력회복 및 폐지
- 인증서 관련 정보 공고
- 시점확인서비스
- 기타 인증서비스와 관련된 업무

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.

- 인증업무 휴지·정지 또는 폐지
- 전자서명인증업무준칙
- 인증서에 대한 폐지 목록
- 기타 인증업무 수행 관련 정보 등

나. 전자서명생성정보의 보호

"정보인증"은 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 당해 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 확인하여야 하며, 당해 신청내용의 무결성을 확인하여야 합니다.

마. 가입자 개인정보보호

"정보인증"은 인증서비스 중 취득한 개인정보를 보호하여야 하며, 수집한 개인정보를 업무 목적으로만 사용하여야 합니다.

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, 효력 정지, 효력회복 또는 폐지 등의 신청을 접수 등록하는 가입자 등록 업무를 위탁받은 외부기관을 의미합니다.

나. 등록대행기관은 가입자에 대한 신원확인, 인증서 발급, 효력 정지, 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, 효력 정지, 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 확인하여야 하며, 당해 신청내용의 무결성을 확인하여야 합니다.

다. 전자서명인증업무준칙 및 계약 이행

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

라. 배상책임

등록대행기관이 전자서명법령 및 전자서명인증업무준칙 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 전자서명인증사업자로부터 전자서명인증을 받은 자를 말합니다.

1.3.8.2 책임과 의무사항

가. 가입자는 자신의 사용 목적에 맞는 인증서를 선택해서 신청해야 하며, 정확한 정보를 "정보인증"에 제공하여야 합니다. 인증서 내의 정보를 신뢰하거나 해당 인증서를 이용하여 전자서명을 검증하는 이용자에 대하여 가입자의 잘못된 정보로 인해 발생하는 책임은 모두 가입자에게 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. 하지만 대리인이 가입자를 대신하여 전자서명을 할 수는 없습니다.

1.3.10 이용자

1.3.10.1 정의

전자서명인증사업자가 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 방

법으로 "정보인증"과 가입자에게 손해를 입히면 "정보인증"과 가입자에게 그 손해를 배상해야 합니다.

1.4 인증서 종류

1.4.1 인증서의 발급대상

가. "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. 다만, "정보인증"이 제공하는 서비스에 대하여는 "정보인증"이 발급한 인증서는 용도와 무관하게 사용하실 수 있습니다.

<table>
<tr><th colspan="3">구 분</th><th>용 도</th></tr>
<tr><td rowspan="3">개인</td><td colspan="2">범용</td><td>인증서를 필요로 하는 일반 전자거래의 모든 분야에서 사용 가능</td></tr>
<tr><td rowspan="2">용도제한용</td><td>은행용</td><td>❿ 은행 업무
❿ 정부 민원 업무(단, 전자입찰 등 제외)
❿ 전자서명인증사업자 간 합의된 업무</td></tr>
<tr><td>기 타</td><td>개별 계약에 따름</td></tr>
<tr><td>법인, 단</td><td colspan="2">범용</td><td>인증서를 필요로 하는 일반 전자거래의 모든 분야에</td></tr>
</table>

체, 개인사업자		서 사용 가능
	용도제한용	개별 계약에 따름
서 버		인터넷상에서 서비스를 제공하는 서버를 인증

1.4.3 인증서 유효기간

인증서의 유효기간은 원칙적으로 1년으로 합니다. 인증서의 유효기간은 "정보인증"의 정책에 따라 변경될 수 있습니다.

1.4.4 인증서가 사용될 수 있는 이용 분야 또는 해당 인증서의 사용이 금지되는 이용 분야

인증서는 인터넷 뱅킹, 온라인증권거래, 쇼핑 등 전자거래 전반에서 신원확인 및 전자서명 수단으로 이용 중이며, 이용 분야도 금융 분야에서 비금융분야로 확대되었습니다.

가. 인증서 이용 분야

* 금융 분야

- 인터넷 뱅킹, 사이버 증권, 사이버보험 등

* 전자상거래분야

- 전자계약, 전자무역, 인터넷쇼핑 등

* 공공분야

- 전자조달, 입찰, 전자민원서비스, 청약

* 기타분야

- 전자투표, 전자세금계산서, 전자의료, 수강 신청 등

나. 인증서 사용이 금지되는 이용 분야

"정보인증"은 인증서 사용이 제한된 용도제한용 인증서를 발급할 수 있으며, 제한된 용도 외에는 인증서 사용이 금지됩니다.

1.5 준칙의 관리

1.5.1 준칙 관리부서 및 연락처

- 관리부서 : "정보인증" 인증영업팀
- 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. 전자서명인증업무준칙에 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 각호의 사항이 포함된 전자서명인증업무준칙을 작성하여 내부결재 후 인터넷 홈페이지 등에 공지함을 원칙으로 합니다. 전자서명인증업무준칙 중 다음 각목의 내용을 변경한 때도 또한 같습니다.

가. 인증서비스의 종류

나. 인증서비스의 요금, 이용범위 및 유효기간 등 이용조건

다. 인증업무의 수행방법 및 절차

라. 그 밖에 인증업무의 수행에 필요한 사항

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 말한다.

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

1) 서명자의 신원

2) 서명자가 해당 전자문서에 서명하였다는 사실

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

라. ″전자서명검증정보″란 전자서명을 검증하기 위하여 이용하는 전자적 정보를 말한다.

마. ″인정사업자″란 전자서명법 제8조에 따라 운영기준 준수 사실의 인정을 받은 전자서명인증사업자를 말한다.

바. "전자서명인증시스템"이란 인정사업자가 전자서명인증서비스를 제공하기 위해 운영하는 다음 각호의 시스템을 말한다.

1) 가입자의 등록정보를 관리하기 위한 시스템

2) 전자서명생성정보를 생성·관리하기 위한 시스템

3) 인증서를 생성·발급·관리하기 위한 시스템

4) 기타 전자서명인증업무의 수행과 관련된 시스템 및 설비

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

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

자. "전자서명인증업무"란 전자서명인증, 전자서명인증 관련 기록의 관리 등 전자서명인증서비스를 제공하는 업무를 말한다.

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 인증서, 인증서 효력 정지 및 폐지 목록 등 전자서명인증업무와 관련된 정보를 인증관리체계에 의하여 이중화 구성(Active-Active)으로 안정적으로 직접 운영하고 있으며, 누구든지 그 사실을 항상 확인할 수 있도록 공고합니다.

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

2.2 공고방법

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

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

- 공고 위치 : ldap.signgate.com:389
- 공고방법 : 누구든지 확인 가능한 인터넷망

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 인증서 발급에 있어 가입자에게 다음과 같은 법적 이름을 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

다. "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.

라. DN이 중복되는 경우에 가입자에게 새로운 DN을 요청하며, 가입자는 "정보인증"의 인증서비스에 가입하려면 이에 응해야 합니다. "정보인증"은 다양한 이름을 수용하기 위해 특별한 해석규칙을 적용하지 않습니다.

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

3.2 인증서 신규 발급 시 신원확인

"정보인증" 또는 등록대행기관은 신원확인증표 등을 통해 가입 신청자의 신원을 확인합니다. 이 경우 "정보인증" 또는 등록대행기관은 원칙적으로 직접 대면하여 신원을 확인하나, 「금융실명거래 및 비밀보장에 관한 법률」에 의거 금융기관에서 실지명의가 확인된 전자금융거래 가입자가 인증서를 발급받으려는 경우에는 정보통신망을 통하여 신원을 확인할 수 있습니다.

3.2.1 신원확인 방법

3.2.1.1 대면 신원확인 방법

인증서 신청 주체는 개인 또는 법인/단체/개인사업자이며, 이 신청 주체가 직접 또는 대리인이 "정보인증" 또는 등록대행기관에 다음 아래의 인증서 발급 신청서류를 제출하여 신청하여야 합니다.

가. 개인

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

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 시청서

- 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)

3.2.1.2 온라인 신원확인 방법

"금융실명거래 및 비밀보장에 관한 법률" 제2조 제1호 각 목에 따른 금융기관에서 실지 명의가 확인된 전자금융거래 가입자를 대상으로 그의 사전동의를 받아 정보통신망을 통하여 신원을 확인하여 발급될 수 있습니다.

<사전동의 방법>

대상 고객	개인 또는 법인
대상 업무	인증서 발급 및 재발급
사전동의 신청 및 변경방법	온라인 신원확인 (단, 미동의에서 동의로 변경은 대면확인 원칙)

이 경우 아래의 사항을 확인합니다.

- 전자금융거래 가입자의 계정(ID)과 그 비밀번호 또는 계좌번호와 그 비밀번호

- 전자금융거래 가입자의 주민등록번호

- 금융기관이 전자금융거래를 위하여 가입자에게 제공한 일회용 비밀번호(보안카드의 비밀번호를 포함한다.) 또는 가입자 본인만이 알 수 있는 두 가지 이상의 정보

- 위에서 규정된 사항 외에 전자금융거래 가입자의 신용카드 정보 등 신원을 확인할 수 있는 정보. 다만, 전자금융거래 가입자가 해외체류자, 법인, 단체, 외국인

또는 점자 보안카드 사용자(해당 정보 확인에 동의한 점자 보안카드 사용자는 제외한다.)인 경우는 제외함

3.2.2 신원확인 절차

가. 개인

"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

"정보인증" 또는 등록대행기관은 법인(단체)에 대한 신원확인을 위해 제출된 인증서비스 신청서와 법인 및 단체의 신원확인증표 및 추가서류의 법인명, 대표자 성명, 사업자등록번호 등을 통해 신원확인을 합니다.

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

다. "정보인증" 또는 등록대행기관은 다음 각호에 의거 가입자가 제출한 신원확인증표의 진정성을 확인합니다.

1) 주민등록증의 경우

- 행정안전부 ARS 1382에 전화하여 확인

- 정부24 홈페이지(www.gov.go.kr)에 접속하여 '주민등록증 진위확인' 선택, 주민

등록증에 수록된 성명, 주민등록번호, 발급 일자(8자리)를 입력하여 확인

2) 운전면허증의 경우

- 경찰청 교통 민원 24시(www.efine.go.kr)에 접속하여 '운전면허증 진위여부조회' 선택, 운전면허증에 수록된 생년월일, 성명, 면허번호, 식별번호를 입력하여 확인

3) 사업자등록증의 경우

- 국세청 홈페이지(www.nts.go.kr)에 접속하여 '조회/발급'선택, 사업자등록증에 명시된 사업자등록번호를 입력한 후 확인

4) 등기사항전부증명서의 경우

- 대법원인터넷등기소 홈페이지(www.iros.go.kr)에 접속하여 '법인등기 열람서비스' 선택, 등기사항전부증명서에 명시된 등기번호를 입력하여 확인

3.2.3 가입자의 전자서명생성정보 소유증명 방법

"정보인증"은 가입자 소프트웨어를 통해 가입 신청자가 제출한 전자서명검증정보의 유일성과 정보의 합치 여부의 확인을 통하여 전자서명생성정보의 소유자를 확인합니다.

3.2.4 가입자가 인증서 발급 신청서에 기재한 사항 중 전자서명인증사업자가 해당 내용의 정확성을 확인하는 사람

"정보인증" 또는 등록대행기관은 가입자가 인증서비스 신청서에 기재한 사항과 신원확인증표 및 제출된 추가서류 등을 통해 신청내용의 정확성을 확인합니다.

3.3 인증서 갱신 발급, 재발급 및 변경 시, 신원확인

3.3.1 갱신 발급

3.3.1.1 신원확인 방법 및 절차

"정보인증"은 보유한 인증서를 이용하여 가입자의 전자서명으로 가입자의 신원을 확인합니다. "정보인증"의 홈페이지(www.signgate.com)에서 온라인으로 신청하며, 새로 생성한 전자서명검증정보는 인증서 갱신 신청서에 포함하여 전송합니다.

3.3.1.2 가입자의 전자서명생성정보 소유증명 방법

"정보인증"은 가입자 소프트웨어를 통해 가입 신청자가 제출한 전자서명검증정보의 유일성과 정보의 합치 여부의 확인을 통하여 전자서명생성정보의 소유자를 확인합니다.

3.3.2 재발급

3.3.2.1 신원확인 방법 및 절차

인증서의 재발급은 〃**3.2.1 신원확인 방법”과 ”3.2.2 신원확인 절차“** 에 따라 신원확인을 합니다.

3.3.2.2 가입자의 전자서명생성정보 소유증명 방법

"정보인증"은 가입자 소프트웨어를 통해 가입 신청자가 제출한 전자서명검증정보의 유일성과 정보의 합치 여부의 확인을 통하여 전자서명생성정보의 소유자를 확인합니다.

3.3.3 가입자 등록정보 변경

3.3.3.1 신원확인 방법과 절차

"정보인증"은 가입자가 등록정보를 변경하고자 하는 때에는 보유한 인증서 또는 〃**3.2.1 신원확인 방법”과 ”3.2.2 신원확인 절차“** 에 따라 신원확인을 합니다.

3.3.3.2 가입자의 전자서명생성정보 소유증명 방법

"정보인증"은 가입자 소프트웨어를 통해 가입 신청자가 제출한 전자서명검증정보의 유일성과 정보의 합치 여부의 확인을 통하여 전자서명생성정보의 소유자를 확인합니다.

3.4 인증서 효력 정지·효력회복·폐지 시, 신원확인

3.4.1 효력 정지 신원확인 방법 및 절차

가. "정보인증"을 방문하여 정지하는 경우

1) 인증서 효력 정지 신청서 제출

가입자는 "정보인증"이 제공하는 ″인증서효력 정지신청서″에 필요한 사항을 기재한 후 "정보인증"을 방문하여 제출합니다.

2) 신원확인

"정보인증"은 ″**3.2.1 신원확인 방법″과 ″3.2.2 신원확인 절차″** 에 따라 신원확인을 합니다.

나. 가입자가 정보통신망을 이용하여 직접 정지하는 경우

가입자는 인증서의 효력을 정지하고자 하면 당사 홈페이지(www.signgate.com)에 접속하여 ″인증서효력 정지″를 선택한 후, 안내에 따라 인증서 효력 정지 절차를 진행합니다. 이때 신원확인은 보유한 인증서의 제출을 통하여 확인합니다.

3.4.2 효력회복 신원확인 방법 및 절차

가. 인증서 효력회복 신청서 제출

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

나. 신원확인

"정보인증"은 ″**3.2.1 신원확인 방법″과 ″3.2.2 신원확인 절차″** 에 따라 신원확인을 합니다.

3.4.3 폐지 신원확인 방법 및 절차

가. "정보인증"을 방문하여 폐지하는 경우

1) 인증서 폐지신청서 제출

가입자는 "정보인증"이 제공하는 ″인증서 폐지신청서″에 필요한 사항을 작성한 후 "정보인증"을 방문하여 제출합니다.

2) 신원확인

"정보인증"은 ″**3.2.1 신원확인 방법″과 ″3.2.2 신원확인 절차″** 에 따라 신원확인을 합니다.

나. 가입자가 정보통신망을 이용하여 직접 폐지하는 방법

가입자는 인증서를 폐지하고자 하면 당사 홈페이지(www.signgate.com)에 접속하여 ″인증서 폐지하기″를 선택한 후, 안내에 따라 인증서의 폐지 절차를 진행합니

다. 이때 신원확인은 보유한 인증서의 제출을 통하여 확인합니다.

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"의 홈페이지를 방문하여 인증서비스 신청서를 작성한 후 등록대행기관에 방문하여 신청서와 신원확인증표, 추가서류를 제출하여 신원확인을 받아야 합니다.

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

4.2 인증서 발급 신청 처리

4.2.1 인증서 발급요청

가. 가입 신청자는 "정보인증"이 부여한 가입자등록번호(참조번호/인가 코드)를 사용하여 "정보인증"에 인증서의 발급을 요청합니다. 이때 "정보인증"은 정상적으로 신청이 완료된 자에게 인증서를 발급합니다. 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

다. 가입 신청자는 가입자등록번호(참조번호/인가 코드)를 부여받은 날로부터 30일 이내에 인증서를 발급받아야 합니다.

4.3 인증서 발급 절차 및 보호조치

가. "정보인증"은 가입자등록번호를 이용하여 가입자 정보 및 전자문서의 위•변조 여부를 확인합니다.

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

다. "정보인증"은 가입자 소프트웨어를 통해 가입 신청자가 제출한 전자서명검증정보의 유일성과 정보의 합치 여부의 확인을 통하여 전자서명생성정보의 소유자를 확인합니다.

라. "정보인증"에서 발급하는 인증서에는 다음의 사항이 포함됩니다.

① 가입자의 이름

② 가입자의 전자서명검증정보

③ 가입자와 "정보인증"이 이용하는 전자서명 방식

④ 인증서의 일련번호

⑤ 인증서의 유효기간

⑥ "정보인증"의 명칭 등 전자서명인증사업자임을 확인할 수 있는 정보

⑦ 인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항

⑧ 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격 등의 표시를 요청한 경우 이에 관한 사항

⑨ 인증서임을 나타내는 표시

마. "정보인증"의 등록대행기관(RA)은 인증서의 발급에 필요하여 입력한 가입자 정보를 등록대행기관(RA)의 인증서로 전자서명하여 안전한 암호알고리즘을 이용하여 암호화한 다음 정보통신망을 이용하여 "정보인증"에 안전하게 전달하여 기밀성을 보장합니다.

바. "정보인증"이 발급하는 인증서의 가입자 DN을 구성하는 정보는 사용자 이름, RA 정보, "정보인증"의 정보로 구성합니다. 다만, 동명이인(同名異人)이 존재할 때는 이름 뒤에 숫자를 증가시켜 유일성을 보장합니다.

사. "정보인증"은 등록대행기관 등과 정보통신망을 이용하여 가입자 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, 이를 안전하게 저장•관리해야 합니다.

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

인증서 갱신은 인증서 유효기간이 만료 60일 전부터 유효기간 만료일까지 전자서명생성정보와 유효기간이 갱신된 동일한 종류의 새로운 인증서를 발급하는 것을 말합니다.
다만, 갱신신청 기간은 "정보인증"이 가입자의 편의 등을 고려하여 신청 기간을 조정할 수 있습니다.

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. "정보인증"은 인증서를 보유한 고객이 인증서의 유효기간을 연장하고자 갱신을 신청할 경우 보유한 인증서를 이용하여 가입자의 신원을 확인합니다. "정보인증"의 홈페이지(www.signgate.com)에서 온라인으로 신청하며, 새로 생성한 전자서명검증정보는 인증서 갱신 신청서에 포함하여 전송합니다.

나. 인증서의 갱신은 그 유효기간이 만료되기 60일 전부터 전자서명생성정보와 유효기간이 갱신된 동일한 종류의 새로운 인증서를 발급하며, 만료 기간 이후로부터 1년간(다년간 인증서의 경우는 2~3년간) 유효합니다. 인증서 갱신 후 가입자에게 이를 확인할 수 있도록 표시하여 줍니다.

다. 가입자가 인증서 갱신을 신청할 때 신청한 전자문서의 위•변조 여부 등은 가입자의 전자서명 검증을 통하여 확인합니다.

라. 가입자는 가입자 소프트웨어를 이용하여 국제표준인 인증서관리프로토콜(CMP)을 이용하여 전자서명을 수행하여 인증서의 갱신을 수행합니다.

마. 갱신 발급의 경우 가입자의 DN은 인증서가 유효하게 유지되는 동안에는 변경되지 않고 동일하게 사용합니다.

4.6.4 가입자가 갱신된 인증서를 받는 방법

가입자가 온라인으로 인증서 갱신신청을 하면 "정보인증"은 갱신 여부를 검토 후 갱신이 허용되면 새로운 유효기간의 인증서를 새로 발급함으로써 갱신 발급된 인증서를 받습니다.

4.7 인증서 재발급

4.7.1 재발급 요건

"정보인증"은 다음과 같은 경우 당해 인증서를 잔여 유효기간 내에 다시 사용할

수 있도록 재발급합니다. 이때 전자서명생성정보는 새로 생성하고 DN은 동일한 것을 사용합니다.

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

나. 가입자의 성명 또는 상호가 변경되어 재발급을 신청한 경우

다. "정보인증"이 자신의 전자서명생성정보에 대한 분실·훼손 또는 도난·유출되었음을 인지한 경우

라. "정보인증"이 자신의 전자서명 알고리즘에 대한 취약성을 인지한 경우

4.7.2 재발급 신청 주체

개인이 인증서를 재발급받고자 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 "정보인증"의 홈페이지를 방문하여 인증서비스 신청서를 작성한 후 등록대행기관에 방문하여 신청서와 신원확인증표, 추가서류를 제출하여 신원확인을 받아야 합니다.

나. "정보인증"의 등록대행기관은 신청서와 신원확인증표를 비교하여, 개인의 경우에는 성명 및 주민등록번호를, 법인(단체)의 경우에는 법인(단체)명 및 사업자등록

번호를 확인합니다.

4.7.4 재발급된 인증서를 받는 방법

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

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 "정보인증"의 홈페이지를 방문하여 인증서비스 신청서를 작성한 후 등록대행기관에 방문하여 신청서와 신원확인증표, 추가서류를 제출하여 신원확인

을 받아야 합니다.

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

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

가입자는 "정보인증" 홈페이지를 통하여 가입자 등록정보 변경 신청을 할 수 있으며, 이때 신원확인은 보유한 인증서의 제출을 통하여 확인합니다.

4.8.3 가입자 등록정보가 변경된 인증서를 받는 방법

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

4.9 인증서 효력 정지•효력회복•폐지

4.9.1 인증서 효력 정지

4.9.1.1 인증서 효력 정지 요건

인증서 효력 정지 사유는 다음과 같습니다.

가. 가입자 또는 그 대리인이 효력 정지를 신청한 경우

나. 가입자가 전자서명인증업무준칙을 위반한 경우

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

4.9.1.2 인증서 효력 정지 주체

개인이 인증서를 효력 정지할 때에는 본인이 직접 신청하여야 하며, 법인의 경우에는 해당 법인의 임원 또는 직원이 법인을 대리하여 효력 정지할 수 있습니다.

4.9.1.3 인증서 효력 정지 방법 및 절차

가. "정보인증"을 방문하여 정지하는 방법

1) 가입자는 "정보인증"의 홈페이지를 방문하여 효력 정지 신청서를 작성한 후 등록대행기관에 방문하여 신청서와 신원확인증표, 추가서류를 제출하여 신원확인을 받아야 합니다.

2) "정보인증"의 등록대행기관은 신청서와 신원확인증표를 비교하여, 개인의 경우에는 성명 및 주민등록번호를, 법인(단체)의 경우에는 법인(단체)명 및 사업자등록번호를 확인합니다.

나. 가입자가 정보통신망을 이용하여 직접 정지하는 방법

가입자는 인증서의 효력을 정지하고자 할 때 당사 홈페이지(www.signgate.com)에 접속하여 "인증서 효력 정지"를 선택한 후, 안내에 따라 인증서 효력 정지 절차를 진행합니다. 이때 신원확인은 보유한 인증서의 제출을 통하여 확인합니다.

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 당해 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 "정보인증"의 홈페이지를 방문하여 효력회복신청서를 작성한 후 등록대행기관에 방문하여 신청서와 신원확인증표, 추가서류를 제출하여 신원확인을 받아야 합니다.

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

4.9.2.4 효력회복까지 처리되는 소요 시간

"정보인증"은 가입자가 인증서의 효력을 회복시키는 경우에 유효기간 및 종류에 상관없이 신속하게 조치합니다.

4.9.3 인증서 폐지

4.9.3.1 인증서 폐지 요건

가. "정보인증"은 다음 사유 발생 시 당해 인증서를 폐지합니다. 제3항 내지 제7항의 사유가 발생한 때에는 가입자 또는 그 대리인의 신청 여부와 관계없이 직권으로 폐지할 수 있습니다.

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 전자서명인증업무준칙을 위반한 경우

6) 가입자가 인증서 효력회복 신청기한 내에 효력회복을 신청하지 아니한 경우

7) 가입자의 신원확인이 적법하게 이루어지지 않았음을 "정보인증"이 인지한 경우

나. 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출 등의 긴급한 사유로 인증서의 폐지를 요청하는 때에는 사전에 등록된 2개 이상의 개인정보를 확인하는 등의 신뢰할 방법을 통하여 당해 가입자의 본인 여부를 확인하고 해당 신청서를 폐지합니다.

다. "정보인증"은 가입자로부터 "정보인증"의 전자서명생성정보에 대한 취약성을 통보받거나, 기타 사유로 인하여 "정보인증"의 전자서명생성정보가 분실, 훼손, 도난, 유출되었음을 인지한 경우 또는 전자서명 정보의 취약성 및 알고리즘의 취약성을 인지한 경우, 당해 가입자의 인증서를 폐지합니다.

라. 폐지 사유

발급대상	폐지신청 사유	폐지신청 시기	폐지 신청자	신청 시 첨부서류
개 인	사망, 실종, 파산, 한정치산, 금치산	사망, 실종, 파산, 한정치산, 금치산 선고 즉시	법 정 대리인	사망, 실종, 파산, 한정치산, 금치산 입증서류 법정대리인 증명서류
법인/ 단체	파산, 청산, 해산, 사업자등록 취	법인/단체 : 파산, 청산, 해산결의 즉시 개인사업자 : 사업자등	대표자	파산, 청산, 해산 결의서류 (법인의 경우)

서 버	소 사업자등록취소 서버운영 중지 서버폐기	록 취소 전 1. 사업자등록증 반납 전 2. 서버운영 중지 전 3. 서버폐기 전		

※ "정보인증"은 위의 폐지신청 사유를 인지한 경우, 가입자 또는 그 대리인의 신청 여부와 관계없이 직권으로 폐지할 수 있습니다.

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.

4.9.3.3 인증서 폐지 방법 및 절차

가. "정보인증"을 방문하여 폐지하는 방법

1) 가입자는 "정보인증"의 홈페이지를 방문하여 폐지신청서를 작성한 후 정보인증 또는 등록대행기관을 방문하여 신청서와 신원확인증표, 추가서류를 제출하여

신원확인을 받아야 합니다.

2) "정보인증"과 등록대행기관은 신청서와 신원확인증표를 비교하여, 개인의 경우에는 성명 및 주민등록번호를, 법인(단체)의 경우에는 법인(단체)명 및 사업자등록번호를 확인합니다.

나. 가입자가 정보통신망을 이용하여 직접 폐지하는 방법

가입자는 인증서를 폐지하고자 할 때 당사 홈페이지(www.signgate.com)에 접속하여 "인증서 폐지하기"를 선택한 후, 안내에 따라 인증서의 폐지 절차를 진행합니다.

4.9.4 정보통신망을 통해 전송되는 가입자 정보의 전송방법

"정보인증"은 정보통신망을 이용하여 가입자 정보를 송/수신하는 경우, 전자서명 및 암호화를 통해 정보의 기밀성 및 무결성을 확보합니다.

4.9.5 정보통신망을 통해 전송되는 가입자 정보의 기밀성, 무결성 등의 확보를 위한 정보보안 방법

"정보인증"은 정보통신망을 이용하여 가입자 정보를 송/수신하는 경우, 전자서명 및 암호화를 통해 정보의 기밀성 및 무결성을 확보합니다.

4.9.6 인증서 효력 정지 및 폐지 목록의 발행주기

"정보인증"은 인증서 효력 정지 및 폐지 목록을 적어도 매일 1회 갱신합니다.

4.9.7 인증서 효력 정지 및 폐지 목록 발행 시점부터 해당 인증서 효력 정지 및 폐지 목록을 공고하는 데까지 소요 시간

가. "정보인증"은 효력 정지, 효력회복 및 폐지 시 "정보인증" 홈페이지 인증서 관리페이지를 통해 신청하는 경우 실시간으로 처리합니다.
나. 가입자가 등록대행기관을 방문하여 신청한 때에는 신원확인 한 후 등록업무 담당자가 "정보인증"에 전달하는 즉시 처리합니다. 이때 가입자가 서류를 제출한 후부터 1일 정도 소요될 수 있습니다.

4.9.8 인증서 효력 정지 상태 유지 가능 기간

가입자는 인증서의 효력이 정지된 날로부터 6개월 이내에 그 회복을 신청하여야 합니다. 이 기간 내에 신청하지 않으면 당해 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.

4.11.2 인증서비스 가입 철회 시 인증서 폐지와 개인정보 파기

가입자가 서비스 가입 철회 시 인증서 폐지와 가입자의 개인정보는 "정보인증"의 개인정보처리방침에 따라 파기합니다.

4.12 기타 부가서비스

4.12.1 시점확인서비스(TSA)

"정보인증"은 서비스제공기관과의 계약으로 시점확인서비스를 제공할 수 있습니다. 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 핵심인증시스템을 보호하기 위하여 핵심인증시스템별로 분리된 별도의 통제구역 내에 설치하여 운영합니다.

가. 가입자 등록정보 관리 기능을 제공하는 설비, 전자서명생성정보 관리, 인증서 생성·발급 기능을 제공하는 설비는 동일 운영실에 설치할 수 있으나 다른 설비와는 별도 운영실로 분리합니다.

나. 인증서 공고기능을 제공하는 설비는 다른 설비와는 별도 운영실로 분리합니다.

다. 인증서 상태확인 기능을 제공하는 설비, 시점확인 기능을 제공하는 설비는 동일 운영실에 설치할 수 있으나 다른 설비와는 별도 운영실로 분리합니다.

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 모니터링 시스템과 침입 감지 시스템 등 감시통제시스템을 설치, 운영합니다.

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

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

5.1.1.4 물리적 잠금장치에 관한 사항

가. "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 인증시스템을 안전하게 보호하기 위하여 바닥으로부터 떨어져 설치합니다.

5.1.4 화재 예방

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

나. "정보인증"은 핵심인증시스템실 등에 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 효력 정지 및 폐지 목록 등을 물리적으로 격리된 원격지에 백업하여 당해 인증서를 신청한 날로부터 5년간 보관합니다.

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

5.1.8 항온/항습, 통풍설비에 관한 사항

가. "정보인증"은 전자서명인증시스템의 안정적인 운영을 위한 온도 및 습도를 일정하게 유지하기 위해 항온 항습 장치를 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 '정보자산관

리지침’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 ‘인증센터 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 생성업무는 3인 이상이 공동으로 수행합니다.

나. 가입자의 전자서명생성정보를 생성하는 경우, 2인 이상의 권한 있는 직원이 공동으로 이를 수행합니다.

다. 기타의 전자서명인증업무는 2인 이상이 공동으로 수행합니다.

라. 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 전자서명인증업무준칙에 인가되지 않는 행위를 한 경우에는 내부규정인 '상벌지침' 에 따라 해당 직원을 징계합니다.

5.4 감사기록

5.4.1 감사기록의 유형 및 보존 기간

가. "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 전자서명정보를 생성·접근·파기한 내역

③ 인증서를 생성·발급·갱신·효력 정지 또는 폐지한 내역

④ 가입자인증서 등을 등록 및 관리한 사실

⑤ 핵심인증시스템의 시작과 종료 사실

⑥ 로그인(Login) 및 로그오프(Logoff) 사실

⑦ 기타 핵심인증시스템 관리자의 주요 활동 사실

5.4.2 감사기록 검토 등 보호조치

가. 감사기록 검토 및 보호

관리책임자는 사건 발생 시 감사기록을 세밀히 검토하고 보존합니다. 각 시스템의 감사기록은 관리책임자에 의해 총괄 관리되며 시스템의 각 업무관리자는 당해 업무에 대한 감사기록만 열람할 수 있습니다.

5.4.3 감사기록 백업주기 및 절차

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

나. 백업과 관련한 상세한 절차는 내부지침 '인증센터 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 인증업무

나. "정보인증" 핵심인증시스템 등의 운영 업무

5.5.2 기록의 보존 기간

"정보인증"은 5.5.1의 보존 대상 기록을 인증서 유효기간 만료일로부터 5년간 보존합니다.

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 '인증센터 운영매뉴얼'에 따라 실시합니다.

5.6 전자서명인증사업자의 전자서명생성정보 갱신

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

나. "정보인증"은 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되는 안전한 키 생성시스템에서 전자서명생성정보를 생성합니다.

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

5.7 장애 및 재해 복구

5.7.1 인증업무 장애 및 재해 유형별 처리 및 복구 절차

"정보인증"은 전자서명인증업무와 관련하여 발생하는 장애 또는 재해에 대해 다음과 같이 유형별로 나누어 내부지침 '인증센터 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 전자서명인증서비스를 제공합니다.

5.8 업무 휴지, 폐지, 종료

5.8.1 전자서명인증업무 휴지

가. 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 게시하여야 합니다.

나. 통보하거나 게시하는 내용에는 요금의 반환, 가입자의 개인정보 폐기 등 가입자 보호조치가 포함되어야 합니다.

5.8.2 전자서명인증업무 폐지 및 종료

가. 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 게시하여야 합니다.

나. 통보하거나 게시하는 내용에는 요금의 반환, 가입자의 개인정보 폐기 등 가입자 보호조치가 포함되어야 합니다.

6. 기술적 보호조치

6.1 전자서명생성정보 보호

6.1.1 전자서명생성정보 생성

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

나. "정보인증"은 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되는 안전한 키 생성시스템에서 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 및 KCDSA 경우 : 2,048bit 이상

나. HAS-160 및 SHA-1 경우 : 160bit 이상

다. ECDSA 경우 : 163bit 이상

라. SHA-256 경우 : 256bit

6.2 전자서명생성정보 보호조치

6.2.1 전자서명생성정보의 저장 시 보호조치

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

6.2.2 전자서명생성정보의 이용 시 보호조치

"정보인증"의 전자서명생성정보 활성화 작업은 다자인증 통제(최소 2명 이상) 하에서 활성화합니다.

6.2.3 전자서명생성정보의 백업 보관 시 보호조치

가. "정보인증"은 백업된 전자서명생성정보 중 1부를 전자서명인증업무 수행 시설

과는 별도의 원격지 저장설비에 안전하게 보관합니다.

나. "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 "정보인증"의 인증서 유효기간이 만료되거나 전자서명생성정보가 훼손, 유출되었을 때 해당 전자서명생성정보 저장매체를 물리적으로 완전히 파기하거나, 전자서명생성정보를 삭제합니다.

나. "정보인증"은 관리책임자와 보안관리자의 입회하에 백업된 전자서명생성정보와 그 원본을 안전하게 파기합니다.

6.3 전자서명생정정보 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 관리합니다

6.4 데이터 보호조치

"정보인증"은 전자서명인증시스템 데이터 보호조치에 관한 사항을 내부지침인 '데

이터베이스 보안 지침', '인증센터 운영매뉴얼'에 별도로 규정하고 있습니다.

6.5 시스템 보안 통제

"정보인증"은 인증시스템 보안 통제에 관한 사항을 내부지침인 '정보시스템 운영 보안 지침', '인증센터 운영매뉴얼'에 별도로 규정하고 있습니다.

6.6 시스템 운영 관리

"정보인증"은 인증시스템 운영 관리 등에 관한 사항을 내부지침인 '정보시스템 운영 보안 지침', '인증센터 운영매뉴얼'에 별도로 규정하고 있습니다.

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

6.8 시점확인서비스 보호조치

"정보인증"은 시점확인서비스를 제공하는 경우 인증서와 동일한 물리적 절차적 기술적 보호조치를 수행합니다.

7. 인증서 형식

7.1 인증서 형식

"정보인증"의 인증서 프로파일은 다음과 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	사용자 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	- 사용자의 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=사용자 알림 Qualifier: Notice Text=이 인증서는 공동 인증서입니다
Policy Mappings	-	-	-	-
Subject Alternative Names	n	o	m	RFC822 Name=email
		m	m	Other Name = EVID
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

7.2 인증서 유효성 확인 정보 형식

"정보인증"의 인증서 효력정지 및 폐지 목록(CRL) 프로파일은 다음과 같습니다.

기본 필드 명	생성	처리	입력 값
Version	m	m	Version 2
Signature	m	m	sha256 with RSA (256byte)
Issuer	m	m	C(Country)는 printableString 그 외의 속성값은 utf8String

This Update	m	m	- 게시 날짜
Next Update	m	m	- 만료 날짜 (유효기간: 24시간)
Revoked Certificates	-	-	제공됨 (목록이 없는 경우 값이 없음)
-User Certificates	m	m	폐지된 인증서의 일련번호 입력
-Revocation Date	m	m	폐지날짜 입력
-CRL Entry Extensions	m	m	아래 참고
CRL Extensions	m	m	아래 참고

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 b : critical or non-critical - : not defined

m: mandatory r: recommended o: optional x: forbidden or not recommended

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	사용자 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	- 사용자의 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=사용자 알림 Qualifier: Notice Text=이 인증서는 공동 인증서입니다
Policy Mappings	-	-	-	-
Subject Alternative Names	n	m	m	Other Name = EVID
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.

8.2 평가자의 신원, 자격

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

나. 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, 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

가. 과학기술정보통신부 장관은 운영기준 준수 사실의 인정을 받은 전자서명인증사업자가 전자서명법 제17조(시정명령) 각호의 어느 하나에 해당하는 경우에는 기간을 정하여 시정을 명할 수 있습니다.

1. 운영기준을 준수하지 못하게 된 경우

2. 제13조 제1항에 따른 운영기준 준수 사실의 표시에 관한 사항을 위반한 경우

3. 제14조에 따른 신원확인에 관한 사항을 위반한 경우

4. 제15조 제1항·제5항에 따른 전자서명인증업무준칙 작성·게시에 관한 사항을 위반하거나 전자서명인증업무준칙을 준수하지 아니한 경우

5. 제15조 제2항부터 제5항까지에 따른 전자서명인증업무의 휴지·폐지에 관한 사항을 위반한 경우

6. 제16조 제1항에 따른 자료를 제출하지 아니하거나 거짓 자료를 제출한 경우

또는 관계 공무원의 출입·검사를 거부·방해하거나 기피한 경우

7. 제20조 제2항을 위반하여 보험에 가입하지 아니한 경우

나. 운영기준 준수 사실의 인정을 받은 전자서명인증사업자는 기간 내에 시정명령을 이행하여야 합니다.

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/년, 부가세 포함)

개인	범용		4,400
	용도제한용	은행/신용카드/보험용	・인증서 이용자 혹은 가입자와의 계약 관계에 따름
		기 타	

법인, 단체, 개인사업자	범용	110,000
	용도제한용	• 인증서 이용자 혹은 가입자와의 계약 관계에 따름
서 버		550,000

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 인증업무 수행과 관련하여 가입자 또는 인증서를 신뢰한 이용자에게 손해를 입힌 때에는 배상의 타당성이 인정된 가입자 또는 이용자만 그 손해를 배상합니다. 다만, 그 손해가 불가항력으로 인하여 발생한 경우에는 그 배상책임이 경감되고, 전자서명사업자가 과실 없음을 입증한 경우에는 그 배상책임이 면제됩니다.

나. "정보인증"은 "정보인증"의 귀책 사유로 가입자가 효력 정지 또는 폐지신청 이후부터 CRL 공고 전까지의 시간에 발생한 가입자와 이용자의 손해를 배상합니다.

9.2.2 배상책임 면책

"정보인증"은 다음에서 배상책임을 지지 않습니다.

가. "정보인증"이 본 준칙에서 정한 인증서별 발급대상, 용도를 가입자 임의로 변

경, 사용하여 발생한 손해

나. 인증서 발급(신규, 재발급, 변경, 갱신) 및 인증서 효력 정지, 폐지 목록의 공고 등과 같은 인증서비스 제공과정에서 통신 경로 장애 또는 가입자 시스템 장애 등 "정보인증"의 귀책 사유가 아닌 원인으로 인하여 발생한 손해

다. 가입자의 고의 또는 과실로 인하여 발생한 손해

라. 이용자의 고의 또는 과실로 인하여 발생한 손해

마. 가입자가 그릇되게 제공한 정보

바. 가입자의 전자서명 생성정보 관리 부주의(정보 노출, 분실, 변조 등)

사. "정보인증"이 발급한 인증서 및 인증업무와 관련하여 발생하는 직접적이고, 보상적 손해 이외의 손해

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

자. 전시, 사변, 천재지변 또는 이에 따르는 비상사태에 의하여 발생한 손해

차. 법적인 효력이 없는 시험용 인증서를 목적 외의 용도로 사용함으로써 발생한 손해

카. 환불 또는 거래 취소된 인증서를 이용하여 발생한 손해

타. 인증서 분실 신고인 이 전화를 받지 아니하여 발생하는 손해

파. 기타 "정보인증"의 과실 없이 발생한 손해

9.2.3 등록대행기관의 배상책임

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

나. 등록대행기관은 "가"의 손해배상책임을 담보하기 위하여 보험에 가입할 수 있습니다.

9.2.4 가입자의 배상책임

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

9.2.5 이용자의 배상책임

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

9.3 영업비밀

"정보인증"은 "부정경쟁방지 및 영업비밀보호에 관한 법률"을 준수하고 있으며, 당사의 상표・상호 등을 부정하게 사용하는 등의 부정경쟁행위와 당사의 영업비밀을 침해하는 행위를 하면 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

"정보인증"은 지식재산권 보호와 관련된 법령을 준수합니다.

9.6 보증

"정보인증"은 가입자가 제출한 정보 중 인증서비스를 제공하는 데 필요한 최소한의 정보에 대해서만 사실 여부를 확인하며, 해당 정보에 대한 사실성을 이용자에게 보증합니다.

9.7 보증 예외 사항

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

9.8 보험의 보상 범위

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

9.9 배상 한계

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

9.10 준칙의 효력

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

9.11 통지 및 의사소통

가. "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 전자서명인증업무준칙의 변경 이력을 관리하여야 합니다.

9.13 분쟁 해결

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

나. "정보인증"과 가입자 및 이용자 간 분쟁 발생 시 조정을 받기 위해서는「전자문서 및 전자거래 기본법」제32조에 따른 전자문서 전자거래 분쟁 조정위원회에 조정을 신청할 수 있습니다. 전자서명인증체계 관련자에게 전달되는 전자문서가 법적 효력을 갖기 위해서는 다음의 요건을 갖추어야 합니다.

1) 인증서에 기초한 전자서명을 포함하며, 전자서명은 전자서명법 제2조(정의) 제2호 각 목의 사항을 나타낼 것

2) 전자서명에 사용된 인증서가 유효한 상태이며, 정지 또는 폐지 상태가 아닐 것

다. 전자서명인증서비스 관련 분쟁이 발생하면 그 담당 기관은 "정보인증" 본사 소재지를 담당하는 지방법원이 됩니다.

9.14 준거법

본 준칙은 대한민국의 법 및 관계 법령에 따라서 해석되고 적용됩니다.

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.

ㅍ