한국정보인증 주식회사
인증업무준칙

Korea Information Certificate Authority
Certification Practice Statement

v.1.05

2019 년 11 월

인증업무준칙 제정 및 개정 내역

NO.	버 전	제정 및 개정일	결재자	제정 및 개정의 주요내용
1.	V1.00	2018. 07. 23.	권갑상	한국정보인증 인증업무준칙 제정
2.	V1.01	2018. 07. 30.	권갑상	인증업무준칙 및 인증서 게시 URL 수정
3.	V1.02	2018. 09. 04.	권갑상	인증업무준칙 수정
4.	V1.03	2019. 08. 02.	권갑상	AATL 용 인증서 OID 추가
5.	V1.04	2019. 08. 07.	권갑상	AATL 용 인증서 OID 추가
6.	V1.05	2019. 11. 21.	권갑상	인증기관 개인키 삭제 및 파기 사유 추가, 인증업무준칙 개정일 수정(V1.03, V1.04)

목 차

1. 소개

1.1. 개요

본 문서는 RFC 3647을 기준으로 작성되었으며 인증기관 주식회사에서 운영하는 인증기관의 인증서 발급 및 관리, 운영에 필요한 사항을 정하며 관련 당사자들의 책임과 의무사항에 대해 규율한다.

1.2 문서명 및 식별

본 문서의 명칭은 인증업무준칙으로 대한민국 내의 관계 법령을 준수한다. 인증업무준칙은 인증기관의 인증서 정책, 인증서 발급·관리, 운영정책 등 전자서명인증과 관련된 업무에 관하여 필요한 사항 및 전자서명인증체계 관련자들의 책임 및 권리관계에 관한 사항을 정함을 목적으로 한다.

AATL 을 위한 OID는 인증기관의 OID에 종속되면 아래와 같다.

1.2.410.200085.2.1.1	– KICA Accredited Certificate
1.2.410.200085.3.1	– KICA AATL
1.2.410.200085.3.1.1.1.1	– KICA AATL – Individual Subscriber
1.2.410.200085.3.1.1.2.1	– KICA AATL – Individual Subscriber
1.2.410.200085.3.1.1.2.2	– KICA AATL – Individual Subscriber
1.2.410.200085.3.1.2.1.1	– KICA AATL – Organizational Subscriber
1.2.410.200085.3.1.2.2.1	– KICA AATL – Organizational Subscriber
1.2.410.200085.3.1.2.2.2	– KICA AATL – Organizational Subscriber
1.2.410.200085.3.2	– KICA Secure AATL
1.2.410.200085.3.2.1.1.1	– KICA Secure AATL – Individual Subscriber
1.2.410.200085.3.2.1.1.2	– KICA Secure AATL – Individual Subscriber
1.2.410.200085.3.2.2.1.1	– KICA Secure AATL – Organizational Subscriber
1.2.410.200085.3.2.2.1.2	– KICA Secure AATL – Organizational subscriber

1.3 전자서명인증체계 관련자

1.3.1 인증기관

인증기관은 다음과 같은 인증업무를 제공한다.

- O 신원확인
- O 인증서 발급
- O 인증서 폐지

O 인증서 관련 정보의 공고
O 시점확인 서비스
O OCSP (온라인 인증서 상태 프로토콜) 서비스

1.3.2 등록대행기관

인증기관은 신원확인 등의 업무 위탁을 위하여 등록대행기관을 운영 및 관리할 수 있다.

1.3.3 가입자

가입자라 함은 인증기관으로부터 인증서를 발급받은 자를 의미하며 이에는 개인, 사업자가 있다.

1.3.4 신뢰당사자

신뢰당사자라 함은 인증기관에서 발급한 인증서를 신뢰하고 사용하는 자를 의미한다.

1.4 인증서의 종류

1.4.1 인증서 이용 범위 및 용도

인증기관이 발급한 인증서는 가입자가 소유하고 있는 개인키에 합치한다는 사실을 확인 및 증명하기 위하여 사용된다. 인증기관에서 발급하는 인증서는 전자서명용 인증서이며 이는 전자문서(계약문서 등)에 기명날인 또는 서명하는 용도로 사용된다.

1.4.2 인증서 이용제한

인증서는 발급 시의 이용 범위 또는 용도 내에서만 이용되어야만 한다. 누구든지 인증서의 이용 범위 또는 목적에 벗어나 부정하게 사용하여서는 아니 된다.

1.5 인증업무준칙의 관리

1.5.1 인증업무준칙 수립 및 개정 기관

인증기관인 인증기관은 인증업무준칙을 수립하고 개정한다.

1.5.2 수립 및 개정 담당자

인증업무준칙의 수립 및 개정 관련한 연락처는 다음과 같다.

O URL: trust.signgate.com
O E-mail: webmaster@signgate.com
O 주소: 경기도 성남시 판교로 242 판교디지털센터 C동 5층
O 전화: 02-360-3251

1.5.3 수립 및 개정 담당기관

인증기관은 기술연구소 소장이 인증업무준칙의 변경이 필요하다고 판단한 경우에 이를 개정할 수 있다.

1.5.4 시행 절차

인증기관은 제·개정된 인증업무준칙을 웹사이트에 공고한다. 개정된 인증업무준칙은 웹사이트에 게시한 후 10일 이후부터 효력을 발생한다.

1.6 정의 및 약어

O DN(Distinguished Name): 인증서 발급자 및 소유자를 확인하기 위하여 사용하는 이름형식을 의미한다.
O 전자문서(전자 메시지): 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 의미한다.
O 전자서명: 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 의미한다.
O 개인키: 전자서명을 생성하기 위하여 이용하는 전자적 정보를 의미한다.
O 공개키: 전자서명을 검증하기 위하여 이용하는 전자적 정보를 의미한다.
O 인증: 개인키가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 의미한다.
O 인증서: 개인키가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 의미한다.
O 인증기관: 전자서명 인증서를 발급하는 신뢰 기관으로 인증서 폐지목록을 주기적으로 발행하며, 디렉토리 시스템에 인증서와 인증서 폐지목록을 게시 등의 인증업무를 담당한다.
O 등록기관: 인증기관의 인증업무 중 신청자에 대한 신원확인과 가입자 정보를 등록, 관리하며 인증서 신청 및 인증서 폐지 신청 등의 업무를 수행하는 기관을 말한다.
O 객체식별자(OID: Object Identifier): 인증서에는 가입자(DN), 발급자, 버전, 등 기본 정보 외에 알고리즘, 인증서 정책, 키용도, 인증서 속성 등이 포함되며, 정보들이 표현하는 대상을 객체라 한다. 이러한 객체들을 유일하게 중복되지 않고 식별하기 위해서는 각 객체에 고유번호를 부여하는 방법이 사용되며 이것을 객체식별자라 한다.

O 가입자: 인증기관으로부터 인증서를 발급 받은 개인 또는 사업자를 말한다.
O 시점확인: 시점확인을 요청한 전자문서에 대하여 당해 전자문서가 인증기관에 제시된 특정시점을 확인하여 알려주는 기관을 말한다.
O 온라인 인증서 상태 프로토콜 (OCSP: Online Certificate Status Protocol): 인증서 폐지목록을 획득하지 않고도 실시간으로 인증서의 상태를 검증할 수 있도록 하는 인증서 상태 실시간검증프로토콜을 말한다.
O 인증업무: 인증서 발급, 갱신, 폐지, 가입자 정보 등록, 변경, 인증서 폐지 목록의 공고 등 인증서 및 인증관련 기록의 관리 등의 업무를 말한다.

2. 공고 및 보관

2.1 저장소

인증기관은 인증업무준칙을 포함하여 인증서비스에 필요한 신청 양식과 관련 규칙을 웹사이트에 게시한다.

2.2 정보공개 채널

인증기관은 법률상 보호되는 개인정보가 아닌 인증서 발급 및 관리에 관련된 정보를 누구든지 그 사실을 항상 확인할 수 있도록 웹사이트를 통해 게시한다.

- O 인증업무준칙: trust.signgate.com
- O 인증서 폐지목록: ldap://signca.signgate.com:389
- O 인증기관 인증서: trust.signgate.com

2.3 정보공개 빈도

인증기관은 인증서 효력정지 및 폐지목록을 매일 1회 주기적으로 게시한다. 인증업무준칙의 개정은 효력발생일 10일 이전에 웹사이트에 게시하여 누구든지 확인할 수 있도록 한다.

2.4 접근 통제

인증업무준칙과 인증서 발급 및 관리 등에 관한 정보는 누구든지 그 사실을 웹사이트에서 확인할 수 있도록 게시한다.

인증기관은 기밀정보가 공개되지 않고 변경되지 않도록 보호해야 한다. (9.3 항 참조)

3. 인증서 식별 및 인증

3.1 인증서 명칭 및 DN 체계

3.1.1 명칭의 사용

인증서와 인증서 효력정지 및 폐지목록 내의 기본영역에 사용되는 명칭은 X.500 DN 규격을 준용한다.

3.1.2 명칭의 의미

인증기관에서 발급한 인증서 내의 DN에는 개인명 또는 개인식별번호, 사업자명 또는 사업자식별번호를 사용한다.
AATL 디지털 서명 용도의 인증서인 경우, DN은 개인명 또는 사업자명을 사용한다.

3.1.3 신청인을 식별할 수 없는 익명의 인증서

인증기관은 신청인을 식별할 수 없는 익명 인증서를 발급하지 아니한다.

3.1.4 인증서 DN 규칙

인증기관에서 발급한 인증서 DN은 X.500 및 ASN.1을 준용한다.

3.1.5 인증서 DN 유일성

인증서의 DN은 유일한 값을 가진다.

3.1.6 인증서 DN에 상표 사용

인증서 신청자는 타인의 지식재산권을 침해하는 상표를 사용하는 것이 금지된다.

3.2 최초 신원확인

3.2.1 개인키의 소유 확인 방법

신청인 또는 신청인 대리인이 PKCS#10 형식의 인증서 서명 요청(Certificate Signing Request) 또는 암호학적으로 동등한 증명 양식을 제공함으로 신청인이 본인의 개인키를 소유함을 증명해야 한다.

3.2.2 사업자 신원확인

인증기관 또는 등록기관은 다음의 3가지중 하나를 통하여 사업자의 신원을 확인한다.
O 사업자번호
O 사업자등록증
O 사업자 이메일 인증

3.2.3 개인 신원확인

인증기관 또는 등록기관은 다음의 2가지중 하나를 통하여 신청인의 신원을 확인한다.
O 개인식별번호
O 본인확인기관

3.2.4 미검증 가입자 정보

신원이 확인되지 않은 인증서의 신청에 대해서는 인증서를 발급하지 아니한다.

3.2.5 권한 확인

인증기관 또는 등록기관은 인증서 신청인 권한을 확인하는 경우, 다음 방법에 의하여 신원을 확인한다.
O 개인의 경우, 개인식별번호 또는 본인확인기관을 통해 신원확인의 기준 및 방법에 따라 신원을 확인
O 사업자의 경우, 사업자번호 또는 사업자등록증, 또는 이메일정보를 통해 사업자의 신원을 확인
O 사업자 대리인인 경우, 사업자등록증, 재직증명서 또는 법인의 전화 및 이메일정보를 이용하여 등록기관이 신청인의 신원확인이 확인 가능한 값으로 대리권한을 지녔는지 여부를 확인

3.2.6 상호운영 기준

해당사항 없음

3.3 키 교체 요청에 대한 신원확인과 인증

3.3.1 반복적인 키 교체에 대한 신원확인과 인증

해당사항 없음

3.3.2 인증서 폐지 후 키 교체에 대한 신원확인과 인증

폐지 후 키교체 요청에 대해 인증기관 및 등록기관은 3.2 항의 최초 신원확인 항목과 동일한 검증 절차를 수행한다.

3.4 폐지 요청에 대한 신원확인과 인증

가입자는 더 이상 사용하지 않거나 인증서 및 키 쌍이 손상될 수 있다고 의심되면 가입자는 유효 인증서와 비밀번호 또는 개인식별번호로 신원을 확인하고 인증하여 인증서를 폐지할 수 있다. AATL 전자서명 용 인증서의 폐지 요청에 대한 신원확인 및 인증은 유효한 인증서 및 비밀번호를 사용한다.

4. 인증서 발급 등 관리 절차

4.1 인증서 발급 신청

4.1.1 인증서 발급 신청자

가입자는 신원확인을 통하여 인증서 발급을 신청할 수 있으며, 이에는 개인, 사업자가 있다.

4.1.2 인증서 신청 절차 및 책임

가입자는 인증업무준칙에 정해진 방법에 따라 신원확인을 한 후 온라인상으로 인증서 발급을 신청한다. 인증기관은 가입자의 개인키를 생성하거나 보관하지 않는다.

4.2 인증서 신청 처리

4.2.1 신원확인 및 인증절차

인증기관 또는 등록기관은 본 인증업무준칙의 3.2항에 명시된 절차대로 신원을 확인한다.

4.2.2 인증서 신청 승인 및 거절

인증기관 또는 등록기관은 본 인증업무준칙의 3.2항에 명시된 절차를 충족하지 못하는 경우 인증서 신청을 거절할 수 있다.

4.2.3 신청 처리 소요 시간

가입자가 본 인증업무준칙의 3.2항에 따라 신원확인이 정상적으로 처리된 경우 인증기관은 인증서 요청 후 7일 이내에 인증서를 발급한다.

4.3 인증서 발급

4.3.1 인증서 발급 절차

인증기관은 인증서를 신규 발급하기 전에 다음과 같은 항목을 발급시스템을 통해 확인하고 인증서를 발급한다.
O 가입자가 제출한 공개키 정보 유일성 확인
O 가입자가 제출한 DN 값 및 키 사용 용도 확인

4.3.2 인증서 발급 사실 공고

인증기관은 인증서 발급 시, 인증서 발급 사실을 발급완료 메시지 또는 가입자가 신청 시 작성한 이메일 주소로 공지한다.

4.4 인증서 수령

4.4.1 인증서 수령 절차

가입자는 인증서 발급 관리프로그램을 통해 인증서를 발급 및 수령한다. 가입자가 해당 인증서를 수령하면, 가입자가 발급받은 인증서의 관련 정보가 정확함을 승인 하였다고 간주한다.

4.4.2 인증서 게시

인증기관은 가입자의 인증서를 공개된 저장소에 게시하지 않는다. 단, 가입자가 인증서를 요청하는 경우에는 제공할 수 있다.

4.4.3 신뢰 당사자에게 인증서 게시

인증기관은 신뢰 당사자에게 가입자의 인증서를 게시하지 않는다.

4.5 키 쌍 및 인증서 용도

4.5.1 가입자의 개인키 및 인증서 사용 용도

가입자의 개인키는 전자서명 및 암호화 통신 등 인증업무 수행을 위해서만 사용한다.

4.5.2 신뢰 당사자의 공개키 및 인증서 사용 용도

해당사항 없음.

4.6 인증서 갱신발급

인증서 갱신발급은 정책적으로 인정하지 않는다. 인증서 유효기간이 만료된 가입자는 인증서를 신규로 발급하여야 하며 그 때 절차는 신규발급과 동일한 절차를 따른다.

4.6.1 인증서 갱신 기준

해당사항 없음.

4.6.2 인증서 갱신 신청자

해당사항 없음.

4.6.3 인증서 갱신 절차

해당사항 없음.

4.7 인증서 키 교체

4.7.1 인증서 키 교체 기준

가입자는 다음 각 호에 해당하는 경우 인증서의 키 교체를 받을 수 있다.
O 가입자가 인증서의 비밀번호를 잊은 경우
O 가입자의 개인키가 손상, 유출 또는 변경되었다고 우려되는 경우

4.7.2 인증서 키 교체 신청자

키 교체는 인증기관이 수행하거나 가입자가 신청할 수 있다.

4.7.3 인증서 키 교체 절차

인증서 키 교체는 인증서 신규 발급과 동일한 절차로 진행한다.

4.7.4 인증서 키 교체 통지

인증서 키 교체 통지는 인증서 신규 발급과 동일한 절차로 진행한다.

4.7.5 인증서 키 교체 승인

인증서 키 교체 승인은 인증서 신규 발급과 동일한 절차로 진행한다.

4.7.6 인증서 키 교체 게시

인증서 키 교체 게시는 인증서 신규 발급과 동일한 절차로 진행한다.

4.7.7 인증서 키 교체 신뢰 당사자 통보

인증서 키 교체의 통보는 인증서 신규 발급과 동일한 절차로 진행한다.

4.8 인증서 정보 변경

한국정보인증은 기존에 발급한 인증서 내용을 변경하지 않는다. 가입자가 정보 요청 사항에 따라 신규 인증서 발급 또는 인증서 키 교체로 분류되어 처리한다.

4.8.1 인증서 정보 변경 신청 기준

해당사항 없음

4.8.2 인증서 정보 변경 신청자

해당사항 없음

4.8.3 인증서 정보 변경 절차

해당사항 없음

4.8.4 인증서 정보 변경에 대한 통보

해당사항 없음

4.8.5 인증서 정보 변경 승인

해당사항 없음

4.9 인증서 폐지 및 효력정지

4.9.1 인증서 폐지 사유

인증기관은 다음의 사유가 발생한 경우에 당해 가입자 인증서를 폐지한다.
O 가입자가 인증서 폐지를 신청한 경우
O 가입자가 악위적인 방식이나 기타 부정한 방법으로 인증서를 발급 받은 사실 또는 이용한 사실을 인지하였거나, 그 가능성을 객관적으로 인지한 경우
O 가입자의 개인키가 분실·훼손 또는 도난·유출된 사실을 인지한 경우
O 가입자가 본 인증업무준칙을 위반한 경우
O 가입자의 신원확인이 적법하게 이루어 지지 않았음을 인증기관이 인지한 경우

4.9.2 인증서 폐지 신청인

가입자는 자신의 인증서에 대한 폐지를 신청할 수 있다. 인증기관은 4.9.1 항의 폐지 사유에 따라 가입자 인증서를 폐지할 수 있다.

4.9.3 인증서 폐지 절차

가입자는 신규발급 신청에 준하는 절차로 신원확인을 거친 후 해당 인증서 폐지를 인증기관에 신청할 수 있다.
인증기관은 인증서가 부정 발급된 사실을 인지한 경우 또는 가입자의 개인키가 분실 또는 유출된 사실을 인지한 경우에는 신청이 없어도 직권으로 인증서를 폐지할 수 있다.

4.9.4 인증서 폐지 유예기간

인증기관은 인증서 폐지 유예기간을 두지 않는다.

4.9.5 인증서 폐지 처리기간

인증기관은 폐지 신청 후 24시간 이내 해당 인증서 폐지 업무를 개시한다.

4.9.6 신뢰 당사자를 위한 인증서 폐지 확인 요구사항

인증기관은 인증서 유효성 검증을 위해 인증서폐지목록을 제공한다.

4.9.7 인증서 폐지 목록 발행 빈도

온라인 인증서폐지목록은 최소 1일마다 주기적으로 발행하며, 오프라인 인증서폐지목록

은 최소 90일 마다 주기적으로 발행한다.

4.9.8 인증서 폐지 목록 발행 최대 소요시간

온라인 인증서폐지목록은 발행일로부터 최대 1일 이내에 발행된다. 오프라인 인증서폐지목록은 발행일로부터 최대 10일 이내에 발행된다.

4.9.9 온라인 인증서 상태 검증

인증 기관은 한국정보인증(KICA)에서 발급 한 가입자 인증서의 온라인 인증서 상태 프로토콜 (OSCP)을 지원한다. 온라인 인증서 상태 확인(OCSP) 주소는 다음과 같다.
O URL: http://signocsp.signgate.com:9020

4.9.10 온라인 인증서 상태 검증 요구사항

인증서의 검증자는 온라인 인증서 상태 프로토콜(OSCP)을 사용하여 인증서의 유효성을 검증해야 한다.

4.9.11 인증서 폐지 기타 알림 수단

해당사항 없음.

4.9.12 키 교체 또는 키 손상의 특수 요구사항

인증기관의 개인키가 손상되었거나 손상이 의심되는 경우, 인증기관은 재난복구계획에 따라 해당 인증서의 상응하는 개인키를 교체한다.

4.9.13 인증서 효력정지 사유

해당사항 없음.

4.9.14 인증서의 효력정지 신청인

해당사항 없음.

4.9.15 인증서의 효력정지 신청 절차

해당사항 없음.

4.9.16 인증서의 효력정지 기간

해당사항 없음.

4.10 인증서 상태 서비스

4.10.1 서비스 운영 특징

해당사항 없음.

4.10.2 서비스 가용성

해당사항 없음.

4.10.3 서비스 운영 기타사항

해당사항 없음.

4.11 인증 서비스 해지 및 종료

인증서비스는 다음의 경우에 해지 및 종료 된다.
O 한국정보인증 인증기관이 운영을 중단한 경우
O 한국정보인증 인증기관에서 발급한 모든 인증서가 키 교체없이 폐지된 경우
O 가입자가 인증서를 폐지하거나 인증서가 만료된 경우

4.12 키 위탁 및 복구

해당사항 없음.

4.12.1 키 위탁 및 복구 정책 및 실행

해당사항 없음.

4.12.2 세션 키 캡슐화 및 복구 정책

해당사항 없음.

5. 인증업무 시설 및 장비 보호조치

5.1 물리적 보호조치

5.1.1 장소 위치 및 구성

인증기관은 인증시스템을 별도의 통제구역 내에 설치운영하고, 해당 시스템을 물리적 접근통제를 위하여 보안캐비닛 내에 설치한다.
최상위인증기관(RootCA) 시스템은 전자기 제어 장치와 함께 설치하여 운영한다.

5.1.2 물리적 접근 통제

인증기관은 외부인의 침입이나 불법적 접근 등의 물리적 위협으로부터 인증시스템 등이 설치된 장소를 보호합니다.
인증기관은 이상 상황 발생시 경보 기능을 갖는 CCTV 카메라 및 모니터링 시스템과 침입감지 시스템 등 감시통제시스템을 설치, 운영한다.
인증기관의 출입통제 시스템은 신원확인카드, 지문인식 및 무게감지 장치 등을 다중으로 결합하여 통제구역에 대한 접근을 통제한다.
인증기관은 보안경비요원을 배치하여 보안경비업무를 수행한다.

5.1.3 전원 및 공기조절시스템

인증기관은 갑작스러운 정전으로 인한 심각한 피해를 방지하기 위하여 무정전전원공급장치를 사용한다.
인증기관은 온도 및 습도를 일정하게 유지하기 위한 항온항습장치를 설치한다.

5.1.4 수해 방지

인증기관은 침수로부터 인증시스템을 안전하게 보호하기 위하여 바닥으로부터 이격하여 설치한다.

5.1.5 화재 예방

인증기관은 인증시스템실 등에 화재 탐지기, 휴대용 소화기 및 자동소화설비를 설치한다.

5.1.6 매체 저장

인증기관은 주요 저장·기록매체를 금고에 저장하여 물리적으로 접근을 통제한다.

5.1.7 폐기물 처리

인증기관은 문서, 디스켓 등을 폐기하는 경우 물리적으로 이를 파기한다.

5.1.8 원격지 백업

인증기관은 인증센터가 발급한 인증서, 인증서 효력정지 및 폐지목록 등을 물리적으로 격리된 원격지에 백업하여 당해 인증서의 효력이 소멸된 날부터 10년간 보관한다.
인증기관은 원격지 백업 설비의 안전한 운영을 위하여 CCTV카메라 설치 및 생체인식장치 설치 등을 통해 접근통제를 한다.

5.2 절차적 보호조치

5.2.1 주요업무 담당자

인증기관은 인증업무의 안전성과 신뢰성을 확보하기 위하여 업무를 역할별로 아래와 같이 정의하여 수행한다.

- O 정책 관리자
- O 인증업무 운영 관리자
- O 인증시스템 운영자
- O 보안 감사자
- O 보안 관리자

인증기관은 인증업무의 안정성과 신뢰성을 확보하기 위하여 정책 관리자, 인증업무 운영 관리자, 및 보안 감사자의 직무를 분리한다.

5.2.2 주요업무별 수행 인원

키 생성 업무는 3인 이상이 공동으로 수행하고, 기타 인증 업무는 2인 이상이 공동으로 수행한다.

5.2.3 주요업무별 인원 신원확인

해당사항 없음

5.2.4 주요업무별 역할 분리

인증기관은 인증업무의 안전성과 신뢰성을 확보하기 위하여 업무를 역할별로 분리하여 수행한다.

5.3 인적 보안

5.3.1 자격 요건

인증업무 인력의 경력 등 요구사항 및 신원확인 절차에 관한 사항, 교육 등 자격 요건에 관한 사항은 내부 규정에서 별도로 규정하고 있다.

5.3.2 신원확인

인증기관은 회사의 정보보안정책 또는 인사관리정책에 따라 직원 채용 시 필요한 사항에

대해 검증한다.

5.3.3 교육 및 훈련

인증업무를 담당하는 모든 직원은 아래와 같이 업무수행에 필요한 보안규정 내부관리절차 및 기술교육을 이수한다.

O 인증센터 개요 및 현황
O 인증 업무 담당자의 역할 및 책임
O PKI 개요
O 정보보안 등

5.3.4 재교육 및 훈련

인증업무를 담당하는 모든 직원은 매년마다 업무수행에 필요한 교육을 이수해야만 한다.

5.3.5 직무 이동 및 순환

해당사항 없음

5.3.6 비인가 행위 처벌

허가되지 않은 행위를 한 인력에 대해서는 관련 규정에 따라 징계한다.

5.3.7 독립 계약자 요건

해당사항 없음

5.3.8 직원 문서 공개

인증업무를 수행하는 인력은 담당 업무에 따라 필요한 내부 자료를 열람할 수 있다.

5.4 감사 로그

5.4.1 감사 로그의 종류

인증기관은 등록정보관리, 개인키 생성·관리, 인증서 생성·발급·검증 및 시점 확인 기능을 지원하는 시스템(이하"인증시스템"이라 한다)에서 발생한 사건들을 기록한다.

인증기관은 아래와 같은 주요 사항에 대한 감사 로그를 관리한다.

O 인증기관 키 생명주기 관리
O 인증서 생명주기 관리
O 핵심인증시스템의 시작과 종료 사실
O 핵심인증시스템 관리자의 주요 활동 사실
O 보안 관련 이벤트 등

5.4.2 감사 로그 처리 주기

감사 로그는 보안 감사자에 의해 월 1회 이상 감사 로그의 무결성에 대한 검증 및 비인가 활동에 대한 검토를 수행한다.

5.4.3 감사 로그 보관 기간

인증기관은 발생한 감사 로그를 발생일로부터 10년 동안 보관한다.
인증기관은 저장 공간의 가용성과 관리의 효율성을 고려하여 유형에 따라 보관한다.

5.4.4 감사 로그 보호

감사 로그는 보안 감사자에 의해 총괄 관리되며 시스템의 각 업무 관리자는 당해 업무에 대한 감사 기록만 열람할 수 있다.

5.4.5 감사 로그 백업 절차

인증기관은 변경된 내역에 대해 매일 백업을 실시하고 있으며, 전체 감사 로그에 대해서는 주단위로 백업을 실시한다.

5.4.6 감사 로그 취합 시스템

감사 로그는 내부 시스템에서 생성되고 저장된다.

5.4.7 감사 로그 대상에 대한 통보

감사 로그를 발생시킨 개인 및 사업자에게 감사 수행과 관련하여 별도 통지를 하지 않는다.
보안위반사건 발생 시 담당업무관리자에게 지체없이 통보한다.

5.4.8 취약점 측정

인증기관은 업무를 수행함에 있어서 효율적인 보안관리를 위하여 정기적으로 자체 점검을 실시한다.

5.5 기록 보존

5.5.1 기록 보존 대상의 종류

인증기관은 다음의 업무와 관련된 내역을 기록 보존한다.
O 인증기관의 인증서 발급 및 관리 등 인증 업무
O 인증기관의 핵심인증시스템 등의 운영 업무

5.5.2 보존기록 보관 기간

인증기관은 발생한 보존기록을 발생일로부터 10년 동안 보관한다.

5.5.3 보존기록 보호

인증기관은 인증업무 내부규정에 의하여 인증기관의 직원을 문서관리자로 정하며, 문서관리자는 모든 보존기록을 관리하며 기타 관리자들은 자신의 업무범위내의 보존기록에 대해서만 조회가 가능하다.

인증기관은 보존기록의 위·변조 및 훼손 등을 방지하기 위하여 다음과 같이 보존기록을 보호한다.
O 전자문서는 전자서명하여 안전하게 보관
O 일반문서는 잠금장치가 설치된 캐비닛에 보관

5.5.4 보존기록 보관 절차

인증기관의 전자화된 보존기록은 백업장비를 이용하여 별도의 매체에 보관된다.

5.5.5 보존기록 타임스탬프 요건

해당사항 없음

5.5.6 보존기록 취합 시스템

보존기록은 내부 시스템에서 생성되고 저장된다.

5.5.7 보존기록 검증 절차

문서관리자만 보존기록에 접근 가능하다.
보존기록에 대한 검증절차는 인증기관의 내부절차에 따른다.

5.6 키 변경

인증시스템의 키 유효기간이 만료하거나 서명키의 비밀번호 분실, 키 파손 등의 사유가 발생한 경우, 인증시스템은 동일한 기능과 권한이 있는 키를 교체한다. 키 교체 절차는 키 신규발급절차와 동일한 절차로 수행한다.

5.7 장애 및 재해복구

5.7.1 시스템 자원 및 소프트웨어 장애 발생에 대한 대책

인증기관은 인증시스템 업무에 심각한 위험을 초래하는 재난이 발생한 경우 재난복구계획에 따라 기반시설과 전산장비를 복구한다.

5.7.2 시스템 자원, 소프트웨어, 데이터의 훼손·손실대책

인증기관은 인증기관 인증서 등의 주요 데이터 훼손·손실이 발생하였을 경우 기록 보존된 자료를 이용하여 복구한다. 시스템 자원 및 소프트웨어가 훼손되었을 경우 예비 자원을 가용하여 복구한다.

5.7.3 개인키 손실에 대한 복구 절차

인증기관의 보관설비에 보관 중인 개인키 백업본을 인증서비스에 사용하도록 한다.
개인키가 불법적으로 유출된 것으로 판단될 경우 서비스 중단 공고 절차에 준한 보고 및 공지절차를 수행하고 인증기관은 인증기관 개인키를 재발급하고 이에 따른 개인과 사업자에게 발급된 모든 키를 재발급한다.

5.7.4 업무연속성 계획 수립

인증기관은 인증서 발급, 갱신, 폐지 등 인증관리 업무, 개인키 등 관리업무, 점검 업무와 핵심/주요 업무가 정보자산 및 설비자산 장애, 테러, 정전, 지진, 화재, 풍수해 등으로 업무가 중단되지 않도록 업무연속성 계획을 수립한다.
업무연속성 계획을 수립함으로써 인적·물적 자원의 피해가 발생한 시점에 가장 효율적인 활동 방법을 제시하여, 인증기관의 운영 업무와 전자서명인증 관리 핵심업무 중단기간을 최소화한다.

5.8 인증기관 또는 등록기관의 종료

인증기관의 인증서비스를 중단하거나 중단할 경우에는 해당 행위에 대한 영향을 최소화하여 진행해야 한다. 주요 수행 사항은 다음과 같다.

- O 모든 가입자에게 실질적이고 합리적인 사전 통지를 제공
- O 최소 1년 동안 인증업무준칙에서 요구하는 감사 로그 및 보존 기록을 유지
- O 운영 중단 시점 이전에 유효한 모든 인증서를 폐지

6. 기술적 보호조치

6.1 개인키 생성 및 절차

6.1.1 개인키 생성 절차

인증기관은 키 생성 절차에 따라 생성한다.
인증기관은 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되는 안전한 키 생성 시스템 또는 FIPS 140-2 레벨 3 인증을 받은 하드웨어 보안 모듈(HSM)에서 키를 생성한다. 키 생성 작업은 권한이 부여된 최소3인의 참여로 실시한다.
가입자는 인증서의 용도에 따라 적합하고 안전한 방식으로 가입자 키 쌍을 생성한다.
AATL 디지털 서명 용도의 인증서 가입자 키 쌍의 경우 FIPS 140-2 레벨 2 인증을 받은 하드웨어 보안 모듈(HSM)에서 생성한다.

6.1.2 가입자 개인키 전달 절차

가입자에게 개인키를 전달할 필요가 없다.

.

6.1.3 공개키 전달 절차

인증기관은 PKCS#10 형식의 CSR을 최상위인증기관(RootCA)에 제출한다.

6.1.4 인증기관 공개키 전달 절차

인증기관 공개키는 인증기관에서 운영하는 최상위인증기관에 의해 전자서명된다. 인증기관인증서가 신뢰당사자에게 전달할 수 있도록 신청인이 발급된 인증서를 수령 시 인증기관 인증서를 전달할 수 있는 절차를 수립하여 이행한다.

6.1.5 개인키의 키 길이

인증기관에서 운영하는 최상위인증기관 키 길이는 RSA 4096 bit를 사용하고, 인증기관의 키 길이는 2048 bit, 가입자 인증서 키 길이는 2048 bit를 사용한다. 키를 생성하는 데 사용되는 알고리즘은 다음과 같다.
O 알고리즘: RSA
O 해쉬 알고리즘: SHA-256

6.1.6 공개키 매개변수 생성 및 품질 검사

해당사항 없음

6.1.7 개인키 사용 용도

인증기관 인증서와 가입자 인증서는 전자서명 용도로 사용되어야 한다. 가입자 인증서 확장 키 사용 필드에 키 사용 용도가 명시되어 있다. 해당 사항은「인증센터 인증서 프

로파일 규격」을 참조한다.

6.2 개인키 보호 및 암호화 모듈

6.2.1 개인키 보관 장치

인증기관 키 쌍은 FIPS 140-2 레벨 3 인증을 받은 하드웨어 보안 모듈(HSM)에 보관하여 운영한다.

6.2.2 다중 통제

인증기관은 내부 키 생성 절차에 의해 인증기관 키 쌍 생성을 수행한다. 키 쌍 생성시 최소 3인 또는 그 이상의 인원이 참여한다.

6.2.3 개인키 위탁

인증기관은 인증기관의 키 쌍을 제 3자에게 위탁하지 않는다.

6.2.4 개인키 백업

인증기관 개인키는 백업 절차에 따라 안전한 위치에 보관된다. 백업된 개인키는 FIPS 140-2 레벨3 이상의 암호화 장비 토큰에 보관되며, 해당 토큰은 내화 금고 내에 안전하게 보관된다.

6.2.5 개인키 보관

인증기관은 유효기간이 만료된 인증기관 개인키를 보관하지 않는다.

6.2.6 개인키 추출

인증기관 개인키는 백업 목적으로만 하드웨어 보안 모듈(HSM)을 사용하여 암호화되어 추출한다.

6.2.7 개인키 저장

인증기관 개인키는 하드웨어 보안 모듈(HSM) 내부에 암호화되어 저장된다.

6.2.8 개인키 활성화

인증기관 개인키는 2명 이상의 운영자에 의해 다중 통제(two factor authentication) 아래 활성화할 수 있다.

6.2.9 개인키 비활성화

인증기관 개인키는 2명 이상의 운영자에 의해 다중 통제(two factor authentication) 아래 비

활성화할 수 있다.

6.2.10 개인키 삭제 및 파괴

인증기관은 다음과 같은 사유로 인증기관 개인키를 파기할 수 있으며 하드웨어 보안 모듈(HSM)에서 삭제되며 백업된 개인키도 삭제된다.

O 인증기관 인증서 유효기간이 만료되었음
O 인증기관 개인키가 훼손, 유출 및 손상되었거나 가능성이 있음
O 기타 인증기관의 사유

가입자는 개인 키가 더 이상 필요하지 않을 때 웹 사이트에 직접 액세스하여 가입자의 개인 키와 인증서를 삭제할 수 있다.

6.2.11 암호화 모듈 등급

본 문서의 6.2.1을 참조한다.

6.3 전자서명키쌍 관리

6.3.1 공개키 보관

공개키는 본 문서의 5.5.2에 정의된 기간 동안 인증기관 데이터베이스에 보관된다.

6.3.2 인증서 유효기간

인증서 유효기간은 인증서 필드에 명시된 유효기간 종료시점에 만료가 된다. 인증기관 및 가입자 인증서의 유효기간은 아래와 같다.

O 인증기관용 인증서: 10년
O OCSP 인증서: 10년
O 시점확인용 인증서: 10년
O 사용자 인증서: 1년, 2년, 3년

6.4 활성화 데이터

활성화 데이터는 하드웨어 보안 모듈(HSM)을 작동 및 사용하는데 필요한 정보이다. 활성화 데이터는 조작키와 비밀번호 등이 있다.

6.4.1 활성화 데이터 생성

활성화 데이터는 하드웨어 보안 모듈(HSM)의 사양에 따라 생성된다.

6.4.2 활성화 데이터 보호

활성화 데이터는 조작키와 비밀번호에 의해 보호된다. 접근 인증용 키는 지정된 관리자

에 의해 유지된다.

6.4.3 활성화 데이터 추가 고려사항

해당사항 없음

6.5 컴퓨터 보안

6.5.1 특정 컴퓨터 보안 요건

인증기관의 시스템 정보는 서버 및 OS 통제, 물리적 통제 및 네트워크 통제에 의해 보호되고 있습니다.

6.5.2 시스템 보안 요건

인증기관의 시스템은 ISO-27001 요건에 충족한다.

6.6 생명주기 보안

6.6.1 시스템 개발 통제

인증시스템의 기능 변경, 성능 개선 시 인증 업무 정책 관리자 또는 운영 관리자의 승인하에 실시된다.

6.6.2 보안관리 통제

인증시스템에 접근하는 모든 컴퓨터에 대하여 적절한 업무분장이 되어 있으며, 접근 권한을 최소화하여 운영한다.

6.6.3 생명주기 보안 통제

해당사항 없음

6.7 네트워크 보안 통제

인증기관은 네트워크 보안을 위하여 침입탐지시스템 및 침입차단 시스템을 사용한다.

6.8 시점 확인

인증시스템의 시간은 NTP를 사용한다.

7. 인증서 프로파일

7.1 인증서 프로파일

인증기관에서 발급하는 인증서는 RFC 5280을 준수한다.

7.1.1 인증서 버전

X.509 버전3 인증서를 발급한다. (버전 필드 값은 숫자 2로 지정)

7.1.2 인증서 확장

인증서의 확장 필드 사용 여부 등에 관한 사항은「인증센터 인증서 프로파일 규격」을 따른다.

7.1.3 알고리즘 개체 식별자

인증서에 사용되는 암호 알고리즘 개체 식별자는「인증센터 프로파일 규격」을 따른다.

7.1.4 명칭 양식

인증서에 사용되는 명칭 양식은「인증센터 인증서 프로파일 규격」을 따른다.

7.1.5 명칭 제한

인증서에 사용되는 명칭의 제한 사항 및 양식은「인증센터 인증서 프로파일 규격」을 따른다.

7.1.6 인증서 정책 개체 식별자

인증서에 사용되는 인증서 정책 개체 식별자는「인증센터 인증서 프로파일 규격」을 따른다.

7.1.7 정책 제한 확장의 사용

인증서에 사용되는 인증서 정책 제한 확장의 사용은「인증센터 인증서 프로파일 규격」을 따른다.

7.1.8 정책 한정자 구문 및 의미

인증서에 사용되는 인증서 정책 한정자 구문 및 의미는「인증센터 인증서 프로파일 규격」을 따른다.

7.1.9 주요 인증서 정책 확장에 대한 의미와 처리 절차

인증서의 정책 확장에 대한 의미와 처리 절차는「인증센터 인증서 프로파일 규격」을 따

른다.

7.2 CRL(인증서 효력정지 및 폐지목록) 프로파일

7.2.1 CRL(인증서 효력정지 및 폐지목록) 버전

인증기관에서 발급하는 인증서 폐지목록(CRL)은 RFC 5280을 준수한다.

7.2.2 CRL 확장 필드

인증서 폐지목록 확장 필드는「인증센터 인증서 프로파일 규격」을 따른다.

7.3 OCSP 인증서 프로파일

7.3.1 OCSP (온라인 인증서 상태 프로토콜) 인증서 프로필 버전

OCSP에 사용되는 OCSP 인증서 프로파일은「인증센터 인증서 프로파일 규격」을 따른다.

7.3.2 OCSP 인증서 확장 필드

OCSP에 사용되는 OCSP 인증서 확장 필드는「인증서센터 인증서 프로필 규격」을 따른다.

8. 감사 준수 및 기타 평가

인증기관은 인증시스템을 안전하게 운영하기 위하여 인증업무준칙의 모든 사항은 국내외 법제도 및 관련 기술표준을 준용하며, 독립된 제3자에 의해 정기적인 감사를 수행한다.

8.1 평가 빈도 및 환경

인증업무준칙 및 해당 시설 및 장비에 대해 연 1회 정기적으로 감사를 받는다.

8.2 평가 주체 및 자격

감사는 아래와 같이 일정한 자격과 기술을 갖춘 인력이 수행한다.

① 피감사대상자로부터 독립적인 자
② 국내외 법제도 및 관련 기술표준에 대한 충분한 지식이 있는 자
③ PKI 기술, 정보통신기술 및 정보시스템 감사관련 전문가
④ 관련 국제 자격 WebTrust 또는 그에 준하는 자격이 있는 자

8.3 감사 대상에 대한 평가자의 관계

인증기관은 인증 업무 및 운영과 관련하여 아무런 역할이나 책임이 없는 자격을 갖춘 독립적인 감사자인지의 여부를 확인하고 참여시켜야 하며, 감사자와 금전적으로나 사업적으로 이해관계가 없어야 한다.

8.4 평가 범위

평가주체는 인증기관이 제공하는 인증서비스의 품질을 보장하는 시스템, 인증업무준칙의 준수여부, 인증기관 키 관리, 인증서 관리 등의 사항을 준수하는지를 포함한다.

O 인증업무에 관한 시설 및 장비의 안전운영 여부를 점검
O 감사에 필요한 사항의 준비 및 증빙 자료 준비 등
O 방법: 아래 점검분야에 대하여 업무절차를 준수하는지 여부를 점검

① 인증서비스
② 전자서명키 관리
③ 기타 인증업무
④ 시설 및 장비의 관리
⑤ 문서 및 기록의 관리
⑥ 시험 운영 및 정보제공
⑦ 네트워크 및 시스템 보안
⑧ 물리적 보안
⑨ 재해방지
⑩ 관리적 보안 및 비상계획

8.5 평가 결과 조치

감사를 통해 발견된 미비점과 특이점은 보고서에 포함되며, 감사결과에 따라 정책적, 기술적 조치를 취한다.

8.6 평가 결과 공표

감사자는 감사 결과를 인증기관에 보고하고 인증기관은 감사 결과의 요약 및 관련 사항을 웹사이트에 게시한다.

9. 인증 업무 보증 등 기타사항

9.1 인증서비스 수수료

9.1.1 인증서 발급, 재발급 및 갱신 발급 수수료

인증기관은 인증서 발급, 재발급에 대한 수수료를 신청자에게 부과할 수 있다.

9.1.2 인증서 접근 수수료

인증기관은 인증서 열람 및 확인하는 가입자 또는 신뢰당사자에게 수수료를 부과할 수 있다.

9.1.3 인증서 효력정지 및 폐지목록 접근 수수료

인증기관은 인증서 효력정지 및 폐지목록에 접근하는 가입자 또는 신뢰당자사에게 수수료를 부과할 수 있다.

9.1.4 기타 서비스에 대한 수수료

인증기관은 인증서와 관련한 인증서 실시간 유효성 확인 서비스(OCSP), 시점확인서비스(TSA) 등의 부가서비스를 제공할 수 있으며, 이에 대한 수수료를 부과할 수 있다.

9.2 재무적 책임

인증기관은 인증업무 수행과 관련하여 가입자 또는 인증서를 신뢰한 이용자에게 손해를 입힌 때에는 법률상 책임이 인정된 가입자 또는 이용자에 한해 그 손해를 배상한다. 다만, 그 손해가 불가항력으로 인하여 발생한 경우 및 인증기관이 과실 없음을 입증한 경우에는 그 배상책임이 면제된다.

9.2.1 보험적용 범위

인증기관은 책임 보증을 유지한다.

9.2.2 기타 자산

한국정보인증의 재무 정보는 공개되어 있다.

9.3 기밀정보 보호

인증기관은 인증서비스와 관련하여 취득하고 생성된 정보를 안전하게 보호한다. 인증서비스의 안전성 및 신뢰성이 저하될 우려가 있는 정보 및 영업기밀 등 법률상 보호이익이 있는 기밀에 해당하는 내용에 대해서는 기밀로 관리하며, 기밀 정보는 안전하게 보관된다.

9.3.1 기밀 정보의 범위

해당사항 없음.

9.3.2 기밀 정보의 범위를 벗어난 정보

해당사항 없음.

9.3.3 기밀 정보 보호의 책임

해당사항 없음.

9.4 개인 정보 보호

인증기관은 개인정보보호와 관련하여 별도의 '개인정보처리방침'을 정하여 운영하고 있으며, 이는 웹사이트에 게시한다.
인증기관은 고객이 제공한 개인정보 보호를 위하여 국내의 정보통신망법, 개인정보보호법 등 관계 법규를 준수하고 개인정보 처리방침을 수립하여 시행한다.
인증기관은 원칙적으로 수집된 개인정보의 처리 목적이 달성된 경우 또는 개인정보가 불필요하게 되었을 때에는 해당 개인정보를 파기하나 관계 법령의 규정에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리해서 저장 및 관리한다.

9.4.1 개인정보보호 계획

인증기관은 개인정보보호법 등 관계 법, 규정을 준수하며 홈페이지에 게시된 개인정보처리방침에 따라 개인정보를 수집, 보유, 처리한다.

9.4.2 개인정보 기준

웹사이트에 게시된 개인정보처리방침에 따라 개인정보를 수집, 보유한다.

9.4.3 개인정보 제외 기준

해당사항 없음.

9.4.4 개인정보 보호의 책임

인증기관은 개인정보보호법 등 관계 법, 규정을 준수하며 웹사이트에 게시된 개인정보처리방침에 따라 수집, 보유, 처리한다.

9.4.5 개인정보 사용에 대한 통지 및 동의

인증기관은 개인정보 보호법 등 관계 법, 규정을 준수하며 웹사이트와 신청서를 통해 개인정보 사용에 대한 통지 및 정보 주체의 동의를 징수한다.

9.4.6 사법 행정절차에 따른 공개

해당사항 없음.

9.4.7 기타 정보 공개 기준

해당사항 없음.

9.5 지식재산 관련

본 인증업무로부터 파생되는 지식재산권은 인증기관의 소유이며 인증기관의 별도의 명시된 이용허락 없이는 적법하게 사용할 수 없다.

9.6 보증 책임

인증기관은 가입자가 제출한 정보 중 인증서비스를 제공하기 위해 필요한 최소한의 정보에 대해서만 사실여부를 확인하며, 해당 정보에 대한 사실성을 이용자에게 보증한다.

9.6.1 인증기관 보증

해당사항 없음

9.6.2 등록기관 보증

해당사항 없음.

9.6.3 사용자 보증

해당사항 없음

9.7 보증의 철회

인증기관은 가입자가 사위 기타 부정한 방법으로 인증서의 발급을 신청한 경우 및 인증서가 탈취당한 경우 등에는 보증을 철회한다.

9.8 책임의 제한 및 면책

인증기관은 다음 각 목의 경우 배상책임이 제한되거나 면책된다.

가) 인증서 용도를 가입자 임의로 변경, 사용하여 발생한 손해

나) 인증서 발급 (신규, 재발급, 변경) 및 인증서 효력정지, 폐지 목록의 공고 등과 같은 인증서비스 제공과정에서 통신 경로 장애 또는 가입자 시스템 장애 등 인증기관의 귀책사유가 아닌 원인으로 인하여 발생한 손해

다) 가입자의 고의 또는 과실로 인하여 발생한 손해

라) 전시, 사변, 천재지변 또는 이에 준하는 비상사태에 의하여 발생한 손해

마) 정부의 정책변경에 의해 발생한 손해

바) 기타 인증기관의 과실 없이 발생한 손해

9.9 인증업무준칙의 효력

본 인증업무준칙은 웹사이트 게시를 기점으로 효력이 발생하며, 개정시에는 개정 발효일 10일 이전에 웹사이트에 게시한다.

9.10 의사소통 및 통지

본 인증업무준칙은 웹사이트에 게시한다. 본 인증업무준칙과 관련하여 통지, 요구 또는 요청을 하고자 하는 자는 아래의 연락처로 연락할 수 있다.

O URL: trust.signgate.com
O E-mail: webmaster@signgate.com
O Phone: +82-2-360-3251

9.11 인증업무준칙의 관리

9.11.1 개정 절차

인증기관이 인증업무준칙의 정책과 무관한 사소한 변경이나 오류 정정 등의 변경이 필요하다고 판단한 경우 사전 공지 없이 수정할 수 있다. 인증기관은 중요 인증정책의 변경으로 인하여 인증업무준칙을 개정하는 경우에는 내부 품의 절차를 거쳐 해당 내용을 가입자 등이 확인할 수 있도록 적용 10일 이전까지 웹사이트에 게시한다.

9.11.2 개정 게시

인증기관은 인증업무준칙을 개정한 경우에 개정 된 인증업무준칙을 웹사이트에 게시합니다.

9.12 분쟁 해결

9.12.1 준거법 및 재판관할

본 인증업무준칙은 대한민국 내의 관계법령에 따라 해석 및 적용되며, 서울중앙지방법원을 제1심 재판 관할로 한다.