교육부

교육부 행정전자서명
인증업무준칙(CPS)

2019. 12.

교육부
행정전자서명인증센터
Education Public Key Infrastructure Center

차 례

1. 개요

교육부 행정전자서명 인증업무준칙은 RFC 3647의 기준에 따라 교육(행정)기관에 대한 행정전자서명 인증관리체계의 인증업무 정책을 공개한 문서이다. 교육부는 전자정부법 제29조제2항/동법 시행령 제28조/교육부 행정전자서명 인증업무지침 제4조에 따라 교육부 행정전자서명인증센터(Education Public Key Infrastructure Center, 이하 '인증센터'라 한다)를 구축하여 교육(행정)기관에 대한 행정전자서명 인증업무를 수행하고, 교육부 행정전자서명 인증업무준칙(이하 '인증업무준칙'이라 한다)을 인증센터 홈페이지에 게시한다. 교육행정전자서명인증서(이하 '인증서'라 한다)를 사용하는 기관 또는 개인은 언제든지 인증업무준칙을 열람할 수 있다. 이 인증업무준칙은 인증서 발급·관리 등 인증업무를 수행하는 교육부 행정전자서명인증센터, 등록기관 및 원격등록기관과 인증서를 사용하는 사용기관 및 가입자에게 적용한다. 인증센터는 CA/Browser Forum(http://www.cabforum.org)에서 게시한 「Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates」의 현행 버전을 준수한다.

1.1. 목 적

이 인증업무준칙은 교육행정전자서명 인증업무의 수행 및 관리 기준에 대한 구체적인 세부사항을 정함을 목적으로 한다.

1.2. 인증서의 종류

인증센터가 발급하는 인증서의 종류는 다음과 같다.

- 개인용(1.2.410.100001.5.3.1.3)
- 전자관인용(1.2.410.100001.5.3.1.1)
- 서버용(1.2.410.100001.5.3.1.7)
- SSL용(1.2.410.100001.5.3.1.9)[1)]
- 특수목적용(1.2.410.100001.5.3.1.5)
- 등록기관 및 원격등록기관용(1.2.410.100001.5.3.1.3)

1) 국제기준 충족(신규시스템 구축 등) 전 SSL용 인증서 신규/재발급 중단('19.06.03.~)

1.3. 교육행정전자서명 인증체계

1.3.1. 최상위인증기관

행정안전부 최상위인증기관(RootCA)은 행정전자서명 인증관리체계(GPKI)의 안전·신뢰성 있는 운영을 위한 정책·감독 기관으로 다음과 같은 업무를 수행한다.

- 행정전자서명 인증관리체계의 안전·신뢰성 있는 구축 및 운영을 위한 정책 수립
- 인증업무, 인증기관 업무의 위탁, 위탁 취소 및 고시
- 인증업무의 안전성과 신뢰성을 확보하기 위한 인증업무 운영 실태 확인

1.3.2. 교육부 인증기관

교육부 인증기관(CA : Certification Authority)은 행정전자서명 인증관리체계의 최상위 인증기관인 행정안전부 행정전자서명 인증관리센터로부터 인증업무를 위탁받아 운영되는 인증기관으로 교육(행정)기관에 대한 행정전자서명 인증업무를 수행한다.

교육부 인증기관은 인증센터를 구축하여 교육부 행정전자서명인증업무를 수행한다.

1.3.3. 교육부 행정전자서명인증센터

「전자정부법」 제29조제2항 및 시행령 제28조, 「행정전자서명 인증업무지침」제5조에 따라 교육부의 행정전자서명 인증업무를 수행하기 위해 교육부 행정전자서명인증센터를 둔다.

인증센터는 최상위인증기관인 행정전자서명 인증관리센터에서 발급한 인증서를 이용하여 인증업무를 수행하며, 등록기관 및 원격등록기관에서 인증업무를 수행할 수 없는 상당한 이유가 있을 때 해당 기관의 인증업무를 대행할 수 있다.

인증센터는 교육부 인증업무를 수행하며 등록기관 및 원격등록기관의 의무와 책임, 기타 인증업무를 관리·감독한다. 인증센터는 교육행정전자서명 인증업무의 안전성과 신뢰성을 확보하고 가입자 정보를 보호하기 위하여 필요한 경우에는 등록기관 및 원격등록기관에 자료 제출을 요구하거나 인증업무 운영 실태를 점검할 수 있다.

인증센터는 다음과 같은 업무를 수행한다.

- 교육행정전자서명 인증체계의 안전・신뢰성 있는 구축 및 운영을 위한 정책 수립
- 등록기관 및 원격등록기관의 지정 및 관리
- 등록기관 및 원격등록기관, 신청자의 신원확인
- 인증서의 발급, 갱신, 폐지 및 인증서 폐지목록 게시 등 인증업무
- 인증센터에서 발급한 인증서의 유효성 확인
- 가입자 정보 및 기록에 대한 관리
- 기타 인증기관으로서 필요하다고 인정되는 업무

1.3.4. 등록기관 및 원격등록기관

등록기관(RA : Registration Authority) 및 원격등록기관(LRA : Local Registration Authority)은 인증센터로부터 인증서를 발급받아서 다음 각 호의 업무를 수행한다.

- 인증서 발급, 재발급, 갱신, 폐지 등을 위한 신청 접수 및 신청자 신원확인
- 인증서 발급, 재발급, 갱신, 폐지 등과 관련한 가입자 정보의 등록과 갱신
- 기타 등록기관 및 원격등록기관으로서 필요하다고 인정되는 업무

1.3.5. 한국교육학술정보원

한국교육학술정보원은 전문기관으로서 교육부의 인증업무를 지원하며, 교육부장관은 인증센터 운영을 한국교육학술정보원에 위탁한다.

1.3.6. 가입자

인증센터로부터 인증서를 발급 받은 개인 또는 법인·기관 및 단체로, 인증서 발급 대상은 본 문서 4.1.1.과 같다.

1.3.7. 신뢰당사자

신뢰당사자는 인증센터에서 발급한 인증서 또는 전자서명을 신뢰하여 사용하는 개인 또는 법인·기관 및 단체이다. 신뢰당사자는 가입자일수도 있고 아닐 수도 있다.

1.3.8. 기타 참가자

해당사항 없음

1.4. 인증서의 용도

1.4.1. 인증서의 종류 및 용도

인증서는 발급대상에 따라 다음과 같은 용도로 발급한다.

- 개인용 인증서는 교육행정 업무를 담당하는 사람에게 직접 발급되어 사용자인증, 전자결재 등에 활용한다.
- 기관용 인증서는 행정정보를 전자적으로 유통하는 기관에 발급되어 해당기관의 신원확인, 유통 정보의 위·변조 확인, 송신에 대한 부인방지 등에 활용한다.
  - 전자관인용 인증서는 해당기관을 대표하는 관인용인증서로서 교육부 및 소속기관, 시·도교육청 및 소속기관, 유치원·초·중·고등학교, 대학(교), 공공기관(행정기관의 보조기관 및 보좌기관을 포함) 등 과 단위까지 1개의 인증서를 발급한다.
  - 등록기관 및 원격등록기관용 인증서는 가입자 정보 등록·관리 등의 업무 수행을 위해 사용한다.
  - 특수목적용 인증서는 각 기관의 교육행정 업무를 특정인이 처리할 수 없는 경우, 개인용 또는 전자관인용을 대신하여 발급한다. 다만, 특수목적용 인증서는 기관 대표메일 업무, 전자문서 수・발신 업무, 시스템 유지관리 및 위탁운영 업무, 상시 근무가 아닌 시간강사(개인용 인증서 발급 불가) 업무, 대입 업무, 재외한국학교 업무 등에 한하여 발급하고, 이외의 업무에 대해서는 교육부 협의를 거친 후 발급이 가능하다.
  - 서버용 인증서는 각 기관에서 관리하는 정보통신 장비가 교육행정 업무를 처리하고자 하는 경우, 서버 단위로 인증서를 발급한다.
  - SSL용 인증서는 웹서버와 웹브라우저에서 주고받는 정보를 암호화하여 정보의 내용을 보호할 수 있도록 도메인 단위로 발급한다.

1.4.2. 인증서 이용 제한

가입자는 인증서는 발급받은 목적과 용도에 맞게 사용하여야 하며 이용범위와 용도를 벗어나 부정하게 사용하는 것을 금지한다. 또한 유효기간이 만료 또는 폐지된 인증서를 사용하여서는 안 된다.

1.5. 교육부 행정전자서명 인증업무준칙(CPS) 관리

1.5.1. 교육부 행정전자서명 인증업무준칙 제정 및 개정

인증센터는 인증업무준칙을 제정하고 인증정책과 일관성을 유지하기 위해 개정한다.

1.5.2. 교육부 행정전자서명 인증업무준칙의 담당

인증업무준칙과 관련된 담당자의 연락처는 다음과 같다.

- URL : www.epki.go.kr
- 이메일 : epkihelp@keris.or.kr

1.5.3. 교육부 행정전자서명 인증업무준칙의 책임

인증업무준칙의 제정 및 개정의 책임은 인증센터장에게 있다.

1.5.4. 교육부 행정전자서명 인증업무준칙의 개정

인증센터 운영과 관련하여 기술적 또는 절차적인 변경 등의 사유가 발생할 경우에는 인증센터장의 승인을 받아 인증업무준칙을 개정한다.

1.5.5. 교육부 행정전자서명 인증업무준칙 승인 절차

인증업무준칙의 개정 승인은 인증센터장이 하며, 개정 문서 또는 개정 관련 공지사항은 인증센터 홈페이지에 게시하여야 한다.

1.6. 정의 및 약어

- **교육행정전자서명인증서(EPKI)** : 교육행정전자서명이 진정한 것임을 확인·증명할 수 있도록 교육부 행정전자서명인증센터에서 발급하는 전자적 정보를 말한다.
- **전자서명** : 전자문서를 작성한 사람의 신원과 전자문서의 변경여부를 확인할 수 있는 정보로서 당해 전자문서에 고유한 것을 말한다.
- **인증업무** : 인증서 발급·갱신·폐지, 가입자 정보 등록·변경, 인증서·인증서 폐지목록의 게시 등 인증서 및 인증관련 기록의 관리 등의 업무를 말한다.
- **인증서 폐지목록(CRL : Certificate Revocation List)** : 인증서 효력이 상실된 인증서의 목록으로 인증기관에서 주기적으로 발급·게시하는 전자적 정보를 말한다.
- **인증기관(CA : Certification Authority)** : 전자서명 인증서를 발급하는 신뢰 기관으로 인증서 폐지목록을 주기적으로 발행하며, 디렉토리 시스템에 인증서와 인증서 폐지목록 게시 등의 인증업무를 담당한다.
- **인증 :** 교육행정전자서명생성키가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명해 주는 행위를 말한다.

- **실시간 인증서 상태확인(OCSP : Online Certificate Status Protocol)** : 인증서 폐지 목록을 획득하지 않고도 실시간으로 인증서의 상태를 확인할 수 있도록 하는 인증서 상태 실시간확인 프로토콜을 말한다.
- **등록기관(RA : Registration Authority) 및 원격등록기관(LRA : Local Registration Authority)** : 인증기관의 인증업무 중 신청자에 대한 신원확인과 가입자 정보를 등록·관리하며 인증서 신청 및 인증서 폐지 신청 등의 업무를 수행하는 기관을 말한다.
- **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.
- **가입자** : 인증기관으로부터 인증서를 발급 받은 개인 또는 법인·기관 및 단체를 말한다.
- **사용기관** : 정보시스템의 안전성을 확보하기 위해 사용자 신원확인 또는 암호화 등의 목적으로 인증서를 이용하는 기관을 말한다.
- **LDAP(Lightweight Directory Access Protocol)** : 디렉토리 서버와 클라이언트 간의 통신에 사용되는 디렉토리 시스템 접근 프로토콜로서 DAP보다 간결하고 실용적으로 만들어진 프로토콜을 말한다.
- **DN(Distinguished Name)** : 가입자 객체를 명확히 구별할 수 있도록 부여하는 고유한 이름을 말한다. 가입자가 유일한 인증서를 소유함을 식별하기 위한 표준화된 명칭이다.
- **참조번호·인가코드** : 인증서 발급 신청 시 신청자 본인을 확인하기 위해 인증기관에서 부여하는 1회용 비밀번호를 말한다.

2. 게시 및 보관 책임

인증센터는 인증업무준칙을 인증센터 홈페이지(www.epki.go.kr)에 게시한다. 인증센터는 인증서와 인증서 상태 정보를 디렉토리 시스템(ldap.epki.go.kr)에 게시하고 인증서에 변경이 발생한 경우에는 이를 수정하여 게시하여야 한다. 인증센터는 필요시 게시된 인증업무준칙을 변경하며, 변경이 발생한 경우에는 개정 버전과 유효일자를 관리하여야 한다.

2.1. 저장장소

인증센터는 인증업무준칙을 포함하여 인증서비스에 필요한 신청서 양식과 관련 규칙을 인증센터 홈페이지에 게시하여야 한다. 인증서 폐지목록과 발급된 인증서의 정보는 디렉토리 시스템에 게시하여야 한다.

2.2. 정보공개 채널

- URL : www.epki.go.kr
- 이메일 : epkihelp@keris.or.kr

2.3. 정보공개 빈도

인증업무준칙과 인증서 신청양식이 변경된 경우에는 인증센터 홈페이지에 게시한다. 인증서 폐지목록을 매일 1회 주기적으로 게시하여야 한다. 인증서는 발급이 되는 시점에 게시하여야 한다.

2.4. 접근 통제

인증센터 홈페이지에 게시된 정보는 누구나 열람할 수 있도록 공개하여야 한다.

3. 인증서 식별 및 인증

3.1. 인증서의 명칭 및 DN체계

인증서의 명칭 및 DN체계는 X.509 규칙을 준수한다.

3.1.1. 인증서 DN의 종류

인증센터에서 발급한 인증서 DN명은 cn명, ou명, o=Government of Korea, c=kr 체계를 준수한다.

- 서버용 인증서 cn : cn=SVR+기관코드(7)+일련번호(3)
- SSL용 인증서 cn : cn=도메인명
- 개인용 인증서 cn : cn=기관구분자(3)+이름+일련번호(3)
- 등록기관 인증서 cn : cn=RA+기관코드(7)+기관명+일련번호(3)
- 원격 등록기관 인증서 cn: cn=LRA+기관코드(7)+기관명+일련번호(3)
- 특수목적용 인증서 cn : cn=기관코드(7)+(업무명)

단, 전자관인용 인증서의 DN명은 ou=최하위기관명, ou=상위기관명, ou=최상위기관명, o=Government of Korea, c=kr을 준수한다.

3.1.2. 명칭 의미

주체의 공통이름(Common Name) 또는 주체대체이름(Subject Alternative Name) 속성에 포함된 정보는 특정 개인 또는 기관을 식별하여야 한다.

3.1.3. 신청인을 식별할 수 없는 익명의 인증서발급

해당사항 없음

3.1.4. 인증서 DN의 규칙

인증서의 기본영역에 사용되는 명칭과 해석 규칙은 교육부 행정전자서명인증센터 상호연동기술표준 6. OID 및 DN 체계에 따라 의미 있는 식별체계를 갖는다.

3.1.5. 인증서 DN값의 유일성

인증서의 DN은 유일한 값을 갖는다.

3.1.6. 교육부 행정전자서명 상표(Trade marks)의 사용

해당사항 없음

3.2. 최초 신원확인

3.2.1. 인증기관의 초기 신원확인

해당사항 없음

3.2.2. 기관용 인증서의 초기 신원확인

등록기관 및 원격등록기관은 인증서의 신뢰성 확보를 위하여 신청자 정보에 대한 정확성 및 신청자 신원을 확인하는 절차를 거쳐야 하며, 일반적으로 인증서를 신청하는 해당 기관의 부서장 또는 기관장 명의의 공문에 의해 신원확인을 대체할 수 있다.

인증서를 발급받고자 하는 자의 신원을 확인하는 경우에는 「법인세법」에 따른 사업자등록증에 기재된 단체명 및 사업자등록번호에 따른 실지명의를 기준으로 하여야 한다.

공문으로 인증서를 신청하는 기관의 부서장 또는 기관장은 인증서를 발급받고자 하는 자의 명의가 「법인세법」에 따른 사업자등록증에 기재된 단체명 및 사업자등록번호에 따른 실지명의인지의 여부를 확인하여야 한다.

인증신청서(기관용)를 작성한 기관의 행정표준코드가 확인되면 신뢰할 수 있는 기관으로 인정한다.

등록기관 및 원격등록기관은 기관용 인증서 신청을 받은 경우, 반드시 다음의 사항을 확인하여야 한다.

3.2.2.1. 전자관인용(기관용)

- 신청기관이 해당 전자관인용 인증서를 소유함에 있어 “교육부 행정전자서명 인증업무지침” 제12조(인증서 발급 대상 및 종류)와 합치 여부
- 해당 전자관인용 인증서 중복 발급 여부
- 해당 기관을 구분할 수 있는 인증서 내 주체명(Subject Name)의 유일성
- 신청기관의 부서장 또는 기관장 확인 여부
- 신청서 누락사항이 없는지 여부
- 신청서가 【교육행정전자서명인증서 신청서 작성요령】에 따라 작성되었는지 여부
- 기타 행정전자서명 관련 법, 제도, 지침 등에서 요구하는 자료

3.2.2.2. 등록기관 및 원격등록기관용

- 신청기관이 해당 등록기관 또는 원격등록기관용 인증서를 소유함에 있어 “교육부 행정전자서명 인증업무지침” 제12조(인증서 발급 대상 및 종류)와 합치 여부
- 해당 등록기관용 또는 원격등록기관용 인증서 중복 발급 여부
- 해당 기관을 구분할 수 있는 인증서 내 주체명(Subject Name)의 유일성
- 신청기관의 부서장 또는 기관장 확인 여부
- 신청서 누락사항이 없는지 여부
- 신청서가 【교육행정전자서명인증서 신청서 작성요령】에 따라 작성되었는지 여부
- 기타 행정전자서명 관련 법, 제도, 지침 등에서 요구하는 자료

3.2.2.3. 특수목적용(업무용)

- 신청기관이 해당 특수목적용 인증서를 소유함에 있어 “교육부 행정전자서명 인증업무지침” 제12조(인증서 발급 대상 및 종류)와 합치 여부
- 해당 특수목적용 인증서 중복 발급 여부
- 해당 업무를 구분할 수 있는 인증서 내 주체명(Subject Name)의 유일성
- 신청기관의 부서장 또는 기관장 확인 여부
- 신청서 누락사항이 없는지 여부
- 업무명이 개인 명칭을 포함하거나, 개인 또는 기관 등을 지칭하지 않는지 여부
- 인증서의 사용목적이 드러나도록 업무명을 명확하게 기재하였는지 여부
- 신청서가 【교육행정전자서명인증서 신청서 작성요령】에 따라 작성되었는지 여부
- 기타 행정전자서명 관련 법, 제도, 지침 등에서 요구하는 자료

3.2.2.4. 서버용(컴퓨터용)

- 신청기관이 해당 서버용 인증서를 소유함에 있어 “교육부 행정전자서명 인증업무지침” 제12조(인증서 발급 대상 및 종류)와 합치 여부
- 해당 서버용 인증서 중복 발급 여부
- 해당 정보통신기기를 구분할 수 있는 인증서 내 주체명(Subject Name)의 유일성
- 신청기관의 부서장 또는 기관장 확인 여부
- 신청서 누락사항이 없는지 여부
- 신청서가 【교육행정전자서명인증서 신청서 작성요령】에 따라 작성되었는지 여부
- 기타 행정전자서명 관련 법, 제도, 지침 등에서 요구하는 자료

3.2.2.5. SSL용

- 신청기관이 해당 SSL용 인증서를 소유함에 있어 “교육부 행정전자서명 인증업무지침” 제12조(인증서 발급 대상 및 종류)와 합치 여부
- 해당 도메인에 SSL용 인증서 중복 발급 여부
- 해당 도메인을 구분할 수 있는 인증서 내 주체명(Subject Name)의 유일성
- WHOIS 검색을 통해 신청기관이 해당 도메인을 소유하였는지의 여부
- 해당 도메인이 IP주소 또는 내부도메인을 포함하지 않았는지 여부
- 신청기관의 부서장 또는 기관장 확인 여부
- 신청서 누락사항이 없는지 여부
- 신청서가 【교육행정전자서명인증서 신청서 작성요령】에 따라 작성되었는지 여부
- 기타 행정전자서명 관련 법, 제도, 지침 등에서 요구하는 자료

3.2.3. 개인용 인증서의 초기 신원확인

등록기관 및 원격등록기관은 인증서의 신뢰성 확보를 위하여 신청자 정보에 대한 정확성 및 신청자 신원을 확인하는 절차를 거쳐야 하며, 일반적으로 인증서를 신청하는 해당 기관의 부서장 또는 기관장 명의의 공문에 의해 신원확인을 대체할 수 있다.

인증서를 발급받고자 하는 자의 신원을 확인하는 경우에는 다음 각 호의 구분에 따른 실지명의를 기준으로 하여야 하며, 공문으로 인증서를 신청하는 기관의 부서장 또는 기관장은 인증서를 발급받고자 하는 자의 명의가 다음 각 호에 따른 실지명의인지의 여부를 확인하여야 한다.

1. 내국인의 경우에는 「주민등록법」에 따른 주민등록표(주민등록증)에 기재된 성명 및 주민등록번호
2. 외국인의 경우에는「출입국관리법」에 따른 등록외국인기록표(외국인등록증)에 기재된 성명 및 등록번호

등록기관 및 원격등록기관은 개인용 인증서 신청서를 접수한 경우에는 다음의 사항을 반드시 확인하여야 한다.

- 신청자가 해당 개인용 인증서를 소유함에 있어 “교육부 행정전자서명 인증업무지침” 제12조(인증서 발급 대상 및 종류)와 합치 여부
- 신청자의 소속, 이름, 주민등록번호 등
- 신청자의 인증서 중복 발급 여부
- 신청자를 구분할 수 있는 인증서 내의 주체명(Subject Name)의 유일성
- 신청기관의 부서장 또는 기관장 확인 여부
- 신청서 누락사항이 없는지 여부
- 신청서가 【교육행정전자서명인증서 신청서 작성요령】에 따라 작성되었는지 여부
- 기타 행정전자서명 관련 법, 제도, 지침 등에서 요구하는 자료

3.2.4. 신원이 확인되지 않은 인증서의 발급

신원이 확인되지 않은 인증서는 발급하지 않는다.

3.2.5. 권한의 발효

인증서는 발급과 동시에 권한이 발효된다.

3.2.6. 상호 운용 기준

인증기관은 최상위인증기관의 인증서신뢰목록(CTL) 기반으로 공인전자서명인증체계(NPKI)와 상호 운용한다.

3.3. 키 교체(Re-key)에 대한 신원확인과 인증

3.3.1. 키갱신(Routine Re-key) 신원확인과 인증

가입자 유효 인증서와 비밀번호로 신원을 확인하고 인증한다.

3.3.2. 인증서 폐지 후 키교체 신원확인과 인증

인증서 만료 등 인증서 폐지 후 키교체 시, 가입자는 본 문서 4.1.과 동일한 절차를 거쳐 인증서를 재발급 받아야 한다.

3.4. 폐지 요청에 대한 신원확인과 인증

가입자가 인증센터 홈페이지에서 직접 인증서를 폐지할 경우, 유효 인증서와 비밀번호로 신원을 확인하고 인증한다. 또한, 가입자는 본 문서 4.1.과 동일한 절차를 거쳐 인증서를 폐지할 수 있다.

4. 인증서 생명주기 운영 요건

4.1. 인증서 신청

4.1.1. 인증서 발급 대상 및 종류

인증서는 「교육부 행정전자서명 인증업무지침」 제12조(인증서 발급 대상 및 종류)에 따라 다음 각 호에 해당하는 기관 또는 업무담당자에게 발급할 수 있으며, 업무담당자는 각 호에 해당하는 기관 소속 공무원, 교직원 및 상시근무 직원(4대 보험을 납부하는 자)으로 한다.

1. 교육부 및 소속기관
2. 시·도교육청 및 소속기관
3. 「유아교육법」에 따른 학교, 「초·중등교육법」에 따른 각급학교, 「고등교육법」에 따른 각급학교, 그 밖의 다른 법률에 따라 설치된 각급학교 및 소속기관
4. 교육부장관의 지도·감독을 받는 공공기관 및 유관기관
5. 「사립학교법」 제2조제2호의 학교법인, 「국립대학법인 서울대학교 설립·운영에 관한 법률」에 따른 국립대학법인 서울대학교, 「국립대학법인 인천대학교 설립·운영에 관한 법률」에 따른 국립대학법인 인천대학교, 그 밖의 다른 법률에 따라 설치된 학교법인
6. 「재외국민의 교육지원 등에 관한 법률」 제2조제3호의 한국학교
7. 그 밖에 교육부장관이 지정하는 기관

「교육부 행정전자서명 인증업무지침」 제12조제1항 각 호에 따른 기관별 발급 가능한 인증서의 종류는 다음과 같다. 다만, 제12조제1항 제7호 “그 밖에 교육부장관이 지정하는 기관”에 발급 가능한 인증서의 종류는 교육부장관이 해당 기관을 지정할 때 결정할 수 있다.

발급대상	개인용	관인용	SSL용 (서버용)	특수목적용
제12조제1항 제1호	O	O	O	O
제12조제1항 제2호	O	O	O	O
제12조제1항 제3호	O	O	O	O
제12조제1항 제4호	O	O	O	O
제12조제1항 제5호				O
제12조제1항 제6호				O

4.1.2. 인증서 신청 절차 및 책임

인증서 신청자는 인증센터 홈페이지에 게시된 신청서를 【교육행정전자서명인증서 신청서 작성요령】에 따라 누락없이 작성한 후, 등록기관 및 원격등록기관에 공문으로 인증서를 신청한다. SSL용 인증서 발급을 신청하는 경우, 인증서 신청자는 WHOIS 검색을 통해 신청기관이 해당 도메인을 소유하였는지의 여부를 확인한 후, 인증서를 신청하여야 한다. 또한, 인증센터는 IP주소에 대한 SSL용 인증서는 발급하지 않는다.

등록기관용 인증서 신청자는 인증센터 홈페이지에 게시된 신청서를 작성한 후 인증센터에 공문으로 인증서를 신청하여야 한다.

제출한 신청서의 신청정보는 정확하여야 하며 인증서 신청자 및 해당기관(부서)장은 신청내용에 대하여 책임을 진다.

4.2. 인증서 신청 처리

4.2.1. 신원확인 및 인증

인증기관은 등록기관을 지정·관리할 수 있으며, 등록기관은 하위의 원격등록기관을 지정·관리할 수 있다. 인증기관, 등록기관 및 원격등록기관은 신청자 정보에 대한 정확성 및 신원을 확인하는 절차를 거쳐야 하며, 일반적으로 인증서를 신청하는 해당 기관의 부서장 또는 기관장 명의의 공문에 의해 신원확인을 대체할 수 있다. 신원확인 절차를 거친 신청자에게만 인증 정보를 제공하여야 한다.

4.2.2. 신청에 대한 승인 및 거절

인증기관은 등록기관용 인증서 신청자의 신원 확인과정에서 신청서 내용이 허위로 기재되었거나 누락된 경우, 신청자가 인증서 발급 대상이 아닌 경우, 또는 신청자가 등록기관의 대표 자격이 없다고 판단될 경우 등 특정한 사유가 있을 경우에는 신청을 거절할 수 있으며 거절 사유를 신청기관에 통보하여야 한다.

등록기관 및 원격등록기관은 신청자의 신원 확인과정에서 신청서 내용이 허위로 기재되었거나 누락된 경우, 제출된 서류만으로 신청자의 신원확인이 불가능한 경우, 또는 신청자가 인증서 발급 대상이 아닌 경우 등 특정한 사유가 있을 경우에는 신청을 거절할 수 있으며 거절 사유를 신청기관에 통보하여야 한다.

4.2.3. 신청 처리 소요 시간

인증기관, 등록기관 및 원격등록기관은 인증서 신청서를 접수한 경우, 3일 이내에 처리하여야 한다. 단, 폐지 및 효력정지 신청의 경우에는 공문 접수 후 즉시 처리한다.

4.3. 인증서 발급

인증기관이 발급하는 인증서는 전자정부법 시행령 제30조(인증서의 발급)에 의거하여 다음 각 호의 사항이 포함되어야 한다.

- 주체명(Subject Name)
  - 개인용인 경우 소속기관 및 개인을 구분하는 이름 등
  - 전자관인용인 경우 기관의 명칭
  - 특수목적용인 경우 기관 및 업무를 구분하는 명칭
  - 서버용인 경우 기관 및 서버를 구분하는 명칭
  - 등록업무 수행기관인 경우 등록기관, 원격등록기관을 구분하는 명칭
- 가입자 등의 행정전자서명검증키
- 가입자 등과 인증기관이 이용하는 전자서명의 방식
- 인증서 일련번호
- 인증서 유효기간
- 소관 인증기관의 명칭
- 인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항
- 가입자 등이 대결(代決)하는 경우 이에 관한 사항

4.3.1. 인증서 발급 절차

인증센터는 등록기관 및 원격등록기관의 신원확인을 거친 신청자에게만 인증서를 발급한다. 인증서 신청 절차는 본 문서 4.1.을 따른다.

인증센터는 인증서 발급 신청 승인 시 SMS와 E-MAIL로 승인 처리 메시지를 발송한다.

인증서 신청자는 인증센터 홈페이지에 접속한 후 부여받은 '참조번호·인가코드'의 유효기간(30일) 내에 인증서를 발급받아야하며, 유효기간 내에 인증서를 발급받지 않은 경우에는 인증서 발급을 재신청하여야 한다.

인증서는 신청자가 온라인으로 발급 받는 것을 원칙으로 한다. 다만, 특정한 사유로 신청자 환경에서 발급받을 수 없는 경우에는 신청자의 동의를 얻어 등록기관 또는 원격등록기관 등에서 안전한 방법으로 신청자의 인증서를 발급받아 신청자에게 전달할 수 있다.

인증센터는 인증서를 발급할 경우에는 반드시 다음의 내용을 확인하여야 한다.

- 신청자의 본인 확인 여부
- 유효한 참조번호/인가코드 사용 여부
- 인증서 신청자의 행정전자서명키 유일성 확인
- 인증서 신청자가 제출한 행정전자서명검증키에 합치하는 행정전자서명생성키의 소유 여부 검증

- 주체명(subject Name)의 유일성 확인
- 동일한 가입자가 동일한 인증서 정책에 해당하는 인증서 발급여부 확인
- (SSL용인 경우) PKCS#10 형식의 인증서 서명 요청(Certificate Signing Request : CSR)파일 정합성 및 전자서명 여부 등

4.3.2. 인증서 발급 통지

인증센터는 인증서가 발급되는 즉시 홈페이지에서 가입자에게 발급완료 메시지(팝업)를 제공하여야 하며, SSL용 인증서의 경우에는 별도의 E-MAIL 메시지를 발송하여야 한다.

4.4. 인증서 수령

4.4.1. 인증서 수령 절차

인증서는 신청자가 인증센터 홈페이지에서 인증서발급·관리프로그램을 통해 직접 발급 및 수령한다. 신청자는 발급받은 인증서의 유효기간, 용도, 발급기관 등 정보를 확인하여야 하며 인증센터로 별도의 통보를 하지 않는 경우에는 인증서 내용이 정확한 것으로 간주한다.

4.4.2. 인증서 게시

인증센터는 인증서 발급과 동시에 공개된 저장소(디렉토리)에 인증서를 게시하여야 한다.

4.4.3. 인증서 발급 공지

해당사항 없음

4.5. 인증키쌍 및 인증서 용도

4.5.1. 행정전자서명생성키(개인키) 사용 용도

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

4.5.2. 행정전자서명검증키(공개키) 사용 용도

가입자의 공개키는 행정전자서명검증키(공개키) 확장 필드에 명시된 용도로만 사용한다.

- digitalSignature는 신원 확인(entity authentication), 데이터 무결성(data origin authentication with integrity)등의 용도로 사용한다.
- nonRepudiation은 부인방지 서비스를 제공하기 위한 전자서명 검증 시 사용한다.
- KeyEncipherment는 키 전송(key transport) 시 사용한다.
- DataEncipherment는 소유자의 데이터를 암호화하는 데 사용한다.
- KeyAgreement는 키 합의(key agreement) 시 사용한다.

- encipherOnly는 keyAgreement 비트가 설정된 경우에는 소유자 공개키가 키 합의(key agreement)를 수행하는 동안 데이터 암호화용으로 사용한다.
- decipherOnly는 keyAgreement 비트가 설정된 경우에는 소유자 공개키가 키 합의(key agreement)를 수행하는 동안 데이터 복호화용으로 사용한다.

인증센터는 발급한 유효 인증서를 공개된 저장소(디렉토리)에 게시하여야 한다. 일반적으로 가입자 인증서의 공개키 획득 시 공개된 저장소(디렉토리)를 활용할 수 있다.

4.6. 인증서 갱신

4.6.1. 인증서 갱신 기준

가입자는 인증서 유효기간이 만료되기 90일 전부터 만료일까지 인증서를 갱신하여 유효기간을 연장할 수 있다. 가입자는 인증센터 홈페이지에서 인증서를 직접 갱신할 수 있다. 단, SSL용 인증서는 갱신할 수 없으며 본 문서 4.7.3.에 따라 재발급하여야 한다.

4.6.2. 인증서 갱신 신청자

유효한 인증서를 보유한 가입자만 인증서 갱신을 신청할 수 있다.

4.6.3. 인증서 갱신 절차

가입자가 직접 인증센터 홈페이지에서 인증서를 갱신하여야 한다. 인증기관에서 발급한 유효 인증서를 가지고 있을 경우에는 갱신에 대한 공문 제출 및 재등록 절차는 필요하지 않다.

인증센터는 인증서 갱신 시 다음의 내용을 확인 후, 인증서 갱신을 승인하여야 한다.

- 인증서 갱신 신청자의 행정전자서명키 유일성 확인
- 인증서 갱신 신청자가 제출한 행정전자서명검증키에 합치하는 행정전자서명생성키의 소유 여부 검증
- 가입자의 본인 확인 여부
- 인증서 유효기간 및 유효한 인증서 소유 여부
- 인증서 갱신발급 주체명(subject Name) 정보와 이전 인증서 주체명(subject Name)의 동일성 확인 등

단, SSL용 인증서는 갱신할 수 없으며 본 문서 4.7.3.에 따라 재발급하여야 한다.

4.6.4. 인증서 갱신 통지

인증센터는 인증서의 유효기간 만료 90일 전과 15일 전 가입자에게 SMS와 E-MAIL을 통해 갱신안내 메시지를 발송하여야 한다. 또한, 가입자의 인증서 갱신 완료 즉시 홈페이지를 통해 갱신 완료 메시지(팝업)를 제공하여야 한다.

4.6.5. 인증서 수령 절차

가입자의 인증서 갱신 후 수령은 본 문서 4.4.1.과 동일하다.

4.6.6. 인증서 갱신 게시

인증센터는 인증서 갱신과 동시에 공개된 저장소(디렉토리)에 인증서를 게시하여야 한다.

4.6.7. 인증서 갱신 공지

해당사항 없음

4.7. 인증서 재발급

4.7.1. 인증서 재발급 기준

가입자는 다음 각 호에 해당하는 경우 인증서를 재발급 받을 수 있다.

- 인증서 유효기간이 경과한 경우
- 인증서 비밀번호를 잊은 경우
- 가입자의 교육행정전자서명생성키가 손상·유출 또는 변경되었다고 우려되는 경우
- 소속기관명 및 가입자명 등 인증서 관련정보가 변경된 경우

4.7.2. 인증서 재발급 신청자

본 문서의 4.1.1. 대상자만 인증서 재발급을 신청할 수 있다.

4.7.3. 인증서 재발급 절차

인증센터는 등록기관 및 원격등록기관의 신원확인을 거친 신청자에게만 인증서를 재발급한다. 인증서 신청 절차는 본 문서 4.1.을 따른다.

인증센터는 인증서 재발급 신청 승인 시 SMS와 E-MAIL로 승인 처리 메시지를 발송한다.

인증서 신청자는 인증센터 홈페이지에 접속한 후 부여받은 '참조번호·인가코드'의 유효기간(30일) 내에 인증서를 발급받아야 하며, 유효기간 내에 인증서 발급을 받지 않은 경우에는 인증서 발급을 재신청하여야 한다.

인증서는 신청자가 온라인으로 재발급 받는 것을 원칙으로 한다. 다만, 특정한 사유로 신청자 환경에서 재발급 받을 수 없는 경우에는 신청자의 동의를 얻어 등록기관 또는 원격등록기관 등에서 안전한 방법으로 신청자의 인증서를 재발급 받아 신청자에게 전달할 수 있다.

- 신청자의 본인 확인 여부
- 유효한 참조번호/인가코드 사용 여부
- 인증서 신청자의 행정전자서명키 유일성 확인
- 인증서 신청자가 제출한 행정전자서명검증키에 합치하는 행정전자서명생성키의

소유 여부 검증

- 인증서 재발급 주체명(subject Name) 정보와 이전 인증서 주체명(subject Name) 동일성 확인
- (SSL용인 경우) PKCS#10 형식의 인증서 서명 요청(Certificate Signing Request : CSR)파일 정합성 및 전자서명 여부 등

인증센터는 인증서가 재발급되는 경우에는 재발급 시점부터 인증서의 남은 유효기간을 부여하여야 한다.

4.7.4. 인증서 재발급 통지

본 문서 4.3.2.와 동일하다.

4.7.5. 인증서 수령 절차

가입자의 인증서 재발급 후 수령은 본 문서 4.4.1.와 동일하다.

4.7.6. 인증서 재발급 게시

인증센터는 가입자 인증서의 재발급과 동시에 공개된 저장소(디렉토리)에 인증서를 게시하여야 한다.

4.7.7. 인증서 재발급 공지

해당사항 없음

4.8. 인증서 변경

4.8.1. 인증서 변경 상황

가입자의 이름 또는 기관 명칭, 조직정보 등 가입자 인증서 내 정보가 변경되었을 경우, 가입자는 인증서를 변경하여야 한다. 인증서 변경은 기 발급받은 인증서 내 정보를 변경하는 것이기 때문에 가입자는 기존 인증서를 폐지한 후 인증서를 재발급 받아야 한다.

단, 나이스시스템과 사용자정보가 현행화되는 17개 시·도교육청은 인사이동 등으로 타 시도로 소속기관이 변경(전출)되는 경우에는 인증센터와 연계하여 인증서를 폐지할 수 있으며, 가입자는 변경된 기관에서 인증서를 재발급 받아야 한다. 동일 시·도로 인사이동일 경우, 가입자 부서정보만 자동으로 변경되며, 기존 인증서는 사용할 수 있다.

정부조직법에 의하여 교육부 및 직속기관, 시·도교육청, 대학(교), 공공기관 등의 조직명이 변경되는 경우에는 변경대상 인증서를 폐지한 후 재발급 받아야 한다.

4.8.2. 인증서 변경 대상

본 문서의 4.1.1. 대상자만 인증서 변경을 신청할 수 있다.

4.8.3. 인증서 변경 요청 처리

인증센터, 등록기관 및 원격등록기관은 인증서 변경 요청에 대하여 본 문서의 3.2.와 동일한 신원확인 절차를 거친다.

4.8.4. 인증서 발급 통지

본 문서 4.3.2.와 동일하다.

4.8.5. 인증서 수령 절차

본 문서 4.4.1.과 동일하다.

4.8.6. 인증서 변경 게시

인증센터는 인증서 변경(재발급)과 동시에 공개된 저장소(디렉토리)에 인증서를 게시하여야 한다.

4.8.7. 변경된 인증서 발급 공지

해당사항 없음

4.9. 인증서 폐지 및 효력정지

4.9.1. 인증서 폐지 기준

인증센터, 등록기관 및 원격등록기관의 인증담당자는 다음 각 호의 어느 하나에 해당하는 사유가 발생한 경우 해당 인증서를 폐지하여야 한다.

- 가입자가 인증서 폐지를 신청한 경우
- 가입자가 퇴직 등의 사유로 「교육부 행정전자서명 인증업무지침」제12조(인증서 발급 대상 및 종류)에 해당하지 않게 된 경우
- 가입자가 부정한 방법으로 인증서를 발급받은 사실을 인지한 경우
- 가입자 인증서 내의 정보(조직정보 등)가 변경된 사실을 인지한 경우
- 가입자 재직상태(퇴직, 전출 등)가 변경된 사실을 인지한 경우
- 가입자의 행정전자서명생성키가 분실·훼손 또는 도난·유출된 사실을 인지한 경우
- 가입자 인증서에 사용된 인증센터 행정전자서명생성키가 분실·훼손 또는 도난·유출되었거나 안전하지 않다고 인지한 경우
- 기관용 인증서의 부적절한 사용 및 관리를 인지한 경우
- 그 밖에 인증서 폐지가 필요하다고 판단되는 경우

가입자는 다음의 사유가 발생한 경우 인증서를 폐지하여야 한다.

- 가입자 인증서 내의 정보(조직정보 등)가 변경된 경우
- 가입자가 퇴직 등의 사유로 「교육부 행정전자서명 인증업무지침」 제12조(인증서 발급 대상 및 종류)에 해당하지 않게 된 경우
- 가입자의 행정전자서명생성키가 분실·훼손 또는 도난·유출되었거나 안전하지 않다고 인지한 경우
- 그 밖에 인증서 폐지가 필요하다고 판단되는 경우

4.9.2. 인증서 폐지 신청자

가입자는 인증서 폐지를 신청할 수 있다. 다만, 가입자가 퇴직 등의 사유로 직접 인증서 폐지 신청이 어려운 경우에는 해당 기관에서 등록기관 및 원격등록기관으로 부서장 또는 기관장 명의의 공문을 통해 인증서 폐지를 신청할 수 있다. 또한, 인증센터, 등록기관 및 원격등록기관은 본 문서 4.9.1.에 따라 해당 인증서를 폐지할 수 있다.

4.9.3. 인증서 폐지 절차

가입자는 기 발급된 인증서가 유효한 인증서일 경우에는 인증센터 홈페이지에서 직접 폐지할 수 있다. 단, SSL용 인증서는 제외한다. SSL용 인증서의 경우에는 가입자는 본 문서 4.1.과 동일하게 인증서 폐지를 신청하여야 하며, 인증서 폐지 신청은 본 문서 4.2.와 같이 처리하여야 한다. 가입자가 기 발급된 인증서를 분실한 경우, 본 문서 4.1.과 동일하게 인증서 폐지를 신청하여야 하며, 인증서 폐지 신청은 본 문서 4.2.와 같이 처리하여야 한다.

4.9.4. 인증서 폐지 게시

인증센터는 인증서 폐지목록을 1일마다 주기적으로 공개된 저장소(디렉토리)에 게시하여야 한다.

인증센터는 가입자의 인증서 폐지 즉시 해당 인증서를 인증서 폐지목록에 추가하고 공개된 저장소(디렉토리)에서 삭제하여야 한다. 또한 실시간 인증서 상태확인서비스도 함께 제공하여야 한다.

4.9.5. 인증서 폐지 소요 시간

가입자는 본 문서 4.9.1.의 폐지 사유가 발생한 경우에는 즉시 인증서를 폐지하여야 한다.

등록기관 및 원격등록기관은 가입자가 인증서의 폐지를 신청할 경우, 폐지신청 공문 접수 후 즉시 처리하여야 한다.

4.9.6. 인증서 폐지 확인 요구사항

인증서 검증자는 인증서 폐지목록 또는 실시간 인증서 상태확인 서비스를 이용하여 인증서 유효성을 확인하여야 한다.

4.9.7. 인증서 폐지목록 발행 빈도

인증서 폐지목록은 1일 주기로 발행한다.

4.9.8. 인증서 폐지목록 발행 최대 지연 시간

인증센터는 인증서 폐지목록을 주기적으로 자동 발행한다.

4.9.9. 온라인 인증서 폐지 및 상태 확인

온라인 인증서 폐지 및 상태 정보는 공개된 저장소 및 실시간 인증서 상태확인을 통해 확인 가능하다.

4.9.10. 온라인 인증서 폐지 및 상태 확인 요구사항

인증서 검증자는 가장 최근에 발행된 인증서 폐지목록 또는 실시간 인증서 상태확인 응답자를 이용하여 인증서 유효성을 확인하여야 한다.

4.9.11. 인증서 폐지 정보 유효성 검증의 다른 방법

해당사항 없음

4.9.12. 키교체 또는 키손상의 특수 요구사항

가입자는 행정전자서명생성키 손상 시 본 문서 4.9.3.에 따라 인증서를 폐지하거나 4.7.3.에 따라 인증서를 재발급 받아야 한다.

4.9.13. 인증서의 효력정지 기준

인증센터, 등록기관 및 원격등록기관은 다음의 사유가 발생한 경우 해당 인증서의 효력을 정지하여야 한다.

- 가입자가 인증서 효력정지를 신청한 경우
- 가입자의 행정전자서명생성키가 분실·훼손 또는 도난·유출되었다고 의심되는 경우
- 가입자가 인증서비스 관련 법, 법령, 시행규칙 및 인증업무준칙을 위반한 경우
- 그 밖에 인증서 효력정지가 필요하다고 판단되는 경우

가입자는 다음의 사유가 발생한 경우에는 인증서의 효력을 정지하여야 한다.

- 가입자가 장기간 해당 인증서를 사용하지 않을 경우
- 가입자의 행정전자서명생성키가 분실·훼손 또는 도난·유출되었다고 의심되는 경우
- 그 밖에 인증서 효력정지가 필요하다고 판단되는 경우

4.9.14. 인증서의 효력정지 신청자

가입자는 인증서 효력정지를 신청할 수 있다. 다만, 가입자가 휴직 등의 사유로 직접 인증서 효력정지 신청이 어려운 경우에는 해당 기관에서 등록기관 및 원격등록기관으로 부서장 또는 기관장 명의의 공문을 통해 인증서 효력정지를 신청할 수 있다.

인증센터, 등록기관 및 원격등록기관은 본 문서 4.9.13.에 따라 해당 인증서를 효력정지할 수 있다.

4.9.15. 인증서의 효력정지 절차

가입자는 본 문서 4.9.13.에 의거하여 인증센터 홈페이지를 통해 직접 자신의 인증서를 효력정지 할 수 있다. 단, SSL용 인증서는 제외한다. SSL용 인증서의 경우에는 가입자는 본 문서 4.1.과 동일하게 인증서 효력정지를 신청하여야 하며, 인증서 효력정지 신청은 본 문서 4.2.와 같이 처리하여야 한다. 가입자가 기 발급된 인증서를 분실한 경우, 본 문서 4.1.과 동일하게 인증서의 효력정지를 신청하여야 하며, 인증서 효력정지 신청은 본 문서 4.2.와 같이 처리하여야 한다.

가입자는 인증서 효력회복 시, 본 문서 4.1.과 동일하게 인증서의 효력회복을 신청하여야 하며, 인증서 효력회복 신청은 본 문서 4.2.와 같이 처리하여야 한다.

4.9.16. 인증서 효력정지 기간 제한

가입자는 인증서가 효력정지된 일자부터 180일 이내에 인증서의 효력회복을 신청할 수 있다. 단, 180일 이내에 효력회복을 하지 않은 인증서는 자동으로 폐지된다.

4.10. 인증서 상태 서비스

4.10.1. 운영상 특징

인증서 상태는 인증서 폐지목록과 실시간 인증서 상태확인 서비스로 확인할 수 있다.

4.10.2. 서비스 가용성

인증센터는 계획된 서비스 중단을 제외하고는 인증서 상태 서비스를 365일 24시간 제공하여야 한다.

4.10.3. 선택적 기능

해당사항 없음

4.11. 인증서비스 해지 및 종료

다음과 같은 경우에는 인증서비스가 해지 및 종료된다.

- 교육부 인증기관이 운영을 중단할 경우
- 교육부 인증기관에서 발급한 모든 인증서가 갱신 또는 재발급없이 폐지된 경우
- 가입자가 인증서를 폐지하거나 인증서가 갱신없이 만료된 경우

4.12. 키위탁(Key Escrow) 및 복구

해당사항 없음

5. 시설 관리 및 운영 보호조치

5.1. 물리적 보호조치

5.1.1. 위치 및 시설

교육행정전자서명 인증시스템은 인증센터(한국교육학술정보원 전산센터) 내 위치하고 있으며, 인증센터는 행정전자서명 인증기관 구성요건에 따라 인증시스템을 운영하여야 한다.

5.1.2. 물리적 접근

교육행정전자서명 인증시스템은 보안요원의 통제에 따라 승인된 인력의 출입과 접근만을 허용하며 해당 출입내역을 기록하여야 한다.

5.1.3. 전원 및 공조시설

교육행정전자서명 인증시스템은 정전 및 변압의 위험에 대비하여 무정전 전원 공급장치(UPS)로부터 전원을 공급받는다. 교육행정전자서명 인증시스템이 위치한 전산실은 적합한 온도와 습도를 유지하여야 한다.

5.1.4. 침수 대비

인증센터는 교육행정전자서명 인증시스템을 침수로부터 안전하게 보호하기 위해 전산실 바닥으로부터 이격하여 설치하여야 한다.

5.1.5. 화재 예방 및 보호

인증센터는 화재 탐지 및 자동 소화 설비가 설치된 공간에서 교육행정전자서명 인증시스템을 운영하여야 한다.

5.1.6. 매체 저장

인증센터는 교육행정전자서명 인증시스템에 보관된 데이터의 손실 파손의 위험으로부터 주요 정보를 보호하기 위해 백업장비를 이용하여 백업하여야 한다.

5.1.7. 폐기물 처리

인증센터는 교육행정전자서명 인증시스템을 폐기할 경우에는 폐기물의 종류에 따라 안전하게 처리하여야 한다.

5.1.8. 원격지 백업

인증센터는 교육행정전자서명 인증시스템의 데이터 보호를 위해 물리적으로 분리된 백업센터에 원격백업을 수행하여야 한다.

5.2. 절차적 보호조치

5.2.1. 신뢰된 역할

교육행정전자서명 인증체계의 신뢰성을 확보하기 위해 인증센터 운영 책임자는 다음과 같이 신뢰성 역할을 지정하고 승인하여야 한다. 지정된 신뢰성 역할은 매년 현행화하여야 한다.

- 인증업무 정책 관리자는 교육행정전자서명 인증업무 정책 수립, 등록, 유지 및 개정하여야 한다.
- 보안관리자는 출입통제 등 인증센터 보안을 통제·관리하여야 한다.
- 인증업무 운영 관리자는 인증시스템의 설치, 운영 및 유지보수의 업무를 총괄하여야 한다.
- 인증시스템 운영자는 인증시스템 운영 및 유지보수 업무를 수행하여야 한다.
- 서비스데스크는 고객 문의에 대한 상담 업무를 수행하여야 한다.
- 키 생성 담당자는 인증기관 키 생성 및 활성화 업무를 수행하여야 한다.
- 인증업무 개발자는 인증 홈페이지 등을 관리하여야 한다.

5.2.2. 업무별 수행인력 수

- 키 생성 담당자는 2인 이상의 직원을 배치하여 인증기관 키 생성 및 활성화 업무를 수행하여야 한다.
- 인증시스템 운영자는 2인 이상의 직원을 배치하여 인증시스템 운영 및 유지보수 업무를 수행하여야 한다.

5.2.3. 업무 담당자 신원 확인 및 인증

인증센터 업무 담당자는 신원카드 및 지문을 통하여 인증센터 출입을 통제하여야 한다. 인증 업무시스템 접근 시 각 계정 또는 인증서로 접근 통제하여야 한다.

5.2.4. 직무 분리가 필요한 역할

- 인증서 신청에 대한 정보 검증
- 인증서 생성, 발급 또는 폐지
- 인증기관 키생성 등

5.3. 인력 관리

5.3.1. 자격 요건

운영인력은 국가가 인정한 정보통신 관련 자격을 취득하거나 이에 준하는 업무 경력을 보유 하여야 한다.

5.3.2. 신원확인

교육행정전자서명 인증체계의 운영인력은 신원확인 결과 결격 사유가 없어야 한다.

5.3.3. 교육 및 훈련

인증업무 수행 인력은 다음과 같이 업무수행에 필요한 보안규정 내부관리절차 및 기술교육을 이수하여야 한다.

- 인증센터 개요 및 현황
- 인증업무 담당자의 역할 및 책임
- PKI 개요
- 정보보안 등

5.3.4. 재교육 및 훈련

인증업무 수행 인력은 매년 보안 및 관련 기술 교육을 이수하여야 한다.

5.3.5. 직무 이동 및 순환

해당사항 없음

5.3.6. 비인가 행위 처벌

허가되지 않은 행위를 한 인력에 대해서는 관련 규정 및 법에 따라 징계하여야 한다.

5.3.7. 독립 계약자(Independent contractor) 요건

해당사항 없음

5.3.8. 직원의 문서공개

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

5.4. 감사로깅(Audit logging) 절차

교육행정전자서명 인증시스템은 주기적인 감사를 위해 주요 이벤트에 대한 로그(Log)를 보관하여야 한다.

5.4.1. 로그의 유형

감사로그는 인증서 생명주기, 인증기관 키관리, 시스템 접근 등을 포함하여야 하며, 인증센터는 다음과 같은 주요 사항에 대한 로그를 기록하여야 한다.

- 인증기관 키 생명주기 관리
- 인증서 생명주기 관리
- 신뢰된 역할 이벤트
- 보안관련 이벤트 등

각 로그 개체는 다음의 요소를 포함하여야 한다.

- 이벤트 번호
- 이벤트가 발생한 날짜 및 시간
- 이벤트 내용
- 이벤트 처리결과

5.4.2. 로그의 검토 주기

인증센터는 월 1회 이상 감사로그의 무결성에 대한 검증 및 비인가 활동에 대한 검토를 수행하여야 한다.

5.4.3. 감사로그의 보관 기간

인증센터는 저장 공간의 가용성과 관리의 효율성을 고려하여 유형에 따라 로그를 보관하여야 한다.

5.4.4. 감사로그의 보호

인증센터는 권한 없는 자의 감사로그 열람, 수정, 삭제 또는 기타 변조로부터 감사로그를 보호하여야 한다.

5.4.5. 감사로그의 백업

인증센터는 감사로그를 실시간 백업하여야 한다.

5.4.6. 로그 취합 시스템

인증센터는 감사로그를 내부 시스템에 저장하여야 한다.

5.4.7. 로그 대상에 대한 통지

인증센터는 로그를 발생시킨 개인 및 기관에게 감사수행과 관련하여 별도 통지하지 않는다.

5.4.8. 취약점 측정

취약점은 인증시스템의 기능을 유지하는데 해를 끼칠 가능성이 있거나 위협이 되는 요소이며, 인증센터는 이를 식별하고 줄이기 위한 기술적 관리적 부분을 평가하여야 한다.

5.5. 기록의 보관

5.5.1. 기록의 종류

인증센터는 인증서를 발급하기 위해 필요한 정보를 기록으로 관리하여야 한다.

5.5.2. 기록의 보관 기간

기록의 보관 기간은 전자정부법 시행령 제33조를 따른다.

5.5.3. 기록의 보호

인증서 신청기록은 변조되지 않도록 전자파일로 변환하여 정보시스템에 보관하여야 한다. 기록의 유실로부터 정보를 보호하기 위해 정보시스템을 주기적으로 백업하고 관리하여야 한다.

5.5.4. 기록의 보관 절차

전자화된 기록은 백업장비를 이용하여 별도의 매체에 보관하여야 한다.

5.5.5. 기록의 시점보유(Time-Stamping) 요건

해당사항 없음

5.5.6. 기록 취합 시스템

관련 기록은 전자결재 시스템으로 취합하여야 한다.

5.5.7. 정보의 청구 절차

교육행정전자서명 인증시스템과 관련된 정보는 인증센터와 사전협의 후 요청기관 명의의 공문을 통해 요청하여야 한다. 인증센터는 공문으로 접수된 요청에 대해서 공문으로 회신하여야 한다.

5.6. 키 변경

교육행정전자서명 인증시스템의 키 유효 기간이 만료하거나 서명키의 비밀번호 분실, 키 파손 등의 사유가 발생한 경우, 교육행정전자서명 인증시스템은 동일한 기능과 권한이 있는 키를 재발급하여야 한다. 키의 재발급 절차는 키 신규발급 절차와 동일한 절차로 수행하여야 한다.

5.7. 재해 복구

재해 발생시 교육행정전자서명 인증시스템은 물리적으로 독립된 위치의 장소에서 업무를 재개할 수 있다.

5.7.1. 정보시스템 재해 복구 절차

교육행정전자서명 인증시스템의 업무에 심각한 위험을 초래하는 재해가 발생한 경우, 재해 복구 절차에 따라 기반시설과 전산장비를 복구하고, 인증센터의 인증업무를 재개하여야 한다.

5.7.2. 정보시스템 자원이 손상된 경우의 절차

재해 복구 절차에 따라 소산된 키를 이용하여 인증관리체계를 복구하여야 한다.

5.7.3. 키 손상에 대한 복구 절차

인증기관 서명키의 파손 또는 사용에 위험이 발생한 경우에는 인증기관은 인증기관 서명키를 재발급하고 이에 따른 기관과 개인에게 발급된 모든 키를 재발급하여야 한다.

5.7.4. 업무연속성 확보

교육행정전자서명 인증시스템은 주 센터와 백업센터체계로 운영되며 장애 및 재해로 인해 주 센터에서 인증서비스를 제공하지 못하는 경우에는 12시간 이내에 백업센터로 기반 인프라, 정보시스템 및 인력을 포함한 대체 운영체계를 가동하여야 한다.

5.8. 인증기관 또는 등록기관의 종료

인증기관 인증업무 종료시, 인증기관은 최상위인증기관과 협의하여 인증기관의 인증업무를 최상위인증기관이 지정하는 인증기관으로 인계하여야 한다. 등록기관의 위임 종료시, 인증기관은 이를 공지하고 등록기관의 위임 종료로 인한 업무공백이 발생하지 않도록 한다. 인증업무를 종료하고자 하는 등록기관은 인증기관과 협의하여 해당 기관의 인증업무를 인증기관이 지정하는 등록기관으로 인계하여야 한다.

6. 기술적 보호조치

6.1. 키 쌍 생성 및 절차

6.1.1. 키 쌍 생성 절차

인증기관 키 쌍은 키 생성 절차에 따라 생성하여야 한다. 키 생성은 FIPS 140-2 레벨 3 인증을 받은 하드웨어 보안 모듈(HSM)을 사용하여야 한다. 키 생성 작업은 권한이 부여된 최소2인의 참여로 실시하여야 한다.

가입자의 행정전자서명생성키쌍은 가입자에게 제공되는 '인증서발급·관리프로그램'을 이용하여 생성하여야 한다.

6.1.2. 가입자에게 개인키 전달 절차

'인증서발급·관리프로그램'은 가입자를 대신하여 개인키를 생성하고 가입자에 대한 개인키와 인증서를 가입자에게 전달하여야 한다.

6.1.3. 인증서 발급자에게 공개키 전달 절차

가입자의 공개키는 '인증서발급·관리프로그램'이 가입자의 키쌍을 생성한 후 인증시스템으로 가입자 공개키를 전송하여야 한다.

6.1.4. 관련자에게 인증기관 공개키 제공 절차

인증센터 홈페이지에 인증기관 인증서 및 지문 정보(FingerPrint)를 게시하여야 한다.

6.1.5. 키 길이

안전하고 신뢰성 있는 교육행정전자서명 알고리즘을 사용하기 위하여 다음과 같은 크기의 키를 사용하여야 한다.

- KCDSA 및 RSA의 경우 2048비트 이상

6.1.6. 공개키 매개변수 생성 및 품질 검사

가입자 인증서 신규 발급 시 인가코드 HMAC을 활용한 CMP요청 무결성을 확인하여야 한다.

6.1.7. 키 사용 용도

인증기관의 키는 인증서, 인증서폐지목록 서명을 위해 사용한다.

가입자 키는 본 문서 4.5.의 키 사용을 따른다.

6.2. 개인키 보호 및 암호화 모듈

6.2.1. 암호화 모듈의 기준

‘행정전자서명 기술요건’ 및 FIPS-140-2 레벨 3을 만족하는 보안 모듈을 이용하여야 한다.

6.2.2. 다중 통제

인증기관 행정전자서명생성키의 다중 통제는 별도의 접근통제 권한을 가진 자가 수행하며, 지정된 인원 중 2명 이상 참여 하에 다중 통제를 수행하여야 한다.

6.2.3. 개인키 위탁(Escrow)

해당사항 없음

6.2.4. 개인키 백업

인증기관 행정전자서명생성키의 백업키는 하드웨어 보안 모듈(HSM) 백업 장비에 저장하여야 한다.

6.2.5. 개인키 보관

인증기관 행정전자서명생성키 백업 장비는 별도의 안전한 장소에 보관하여야 한다.

6.2.6. 개인키 추출

인증센터는 인증기관 행정전자서명생성키를 백업 목적으로만 하드웨어 보안 모듈(HSM)로 암호화하여 추출하여야 한다.

6.2.7. 개인키 저장

인증센터는 인증기관 행정전자서명생성키를 하드웨어 보안 모듈(HSM) 내부에 안전하게 저장하여야 한다.

6.2.8. 개인키 활성화

복수의 지정된 운영자가 조작키와 비밀번호를 사용하여 인증기관 행정전자서명생성키를 활성화하여야 한다.

6.2.9. 개인키 비활성화

하드웨어 보안 모듈(HSM)은 항상 활성화하여 운영하여야 한다.

6.2.10. 개인키 삭제 및 파괴

인증기관 키가 더 이상 필요하지 않을 경우에는 하드웨어 보안 모듈(HSM) 파티션에서 삭제되며 별도 보관하고 있는 백업데이터도 삭제하여야 한다.

6.2.11. 암호화 모듈 등급

본 문서의 6.2.1.을 참조한다.

6.3. 키 쌍 관리

6.3.1. 공개키 보관

공개키는 본 문서의 5.5.2에 정의된 기간 동안 인증기관 데이터베이스에 보관하여야 한다.

6.3.2. 인증서 운영기간 및 사용기간

가입자 인증서의 유효기간은 2년 3개월로 한다. 단, 특수목적용 인증서의 유효기간은 1년 3개월로 한다.

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. 데이터 생성

인증센터는 FIPS 140-2 인증을 획득한 하드웨어를 사용하고, 활성화 데이터는 하드웨어 보안 모듈(HSM)의 사양에 따라 생성하여야 한다.

6.4.2. 데이터 보호

접근 인증용 키는 지정된 관리자가 관리하며 비밀번호는 인증센터의 암호화 정책을 적용하여야 한다.

6.4.3. 기타 특성

해당사항 없음

6.5. 컴퓨터 보안

관련 시스템에 대해 기술적, 관리적, 물리적 보안방안을 준수하며 보안점검활동을 수행하여 안전하게 관리하여야 한다.

6.5.1. 특정 컴퓨터 보안 요건

인증시스템은 액세스 제어 기능, 작업자 식별 및 확인 기능, 감사 로그 수집 기능, 인증서 폐지목록 생성 기능이 있다.

6.5.2. 시스템 보안 요건

인증시스템 접근 시 접근권한별 보안통제를 요구한다. 시스템 접근 매체는 독립된 장소에서 보호되고 있다.

6.6. 생명주기 보안

6.6.1. 시스템 개발 통제

인증시스템의 기능 변경, 성능 개선 시 인증업무 정책 관리자 및 운영 관리자의 승인하에 실시하여야 한다.

6.6.2. 보안 관리 통제

인증시스템에 접근하는 모든 컴퓨터에 대하여 적절한 업무분장이 되어 있어야 하며, 접근 권한을 최소화하여 운영하여야 한다. 인증시스템 접근을 위해서는 인증센터, 인증업무 정책 관리자 및 운영 관리자의 승인을 득해야 하며, 접근 인력의 업무변경 시 주기적으로 권한을 변경하여야 한다.

6.6.3. 생명주기 보안 통제

해당사항 없음

6.7. 네트워크 보안

인증센터는 침입차단시스템 및 침입탐지시스템을 활용하여 네트워크를 통한 불법적인 침입 및 서비스 방해 공격 등으로부터 인증시스템을 보호하여야 한다.

6.8. 시점 확인(Time-stamping)

인증시스템의 시간은 NTP를 사용하여야 한다.

7. 인증 규격

인증서, 인증서 폐지목록, 실시간 인증서 상태확인 서비스는 “교육부 전자서명인증센터 상호연동기술표준”을 준수하여야 한다.

7.1. 인증서 프로파일 규격

교육행정전자서명 인증체계는 전자서명인증체계 기술규격을 준수하고 X.509 V3 표준을 준용하여야 한다.

7.1.1. 인증서 버전

인증센터는 X.509 V3 인증서를 발급하여야 한다.

7.1.2. 인증서 확장

인증센터에서 발급하는 인증서는 “교육부 전자서명인증센터 상호연동기술표준”에 명시된 인증서 확장 필드를 사용하여야 한다.

7.1.3. 알고리즘 객체 식별자

인증서 알고리즘 OID는 “교육부 전자서명인증센터 상호연동기술표준” 체계를 준수하여야 한다.

sha256WithRSA Encryption	iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) shasha256WithRSAEncryption(11)
sha256	joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1)

7.1.4. 이름 양식

인증서 DN은 “교육부 전자서명인증센터 상호연동기술표준” 체계를 준수하여야 한다.

7.1.5. 이름 제한

해당사항 없음

7.1.6. 인증서 정책 객체 식별자

인증서 정책(Certificate Policies)의 정책 식별자(OID)는 “교육부 전자서명인증센터 상호연동기술표준” 체계를 준수하여야 한다.

7.1.7. 정책 제한 확장의 사용

해당사항 없음

7.1.8. 정책 한정자 구문 및 의미

정책 한정자는 인증서 정책 확장에 명시되어 있으며, 인증업무준칙의 위치와 사용자 알림 문구를 포함하여야 한다.

7.1.9. 주요 인증서 정책 확장에 대한 의미 처리

주요 인증서 정책 확장은 “교육부 전자서명인증센터 상호연동기술표준” 체계를 준수하여야 한다.

7.2. 인증서 폐지목록 프로파일 규격

7.2.1. 버전

인증서 폐지목록의 버전은 X.509 V2이다.

7.2.2. 인증서 폐지목록 확장 필드

인증서 폐지목록의 확장필드는 “교육부 전자서명인증센터 상호연동기술표준” 체계를 준수하여야 한다.

7.3. 실시간 인증서 상태확인 프로파일 규격

교육행정전자서명 인증체계는 인증서비스 이용의 신뢰성 확보를 위한 인증서 유효성 확인 기능을 실시간으로 제공하기 위하여 〖실시간 인증서 상태확인 기술규격〗을 준수하여야 한다.

7.3.1. 버전

실시간 인증서 상태확인 서비스의 버전은 X.509 V1이다.

7.3.2. 실시간 인증서 상태확인 필드

실시간 인증서 상태확인 서비스의 확장필드는 “교육부 전자서명인증센터 상호연동기술표준” 체계를 준수하여야 한다.

8. 감사 준수 및 기타 평가

교육부 행정전자서명 인증업무준칙의 사항은 국내외 법・제도 및 관련 기술표준을 준용하며, 독립된 제 3자에 의해 정기적인 감사를 수행하여야 한다.

8.1. 감사 빈도 및 환경

감사는 매년 주기적으로 수행하여야 한다.

8.2. 감사 주체 및 자격

감사는 다음과 같이 일정한 자격과 기술을 갖춘 인력이 수행하여야 한다.

1. 피감사 대상자로부터 독립적인 자
2. 국내외 법・제도 및 관련 기술표준에 대한 충분한 지식이 있는 자
3. PKI 기술, 정보통신기술 및 정보시스템 감사관련 전문가
4. 관련 국제 자격 WebTrust, ETSI 또는 그에 준하는 자격이 있는 자

8.3. 피감사 대상에 대한 감사자의 관계

감사자는 피감사 대상자와 금전적 또는 사업적 등으로 이해관계가 없어야 한다.

8.4. 감사 범위

감사의 범위는 교육부 행정전자서명 인증업무준칙의 준수 여부, 인증기관 키 관리, 인증서 관리 및 인증시스템관리를 포함하여야 한다.

8.5. 감사 결과 조치

감사를 통해 발견된 미비점과 특이점은 보고서에 포함되며, 감사 결과에 따라 정책적, 기술적 조치를 취하게 되며, 범위는 영향도 등에 따라 결정하여야 한다.

8.6. 감사 결과 공표

교육행정전자서명 인증서비스에 대한 감사결과는 보증보고서(Assurance Report)에 포함하여 인증센터 홈페이지에 공개하여야 한다.

9. 기타 업무상 및 법적 사항

9.1. 요금

교육행정전자서명 인증체계는 국가가 운영하는 정보보호기반 인프라로서 인증서의 발급, 재발급, 갱신의 비용과 기타 요금을 개인 또는 기관에게 청구하지 않는다.

9.2. 재무적 책임

교육행정전자서명 인증체계가 발급하는 인증서와 관련하여 발생한 문제에 대해서 금전적 보상을 하지 않는다.

9.3. 중요 정보 보호

인증센터는 인증서비스와 관련하여 취득하고 생성된 정보를 안전하게 보호하여야 한다.

9.3.1. 중요 정보의 범위

교육행정전자서명 인증서비스의 안전성 및 신뢰성이 저하될 우려가 있는 다음의 정보에 대해서 중요 정보로 관리하여야 한다.

- 인증센터의 행정전자서명생성키
- 인증시스템 및 인증센터의 행정전자서명생성키 접근 정보
- 핵심인증시스템 운영 관련 사항
- 인증서비스 연속성 관련 사항
- 가입자정보
- 감사로그 및 보관된 기록
- 그 밖의 교육행정전자서명 인증서비스의 안전성 및 신뢰성이 저하될 우려가 있는 정보

9.3.2. 중요 정보의 범위를 벗어난 정보

교육행정전자서명 인증서비스의 안전성 및 신뢰성에 영향이 없는 정보에 대해서는 공개하여야 한다.

9.3.3. 중요 정보 보호의 책임

인증센터의 인가된 인력은 교육행정전자서명 인증서비스의 중요 정보를 안전하게 보관하고 관리하여야 한다.

9.4. 개인정보보호

9.4.1. 개인정보보호

인증센터는 개인정보 보호법 등 관련 법령상의 개인정보보호 규정을 준수하며 인증센터의 개인정보처리방침에 따라 개인정보를 수집·보유·처리하여야 한다.

9.4.2. 처리하는 개인정보

인증센터는 개인정보 보호법 등 관련 법령상의 개인정보보호 규정을 준수하며 인증센터의 개인정보처리방침에 따라 개인정보를 수집·보유·처리하여야 한다.

9.4.3. 비공개로 간주되지 않는 정보

해당사항 없음

9.4.4. 개인정보보호 의무

인증센터는 개인정보 보호법 등 관련 법령상의 개인정보보호 규정을 준수하며 인증센터의 개인정보처리방침에 따라 개인정보를 수집·보유·처리하여야 한다.

9.4.5. 개인정보 이용에 대한 통지와 동의

개인정보 보호법 등 관련 법령상의 개인정보보호 규정을 준수하며, 홈페이지와 신청서를 통해 개인정보 이용에 대해 통지하고 정보주체의 동의를 구하여야 한다.

9.4.6. 사법 또는 행정 절차에 따른 공개

인증센터와 등록기관 및 원격등록기관은 인증업무 수행과정에서 얻게 되는 가입자에 관한 정보 및 인증기관 운영과정에서 생성되는 중요 자료에 대해 법원의 명령과 같은 특별한 경우를 제외하고는 인증업무 이외의 목적으로는 이용하거나 공개하지 않는다.

9.4.7. 기타 정보 공개

해당사항 없음

9.5. 지적재산권

교육행정전자서명 인증체계로부터 발생한 모든 지적재산권은 교육부에 있다.

9.6. 보증

9.6.1. 인증센터 보증

인증센터는 발급한 인증서와 관련하여 다음 각 호의 내용을 보증하여야 한다.

- 인증서에 포함된 내용은 인증센터에 등록된 사실
- 인증서는 「전자정부법」 및 시행령, 「행정전자서명 인증업무지침」 및 「교육부 행정전자서명 인증업무지침」 등을 준수하여 발급된 사실
- 인증서 폐지목록 및 인증서 상태확인의 정확성

9.6.2. 등록기관 및 원격등록기관 보증

등록기관 및 원격등록기관은 등록기관 및 원격등록기관 인증업무와 관련하여 국내의 관련 법, 법령, 시행규칙 및 인증업무준칙(CPS)을 준수하여야 한다.

9.6.3. 가입자 보증

가입자는 교육행정전자서명 인증서비스의 이용을 위해서는 정확한 정보를 제공하여야 한다.

가입자는 다음과 같은 인증서를 사용하면 안 된다.

- 유효기간이 경과된 인증서
- 가입자 소관이 아닌 인증서
- 폐지된 인증서
- 행정전자서명생성키가 분실·도난·유출 또는 훼손된 인증서

9.6.4. 신뢰당사자 보증

해당사항 없음

9.6.5. 기타 참여자 보증

해당사항 없음

9.7. 보증의 철회

해당사항 없음

9.8. 책임의 제한

해당사항 없음

9.9. 면책 사항

가입자는 인증서 사용과 공개에 있어 다음과 관련되어 발생되는 손해와 손실 등에

대해 인증센터와 등록기관 및 원격등록기관의 면책을 보장한다.

- 가입자가 잘못 표현했거나 허위로 제공한 사실
- 가입자가 태만, 또는 고의로 제공하지 않은 변경된 사실
- 가입자의 행정전자서명생성키 및 인증서 관리 부주의 등(키 노출, 분실, 변조 등)

인증센터는 국내의 관련 법, 법령, 시행규칙 및 본 준칙에서 정한 사항 이외의 사유로 인한 손해에 대하여 책임을 지지 않으며 가입자와 사용기관간 발생한 문제를 중재하지 않는다.

또한 전쟁, 천재지변 등 불가항력적인 사유로 인한 인증업무 처리지연 또는 처리 불능으로 인한 손해에 대하여 책임을 지지 않는다.

9.10. 유효기간 및 종료

9.10.1. 유효기간

본 교육부 행정전자서명 인증업무준칙은 인증센터 홈페이지 게시를 기점으로 효력을 발생한다.

9.10.2. 종료

본 교육부 행정전자서명 인증업무준칙은 개정된 교육부 행정전자서명 인증업무준칙으로 대체될 때까지 유효하다.

9.10.3. 종료 후 효력

본 교육부 행정전자서명 인증업무준칙이 개정될 경우에도 중요 정보에 대한 책임은 유효하다.

9.11. 의사소통 및 통지

교육부 행정전자서명 인증업무준칙은 인증센터 홈페이지에 게시하여야 한다.

교육부 행정전자서명 인증업무준칙에 대한 의견은 아래의 연락처로 서면 제출할 수 있다.

- URL : www.epki.go.kr
- 이메일 : epkihelp@keris.or.kr

9.12. 개정

9.12.1. 개정 절차

인증업무준칙의 변경이 필요한 경우에는 인증센터장의 사전 승인을 받아 개정하여야 한다. 인증업무준칙의 정책과 무관한 사소한 변경이나 오류 정정 등의 사유가 있는 경우에는 사전 승인 없이 개정할 수 있다.

9.12.2. 개정 공지

인증업무준칙의 변경이 발생한 경우에는 인증센터 홈페이지(www.epki.go.kr)에 개정사항을 게시하여야 한다.

9.12.3. 인증정책 식별명(OID)의 변경사항

해당사항 없음

9.13. 분쟁해결

당사자들은 법적 소송 등 분쟁 해결 절차를 진행하기 전, 인증센터에 분쟁내용을 알리고 분쟁해결을 위해 노력하여야 한다.

9.14. 준거법

인증업무준칙은 국가의 관련법을 준수하며 상충될 경우에는 상위법을 따른다.

9.15. 관련 법률의 준수

인증업무준칙은 전자정부법 및 관련 법령을 준수하여야 한다.

9.16. 별도 부칙

해당사항 없음

9.17. 기타 조항

9.17.1. 인증센터의 책임 및 의무

- 인증센터는 인증업무 수행 시 국내의 관련 법, 법령, 시행규칙 및 인증업무준칙(CPS)을 준수하여야 한다.
- 인증센터는 인증서의 신뢰성이나 유효성에 영향을 미칠 수 있는 다음과 같은 정보를 누구든지 그 사실을 항상 확인할 수 있도록 지체 없이 공고하여야 한다.
  - 인증센터에 대한 정보
  - 가입자 인증서 및 인증서 폐지목록 정보
  - 그 밖에 인증업무 수행관련 정보 등
- 인증센터는 교육부 인증기관용 행정전자서명생성키를 안전하게 저장·관리하여야 하며, 행정전자서명생성키의 안전성이 취약하다고 판단될 경우에는 행정전자서명 인증관리센터로부터 인증서를 재발급 받아야 한다. 이 때, 인증서를 재발급 받은

인증기관은 신규 인증서를 활용하여 기존에 발급한 등록기관 및 가입자 인증서를 모두 재발급하여야 한다.

- 인증센터는 교육부 인증기관용 행정전자서명생성키가 분실·훼손 또는 도난·유출된 경우, 즉시 행정전자서명 인증관리센터에 통보하고 인증업무의 안전과 신뢰성을 확보할 수 있는 대책을 마련하여야 한다.
- 인증센터는 교육부 인증기관용 행정전자서명생성키가 분실·훼손 또는 도난·유출된 경우, 즉시 행정전자서명 인증관리센터에 통보하고 인증업무의 안전과 신뢰성을 확보할 수 있는 대책을 마련하여야 한다.
- 인증센터는 다음 각 호에 해당하는 인증업무에 관한 기록을 안전하게 보관·관리하여야 한다.
  - 인증서 신청, 발급, 폐지 등에 관한 사항
  - 인증서
  - 인증서 폐지목록
  - 인증서 폐지 관련 정보(폐지결정자, 폐지 사유 등)
  - 교육부 인증기관용 행정전자서명생성키 생성 및 관리에 관한 사항
  - 그 밖에 인증업무 관련 사항
- 인증센터는 인증업무 관련 기록의 안전성 및 신뢰성을 위하여 주기적으로 백업정책 및 감사기록 점검 계획을 수립하고 이를 시행하여야 한다.
- 인증센터는 인증업무 수행과정에서 얻게 되는 가입자 정보 및 인증기관 운영과정에서 생성되는 중요자료에 대해 법원의 명령과 같은 특별한 경우를 제외하고는 인증업무 이외의 목적으로 이용하거나 공개하지 말아야 한다.
- 인증센터는 인증업무 수행과정에서 얻게 되는 가입자 정보를 「개인정보보호법」에 따라 보호하여야 한다.
- 인증센터는 신청서 내 필수기재정보의 누락, 부적격자의 신청 등 특정한 사유가 있는 경우 이외에는 인증서 발급, 재발급, 효력정지 및 효력 회복, 폐지 신청을 거부할 수 없으며 거부할 경우에는 그 사유를 밝혀야 한다.

9.17.2. 등록기관 및 원격등록기관의 책임 및 의무

- 등록기관 및 원격등록기관은 인증업무와 관련하여 국내의 관련 법, 법령, 시행규칙 및 인증업무준칙(CPS)을 준수하여야 한다.
- 등록기관 및 원격등록기관은 인증센터로부터 발급받은 인증서의 행정전자서명생성키가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리하여야 하며, 이를 위한 인증서 저장매체 관리에 관한 사항은 「교육부 정보보안 기본지침」의 PC 보안관리 및 휴대용 저장매체 보안관리 관련 규정에 따른다.
- 등록기관 및 원격등록기관은 인증서 발급, 재발급, 효력정지 및 효력회복, 폐지 신청서를 접수하여 교육행정전자서명 등록시스템에 그 사실을 입력하여 관리하여야 한다.

- 등록기관 및 원격등록기관은 신청서 내 필수기재정보의 누락, 부적격자의 신청 등 특정한 사유가 있는 경우 이외에는 인증서 발급, 재발급, 효력정지 및 효력 회복, 폐지 신청을 거부할 수 없으며 거부할 경우에는 그 사유를 밝혀야 한다.
- 등록기관 및 원격등록기관은 인증업무 수행과정에서 얻게 되는 가입자에 관한 정보 및 인증기관 운영과정에서 생성되는 중요 자료에 대해 법원의 명령과 같은 특별한 경우를 제외하고는 인증업무 이외의 목적으로 이용하거나 공개하면 안 된다.
- 등록기관 및 원격등록기관은 인증업무 수행과정에서 얻게 되는 가입자 정보를 「개인정보 보호법」에 따라 보호하여야 한다.
- 등록기관 및 원격등록기관은 인증기관에서 인증 관련 사항을 요구할 경우에는 해당 자료를 제공하여야 한다. 원격등록기관은 등록기관에서 인증 관련 사항을 요구할 경우에는 해당 자료를 제공하여야 한다.
- 등록기관 및 원격등록기관은 인증서 등록업무와 관련하여 다음에 대한 보증 책임이 있다.
  - 신청서에 기재된 정보의 확인
  - 등록시스템에 입력하는 정보의 정확성

9.17.3. 가입자 책임 및 의무

- 가입자는 다음의 경우에는 정확한 정보 및 사실만을 등록기관 또는 원격등록기관에 제공하여야 한다.
  - 인증서 발급, 재발급, 효력정지 및 효력회복, 폐지 신청
  - 인증서에 기재된 가입자 정보의 변경 등
- 가입자는 교육행정전자서명생성키, 인증서, 저장매체(USB, 스마트폰, 스마트카드, 보안토큰 등) 등이 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리하여야 한다.
- 가입자는 인증센터로부터 발급받은 인증서의 유효기간, 용도, 발급기관 등을 확인하고, 인증서의 발급용도(이용범위) 내에서만 인증서를 사용하여야 한다.
- 가입자는 행정전자서명생성키의 분실·훼손 또는 도난·유출 등 인증서 관련 보안사고가 발생한 경우, 시스템 변경 등으로 인증서를 사용하지 않을 경우에는 해당 사실을 즉시 인증센터에 통보하여야 한다.
- 가입자는 「교육부 행정전자서명 인증업무지침」 등 관련 법령 및 인증업무준칙에서 정한 의무 위반 또는 인증서와 관련하여 허위 또는 잘못된 정보의 제공, 인증서 관리 부주의로 인하여 발생되는 손해와 손실 등에 대한 책임을 져야 한다.

9.17.4. 사용기관 책임 및 의무

- 사용기관은 인증센터 가입자 인증서를 신뢰하고자 하는 경우에는 당해 인증서 유효기간, 발급기관, 이용범위 및 용도, 진정성 등을 확인하여야 한다.
- 인증서를 사용하기 전에 인증서 폐지여부 등을 확인하여 유효기간 만료 또는 폐지된

인증서를 사용하여서는 안 된다.

- 인증센터에서 발급한 인증서를 신뢰하고자 하는 경우에는 당 인증서가 사용목적에 적합한가를 판단하여야 하며, 사용기관 오판 등으로 인한 피해는 사용기관 책임이다.

9.17.5. 교육행정전자서명 인증서처리프로그램

교육부장관은 전자문서의 보안성 확보 또는 사용자 신원확인을 위해 인증서를 적용할 경우에는 인증서처리프로그램을 개발·보급하며 이에 대한 기술적 제반 사항을 지원할 수 있다.

인증서처리프로그램 보급 대상은 본 문서의 4.1.1. 대상자에 한하며, 인증센터는 인증서처리프로그램 사용요청 기관의 적용대상시스템 환경 및 사용요청에 대한 적합성 여부를 검토한 후 사용요청기관에 인증서처리프로그램을 제공하여야 한다.