

●정보통신부고시 제2003-51호

전자서명법 제8조의 규정에 의거 전자서명인증업무지침(정보통신부
고시 제2002-46호, 2002.11.15)을 다음과 같이 개정 고시합니다.

2003. 11. 27.

정보통신부장관

전자서명인증업무지침개정

전자서명인증업무지침을 다음과 같이 개정한다.

전자서명인증업무지침

제1장 총 칙

제1조(목적) 이 지침은 전자서명법(이하 “법”이라 한다) 제8조의 규정에
의하여 공인인증업무의 안전성과 신뢰성 확보를 위해 공인인증기관
이 비대칭 암호화 방식의 전자서명기술을 이용한 공인인증업무를
수행함에 있어 지켜야 할 구체적 사항을 정함을 목적으로 한다.

제2조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. “공인인증시스템”이라 함은 가입자의 등록정보 관리, 전자서명키
생성·관리, 공인인증서 생성·발급·관리, 시점확인 기능 등을 지
원하는 시스템으로서 공인인증역무를 위하여 공인인증기관 내에
설치된 시스템을 말한다.
2. “비대칭 암호화 방식”이라 함은 정보를 암호화하기 위하여 사용

하는 키와 암호화된 정보를 복원하기 위하여 사용하는 키가 서로 다른 암호화 방식을 말한다.

3. “전자서명검증키”라 함은 전자서명을 검증하기 위하여 이용하는 전자적 정보를 말한다.
4. “전자서명생성키”라 함은 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.
5. “전자서명키”라 함은 전자서명생성키와 이에 합치하는 전자서명검증키를 말한다.
6. “등록대행기관”이라 함은 공인인증기관을 대신하여 가입자에 대한 신원확인을 수행하고 공인인증서 발급, 효력정지, 효력회복 또는 폐지 등의 신청을 접수·등록하는 자를 말한다.
7. “가입자등록정보”라 함은 공인인증서 신청서, 신청인이 신원확인을 위해 공인인증기관에게 제출한 서류 및 제시한 증명서 등의 사본 그리고 기타 공인인증서 신청에 필요한 전자적 기록 등을 말한다.
8. “네트워크안전운영시스템”이라 함은 침입차단시스템, 침입탐지시스템, 네트워크관리시스템 등 네트워크를 안전하게 운영하기 위한 시스템을 말한다
9. “갱신발급”이라 함은 인증서의 유효기간 만료에 따라 만료 시점 이전에 유효기간을 연장하여 인증서를 발급하는 것을 말한다.
10. “재발급”이라 함은 가입자의 전자서명생성키가 분실·훼손 또는 도난·유출된 경우 해당 인증서를 폐지하고 새로운 전자서명키를 생성하여 인증서를 발급하는 것을 말한다.

11. "변경발급"이라 함은 인증서 소유자의 식별명칭(이하 "DN"이라 한다) 등 인증서 내의 가입자 정보가 변경된 경우 해당 정보를 변경하여 인증서를 발급하는 것을 말한다.

제3조(적용범위) 이 지침은 비대칭 암호화 방식의 전자서명기술을 이용한 공인인증업무에 적용한다.

제2장 공인인증서 관리

제4조(등록정보의 전송) 공인인증기관은 등록대행기관으로부터 공인인증서를 발급받고자 하는 자의 등록정보를 정보통신망을 통하여 전송받는 경우, 당해 등록정보에 대해 등록대행기관의 공인전자서명 및 공인인증기관의시설및장비등에관한규정 제5조제1항제3호의 암호알고리즘에 따른 암호화를 적용하여야 한다. 단, 등록대행기관과의 약정에 따라 공인전자서명외의 전자서명을 이용하는 경우에는 공인인증기관의시설및장비등에관한규정 제5조제1항제1호의 전자서명 알고리즘을 사용하여야 한다.

제5조(공인인증서 발급신청) ①공인인증기관은 공인인증서를 발급받고자 하는 자 또는 가입자로부터 공인인증서의 신규발급·갱신발급·재발급·변경발급 등의 신청이 있는 경우, 법 제15조제6항에서 정하는 신원확인 절차를 준수하여야 하며 당해 신청내용의 무결성을 확인하여야 한다.

②공인인증기관은 제1항의 갱신발급 또는 변경발급 신청의 경우, 당해 가입자에 한하여 공인전자서명을 이용하여 신원확인 및 신청내

용의 무결성을 확인할 수 있다.

③제2항의 규정에 의해 공인전자서명을 이용하여 변경발급 신청에 대한 신원확인 및 신청내용의 무결성을 확인하는 경우, 주민등록표 등본, 법인등기부등본 등 관련 자료를 활용하여 신뢰할 수 있는 방법으로 변경된 정보의 정확성을 확인하여야 한다.

제6조(공인인증서 생성) ①공인인증기관은 전자서명생성키가 공인인증서를 발급받고자 하는 자에게 속한다는 사실을 확인하여야 하며, 공인인증서를 발급받고자 하는 자의 전자서명검증키에 대한 유일성 여부를 확인하여야 한다.

②공인인증기관은 공인인증서를 생성하는 경우 정보통신망이용촉진 및정보보호등에관한법률 제52조의 규정에 의한 한국정보보호진흥원(이하 “보호진흥원”이라 한다)으로부터 인증받은 전자서명검증키에 합치하는 전자서명생성키로 당해 공인인증서에 공인전자서명하여야 한다.

③공인인증기관은 공인인증서를 가입자에게 발급하는 경우 이를 저장소에 공고하여야 한다.

제7조(공인인증서 효력정지·효력회복·폐지 등의 신청) ①공인인증기관은 가입자로부터 공인인증서 효력정지·효력회복·폐지 등의 신청이 있는 경우, 법 제15조제6항에서 정하는 신원확인 절차를 준수하여야 하며 당해 신청내용의 무결성을 확인하여야 한다. 단, 효력정지 또는 폐지 신청의 경우에는 공인전자서명을 이용하여 신원확인 및 신청내용의 무결성을 확인할 수 있다.

②공인인증기관은 가입자가 전자서명생성키 분실·훼손 또는 도난·유출 등으로 긴급하게 해당 공인인증서 폐지를 신청하는 때에는 사전에 등록된 2 이상의 개인정보를 확인하는 등의 신뢰할 수 있는 방법을 통하여 당해 가입자의 본인여부를 확인하고 해당 신청을 처리할 수 있다.

③공인인증기관은 가입자의 공인인증서 효력회복 신청이 있는 경우, 효력이 정지된 날부터 6월 이내에 신청한 것인지 여부를 확인하여야 한다. 또한 공인인증기관은 가입자의 공인인증서가 효력이 정지된 날부터 6월이 지난 경우 이를 폐지하여야 한다.

제8조(공인인증서 효력정지 및 폐지목록 생성) ①공인인증기관은 가입자의 공인인증서를 효력정지·효력회복·폐지하는 경우 공인인증서 효력정지 및 폐지목록을 생성하여야 한다. 이 경우 공인인증기관은 보호진흥원으로부터 인증받은 전자서명검증키에 합치하는 전자서명생성키로 당해 공인인증서 효력정지 및 폐지목록에 공인전자서명하여 이를 저장소에 공고하여야 한다.

②공인인증기관은 가입자의 공인인증서를 효력정지·효력회복·폐지한 때에는 그 사실을 확인할 수 있도록 지체없이 필요한 조치를 취하여야 한다.

제9조(공인인증서 공고 및 유효성 확인 서비스) ①공인인증기관은 이용자가 공인인증서와 공인인증서 효력정지 및 폐지목록을 항상 확인할 수 있도록 저장소를 운영하여야 한다.

②공인인증기관은 이용자가 공인인증서의 유효성을 확인할 수 있도록

록 공인인증서 유효성 확인 서비스를 제공하여야 한다

제3장 전자서명키 관리

제10조(전자서명키 생성) ①공인인증기관은 공인인증기관의시설및장비 등에관한규정 제5조제1항제1호의 전자서명 알고리즘에 따라 전자서명키를 생성하여야 한다.

②공인인증기관은 자신의 전자서명키를 생성하는 경우 3인 이상의 권한 있는 직원이 공동으로 이를 수행하여야 한다.

③공인인증기관이 공인인증서를 발급받고자 하는 자의 전자서명키를 생성하는 경우 2인 이상의 권한 있는 직원이 공동으로 이를 수행하여야 한다.

제11조(전자서명생성키 보호) ①공인인증기관은 공인인증기관의시설및 장비등에관한규정의 **[별표]** 공인전자서명인증체계 기술규격중 6.4의 전자서명키 보호기술 규격을 만족하는 보안 모듈을 이용하여 자신의 전자서명생성키를 보호하여야 한다.

②공인인증기관은 공인인증서를 발급받고자 하는 자의 전자서명키를 생성한 경우 공인인증기관의시설및장비등에관한규정 제5조제1항제3호의 암호 알고리즘에 따라 이를 암호화하여 저장장치에 저장하고, 전자서명생성키의 무결성 보장을 위하여 메시지 인증코드(MAC)등의 정보를 함께 저장하여 이를 가입자에게 직접 전달하여야 한다. 이 경우 공인인증기관은 전자서명키 생성·관리 설비의 기억장소 또는 임시파일에 남아있는 전자서명생성키 및 관련정보를 즉시 삭제

제하여야 한다.

제12조(전자서명생성키 백업) ①공인인증기관은 전자서명생성키 훼손 등으로부터 공인인증업무 제공의 지속성을 보장하기 위하여 전자서명생성키를 백업하여야 한다.

②공인인증기관은 자신의 전자서명생성키를 백업하는 경우 제11조 제1항에서 규정하는 안전성을 보장하여야 한다.

③공인인증기관은 백업된 전자서명생성키를 전자서명생성키의 원본과 분리하여 2부를 작성한 후, 1부는 공인인증업무를 수행하는 시설에 보관하고, 1부는 공인인증업무를 수행하는 시설로부터 10km이상의 원격지 저장설비에 안전하게 보관하여야 한다.

제13조(전자서명생성키 파기) 공인인증기관은 관리책임자 및 보안관리자의 입회 하에 백업된 전자서명생성키와 그 원본을 안전하게 파기하여야 한다.

제14조(전자서명생성키 분실·훼손 또는 도난·유출) 공인인증기관은 자신의 전자서명생성키가 분실·훼손 또는 도난·유출된 경우 모든 이용자가 이 사실을 알 수 있도록 홈페이지 게시 등 적절한 조치를 취하여야 한다.

제4장 기타 공인인증업무

제15조(시점확인 기능의 제공) 공인인증기관은 가입자 또는 이용자가 전자문서에 대한 시점확인을 신청하는 경우, 시점확인서비스를 제공할 수 있다.

제16조(시각수신 및 시각보정) 공인인증기관은 시점확인 시 정확한 시각정보를 제공하기 위하여 시각수신 장비를 운영하여야 하며, 시점확인 시스템의 시각보정 기능을 지속적으로 사용하여야 한다. 아울러 시각보정 기능에 오류가 발생한 경우에는 시점확인서비스를 즉각 중단하여야 한다.

제17조(시점확인 기록의 보관) 공인인증기관은 시점확인토큰 등 시점확인업무와 관련한 기록을 안전하게 보관하여야 한다.

제18조(전자문서의 보관) ①공인인증기관은 시점확인 신청자의 요청이 있는 경우 시점확인 대상이 되는 전자문서 또는 전자서명을 보관할 수 있다.

②제1항의 규정에 의해 시점확인 대상이 되는 전자문서를 보관하는 경우 해당 전자문서를 공인인증기관의시설및장비등에관한규정 제5조제1항제3호의 암호알고리즘에 따라 암호화하여 권한없는 사용자가 내용을 열람할 수 없도록 하여야 한다.

제19조(시점확인 기록 등의 백업) 공인인증기관은 제17조 및 제18조의 규정에 의해 시점확인 기록 등을 보관하는 경우 해당 기록을 백업한 후, 공인인증업무를 수행하는 시설로부터 10km 이상의 원격지 저장설비에 안전하게 보관하여야 한다.

제20조(기타 부가업무) 공인인증기관은 시점확인 이외에도 공인전자서명을 이용하여 부가업무를 수행할 수 있다.

제5장 기타 운영관리

제21조(기술규격의 준수) 공인인증기관은 공인인증업무 수행 시 공인인증기관의시설및장비등에관한규정 **별표의** 전자서명인증체계 기술규격을 준수하여야 한다.

제22조(공인인증서의 이용범위 및 용도 준수) 공인인증기관은 보호진흥원으로부터 발급받은 공인인증서의 사용 시 해당 공인인증서에 명시된 이용 범위 및 용도에 따라 공인인증서를 사용하여야 한다.

제23조(공인인증업무 절차의 준수) ①공인인증기관은 공인인증업무의 절차 및 방법이 변경된 경우 이를 공인인증업무준칙 및 내부규정에 반영하여야 하며, 다음 각호의 사항을 포함한 제·개정 관련 기록을 유지·관리하여야 한다.

1. 개정 사유

2. 제·개정된 모든 규정

②공인인증기관이 다음 각호의 시스템을 설치·운영 및 유지·보수하는 경우에는 2인 이상의 직원이 공동으로 이를 수행하여야 한다.

1. 가입자의 등록정보관리 기능을 지원하는 시스템

2. 공인인증서 생성·발급·관리 기능을 지원하는 시스템

3. 시점확인 기능을 지원하는 시스템

제24조(시설 및 장비에 관한 사항) ①공인인증기관은 공인인증기관 지정 시 심사를 받은 시설 및 장비를 이용하여 공인인증업무를 수행하여야 한다.

②공인인증기관은 공인인증업무 수행을 위한 시설 및 장비의 변경이 필요한 경우 이를 정보통신부장관에게 신고하여 변경 내용의 적

절성을 확인받은 후 공인인증업무에 적용하여야 한다. 단, 침해사고, 자연재해, 시스템 오류 등으로 인하여 긴급한 조치가 필요한 경우에는 변경 내용을 미리 적용할 수 있으며 적용 후 7일 이내에 신고하여야 한다.

③제2항의 규정에 의해 시설 및 장비의 변경 사항을 신고함에 있어 다음 각호의 사항과 관련된 시설 및 장비의 변경에 대해서는 신고 대상에서 제외한다.

1. 주기적인 운영체제 패치 또는 업그레이드
2. 기존 설비의 부하분산 및 성능향상을 위한 CPU, 하드디스크, 메모리 등의 하드웨어 추가 또는 교체
3. 공인인증업무의 안전성을 해치지 않는 범위 내에서 전기설비, 방음설비 등의 물리적 설비 추가 또는 교체

③공인인증기관은 공인인증업무수행을 위한 시설 및 장비를 변경한 경우 해당 사실을 기록·유지하여야 한다.

④공인인증기관은 다음 각호의 시설 및 장비에 대하여 형상관리를 하여야 한다.

1. 공인인증시스템 및 가입자 소프트웨어
2. 네트워크 구성 및 장비
3. 네트워크안전운영시스템 및 서버 관리시스템
4. 출입통제 관련 시스템
5. 기타 운영시스템

⑤공인인증기관은 가입자 소프트웨어 배포 시 당해 소프트웨어에

대하여 무결성을 보장할 수 있는 전자서명 또는 해쉬값 등을 관리하여야 한다.

제25조(공인인증업무 기록의 관리) ①공인인증기관은 다음 각호의 기록을 공인인증서 효력이 소멸된 날로부터 10년 동안 보관하여야 한다.

1. 공인인증서 신청(발급/효력정지/효력회복/폐지) 및 처리에 관한 기록
2. 신청인이 신원확인을 위해 공인인증기관에게 제출한 서류 및 제시한 증명서 등의 사본
3. 공인인증서
4. 공인인증서 효력정지 및 폐지목록
5. 공인인증서폐지에 관한 정보

가. 공인인증서폐지가 법 제18조제1항제2호 내지 제4호의 규정에 의하여 발생한 경우 이를 결정한 자의 성명, 주민등록번호가 기재된 인증서폐지사유에 관한 기록

6. 공인인증기관이 가입자의 전자서명키를 생성한 경우 전자서명키의 생성에 관한 기록과 가입자의 전자서명키 수령서
7. 공인인증기관의 전자서명키 생성 및 관리에 관한 기록

②제1항 각호의 자료 중 종이문서는 마이크로필름으로, 전자적인 정보는 광디스크 등의 정보저장매체로 보관할 수 있다.

③공인인증기관이 정보통신망을 통하여 공인인증서 갱신발급·변경발급·효력정지 및 폐지 신청을 받는 경우에는 제1항제1호의 공인인증서 신청 기록을 가입자의 공인전자서명이 첨부된 전자문서로

보관할 수 있다.

④공인인증기관은 제1항의 규정에 의한 기록을 공인인증업무를 수행하는 시설과 해당 시설로부터 10Km이상의 원격지 저장설비에 각각 1부씩 보관하여야 한다.

제26조(공인인증업무 기록 관리의 대행) ①등록대행기관이 불가피한 사유로 등록업무 관련 기록을 자체보관 하여야 하는 경우, 공인인증기관은 등록대행기관의 요청에 의해 제25조제1항제1호 및 제2호의 기록은 등록대행기관이 보관토록 할 수 있다. 단, 공인인증기관의 요청이 있는 경우 등록대행기관으로 하여금 관련 기록을 제출하도록 하여야 한다.

②제1항의 규정에 의해 제25조제1항제1호 및 제2호의 기록을 등록대행기관에서 보관하는 경우 공인인증기관은 다음 각호의 정보를 등록대행기관의 공인전자서명이 첨부된 전자문서로 전송받아 제25조에 따라 보관하여야 한다. 단, 등록대행기관과의 약정에 따라 공인전자서명외의 전자서명을 이용하는 경우에는 공인인증기관의시설 및장비등에관한규정 제5조제1항제1호의 전자서명 알고리즘을 사용하여야 한다.

1. 신원확인 정보

가. 가입자 이름(성명 또는 법인명)

나. 가입자 식별번호(주민등록번호 또는 사업자등록번호 등)

다. 기타 필요한 정보

2. 인증서 발급을 위한 기본정보

가. 신청 인증서의 종류

나. 신청 구분(신규/갱신/재발급, 효력정지/회복 또는 폐지)

다. 기타 필요한 정보

③제1항의 규정에 의해 공인인증기관이 등록대행기관에게 기록의 보관을 위임하는 경우, 공인인증기관은 등록대행기관으로 하여금 기록 보관을 위해 사무공간과 분리되어 있고 출입통제장치가 설치되어 있는 별도의 공간에 잠금장치가 있는 캐비닛 또는 금고를 구비하도록 하여야 한다.

제27조(감사기록의 관리) 공인인증기관은 다음 각호의 감사기록의 이 상유무를 확인하여야 한다.

1. 공인인증업무 운영과 관련된 기록
2. 공인인증시스템, 출입통제 시스템, 네트워크 보안 시스템에서 생성되는 기록

제28조(등록대행기관의 관리) 공인인증기관은 등록대행기관에게 등록 업무를 위임하는 경우 다음 각호의 사항을 1년마다 1회이상 점검하여야 한다. 단, 모든 등록대행기관이 2년에 1회이상 점검받을 수 있도록 하여야 한다.

1. 공인인증서 신청인의 신원확인 업무
2. 공인인증서 신청서의 접수·등록 업무
3. 공인인증기관에게 가입자의 등록정보를 안전하게 전달. 단, 제26조제1항의 규정에 의해 제25조제1항제1호 및 제2호의 기록 보관을 대행하는 경우에는 기록 보관 업무를 점검

4. 등록시스템의 관리

가. 공인인증서 발급정책에 따른 DN 부여

나. 공인인증기관에서 생성한 참조번호 및 인가코드의 출력

다. 등록시스템 접근통제 등 보안기능

5. 등록업무 수행과 관련한 개인정보의 보호

6. 기타 공인인증업무와 관련하여 공인인증기관이 위탁한 업무

제29조(공인인증업무의 시험운영) ①공인인증기관은 공인인증업무 개시 전 보호진흥원이 정하는 바에 따라 시험운영을 실시하여야 하며, 해당 시험운영 결과를 보호진흥원에 제출하여야 한다.

②보호진흥원은 제1항의 규정에 의하여 접수한 시험운영 결과에 대한 검토의견을 정보통신부장관과 해당 공인인증기관의 장에게 송부한다.

③보호진흥원은 공인인증기관이 시험운영 결과 정상적인 운영이 가능하다고 판단되는 경우 공인인증업무 수행을 위한 공인인증서를 발급한다.

제30조(정확한 정보제공 및 공고) ①공인인증기관은 보호진흥원에 다음 각호의 정보를 신청하는 경우 해당 신청서식에 정확한 정보 및 사실을 기재하여야 한다.

1. 공인인증서 발급신청

2. 공인인증서 효력정지 및 폐지 신청

3. 공인인증서 효력회복 신청

②공인인증기관은 공인인증서의 신뢰성이나 유효성에 영향을 미칠

수 있는 다음 각호의 정보를 누구든지 항상 확인할 수 있도록 지체 없이 공고하여야 한다.

1. 공인인증기관의 지정
2. 공인인증기관의 인증업무 휴지·정지 또는 폐지
3. 공인인증기관의 지정취소
4. 공인인증기관의 양도·양수 또는 합병
5. 공인인증서에 대한 정보
 - 가. 가입자의 공인인증서
 - 나. 가입자의 공인인증서 효력정지 및 폐지목록 등
6. 기타 공인인증업무 수행관련 정보

부 칙

- ①(시행일) 이 지침은 고시한 날부터 시행한다.
- ②(경과조치) 제11조제1항의 보안모듈 이용 규정은 종전 규정에도 불구하고 2004년 11월 15일부터 시행한다.
- ③(원격지 저장설비에 관한 경과조치) 제12조제3항, 제19조 및 제25조제4항의 규정이 정하는 원격지 저장설비 기준 중 10km 이상에 대한 사항은 2003년 11월 15일부터 시행한다.
- ④(가입자등록서류 보관의 경과조치) 이 고시 이전에 등록대행기관이 신원확인하고 보관하는 있는 가입자 등록서류에 대해서는 이 고시 제 26조에 따라 보관된 것으로 본다