전자서명인증업무준칙

Certification Practice Statement

v1.23

2024년 1월

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

1. 소 개

1.1 개 요

인터넷 등 개방형 정보통신망을 이용하여 처리되는 전자문서의 안전·신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명인증관리체계 및 국가 전체의 공개키 기반 구조 구축·운영에 관한 기본적인 사항을 정함으로써 국가 사회 정보화를 촉진하고, 국민생활의 편익을 증진함을 목적으로 1999년 2월 5일 전자서명법(법률 제5792호)이 제정되어 1999년 7월 1일부터 시행되고 있다.

본 문서는 RFC 3647을 기준으로 작성되었으며, 인터넷진흥원 전자서명인증관리센터에서 운영하는 최상위인증기관 운영 및 관리에 관한 전자서명인증업무준칙을 다룬다.

1.2 문서명 및 식별

본 문서의 명칭은 「전자서명인증업무준칙」으로 전자서명법(개정 2020. 6. 9.), 동법 시행령(시행 2017. 7. 26.), 동법 시행규칙(시행 2017. 7. 26.)을 준수한다. 이하 언급되는 전자서명법령의 조항은 해당 일자의 법령의 조항을 의미하고, 현행 법령의 준수가 필요한 경우, 현행 법령으로 명시하도록 한다.

전자서명인증업무준칙은 한국인터넷진흥원의 인증서 정책, 인증서 발급·관리, 보안통제, 기타 운영 정책·절차 등 전자서명인증과 관련된 업무에 관하여 필요한 사항 및 인터넷진흥원과 공인인증기관 등의 책임·의무에 관한 사항을 정함을 목적으로 한다.

KISA Certificate Policies OID : npki-cp {1 2 410 200004 2}

1.3 공인전자서명인증체계 관련자

1.3.1 전자서명인증관리센터

전자서명인증관리센터는 전자서명법 제10조, 제12조 및 제25조의 규정에 의하여 전자서명인증관리체계에서 최상위인증기관의 임무와 역할을 수행하기 위하여 다음과 같은 업무를 수행한다.

o 안전한 전자서명인증관리체계의 구축운영
o 인증업무를 폐지한 공인인증기관의 가입자인증서등 인수

o 지정이 취소된 공인인증기관의 가입자인증서등 인수
o 전자서명 인증기술의 개발 및 보급
o 상호인정 등 국제협력 지원
o 기타 전자서명 인증과 관련된 업무
o 공인인증기관의 전자서명검증정보에 대한 인증 등 인증업무 수행
o 공인인증서 효력정지 및 폐지목록 발급
o 시점확인 서비스

1.3.2 공인인증기관

공인인증기관은 전자서명법 제4조의 규정에 의하여 지정받은 국가기관·지방자치단체 또는 법인으로서 가입자에게 다음과 같은 공인인증역무를 제공한다. 다만 전자서명법 제5조의 결격사유에 해당하는 자는 공인인증기관으로 지정받을 수 없다.

o 신원확인
o 공인인증서 발급
o 공인인증서 효력정지 및 폐지
o 공인인증서 갱신
o 공인인증서 관련 정보 공고
o 시점확인 서비스 등

1.3.3 등록대행기관

공인인증기관은 전자서명인증업무지침에 따라 등록대행기관을 운영 및 관리할 수 있으며, 전자서명인증관리센터는 별도의 등록대행기관을 운영 및 관리하지 않는다.

1.3.4 가입자

전자서명법 제4조의 규정에 의하여 지정된 공인인증기관만이 개인 및 법인에게 인증서를 발급한다.

1.3.5 신뢰당사자

신뢰당사자는 전자서명인증관리센터에서 발급한 인증서를 신뢰하고 사용하는 자로서 다음과 같다.

o 공인인증기관
o 공인인증기관의 가입자
o 전자서명법 제27조의2의 규정에 의하여 상호인정을 체결한 국외 인증기관
o 전자서명법 제27조의2의 규정에 의하여 상호인정을 체결한 국외 인증기관의 가입자등

1.3.6 기타 참여자

해당사항 없음

1.4 공인인증서의 종류

1.4.1 공인인증서 이용범위 및 용도

전자서명인증관리센터가 발급한 인증서는 전자서명인증관리센터 또는 공인인증기관에서 소유하고 있는 전자서명생성정보에 합치한다는 사실을 확인 및 증명하기 위하여 사용된다.

전자서명법 제15조제4항 및 제25조제2항의 규정에 의하여 전자서명인증관리센터는 공인인증기관의 신청이 있는 경우, 다음과 같은 공인인증서를 발급할 수 있다.

인증서 구분	용도
공인인증기관용 인증서	가입자 공인인증서 발급
OCSP용 인증서	OCSP 응답에 대한 전자서명
시점확인용 인증서	시점확인 응답에 대한 전자서명

1.4.2 공인인증서 이용 제한

전자서명인증관리센터가 공인인증기관에게 발급한 공인인증서와 공인인증기관이 가입자에게 발급한 공인인증서는 발급 시의 이용범위 또는 용도 내에서만 이용되어야 한다. 또한 누구든지 공인인증서를 이용범위 또는 용도에 벗어나 부정하게 사용하여서는 아니 된다.

1.5 전자서명인증업무준칙의 관리

1.5.1 전자서명인증업무준칙 수립 및 개정 기관

전자서명인증관리센터는 전자서명인증업무준칙을 수립하고 개정한다.

1.5.2 수립 및 개정 담당자

전자서명인증관리센터의 인증업무에 관련한 연락처는 다음과 같다.

o URL : https://www.rootca.or.kr
o 전자우편 : rootca@kisa.or.kr
o 주소 : 서울시 송파구 중대로 135 IT벤처타워 서관 4층
o 전화 :(02)405-5457

1.5.3 수립 및 개정 담당기관

전자서명인증관리센터는 전자서명인증관리센터장이 전자서명인증업무준칙의 변경이 필요하다고 판단한 경우에 이를 개정한다.

전자서명인증관리센터는 다음의 내용을 포함한 전자서명인증업무준칙의 개정 관련 기록을 유지·관리한다.

o 전자서명인증업무준칙 버전
o 적용 업무 및 범위의 개요
o 전자서명인증업무준칙의 개정 기록
  - 개정된 기존 전자서명인증업무준칙의 규정
  - 개정 내용
  - 개정 사유 등

1.5.4 시행 절차

전자서명인증관리센터는 제·개정된 전자서명인증업무준칙을 전자서명인증관리센터 홈페이지에 공고하며 개별적으로 공인인증기관에게 통보한다.

제·개정된 전자서명인증업무준칙은 신고한 날로부터 시행한다.

1.6 정의 및 약어

o 최상위인증기관 : 전자서명법 제10조, 제12조 및 제25조의 규정에 의하여 전자서명인증관리체계에서 최상위인증기관의 임무와 역할을 수행하는 자

o 공인인증기관 : 공인인증역무를 제공하기 위해야 전자서명법 제4조의 규정에 의하여 지정된 자

o 가입자 : 공인인증기관으로부터 전자서명생성정보를 인증받은 자

o DN(Distinguished Name) : 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격을 준수하고, 인증서 발급자 및 인증서 소유자를 확인하기 위해 사용하는 이름 형식을 말한다.

o 신원확인 : 전자서명인증관리센터는 공인인증서의 신뢰성 확보를 위하여 공인인증서 발급, 갱신, 효력정지 및 폐지 등의 신청시 공인인증기관, 신청인 및 신청정보의 진정성 등을 확인하는 행위를 말한다.

o 실명 : 주민등록표상의 명의, 사업자등록증상의 명의 기타 금융실명거래 및 비밀보장에 관한 법률 시행령(대통령령 제26791호)에 정하는 실지명의를 말한다.

o 전자서명인증관리체계 : 인증서의 발급 및 인증관련 기록의 관리 등 인증역무를 제공하기 위한 체계를 말한다.

o 공인인증서 : 전자서명법 제15조의 규정에 따라 공인인증기관이 발급하는 인증서를 말한다.

o 공인인증업무 : 공인인증서의 발급, 인증관련 기록의 관리등 인증역무를 제공하는 업무를 말한다.

o 전자문서 : 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말한다.

o 전자서명 : 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.

o 전자서명검증정보 : 전자서명을 검증하기 위하여 이용하는 전자적 정보를 말한다.

o 전자서명생성정보 : 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.

2. 공고 및 보관

2.1 저장소

전자서명인증관리센터는 전자서명인증업무준칙을 포함하여 전자서명인증서비스에 필요한 신청서 양식과 관련 규칙을 전자서명인증관리센터 홈페이지에 게시한다. 또한 최상위인증기관 인증서, 공인인증기관 인증서 및 인증서 폐지목록을 인증센터 홈페이지에 게시하여, 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격인 「공인인증기관 간 상호연동을 위한 사용자 인터페이스 기술규격」에 따라 가입자 소프트웨어 및 웹브라우저 소프트웨어에 포함시켜 가입자 또는 신뢰당사자가 이용할 수 있게 한다.

2.2 정보공개 채널

전자서명인증관리센터는 공인인증서 발급 및 관리 등에 관련된 정보를 누구든지 그 사실을 항상 확인할 수 있도록 전자서명인증관리센터 홈페이지를 통해 게시한다.

또한, 전자서명인증관리센터는 공인인증서 발급 및 관리 등에 관련된 정보를 처리한 후 지체 없이 게시하며, 가입자 소프트웨어 또는 웹브라우저 소프트웨어에 포함된 최상위인증기관 인증서의 신뢰여부를 확인할 수 있도록 최상위인증기관 인증서의 해시값을 게시한다.

전자서명인증관리센터는 민감한 정보 및 공인인증기관 인증서 등록 및 처리에서 발생하는 개인정보는 공개하지 않는다.

2.3 정보공개 빈도

전자서명인증관리센터는 공인인증서 효력정지 및 폐지목록을 매주 1회 갱신한 후 누구든지 그 사실을 항상 확인할 수 있도록 지체 없이 전자서명인증관리센터 홈페이지를 통해 게시한다.

전자서명인증업무준칙은 신고한 날로부터 10일 이내에 전자서명인증관리센터 홈페이지에 게시한다.

2.4 접근 통제

전자서명인증업무준칙과 공인인증서 발급 및 관리 등에 관련된 정보를 누구든지 그 사실을 홈페이지에서 항상 확인할 수 있도록 게시한다.

전자서명인증관리센터는 기밀정보가 공개되지 않고 변경되지 않도록 보호해야 한다.

3. 공인인증서 식별 및 인증

3.1 공인인증서의 명칭 및 DN 체계

3.1.1 명칭의 사용

공인인증서, 공인인증서 효력정지 및 폐지목록 내의 기본영역에 사용되는 명칭은 「전자서명인증관리체계 DN 규격」을 준용한다.

3.1.2 명칭 의미

전자서명인증관리센터에서 발급한 공인인증서 내의 DN에는 기관명 또는 법인명을 사용한다.

3.1.3 신청인을 식별할 수 없는 익명의 인증서

전자서명인증관리센터는 익명 인증서를 발급하지 아니한다.

3.1.4 공인인증서 DN 규칙

인증서 내 DN는 X.500 표준 및 ASN.1 구문을 사용한다.

3.1.5 공인인증서 DN 유일성

전자서명인증관리센터에서 발급하는 인증서의 DN은 유일한 값을 가진다.

3.1.6 공인인증서 DN에 상표 사용

해당사항 없음

3.2 최초 신원확인

3.2.1 전자서명생성정보의 소유 확인 방법

공인인증기관은 인증서요청양식을 전자서명인증관리센터에 직접 방문하여 제출한다. 전자서명인증관리센터는 인증서요청양식에 대해 공인인증기관의 전자서명생

성정보로 전자서명을 수행하여 전자서명생성정보의 소유 여부를 확인한다. 전자서명인증관리센터는 공인인증기관의 전자서명생성정보를 검증할 수 있는 체계를 수립하고 운영한다.

3.2.2 기관 신원 확인

전자서명인증관리센터는 공인인증기관이 제출한 공인인증기관 지정서, 사업자등록증 및 법인등기부 등본을 통하여 당해 공인인증기관임을 확인하며, 국가기관·지방자치단체의 경우 이에 상응하는 서류를 통해 당해 공인인증기관임을 확인한다.

3.2.3 개인 신원 확인

전자서명인증관리센터는 공인인증서 신청인을 직접 대면하여 다음 방법에 의하여 신원을 확인한다.

- o 전자서명법 제13조의3에서 정하는 신원확인증표를 통해 제13조의2 신원확인의 기준 및 방법에 따라 신청인의 신원을 확인

- o 신청인이 당해 공인인증기관의 소속 직원임을 확인할 수 있는 서류를 통해 신원을 확인

3.2.4 미검증 가입자 정보

해당사항 없음

3.2.5 권한 확인

전자서명인증관리센터는 공인인증서 신청 대리인을 직접 대면하여 다음 방법에 의하여 신원을 확인한다.

- o 전자서명법 시행규칙 제13조의3에서 정하는 신원확인증표를 통해 전자서명법 시행규칙 제13조의2 신원확인의 기준 및 방법에 따라 대리인의 신원을 확인

- o 신청 대리인이 당해 공인인증기관의 소속 직원임을 확인할 수 있는 서류로 신원을 확인하며, 신청 대리인이 신청인의 대리권한을 지녔는지 여부를 확인

3.2.6 상호운영 기준

전자서명인증관리센터는 대한민국 행정안전부에서 운영하는 행정전자서명체계와 상호연동을 위해 인증서신뢰목록을 발급한다. 그러나 행정안전부 행정전자서명인증관리센터에서 직접적으로 인증서를 받아서 운영하는 교차인증은 허용하지 않는다.

3.3 재발급 신청 시 신원확인

3.3.1 전자서명키 유효기간 만료에 따른 재발급 신청 시 신원확인

공인인증기관이 자신의 전자서명키 유효기간 만료되어 공인인증서 재발급을 신청하는 경우 전자서명인증관리센터는 신규 발급 신청에 준하는 절차로 신원을 확인한다.

3.3.2 전자서명키 폐지에 따른 재발급 신청 시 신원확인

공인인증기관이 자신의 전자서명키 폐지로 해당 공인인증서 폐지 후 재발급을 신청하는 경우 전자서명인증관리센터는 신규 발급 신청에 준하는 절차로 신원을 확인한다.

3.4 폐지 신청 시 신원확인

공인인증기관이 자신의 공인인증서 폐지를 신청하는 경우 전자서명인증관리센터는 신규 발급 신청에 준하는 절차로 신원을 확인한다.

4. 공인인증서 발급 등 관리 절차

4.1 공인인증서 발급 신청

4.1.1 공인인증서 발급 신청자

공인인증기관의 대표자 또는 대리인이 전자서명인증관리센터에 방문하여 공인인증서의 발급을 신청한다.

- o 신원확인
- o 공인인증서 발급
- o 공인인증서 효력정지 및 폐지
- o 공인인증서 갱신
- o 공인인증서 관련 정보 공고
- o 시점확인 서비스 등

4.1.2 공인인증서 신청 절차 및 책임

공인인증기관은 전자서명인증관리센터의 홈페이지에 접속하여 필요한 정보 및 양식을 전송받거나 직접 교부받아서 신청양식에 필요한 사항을 작성한 후 인터넷진흥원에 직접 방문하여 신청한다.

공인인증기관은 공인인증서 발급 신청을 위해 전자서명인증관리센터로 방문시, PKCS#10 인증서 서명 요청(Certificate Signing Request;CSR) 형식으로 공인인증기관의 공개키를 직접 제출하여야 한다. 전자서명인증관리센터는 공인인증기관의 전자서명생성정보를 생성하거나 보관하지 않는다.

4.2 공인인증서 신청 처리

4.2.1 신원확인 및 인증 절차

전자서명인증관리센터는 공인인증기관이 제출한 공인인증기관 지정서, 사업자등록증 및 법인등기부 등본을 통하여 당해 공인인증기관임을 확인하며, 국가기관지방자치단체의 경우 이에 상응하는 서류를 통해 공인인증기관임을 확인한다.

전자서명인증관리센터는 공인인증서 신청인 또는 대리인을 직접 대면하여 다음 방법에 의하여 신원을 확인한다.

- o 전자서명법 시행규칙 제13조의3에서 정하는 신원확인증표를 통해 동법 시행규칙 제13조의2 신원확인의 기준 및 방법에 따라 신청인의 신원을 확인

- o 신청인이 당해 공인인증기관의 소속 직원임을 확인할 수 있는 서류를 통해 신원을 확인

4.2.2 공인인증서 발급 신청 승인 및 거절

전자서명인증관리센터는 공인인증기관의 신원과 공인인증서 발급 신청서의 정보를 확인한 후 공인인증서를 발급한다. 정확하지 않은 정보가 포함되거나 불분명한 내용이 기재된 경우 전자서명인증관리센터는 신청을 거절할 수 있다.

4.2.3 공인인증서 발급 처리 기간

전자서명인증관리센터는 공인인증기관으로부터 공인인증서 발급 신청이 있는 경우, 20일 이내에 해당 신청에 따른 공인인증서를 발급한다. 다만, 해당 기간 내 발급을 할 수 없는 경우, 해당 사실을 공인인증기관에 통보하고 처리 기간을 연장할 수 있다.

4.3 공인인증서 발급

4.3.1 공인인증서 발급 절차

전자서명인증관리센터는 공인인증서를 신규 발급하기 전에 다음의 공인인증서 신규 발급 신청 내용을 확인한 후 공인인증서를 발급한다.

- o 공인인증서 신청인이 제출한 전자서명검증정보의 유일성 확인
- o 공인인증서 신청인이 제출한 전자서명검증정보가 당해 공인인증기관이 소유한 전자서명생성정보에 합치하는지 여부의 확인
- o 공인인증서 신청인이 제출한 DN의 유일성 확인

4.3.2 공인인증서 발급 사실 공고

전자서명인증관리센터는 공인인증기관이 공인인증서를 수령한 후, 발급된 공인인증서 목록을 전자서명인증관리센터 홈페이지에 게시한다.

4.4 공인인증서 수령

4.4.1 공인인증서 수령 절차

공인인증기관은 공인인증기관의 공인인증서 수령 통보를 받은 후 전자서명인증관리센터에 직접 방문 또는 정보통신망을 통해 공인인증기관의 공인인증서를 수령한다. 공인인증기관 대표자 또는 대리인은 공인인증서 수령 확인함을 서명하여 최상위인증기관에 제출한다.

4.4.2 공인인증서 수령 사실 공고

전자서명인증관리센터는 공인인증기관이 공인인증서를 수령한 후, 발급된 공인인증서 목록을 전자서명인증관리센터 홈페이지에 게시한다.

4.4.3 신뢰당사자에게 공인인증서 발급 사실 통보

전자서명인증관리센터는 공인인증기관의 공인인증서를 발급한 경우, 신뢰당사자가 해당 사실을 알 수 있도록 발급된 공인인증서 목록을 전자서명인증관리센터 홈페이지에 게시하고 개별 통보는 하지 아니한다.

4.5 인증키쌍 및 인증서 용도

4.5.1 전자서명생성정보 사용 용도

공인인증기관이 공인인증역무를 제공함에 있어서 전자서명인증관리센터로부터 인증받은 전자서명검증정보에 합치하는 전자서명생성정보를 사용하여야 한다.

공인인증기관은 신뢰할 수 있는 소프트웨어나 하드웨어 등을 이용하여 안전한 방법으로 자신의 전자서명생성정보를 생성하여야 하며 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격을 만족하는 보안 모듈을 이용하여 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리하여야 한다.

4.5.2 전자서명검증정보 사용 용도

신뢰당사자는 인증서 내 확장필드에 정의된 용도로만 공개키 인증서와 연관된 전자서명검증정보를 사용해야만 한다.

전자서명인증관리센터는 공인인증서를 신규 발급하기 전에 공인인증서 신청인이 제출한 전자서명검증정보의 유일성을 확인한 후 공인인증서를 발급한다.

공인인증기관 인증서 발급 시 별도 계약사항이 존재할 경우 해당 계약사항에서 공개키 사용여부가 포함되었는지 확인하고 필요 시 기재한다.

4.6 공인인증서 갱신발급

4.6.1 갱신발급 신청 기준

공인인증기관의 인증서 갱신 시점은 통상적으로 공인인증기관의 인증서 유효기간 만료일로부터 13개월 전 시점으로 한다.

4.6.2 갱신발급 신청자

공인인증기관의 대표자 또는 대리인이 전자서명인증관리센터에 방문하여 공인인증서 갱신 발급을 신청한다.

4.6.3 갱신발급 절차

공인인증기관이 공인인증서 갱신 발급을 신청하는 경우 전자서명인증관리센터에 신규 발급 신청에 준하는 절차로 신원을 확인한다. 전자서명인증관리센터는 공인인증서를 갱신 발급하기 전에 다음의 공인인증서 갱신 발급 신청 내용을 확인한 후 공인인증서를 갱신 발급한다. 다만, 공인인증기관은 동일한 전자서명생성정보로 공인인증서 갱신발급을 신청할 수 없다.

- o 인증서 신청인이 제출한 전자서명검증정보의 동일성 확인
- o 인증서 신청인이 제출한 DN과 이전 인증서에 기재된 DN 동일성 확인

4.6.4 공인인증서 갱신발급 통보

전자서명인증관리센터는 공인인증서 갱신처리 완료를 공인인증기관 신청인에게 이메일 또는 전화로 통보한다.

4.6.5 공인인증서 갱신 승인

전자서명인증관리센터에서 갱신한 공인인증서의 승인은 4.4.1 공인인증서 수령 절차와 동일하게 수행한다.

4.6.6 공인인증서 갱신 게시

전자서명인증관리센터에 갱신한 공인인증서의 게시는 4.4.2 공인인증서 수령 사실 공고와 동일하게 수행한다.

4.6.7 신뢰당사자에게 공인인증서 갱신 사실 통보

전자서명인증관리센터는 공인인증기관의 공인인증서를 갱신한 경우, 신뢰당사자가 해당 사실을 알 수 있도록 발급된 공인인증서 목록을 전자서명인증관리센터 홈페이지에 게시하고 개별 통보는 하지 아니한다.

4.7 공인인증서 재발급

공인인증서 재발급은 전자서명생성정보가 분실·훼손 또는 도난·유출된 경우 해당 인증서를 폐지하고 새로운 전자서명생성정보를 생성하여 인증서를 발급하는 것을 말한다.

4.7.1 공인인증서 재발급 신청 기준

공인인증기관의 인증서 재발급 시점은 통상적으로 공인인증기관의 인증서 유효기간 내 전 시점으로 한다. 인증서 유효기간이 만료된 경우에는 전자서명인증관리센터는 인증서 신규 발급절차를 따른다.

4.7.2 전자서명생성정보 재발급 신청자

공인인증기관의 대표자 또는 대리인이 전자서명인증관리센터에 방문하여 공인인증서의 재발급을 신청한다.

4.7.3 공인인증서 재발급 절차

공인인증기관이 자신의 전자서명생성정보가 분실·훼손 또는 도난·유출되어

재발급을 신청하는 경우 전자서명인증관리센터는 신규 발급 신청에 준하는 절차로 신원을 확인한다.

전자서명인증관리센터는 공인인증서를 재발급하기 전에 다음의 공인인증서 재발급 신청 내용을 확인한 후 공인인증서를 재발급한다.

- o 공인인증서 신청인이 제출한 새로운 전자서명검증정보의 유일성 확인
- o 공인인증서 신청인이 제출한 새로운 전자서명검증정보가 당해 공인인증기관이 소유한 전자서명생성정보에 합치하는지 여부의 확인
- o 공인인증서 신청인이 제출한 DN의 유일성 확인

4.7.4 공인인증서 재발급 통지

전자서명인증관리센터는 공인인증서 재발급 시, 해당 내용을 공인인증기관 신청인에게 이메일 또는 전화로 통보한다.

4.7.5 공인인증서 재발급 승인

전자서명인증관리센터에서 공인인증서 재발급의 승인은 4.4.1 공인인증서 수령 절차와 동일하게 수행한다.

4.7.6 재발급된 공인인증서 게시

전자서명인증관리센터에서 재발급한 공인인증서 게시는 4.4.2 공인인증서 수령 사실 공고와 동일하게 수행한다.

4.7.7 공인인증서 재발급 사실 신뢰당사자 통보

전자서명인증관리센터는 공인인증기관의 공인인증서를 재발급한 경우, 신뢰당사자가 해당 사실을 알 수 있도록 발급된 공인인증서 목록을 전자서명인증관리센터 홈페이지에 게시하고 개별 통보는 하지 아니한다.

4.8 공인인증서 변경

4.8.1 변경 신청 기준

공인인증기관의 공인인증서 내용 변경 시에는 4.7.1 공인인증서 재발급 신청 기

준을 따른다.

4.8.2 변경 신청자

공인인증기관의 공인인증서 변경신청은 4.1.1 공인인증서 신청자에 적합한 기관만이 신청할 수 있다.

4.8.3 변경 절차

전자서명인증관리센터는 공인인증서 변경 처리를 4.7.3 공인인증서 재발급 절차와 동일하게 수행한다.

4.8.4 공인인증서 변경 통보

전자서명인증관리센터는 공인인증서 변경 완료를 공인인증기관 신청인에게 이메일 또는 전화로 통보한다.

4.8.5 공인인증서 변경 승인

전자서명인증관리센터에서 공인인증서 변경 승인은 4.4.1 공인인증서 수령 절차와 동일하게 수행한다.

4.8.6 공인인증서 변경 게시

전자서명인증관리센터에서 변경한 공인인증서 게시는 4.4.2 공인인증서 수령 사실 공고와 동일하게 수행한다.

4.8.7 신뢰당사자에게 공인인증서 변경 사실 통보

전자서명인증관리센터는 공인인증기관의 공인인증서를 변경한 경우, 신뢰당사자가 해당 사실을 알 수 있도록 발급된 공인인증서 목록을 전자서명인증관리센터 홈페이지에 게시하고 개별 통보는 하지 아니한다.

4.9 공인인증서 폐지 및 정지

4.9.1 공인인증서 폐지 사유

전자서명인증관리센터는 전자서명법 제18조 제1항, 제21조 제4항 및 제25조 제2항의 규정에 의하여 다음의 사유가 발생한 경우에 당해 공인인증기관의 공인인증서를 폐지한다.

- o 공인인증기관이 공인인증서 폐지를 신청한 경우
- o 공인인증기관이 사기나 위조, 기타 부정한 방법으로 공인인증서를 발급받은 사실을 인지한 경우
- o 공인인증기관의 해산사실을 인지한 경우
- o 공인인증기관의 전자서명생성정보가 분실·훼손 또는 도난·유출된 사실을 인지한 경우

4.9.2 공인인증서 폐지 신청인

공인인증기관은 자신의 공인인증서에 대한 폐지를 신청할 수 있다. 전자서명인증관리센터는 전자서명법 제 16조 제1항 및 제25조 제2항의 규정에 의하여 지정이 취소된 공인인증기관의 공인인증서를 폐지한다.

4.9.3 공인인증서 폐지 절차

공인인증기관은 전자서명인증관리센터가 제공하는 공인인증서 폐지신청서에 필요한 사항을 작성한 후 전자서명인증관리센터를 직접 방문하여 제출한다.
전자서명인증관리센터는 공인인증업무준칙 1.3.4.2 전자서명생성정보 취약성에 대한 조치의 규정에 따라 공인인증기관으로부터 전자서명생성정보에 대한 취약성을 통보받은 경우 당해 공인인증기관의 공인인증서를 폐지한다.

전자서명인증관리센터는 공인인증업무준칙 1.3.4.3 전자서명 알고리즘 취약성에 대한 조치의 규정에 따라 공인인증기관으로부터 전자서명 알고리즘에 대한 취약성을 통보받은 경우 당해 공인인증기관의 공인인증서를 폐지한다.

4.9.4 공인인증서 폐지 유효기간

전자서명인증관리센터는 공인인증서 폐지 처리에 대한 유예기간을 두지 않으며 공인인증서 폐지 사유의 정당성이 확인되는 경우 지체없이 인증서를 폐지한다.

4.9.5 공인인증서 폐지 처리기간

전자서명인증관리센터는 공인인증기관의 공인인증서 폐지 사유가 발생하는 경우 지체없이 당해 공인인증서에 대한 공인인증서 효력정지 및 폐지목록을 발급한다.

4.9.6 신뢰당사자에 의한 공인인증서 폐지 확인 요구사항

신뢰당사자는 공인인증서를 사용하기 전에 공인인증서의 효력정지 및 폐지목록을 통하여 당해 공인인증서의 유효성을 검증 확인하여야 한다.

4.9.7 공인인증서 폐지 목록 발행 빈도

전자서명인증관리센터는 공인인증서 효력정지 및 폐지목록을 매주 1회 갱신한 후 누구든지 그 사실을 항상 확인할 수 있도록 지체 없이 전자서명인증관리센터 홈페이지를 통해 게시한다.

4.9.8 공인인증서 폐지 목록 발행 최대 소요 시간

전자서명인증관리센터는 공인인증서 효력정지 및 폐지목록을 갱신한 후 누구든지 그 사실을 항상 확인할 수 있도록 지체없이 게시한다.

4.9.9 공인인증서 온라인 상태 검증

해당사항 없음

4.9.10 공인인증서 온라인 상태 검증 요구사항

해당사항 없음

4.9.11 공인인증서 폐지 기타 알림수단

해당사항 없음

4.9.12 키 교체 또는 키 손상의 특수 요구사항

공인인증기관은 자신의 전자서명생성정보가 안전하지 않다는 사실을 인지하는

경우 전자서명인증관리센터에 지체없이 통보하며 인증업무의 안전·신뢰성을 확보할 수 있는 대책을 강구한다.

4.9.13 공인인증서 효력정지 사유

전자서명인증관리센터는 전자서명법 제17조 제1항 및 제25조 제2항의 규정에 의하여 공인인증기관이 공인인증서 효력정지를 신청한 경우 당해 공인인증시관의 공인인증서 효력을 정지한다.

4.9.14 공인인증서의 효력정지 신청자

공인인증기관은 자신의 공인인증서에 대한 효력정지를 신청할 수 있다.

4.9.15 공인인증서의 효력정지 절차

공인인증기관이 공인인증서 효력정지·효력회복, 폐지를 신청하는 경우 전자서명인증관리센터는 신규 발급 신청에 준하는 절차로 신원을 확인한다.

단, 공인인증기관이 정보통신망을 이용하여 인증서 효력정지 및 폐지를 신청하는 경우 전자서명인증관리센터는 전자서명인증관리센터의 인증업무 내부규정에서 정한 절차에 의하여 신원을 확인한다.

공인인증기관은 전자서명인증관리센터가 제공하는 공인인증서 효력정지 신청서에 필요한 사항을 기재한 후 전자서명인증관리센터를 직접 방문하여 제출하거나 전자서명한 효력정지 신청서를 정보통신망을 이용하여 제출할 수 있다.

4.9.16 공인인증서의 효력정지 기간

공인인증기관은 전자서명법 제17조 제1항 및 제25조 제2항의 규정에 의하여 공인인증서의 효력이 정지된 날로부터 6개월 이내에 공인인증서 효력회복 신청을 하여야 한다.

4.10 공인인증서 상태 서비스

4.10.1 서비스 운영 특징

전자서명인증관리센터는 공인인증기관의 공인인증서에 대한 공인인증서 효력정

지 및 폐지목록을 발급하고 홈페이지에 게시한다.

4.10.2 서비스 가용성

전자서명인증관리센터는 공인인증서 효력정지 및 폐지목록을 갱신하고 누구든지 그 사실을 항상 확인할 수 있도록 지체없이 게시한다.

4.10.3 서비스 운영 기타사항

해당사항 없음

4.11 공인인증 서비스 해지 및 종료

해당사항 없음

4.12 키 위탁 및 복구

4.12.1 키 위탁 및 복구 정책 및 절차

전자서명인증관리센터는 공인인증기관 전자서명키 위탁 및 복구를 하지 않는다.

4.12.2 세션키 캡슐화 및 복구 정책 및 절차

전자서명인증관리센터는 세션키 캡슐키 캡슐화 및 복구를 하지 않는다.

5. 공인인증업무 시설 및 장비 보호조치

5.1 물리적 보호조치

전자서명인증관리센터는 외부인의 침입이나 불법적 접근 등의 물리적 위협으로부터 인증시스템 등이 설치된 장소를 보호한다.

5.1.1 장소 위치 및 구성

전자서명인증관리센터는 인증시스템을 별도의 통제구역 내에 설치운영하고, 해당 시스템을 물리적 접근통제를 위하여 보안캐비닛 내에 설치한다.

5.1.2 물리적 접근 통제

전자서명인증관리센터는 출입통제 시스템은 신원확인카드, 지문인식 및 무게감지 장치 등을 다중으로 결합하여 통제구역에 대한 접근을 통제한다.

전자서명인증관리센터는 이상 상황 발생시 경보 기능을 갖는 CCTV 카메라 및 모니터링시스템과 침입감지 시스템 등 감시통제시스템을 설치·운영한다.

전자서명인증관리센터는 보안경비요원을 배치하여 보안경비업무를 수행한다.

5.1.3 전원 및 공기조절시스템

전자서명인증관리센터는 갑작스러운 정전으로 인한 심각한 피해를 방지하기 위하여 무정전전원공급장치를 사용한다.

전자서명인증관리센터는 온도 및 습도를 일정하게 유지하기 위한 공기조절시스템을 설치한다.

5.1.4 수해 방지

전자서명인증관리센터는 침수로부터 인증시스템을 안전하게 보호하기 위하여 바닥으로부터 이격하여 설치한다.

5.1.5 화재 예방

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

5.1.6 매체 저장

전자서명인증관리센터는 주요 저장·기록매체를 금고에 저장하여 물리적으로 접근을 통제한다.

5.1.7 폐기물 처리

전자서명인증관리센터는 문서, 디스켓 등을 폐기하는 경우 물리적으로 이를 파기한다.

5.1.8 원격지 백업

전자서명인증관리센터는 전자서명인증관리센터가 발급한 공인인증서, 공인인증서 효력정지 및 폐지목록 등을 물리적으로 격리된 원격지에 백업하여 당해 공인인증서의 효력이 소멸된 날부터 10년간 보관한다.

5.2 절차적 보호조치

5.2.1 주요업무 담당자

전자서명인증관리센터는 인증업무의 안전·신뢰성을 확보하기 위하여 업무를 역할별로 아래와 같이 정의하여 수행한다.

- o 정책관리자
- o 보안 관리자
- o 감사 관리자
- o 인증업무 담당자
- o 센터 운영자

전자서명인증관리센터는 인증업무의 안전·신뢰성을 확보하기 위하여 정책관리자, 인증업무 담당자, 보안 관리자 및 감사 관리자의 직무를 분리한다.

5.2.2 주요업무별 수행 인원

키 생성 업무는 3인 이상 또는 그에 준하는 직무 분리 및 최소권한의 원칙을 준수하여 수행한다.

5.2.3 주요업무별 인원 신원확인

주요업무를 담당하기 전 전자서명인증관리센터 직원은 신원확인 및 범죄기록 여부를 확인받아야 한다.

5.2.4 주요업무별 역할 분리

전자서명인증관리센터는 인증업무의 안전·신뢰성을 확보하기 위하여 업무를 역할별로 분리하여 수행한다.

5.3 인적 보안

5.3.1 자격 요건

전자서명인증관리센터의 주요업무 담당자는 대한민국 국민이여야만 한다.

전자서명 인증관리체계 운영인력 중 인증관리센터장과 보안 관리자는 2급 비밀취급인가증을 소지하도록 한다.

5.3.2 신원 확인

전자서명인증관리센터의 운영인력은 국가의 신원확인 결과 결격 사유가 없어야 한다.

전자서명인증관리센터의 주요업무 담당자는 채용 시 인터뷰 및 평가로 업무 수행 능력 및 경험을 확인받아야 한다.

5.3.3 교육 및 훈련

전자서명인증관리센터의 인증업무를 담당하는 모든 직원은 채용 시 또는 채용 후 1년 이내에 업무수행에 필요한 인증업무 법제, 정책 및 인증서 관리 교육을 이수해야만 한다.

o 전자서명법・제도
o 다양한 인증수단
o 전자서명 알고리즘
o 인증서 생성 관리

5.3.4 재교육 및 훈련

전자서명인증관리센터의 인증업무를 담당하는 모든 직원은 매년마다 업무수행에 필요한 인증업무 법제, 정책 및 인증서 관리 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 규정 및 법에 따라 징계한다.

5.3.7 자유직업자 요구사항

자유직업자가 전자서명인증관리센터의 주요업무를 담당할 경우 비인가 행위에 대한 처벌은 5.3.6 절차와 동일하게 수행한다.

5.3.8 직원 문서 공개

전자서명인증관리센터는 주요 인증업무에 대한 내부문서 및 교육 자료는 해당 직원들에게 제공한다.

5.4 감사 기록

5.4.1 감사기록 대상사건의 종류

전자서명인증관리센터는 등록정보관리, 전자서명생성정보 생성·관리, 공인인증서 생성·발급 및 시점확인 기능을 지원하는 시스템 (이하“인증시스템”이라 한다)에서 발생한 사건들을 기록한다.

다음과 같은 인증업무 행위가 발생되면 감사기록이 생성될 수 있다.

o 최상위인증기관 키 관리업무:
  - 키 생성, 키 백업, 키 보관, 키 복구, 키 마이그레이션 및 파괴
o 공인인증기관 인증서 관리업무:
  - 인증서 발급, 갱신, 재발급, 폐지
  - 인증서 폐지목록 생성
o 인증시스템 계정 접속 내역

감사기록은 다음요건을 포함하여 기록한다.

o 감사로그 번호
o 감사로그 일자 및 시간
o 감사로그 내역 및 수행자
o 감사로그 성공여부

5.4.2 감사기록 처리 주기

각 시스템의 감사로그는 발생일로부터 10 년동안 보관하며, 감사관리자는 해당 로그의 이상 유무를 년 1회 검토 한다.

5.4.3 감사기록 보관 기간

전자서명인증관리센터는 발생한 감사로그를 발생일로부터 10년 동안 원격지에 보관한다.

5.4.4 감사기록 보호

각 시스템의 감사기록은 보안 감사자에 의해 총괄 관리되며 시스템의 각 업무 관리자는 당해 업무에 대한 감사기록만 열람할 수 있다.

5.4.5 감사기록 백업 절차

감사 관리자는 감사기록을 검토하고 보존한다.

5.4.6 감사기록 취합 시스템

감사기록은 내부 시스템에서 생성되고 취합된다.

5.4.7 감사기록 대상에 대한 통보

보안위반사건 발생 시 담당업무관리자에게 지체없이 통보한다.

5.4.8 취약점 측정

전자서명인증관리센터는 전자서명인증관리센터 업무를 수행함에 있어서 효율적인 보안관리를 위하여 정기적으로 자체 점검을 실시한다.

5.5 기록 보존

5.5.1 기록 보존 대상의 종류

전자서명인증관리센터는 다음의 업무와 관련된 내역을 기록 보존한다.

- o 공인인증기관의 인증서 발급 및 관리 등 인증 업무
- o 전자서명인증관리센터 핵심인증시스템 등의 운영 업무

5.5.2 보존기록 보관 기간

전자서명인증관리센터는 발생한 보존기록을 발생일로부터 10년 동안 원격지에 보관한다.

5.5.3 보존기록 보호

전자서명인증관리센터는 전자서명인증관리센터의 인증업무 내부규정에 의하여 전자서명인증관리센터의 직원을 문서관리자로 정하며, 문서관리자는 모든 보존기록을 관리하며 기타 관리자들은 자신의 업무범위 내의 보존기록에 대해서만 조회가 가능하다.

전자서명인증관리센터는 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

전자서명인증관리센터는 전자서명인증관리센터의 인증업무 내부규정에 의하여 전자서명인증관리센터의 직원을 문서관리자로 정한다.
문서관리자가 정의되었는지 확인한다.

5.5.5 보존기록 타임스탬프 요건

해당사항 없음

5.5.6 보존기록 취합 시스템

감사기록은 내부에서 생성되고 취합된다.

5.5.7 보존기록 검증 절차

문서관리자만 보존기록에 접근 가능하다. 인증서 접수 및 발급 시 수령대장에 담당자 서명을 득하여 관리한다.

5.6 키 변경

해당사항 없음

5.7 장애 및 재해복구

5.7.1 시스템 자원 및 소프트웨어 장애 발생에 대한 대책

전자서명인증관리센터는 시스템 자원 및 소프트웨어 등에 장애가 발생한 경우에 이중으로 설치한 시스템 자원 및 소프트웨어를 이용하여 복구한다.

5.7.2 데이터의 훼손·멸실에 대한 대책

전자서명인증관리센터는 공인인증기관 인증서 등의 주요 데이터에 훼손·멸실이 발생하였을 경우에 기록 보존된 자료를 이용하여 복구한다.

5.7.3 전자서명키 손실에 대한 복구 절차

전자서명인증관리센터는 인증업무에 이용하고 있는 전자서명인증관리센터의 전자서명생성정보가 안전하지 않다는 사실을 인지하는 경우 당해 전자서명생성정보에 합치하는 전자서명검증정보를 포함하는 전자서명인증관리센터의 인증서를 폐지하고 새로운 전자서명생성정보를 생성하여 전자서명인증관리센터의 인증서를 재발급한다. 전자서명인증관리센터는 새로운 전자서명생성정보를 이용하여 공인인증기관의 공인인증서를 갱신 발급한 후 인증관리체계에 의하여 누구든지 그 사실을 항상 확인할 수 있도록 지체없이 공고하며 인증업무의 안전·신뢰성을 확보할 수 있는 대책을 강구한다.

전자서명인증관리센터는 공인인증기관으로부터 전자서명생성정보에 대한 분실·훼손 또는 도난·유출, 취약성을 통보받은 경우 당해 공인인증기관에게 발급한 공인인증서를 폐지한 후 누구든지 그 사실을 항상 확인할 수 있도록 지체없이 게시한다.

5.7.4 업무연속성 계획 수립

전자서명인증관리센터는 공인인증기관 인증서 발급, 갱신, 폐지 등 공인인증관리 업무, 전자서명생성정보 등 관리업무, 공인인증기관 심사 및 점검 업무와 전자서명 인증기술 등 핵심/주요 업무가 정보자산 및 설비자산 장애, 테러, 정전, 지진, 화재, 풍수해 등으로 업무가 중단되지 않도록 업무연속성 계획을 수립한다.

업무연속성 계획을 수립함으로서 인적·물적 자원의 피해가 발행한 시점에 가장 효율적인 활동 방법을 제시하여, 전자서명인증관리센터 운영 업무와 전자서명인증관리 핵심업무 중단기간을 최소화하고, 200km 이상 떨어진 백업센터를 통해 정상 업무로의 복원을 효과적으로 수행하여 전자서명인증관리센터 정보자산 인프라의 회복력을 향상시키고, 업무중단으로 인한 운영상의 영향을 감소시킨다.

5.8 공인인증기관 또는 등록대행기관의 위임 종료

전자서명인증관리센터는 최상위인증기관으로서 인증기관의 위임 종료 시 이를 공지하고 인증기관이 발급한 인증서를 재발급 한다. 전자서명인증관리센터는 인증기관으로서 등록기관의 위임 종료 시 이를 공지하고 등록기관의 위임 종료 시 업무공백이 발생하지 않도록 한다.

6. 기술적 보호조치

6.1 전자서명생성정보 생성 및 절차

6.1.1 전자서명생성정보 생성 절차

전자서명인증관리센터의 키 쌍 생성절차는 문서화 되어있다.

전자서명인증관리센터는 인가된 자만이 전자서명생성정보를 생성할 수 있도록 한다. 전자서명인증관리센터의 전자서명생성정보 생성시 3명 이상의 다중 통제 아래 전자서명인증관리센터의 키 생성 절차서에 따라 수행한다.

전자서명인증관리센터는 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되는 안전한 키 생성시스템 또는 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격을 만족하는 보안 모듈에서 전자서명생성정보를 생성한다.

6.1.2 가입자 전자서명생성정보 전달 절차

전자서명인증관리센터는 내부 인증시스템 운영 목적을 제외하고는 가입자의 공인인증서를 발급하지 아니한다.

6.1.3 전자서명검증정보 전달 절차

공인인증기관은 인증서 신청서와 함께 PKCS#10 형식의 CSR을 전자서명인증관리센터에 제출한다.

6.1.4 최상위인증기관 전자서명검증정보 제공 절차

인터넷진흥원은 최상위인증기관 인증서를 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격인 「공인인증기관 간 상호연동을 위한 사용자 인터페이스 기술규격」에 따라 가입자 소프트웨어에 포함시키거나, 웹브라우저 소프트웨어에 포함시켜 가입자 또는 신뢰당사자가 이용할 수 있게 한다.

6.1.5 전자서명생성정보의 키 길이

최상위인증기관에서 안전하고 신뢰성있는 전자서명 알고리즘을 사용하기 위하여 다음과 같은 크기의 키 길이를 이용한다.

o ECDSA 및 RSA 경우 : 2,048bit 이상

6.1.6 전자서명검증정보 매개변수 생성 및 품질 검사

전자서명인증관리센터는 가입자 소프트웨어 또는 웹브라우저 소프트웨어에 포함된 최상위인증기관 인증서의 신뢰여부를 확인할 수 있도록 최상위인증기관 인증서의 해시값을 공고한다.

6.1.7 전자서명생성정보 사용 용도

공인인증기관이 공인인증역무를 제공함에 있어서 전자서명인증관리센터로부터 인증받은 전자서명검증정보에 합치하는 전자서명생성정보를 사용하여야 한다.

전자서명인증관리센터의 최상위인증기관 키는 인증서 서명, 인증폐지목록, 인증서신뢰목록 서명에 사용되며 해당 키 사용 용도는 최상위인증기관 인증서 확장필드에 명시되어 있다.

6.2 전자서명생성정보 보호 및 암호화 모듈

6.2.1 전자서명생성정보 보관장치

전자서명인증관리센터는 전자서명생성정보를 안전하게 보관하기 위하여 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격 및 FIPS 140-2 레벨3을 만족하는 보안 모듈을 이용하여 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리하여야 한다.

6.2.2 다중 통제

전자서명인증관리센터의 전자서명생성정보는 3명 이상 관리자 또는 그에 준하는 직무 분리 및 최소권한의 원칙을 준수하여 다중 통제 아래 이용된다.

6.2.3 전자서명생성정보 위탁

전자서명인증관리센터는 인증기관의 개인키를 위탁하지 않는다.

6.2.4 전자서명생성정보 백업

전자서명인증관리센터는 전자서명생성정보의 훼손에 대비하여 전자서명생성정보를 백업하고 금고에 저장하며 키 생성과 동일한 보안 모듈을 사용하여 암호화된 백업키를 관리한다.

또한, 전자서명인증관리센터는 전자서명생성정보의 훼손에 대비하여 전자서명생성정보를 백업하여 나주 본원에 위치한 전자서명인증관리 백업센터에 보관한다. 보관된 전자서명생성정보는 센터 내에서 사용되는 동일한 보안 모듈을 사용하여 암호화된 백업키를 관리한다.

6.2.5 전자서명생성정보 보관

전자서명인증관리센터는 전자서명생성정보를 별도로 보관(Archival)하지 않는다.

6.2.6 전자서명생성정보 추출

전자서명인증관리센터는 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되는 안전한 키 생성시스템 또는 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격을 만족하는 보안 모듈에서 전자서명생성정보를 생성한다.

전자서명인증관리센터는 키 생성 시 보안 모듈 기능을 사용하여 안전한 방식으로 백업키를 복제할 수 있다.

공인인증기관은 신뢰할 수 있는 소프트웨어나 하드웨어 등을 이용하여 안전한 방법으로 자신의 전자서명생성정보를 생성하여야하며 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격을 만족하는 보안 모듈을 이용하여 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리하여야 한다.

6.2.7 전자서명생성정보 저장

전자서명인증관리센터는 전자서명생성정보를 안전하게 저장하기 위하여 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격 및 FIPS-140-2 레벨3을 만족하는 보안 모듈을 이용하여 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 암호화하여 안전하게 관리하여야 한다.

6.2.8 전자서명생성정보 활성화

전자서명인증관리센터의 전자서명생성정보는 3명 이상 관리자 또는 그에 준하는 직무 분리 및 최소권한의 원칙을 준수하여 다중 통제 아래 이용된다.

6.2.9 전자서명생성정보 비활성화

전자서명인증관리센터 전자서명생성정보가 생성된 후 운영자는 암호화 장비 활성화 도구를 제거하여 키 생성에 사용된 보안 모듈을 비활성화 한다.

6.2.10 전자서명생성정보 삭제 및 파괴

전자서명인증관리센터는 인증서의 유효기간이 만료되거나 전자서명생성정보가 훼손·유출되었을 경우에 관리자의 승인 하에 해당 전자서명생성정보 저장매체를 물리적으로 완전히 파기하거나, 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격에 따라 전자서명생성정보를 삭제한다.

6.2.11 암호화 모듈 등급

전자서명인증관리센터는 전자서명생성정보를 안전하게 저장하기 위하여 공인인증 기관의 시설 및 장비 등에 관한 규정의 기술규격 및 FIPS-140-2 레벨3을 만족하는 보안 모듈을 이용하여 전자서명생성정보가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리하여야 한다.

6.3 전자서명키쌍 관리

전자서명인증관리센터가 발급한 인증서는 전자서명인증관리센터 또는 공인인증기관에서 소유하고 있는 전자서명생성정보에 합치한다는 사실을 확인 및 증명하기 위하여 사용된다.

6.3.1 전자서명검증정보 보관

최상위인증기관 전자서명검증정보가 보관되고 있는지 확인한다. 확인하면 아래와 같이 서술한다.

전자서명인증관리센터는 최상위인증기관의 전자서명검증정보를 원격지에 보안모듈을 사용하여 보관한다.

6.3.2 공인인증서 유효기간

전자서명인증관리센터는 전자서명법 제15조 제5항 및 제25조 제2항의 규정에 의하여 공인인증서의 이용범위 및 용도, 이용된 기술의 안전성과 신뢰성 등을 고려하여 공인인증서의 유효기간을 적정하게 정하여야 한다.

o 전자서명인증관리센터의 공인인증서 유효기간은 20년 이내로 한다.

o 전자서명인증관리센터가 발급한 공인인증기관의 공인인증서 유효기간은 다음과 같다.

인증서 구분	유효기간
공인인증기관용 인증서	10년 이내
OCSP용 인증서	10년 이내
시점확인용 인증서	10년 이내

전자서명인증관리센터는 전자서명인증관리센터가 발급한 공인인증서, 공인인증서 효력정지 및 폐지목록 등을 물리적으로 격리된 원격지에 백업하여 당해 공인인증서의 효력이 소멸된 날부터 10년간 보관한다.

6.4 활성화 데이터

활성화 데이터는 하드웨어 보안모듈(HSM)을 작동 및 사용하는데 필요한 정보이다. 활성화 데이터의 예로는 PIN, 암호문과 키 분할 체계 등이 있다.

6.4.1 활성화 데이터 생성

활성화 데이터는 하드웨어 보안모듈(HSM)의 사양에 따라 생성된다.

6.4.2 활성화 데이터 보호

활성화 데이터를 보호하기 위해 사용되는 절차는 데이터가 PIN번호와 접근 인증용 키에 의존한다. 접근 인증용 키는 지정된 관리자에 의해 유지된다. PIN번호는 전자서명인증관리센터의 암호화 정책에 적용된다.

6.4.3 활성화 데이터 추가 고려사항

해당사항 없음

6.5 컴퓨터 보안

6.5.1 특정 컴퓨터 보안 요건

전자서명인증관리센터는 운영체제, 서버, 하드웨어, 소프트웨어 보안체계를 수립하고 운영한다.

6.5.2 시스템 보안 요건

해당사항 없음

6.6 생명주기 보안

해당사항 없음

6.6.1 시스템 개발 통제

전자서명인증관리센터는 최상위인증관리시스템의 기능 변경, 성능 개선시 전자서명인증관리센터장의 승인 하에 실시된다.

6.6.2 보안관리 통제

최상위인증관리시스템에 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

전자서명인증관리센터는 온라인 서비스 제공 시, 네트워크 보안 강화를 위해 네트워크 보안장비를 사용한다.

6.8 시점확인 서비스

전자서명인증관리센터는 신청이 있는 경우 시점확인 서비스 등 기타 부가 서비스를 제공할 수 있다.

7. 공인인증서 프로파일

7.1 공인인증서 프로파일

전자서명인증관리센터가 발급하는 공인인증서의 프로파일은 X.509 버전3 공인인증서의 규격 및 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격인 「전자서명 인증서 프로파일 규격」을 준수한다.

7.1.1 공인인증서 버전

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

7.1.2 공인인증서 확장

공인인증서의 확장 필드 사용 여부 등에 관한 사항은「전자서명 인증서 프로파일 규격」을 따른다.

7.1.3 알고리즘 개체 식별자

공인인증서에 사용되는 암호 알고리즘 개체 식별자는 「전자서명 인증서 프로파일 규격」을 따른다.

7.1.4 명칭 양식

공인인증서에 사용되는 명칭 양식은 「전자서명 인증서 프로파일 규격」을 따른다.

7.1.5 명칭 제한

공인인증서에 사용되는 명칭의 제한 사항 및 양식은 「전자서명 인증서 프로파일 규격」을 따른다.

7.1.6 공인인증서 정책 개체 식별자

공인인증서에 사용되는 공인인증서 정책 개체 식별자는 「전자서명 인증서 프로파일 규격」을 따른다.

7.1.7 정책 제한 확장의 사용

공인인증서에 사용되는 공인인증서 정책 제한 확장의 사용은 「전자서명 인증서 프로파일 규격」을 따른다.

7.1.8 정책 한정자 구문 및 의미

공인인증서에 사용되는 공인인증서 정책 한정자 구문 및 의미는 「전자서명 인증서 프로파일 규격」을 따른다.

7.1.9 주요 인증서 정책 확장에 대한 의미와 처리 절차

공인인증서의 정책 확장에 대한 의미와 처리 절차는 「전자서명 인증서 프로파일 규격」을 따른다.

7.2 공인인증서 효력정지 및 폐지목록 프로파일

7.2.1 프로파일 버전

전자서명인증관리센터가 발급하는 공인인증서 효력정지 및 폐지목록(CRL)의 프로파일은 X.509 버전2 공인인증서 폐지목록의 규격 및 공인인증기관의 시설 및 장비 등에 관한 규정의 기술규격인 「전자서명 인증서 효력정지 및 폐지목록 프로파일 규격」을 준수한다.

7.2.2 프로파일 확장 필드

전자서명인증관리센터는 인증서의 효력을 정지한 경우 인증서 효력정지 및 폐지목록 확장영역 중 폐지사유코드 필드를 이용하여 당해 인증서가 효력정지 되었음을 나타낸다.

7.3 공인인증서 유효성 확인 서비스용 인증서 프로파일

해당사항 없음

7.3.1 프로파일 버전

해당사항 없음

7.3.2 유효성 확인 서비스 확장 필드

해당사항 없음

8. 감사 준수 및 기타 평가

8.1 감사 및 평가 실시 빈도와 환경

전자서명인증관리센터는 인증관리센터 업무를 수행함에 있어서 효율적인 보안 관리를 위하여 정기적으로 감사 또는 평가를 실시한다.

8.2 감사 및 평가 주체와 자격

전자서명인증관리센터는 매년 1회 이상 웹트러스트 감사 또는 이에 준하는 감사(공인인증기관의 보호조치에 관한 규정)를 수행한다.

8.3 감사 대상에 대한 평가자의 관계

감사자는 피감사 대상자와 금전적으로나 사업 등으로 이해관계가 없어야 한다.

8.4 평가 범위

감사의 범위는 전자서명인증업무지침의 준수여부, 인증기관 키 관리, 인증서 관리 및 최상위인증기관 시스템 관리를 포함한다.

8.5 평가 결과 조치

결과 미비사항에 대해서는 조치가 취해지며 합리적인 기간 내에 실행한다.

8.6 평가 결과 공표

해당사항 없음

9. 공인인증업무 보증 등 기타사항

9.1 공인인증서비스 수수료

9.1.1 공인인증서 발급, 재발급 및 갱신 발급 수수료

전자서명인증관리센터는 필요한 경우에 전자서명법 제28조의 규정에 의하여 공인인증서 발급, 재발급 및 갱신 발급을 신청하는 공인인증기관에 대한 수수료를 부과할 수 있다.

9.1.2 공인인증서 접근 수수료

전자서명인증관리센터는 공인인증서를 열람·확인하는 신뢰당사자에게 수수료를 부과하지 않는다.

9.1.3 공인인증서 효력정지 및 폐지목록 접근 수수료

전자서명인증관리센터는 공인인증서 효력정지 및 폐지목록에 접근하는 신뢰당사자에게 수수료를 부과하지 않는다.

9.1.4 기타 서비스에 대한 수수료

전자서명인증관리센터는 필요한 경우에 전자서명법 제28조의 규정에 의하여 기타 서비스에 대한 수수료를 부과할 수 있다.

9.1.5 환불 정책

전자서명인증관리센터는 공인인증서 발급 신청 철회 등에 따른 환불은 공인인증서 발급 수수료를 부과한 경우에 한해 환불한다.

9.2 면책

전자서명인증관리센터는 전자서명법, 동법 시행령 및 시행규칙 또는 전자서명인증업무준칙의 각 규정에서 정한 사항 이외에 사유로 인한 손해 또는 전쟁, 천재지변 등 불가항력적인 사유로 인한 인증업무의 처리지연 또는 처리 불능으로 인한 손해에 대하여는 책임을 지지 않는다.

9.2.1 보험 범위

전자서명인증관리센터는 손해 배상을 위한 별도 보험에 가입하지 않는다.

9.2.2 기타 자산

전자서명인증관리센터는 손해배상을 위한 채권 등 기타 자산은 제공하지 않는다.

9.2.3 신뢰당사자를 위한 보험 또는 보증 범위

전자서명인증관리센터는 신뢰당사자에 대해 전자서명법, 동법 시행령 및 시행규칙 또는 전자서명인증업무준칙의 각 규정에서 정한 사항 이외에 사유로 인한 손해 또는 전쟁, 천재지변 등 불가항력적인 사유로 인한 인증업무의 처리지연 또는 처리 불능으로 인한 손해에 대하여는 책임을 지지 않는다.

9.3 기밀정보 보호

공인인증기관에 발급한 인증서, 인증서 폐지 등 상태 정보, 최상위인증기관의 업무와 관련하여 공고하는 정보는 기밀정보로 간주하지 않는다.

9.3.1 기밀정보 범위

전자서명인증관리센터는 공인인증기관에 제공하는 정보와 관련하여 별도 기밀정보를 취급하지 않는다.

9.3.2 기밀정보 범위에 벗어나는 것으로 간주되는 정보

해당 사항 없음

9.3.3 기밀정보 보호 책임

전자서명인증관리센터는 공인인증기관에 제공하는 정보와 관련하여 별도 기밀정보를 취급하지 않아 해당 사항 없음

9.4 개인 정보 보호

9.4.1 개인 정보 보호 계획

전자서명인증관리센터는 인증업무 수행과 관련하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 의 개인정보에 관한 규정을 준용하며, 개인 정보 보호 계획은 한국인터넷진흥원 개인정보처리방침에 따른다.

9.4.2 비공개로 취급되는 정보

해당 사항 없음

9.4.3 비공개로 간주되지 않는 정보

해당 사항 없음

9.4.4 개인 정보 보호 책임

전자서명인증관리센터는 개인 정보 보호 책임은 한국인터넷진흥원 개인정보처리방침에 따른다.

9.4.5 개인 정보 이용에 대한 고지 및 동의

전자서명인증관리센터는 개인 정보 이용에 대한 고지 및 동의 절차는 한국인터넷진흥원 개인정보처리방침에 따른다.

9.4.6 사법 또는 행정 절차에 따른 공개

전자서명인증관리센터는 개인 정보 관련한 사법 또는 행정 절차에 따른 공개 사항은 한국인터넷진흥원 개인정보처리방침에 따른다.

9.4.7 기타 정보 공개 상황

전자서명인증관리센터는 개인 정보 관련한 기타 정보 공개 사항은 한국인터넷진흥원 개인정보처리방침에 따른다.

9.5 지적재산권

다음 사항에 대한 지적재산권은 저작권법 및 기타 관련 법률에 따라 전자서명인증관리센터에 귀속된다.

- o 전자서명인증관리센터가 개발한 소프트웨어 및 하드웨어
- o 전자서명인증관리센터의 전자서명인증업무준칙
- o 전자서명인증관리센터의 명칭
- o 전자서명인증관리센터가 생성한 전자서명생성정보 등

9.6 보증 책임

9.6.1 최상위인증기관 진술 및 보증

전자서명인증관리센터는 자신이 발급한 공인인증서와 관련하여 다음의 내용을 보증한다.

- o 발급된 공인인증서에 포함된 내용이 틀림없다는 사실
- o 전자서명법의 규정에 의하여 공인인증서가 발급되었다는 사실
- o 공인인증서 효력정지 및 폐지에 대한 내용이 틀림없다는 사실

9.6.2 등록대행기관 진술 및 보증

전자서명인증관리센터는 등록대행기관을 운영하지 않으므로 해당사항 없음

9.6.3 가입자 진술 및 보증

전자서명인증관리센터는 가입자와 별도 계약 등이 수행하지 않으므로 해당 사항 없음

9.6.4 신뢰당사자 진술 및 보증

전자서명인증관리센터는 신뢰당사자와 별도 계약 등이 수행하지 않으므로 해당 사항 없음

9.6.5 다른 참가자의 진술 및 보증

전자서명인증관리센터는 다른 참가자와 별도 계약 등이 수행하지 않으므로 해당 사항 없음

9.7 보증의 철회

해당사항 없음

9.8 책임의 제한

전자서명인증관리센터는 전자서명법, 동법 시행령 및 시행규칙 또는 전자서명인증업무준칙의 각 규정에서 정한 사항 이외에 사유로 인한 손해 또는 전쟁, 천재지변 등 불가항력적인 사유로 인한 인증업무의 처리지연 또는 처리 불능으로 인한 손해에 대하여는 책임을 지지 않는다.

9.9 면책 사항

전자서명인증관리센터는 전자서명법, 동법 시행령 및 시행규칙 또는 전자서명인증업무준칙의 각 규정에서 정한 사항 이외에 사유로 인한 손해 또는 전쟁, 천재지변 등 불가항력적인 사유로 인한 인증업무의 처리지연 또는 처리 불능으로 인한 손해에 대하여는 책임을 지지 않는다.

9.10 전자서명인증업무준칙의 효력

9.10.1 기간

본 전자서명인증업무준칙은 2024년 1월 9일부터 시행한다.

9.10.2 종료

본 전자서명인증업무준칙은 종료일은 갱신된 전자서명인증업무준칙의 효력 시작일로 한다.

9.10.3 경과 조치

본 전자서명인증업무준칙은 종료 후에도 효력이 유효한 사항은 없음

9.11 의사소통 및 통지

해당사항 없음

9.12 전자서명인증업무준칙의 관리

9.12.1 개정 절차

전자서명인증관리센터는 전자서명법 제6조 제2항 및 제25조 제2항의 규정에 의하여 과학기술정보통신부장관이 공인인증업무준칙의 변경을 명한 경우에 이를 개정한다.

전자서명인증관리센터의 센터장이 공인인증업무준칙 및 전자서명인증업무준칙의 변경이 필요하다고 판단한 경우에 이를 개정한다. 전자서명인증관리센터는 다음의 내용을 포함한 전자서명인증업무준칙의 개정 관련 기록을 유지·관리한다.

- o 전자서명인증업무준칙 버전
- o 적용 업무 및 범위의 개요
- o 전자서명인증업무준칙의 개정 기록
  - 개정된 기존 전자서명인증업무준칙의 규정
  - 개정 내용
  - 개정 사유 등

9.12.2 개정 게시

전자서명인증관리센터는 제·개정된 전자서명인증업무준칙을 전자서명인증관리센터 홈페이지에 게시한다.

9.12.3 OID를 변경해야 하는 상황

해당 사항 없음

9.13 분쟁 해결

공인인증업무와 관련하여 분쟁이 발생한 경우, 관계법령에 따라 해결할 수 있음

9.14 준거법

이 전자서명인증업무준칙은 대한민국의 전자서명법 및 관계법령에 따라서 해석되고 적용된다.

9.15 관련 법규 준수

전자서명인증관리센터는 대한민국의 전자서명법 및 관계법령을 준수한다.

9.16 기타 조항

9.16.1 합의 사항

이 전자서명인증업무준칙과 관련하여 별도 합의된 사항은 없음

9.16.2 양도 사항

이 전자서명인증업무준칙과 관련하여 별도 양도된 사항은 없음

9.16.3 분할 사항

이 전자서명인증업무준칙과 관련하여 별도 분할 가능성 조항은 없음

9.16.4 집행

이 전자서명인증업무준칙과 관련하여 별도 집행 가능한 사항은 없음

9.16.5 불가항력

전쟁, 테러, 자연재해, 인터넷 또는 기타 인프라 장애 등 본 준칙의 당사자의 합리적 통제를 벗어난 사건으로 인한 준칙 미이행 사항은 불가항력으로 판단한다.

9.17 기타 조항

이 전자서명인증업무준칙과 관련된 기타 규정은 없음