행정전자서명
최상위 인증기관
인증업무준칙
(RootCA CPS)

2015. 8.

개 정 이 력

번호	작성일	변경내용	작성자	승인자
1.0	15.08	웹트러스트 인증 기준에 따른 신규 작성		
1.0	15.08	최상위인증기관 및 인증기관 인증업무준칙 분리 신규 작성		

< 목 차 >

1. 개 요

행정전자서명 인증업무준칙은 RFC 3647의 기준에 따라 행정전자서명인증체계의 최상위인증업무 및 인증업무 정책을 공개한 문서이다.
행정전자서명 인증업무준칙은 행정전자서명 인증관리센터(‘이하 인증관리센터’)의 홈페이지에 게시된다. 행정전자서명 개인용 및 기관용 인증서를 사용하는 기관 또는 개인은 언제든지 행정전자서명 인증업무준칙을 열람할 수 있다.
본 준칙은 ‘15년 10월 1일을 기준으로 효력을 발휘한다.

1.1 목적

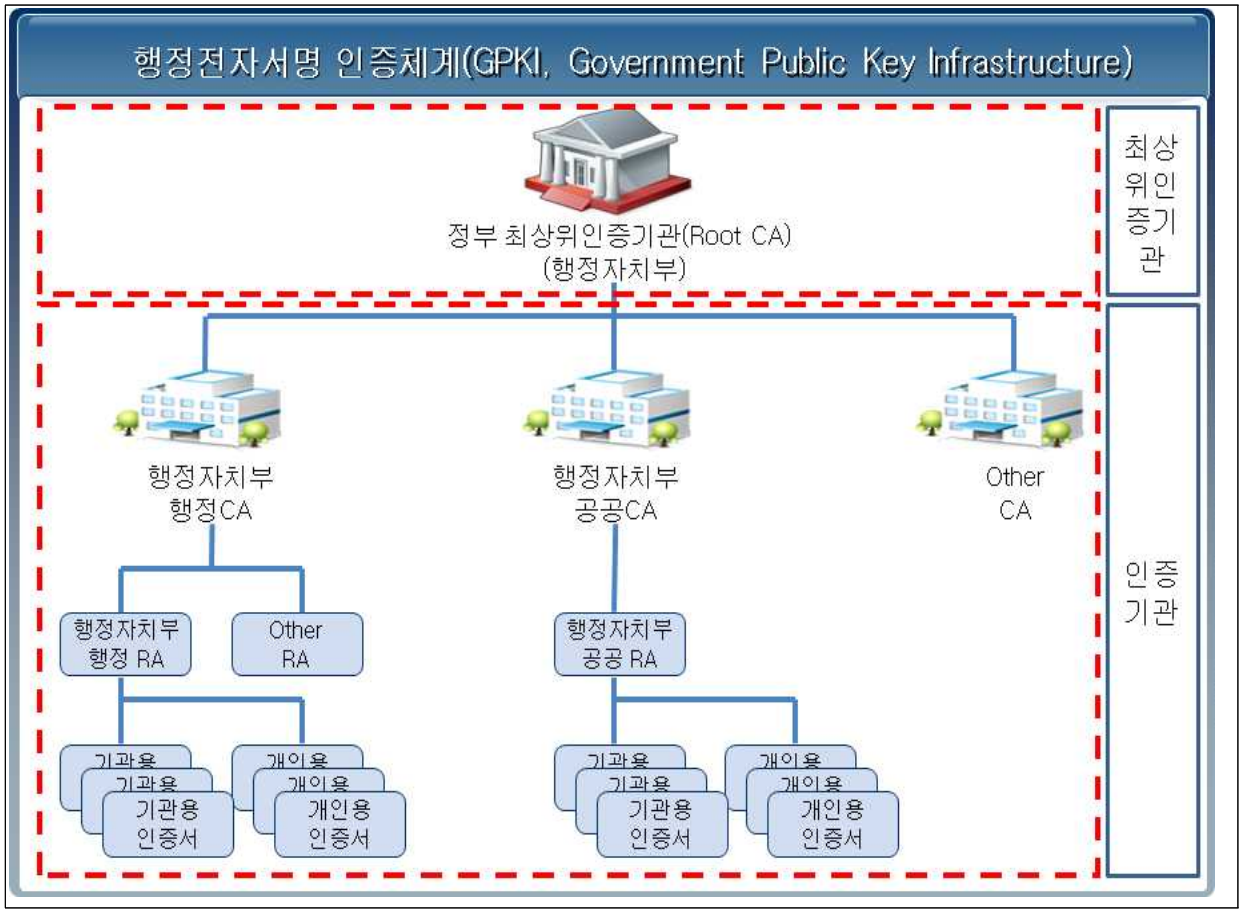
이 준칙은 행정전자서명 인증업무의 수행 및 관리 기준에 따라 구체적인 세부사항을 정함을 목적으로 한다.

1.2 행정전자서명 인증서의 종류

행정전자서명 인증체계가 발급하는 인증기관 인증서는 다음과 같다.

- 행정자치부(1.2.410.100001.5.7)
- 교육부(1.2.410.100001.5.3)
- 대검찰청(1.2.410.100001.5.5)
- 병무청(1.2.410.100001.5.6)
- 법원(1.2.410.100001.5.8)

1.3 행정전자서명 인증체계



1.3.1 행정자치부

행정자치부는 행정전자서명 인증관리체계의 안전·신뢰성 있는 운영을 위한 정책·감독 기관으로 다음과 같은 업무를 수행한다.

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

1.3.2 인증관리센터

인증관리센터는 행정전자서명 인증체계의 최상위인증기관(RootCA) 및 인증기관(CA) 업무를 수행하는 기관이다.
인증관리센터는 다음과 같은 업무를 수행한다.

- 인증기관의 지정 및 인증기관 인증서 발급·관리 등 인증업무
- 인증기관 시설 및 장비 기준 제정
- 인증기관의 시설 및 장비의 안전운영 여부 점검 또는 이에 상응하는 조치
- 인증기관의 인증서와 인증서 폐지목록 게시
- 인증관리센터가 생성한 모든 인증서와 인증서 폐지목록의 보관
- 인증기관 관리에 관련된 정보 및 기록의 유지 등
- 행정전자서명 인증관리체계에 속하는 기관 및 가입자에 대한 인증업무 관련 교육
- 행정전자서명 기술표준 및 행정전자서명과 공인전자서명의 상호 연계 방안 마련
- 기타 최상위인증기관으로서 인증업무와 관련하여 필요하다고 인정되는 업무
- 인증협의회의 소집 및 진행

1.3.3 인증기관

행정전자서명 인증기관(CA : Certification Authority)은 행정자치부장관으로부터 인증업무를 위탁받아 고시에 의해 지정된 기관이다.
인증기관은 다음과 같은 업무를 수행한다.

- 등록기관 지정 및 관리
- 등록기관 및 가입자의 신원확인
- 등록기관 및 가입자 인증서의 발급, 갱신, 폐지 및 인증서 폐지목록의 게시
- 해당 인증기관에서 발급한 인증서의 유효성 확인
- 암호키 위탁·복구 서비스 및 관련 기록의 유지
- 인증업무에 관한 기록의 안전한 보관・관리
- 시점확인서비스 등 기타 인증기관으로써 필요하다고 인정되는 업무

1.3.4 등록기관

행정・공공 인증기관으로부터 인증업무를 위탁받은 등록기관(RA : Registration Authority)은 다음과 같은 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
- 가입자 정보의 보호
- 인증기관으로부터 발급받은 행정전자서명생성키의 안전한 관리

1.3.5 인증협의회

- 인증협의회는 인증업무의 효율적 수행을 위하여 구성된 협의체로 인증기관, 국가정보원 및 민간전문가 등으로 구성한다.
- 인증협의회는 다음의 사항을 협의하기 위하여 필요시 인증관리센터의 장이 소집한다.
- 인증업무 운영을 위한 인증정책에 관한 사항
- 행정전자서명의 이용확산을 위한 제도의 개선 및 관계 법령의 정비에 관한 사항
- 인증기관 간 상호 연계 및 국제협력에 관한 사항
- 기타 행정전자서명의 안전성과 신뢰성 확보 및 이용촉진을 위해 필요한 사항

1.3.6 정부통합전산센터

정부통합전산센터는 정부기관의 주요정보통신기반시설을 운영하는 국가기관이다.
행정전자서명 인증체계의 모든 시스템은 정부통합전산센터의 자산으로 이관되어 있으며, 국가의 주요 정보통신 기반시설 운영 절차에 따라 운영된다. 인증관리 업무와 관련하여 인증시스템에 대한 물리적 보안, 시스템에 대한 접속통제 및 승인 업무를 주관한다.

1.3.7 한국지역정보개발원

한국지역정보개발원은 행정자치부장관으로부터 인증관리센터의 운영업무를 위탁받은 기관이다.
행정전자서명 인증체계를 유지하기 위한 운영업무를 수행한다.

1.4 인증서의 용도

1.4.1 인증서 종류 및 용도

최상위 인증기관이 발급한 인증기관용 인증서는 등록기관용, 개인용 및

기관용 인증서를 발급하는데 사용한다.

1.4.2 행정전자서명 인증서 이용 제한

행정전자서명 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 행정전자서명 인증업무준칙(CPS) 관리

1.5.1 행정전자서명 인증업무준칙 제정 및 개정

인증관리센터는 행정전자서명 인증업무준칙을 제정하고 인증 정책의 일관성을 유지하기 위한 개정을 관리한다.

1.5.2 행정전자서명 인증업무준칙의 담당

행정전자서명 인증업무준칙과 관련된 담당자의 연락처는 다음과 같다.
URL : www.gpki.go.kr
이메일 : gpki@korea.kr

1.5.3 행정전자서명 인증업무준칙의 책임

행정전자서명 인증업무준칙의 제정 및 개정의 책임은 인증관리센터장에게 있다.

1.5.4 행정전자서명 인증업무준칙의 개정

기술적 또는 절차적인 변경 등의 사유가 발생할 경우 인증관리센터장의 승인을 받아 행정전자서명 인증업무준칙을 개정한다.

1.6 정의 및 약어

- **행정전자서명인증서(GPKI)** : 행정전자서명이 진정한 것임을 확인·증명할 수 있도록 하기 위하여 전자정부법 제2조9호에 해당하는 법인·기관 및 단체 또는 그 기관에서 직접 업무를 담당하는 자에게 발급하는 전자적 정보를 말한다.
- **행정전자서명생성키(개인키 private key)** : 행정전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.
- **행정전자서명검증키(공개키 public key)** : 행정전자서명을 검증하기

위하여 이용하는 전자적 정보로 인증서 내에 포함되는 정보를 말한다.

- **행정전자서명 :** 행정기관, 공무원이 사용하는 법적인 효력이 있는 전자서명을 말한다.
- **해쉬 함수(Hash Function) :** 임의의 길이의 문자열을 고정된 길이의 이진 문자열로 매핑하여 주는 함수. 데이터를 자르고, 치환하거나 위치를 바꾸는 방법 들로 결과를 만들어 내며, 이 결과를 해시 값(hash value)이라 한다. 해시 함수는 데이터의 무결성, 인증, 부인 방지 등에서 응용되는 중요한 함수 가운데 하나이다.
- **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 공고 등 인증서 및 인증관련 기록의 관리 등의 업무를 말한다.
- **인증서 폐지목록(CRL : Certificate Revocation List) :** 인증서 효력이 상실된 인증서들의 목록으로 인증기관에서 주기적으로 발급하는 전자적 정보를 말한다.
- **인증기관(CA : Certification Authority) :** 전자서명 인증서를 발급하는 신뢰 기관으로 인증서 폐지목록을 주기적으로 발행하며, 디렉토리 시스템에 인증서와 인증서 폐지목록을 게시 등의 인증업무를 담당한다.
- **인증 :** 행정전자서명생성키가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명해 주는 행위를 말한다.
- **실시간 인증서 상태 검증(OCSP : Online Certificate Status Protocol) :** 인증서 폐지목록을 획득하지 않고도 실시간으로 인증서의 상태를 검증할 수 있도록 하는 인증서상태 실시간검증프로토콜을 말한다.
- **등록기관(RA : Registration Authority) :** 인증기관의 인증업무 중 가입자에 대한 신원확인과 가입자 정보를 등록·관리하며 인증서 신청 및 인증서 폐지신청 등의 인증업무를 수행하는 기관을 말한다.

- **객체식별자(OID : Object Identifier) :** 행정전자서명 인증서 내에는 가입자(DN), 발급자, 버전 등 기본정보 외에 알고리즘, 인증서 정책, 키용도, 인증서 속성 등이 포함되며, 정보들이 표현하는 대상을 객체(Object)라 한다. 이러한 객체들을 유일하게 중복되지 않고 식별하기 위해서는 각 객체에 고유번호를 부여하는 방법이 사용되며, 이것을 객체식별자 (OID, Object Identifier)라 한다.
- **가입자 :** 인증기관으로부터 인증서를 발급받은 개인 또는 법인·기관 및 단체를 말한다.
- **TSA(Time Stamp Authority) :** 시점확인을 요청한 전자문서에 대하여 당해 전자문서가 인증기관에 제시된 특정시점을 확인하여 알려주는 기관을 말한다.
- **LDAP(Lightweight Directory Access Protocol) :** 디렉토리 서버와 클라이언트 간의 통신에 사용되는 디렉토리시스템 접근 프로토콜로서, DAP보다 간결하고 실용적으로 만들어진 프로토콜을 말한다.
- **DN(Distinguished Name) :** 가입자 객체를 명확히 구별할 수 있도록 부여하는 고유한 이름을 말한다. 행정전자서명인증서에 있는 행정기관, 공무원들이 유일한 인증서를 소유하는 것을 식별하기 위한 표준화된 식별 명칭

2. 게시 및 보관 책임

인증관리센터는 행정전자서명 인증업무준칙(CPS)을 인증관리센터 홈페이지(www.gpki.go.kr)에 게시한다.
인증관리센터는 인증서와 인증서의 상태 정보는 정부디렉토리 시스템(ldap://cen.dir.go.kr)에 게시하고 인증서에 변경이 발생한 경우에는 이를 수정하여 게시한다.
인증관리센터는 게시된 행정전자서명 인증업무준칙(CPS)을 필요시 수정 한다. 인증업무준칙(CPS)의 변경이 발생한 경우 개정 버전과 유효 일자를 관리한다.

2.1 저장장소

인증관리센터는 행정전자서명 인증업무준칙을 포함하여 행정전자서명 인증서비스에 필요한 신청서 양식과 관련 규칙을 인증관리센터 홈페이지에 게시한다.
인증기관 폐지목록(ARL)과 발급된 인증서의 정보는 정부디렉토리시스템에 게시한다.

2.2 정보공개 채널

홈페이지 : www.gpki.go.kr
전자메일 : gpki@korea.kr

2.3 정보공개 빈도

행정전자서명 인증업무준칙과 행정전자서명 인증서 신청양식이 변경된 경우 인증관리센터 홈페이지에 게시한다. 인증기관 폐지목록(ARL)을 주 1회 게시한다.

2.4 접근 통제

인증관리센터 홈페이지에 게시된 정보는 누구나 열람 할 수 있도록 공개되어 있다.

2.5 정확한 정보의 유지

인증관리센터는 CPS와 인증기관 폐지목록(ARL)의 정보를 정확하게 유지

하기 위해 필요한 업무를 수행한다.

3. 인증서 식별 및 인증

3.1 인증서의 명칭 및 DN 체계

행정전자서명인증서의 명칭 및 DN체계는 X.509 규칙을 준수한다.

3.1.1 인증서 DN의 종류

인증기관에서 발급한 인증서 DN명은 cn명,ou명,o=,c=kr 체계를 준수한다.

인증기관 인증서 cn : cn=인증기관구분자(2)+기관코드(7)+일련번호(2)

3.1.2 신청인을 식별할 수 없는 익명의 인증서발급

해당사항 없음

3.1.3 인증서 DN값의 유일성

행정전자서명인증서의 DN은 유일한 값을 갖는다.

3.1.4 인증서 DN의 규칙

행정전자서명인증서의 기본영역에 사용되는 명칭과 해석 규칙은 행정전자서명 기술요건 3.OID 및 DN 체계에 따라 의미 있는 식별체계를 갖는다.

3.1.5 행정전자서명 상표(Trade marks)의 사용

해당사항 없음

3.2 최초 신원확인

3.2.1 인증기관의 초기 신원확인

최상위인증기관은 행정자치부장관이 고시한 인증기관에게만 인증기관용 인증서를 발급한다.

인증기관용 인증서는 CSR파일의 공개키를 확인한 후 발급한다.

3.2.2 기관용 인증서의 초기 신원확인

해당사항 없음

(CA)인증기관은 행정전자서명 인증신청서(기관용)를 작성한 기관의 행정

표준코드가 확인되면 신뢰할 수 있는 기관으로 인정한다.

3.2.3 개인용 인증서의 초기 신원확인

해당사항 없음

(CA)인증기관은 정부디렉토리시스템에 인사정보가 등록되어 있는 경우 개인의 신원을 신뢰한다.

3.2.4 신원이 확인되지 않은 인증서의 발급

신원이 확인되지 않은 인증서의 신청에 대해서는 인증서를 발급하지 않는다.

3.2.5 권한의 발효

인증서는 인증서 발급과 동시에 권한이 발효된다.

3.2.6 상호 운용 기준

최상위 인증기관(RootCA)은 인증서신뢰목록(CTL) 기반으로 공인인증체계(NPKI)와 상호 운용 한다

3.3 키 교체 요청에 의한 신원확인과 인증

해당사항 없음

4. 인증서 생명주기 운영 요건

4.1 인증서 신청

인증기관 인증서 발급은 공문으로 신청한다. 공문 발송 시 PKCS#10 인증서 서명 요청(Certificate Signing Request: CSR) 형식으로 인증기관 공개키를 함께 제출해야 한다.

4.1.1 인증서 신청 기준

전자정부법 시행령 제89조 제1항에 의거 행정자치부장관이 인증업무를 위탁한 기관만이 인증기관 인증서를 발급 신청할 수 있다.

4.1.2 인증서 신청 절차 및 책임

인증기관은 제출한 신청서의 신청정보가 정확해야 하며, 신청내용에 대하여 책임을 진다.

4.2 인증서 신청 처리

4.2.1 신원확인 및 인증

최상위인증기관은 인증기관이 신청한 정보의 정확성 및 신원확인을 공문을 통해서만 확인한다. 일반적으로 해당기관의 부서장 또는 기관장 명의의 공문에 의해 신원 확인을 한다. 신원확인 절차를 거친 신청자에게만 인증 정보를 제공한다.

4.2.2 신청에 대한 승인 및 거절

제출된 공문과 신청자의 신원 확인과정에서 신청서 내용이 허위로 기재하였거나 신청자가 인증기관의 대표 자격이 없다고 판단 될 경우, 인증기관 업무 또는 기술적으로 지장이 있다고 판단하는 경우는 신청을 거절할 수 있다. 신청에 대한 승인 및 거절은 공문으로 회신한다.

4.2.3 신청 처리 소요 시간

인증관리센터는 30일 내에 인증서 발급을 수행한다.

4.3 인증서 발급

인증관리센터가 발급하는 인증서는 전자정부법시행령 제30조(인증서의 발

급)에 의하여 다음 각 호의 사항이 포함된다.

- 인증을 받는 행정기관의 명칭
- 가입기관 등의 행정전자서명검증키(공개키)
- 가입기관등과 해당 인증기관이 이용하는 행정전자서명의 방식
- 인증서의 일련번호
- 인증서의 유효기간
- 소관 인증기관의 명칭
- 인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항
- 가입기관 등이 대결(代決)하는 경우 이에 관한 사항

4.3.1 인증서 발급 절차

인증관리센터는 인증서 발급 시 다음의 내용을 확인한다.

- 신청기관이 제출한 요청양식(CSR)에서 행정전자서명검증키(공개키)와 DN을 추출
- 행정전자서명검증키(공개키)의 유일성 확인
- 행정전자서명검증키(공개키)가 인증기관이 소유한 행정전자서명생성키(개인키)와 합치하는 지 확인
- DN의 유일성 확인 및 규격준수 여부 확인

4.3.2 인증서 발급 통지

인증관리센터는 인증기관 인증서를 발급 후 공문으로 통지한다.

4.4 인증서 수령

4.4.1 인증서 수령 절차

인증기관은 공문으로 인증기관 인증서를 수령하며 특별한 사유가 없는 한 거부할 수 없다.

4.4.2 인증서 게시

인증관리센터는 인증기관 인증서 발급과 동시에 공개된 저장소(디렉토리)에 인증서를 게시한다.

4.4.3 인증서 발급 공지

인증관리센터는 인증서가 발급되었음을 웹에 게시하고 필요시 유관 인

증기관에 통보한다.

4.5 인증키 쌍 및 인증서 용도

4.5.1 행정전자서명생성키(개인키) 사용 용도

행정전자서명생성키(개인키)는 전자서명 및 암호화 통신 등 인증업무 수행을 위해서만 사용한다.

4.5.2 행정전자서명검증키(공개키) 사용 용도

인증관리센터는 행정전자서명검증키(공개키) 확장 필드에 명시된 용도로만 사용한다.

- 인증서의 서명을 검증하기 위해 사용될 때 설정된다. 이 비트는 인증기관 인증서에만 해당 (KeyCertSign)
- 인증서 신뢰목록(CTL), 인증서기관 폐지목록(ARL), 인증서 폐지목록(CRL)의 서명을 검증하기 위해 사용될 때 설정되어야 한다. 인증관리센터경우 이 비트는 인증기관 인증서에만 해당 (CRLSign)

인증기관은 발급한 인증서에 대하여 CRL을 제공한다. 일반적으로 인증기관 인증서는 공개된 저장소(디렉토리)에 게시되며 X.509 기반의 경로검증 시 사용된다.

4.6 인증서 갱신

4.6.1 인증서 갱신 기준

인증기관 인증서는 최상위인증기관 인증서 유효기간 내에서 갱신할 수 있다.

4.6.2 인증서 갱신 신청자

 행정자치부장관이 인증업무를 위탁한 기관만이 인증기관 인증서를 갱신 신청할 수 있다.

4.6.3 인증서 갱신 절차

신규 발급절차와 동일하며, 4.6.1을 제외하고 인증서가 갱신되지 않는다. 인증관리센터는 인증서 갱신 시 다음의 내용을 확인한다.

- 신청기관이 제출한 요청양식(CSR)에서 행정전자서명검증키(공개키)

와 DN을 추출

- 행정전자서명검증키(공개키)의 유일성 확인
- 행정전자서명검증키(공개키)가 인증기관이 소유한 행정전자서명생성키(개인키)와 합치하는지 확인
- DN이 기존 발급된 DN과 동일한지 확인 및 규격준수 여부 확인

4.6.4 인증서 갱신 통지

인증관리센터는 인증기관 인증서를 갱신 후 공문으로 통지한다.

4.6.5 인증서 갱신 승인

본 문서 4.6.3에 따라 인증서 갱신을 승인한다. 승인 및 거절은 공문으로 회신한다.

4.6.6 인증서 갱신 게시

인증관리센터는 인증기관 인증서 갱신과 동시에 공개된 저장소(디렉토리)에 인증서를 게시한다.

4.6.7 인증서 갱신 공지

인증관리센터는 인증서가 갱신되었음을 웹에 게시하고 필요시 유관 인증기관에 통보한다.

4.7 인증서 재발급

인증기관의 행정전자서명생성키(개인키) 손상 등 재해발생 시 인증기관 인증서를 폐지하며, 재발급은 하지 않는다.

4.8 인증서 변경

인증기관의 기관명칭 변경되었을 경우를 포함하여 인증기관 인증서는 변경하지 않는다. 인증기관 인증서의 규격 변경 등이 발생했을 경우에는 신규 발급한다.

4.9 인증서 폐지 및 정지

4.9.1 인증서 폐지 기준

인증관리센터는 다음의 사유가 발생한 경우 인증기관의 인증서를 폐지

한다.

- 인증기관의 조직 해산 등 더 이상 인증업무를 수행하지 않을 경우
- 인증기관의 행정전자서명생성키(개인키)가 손상되었을 경우
- 인증기관이 인증서 폐지신청 한 경우
- 인증기관이 인증업무 위탁받은 날로부터 2년 이내 인증업무를 게시하지 못 한 경우

4.9.2 인증서 폐지 신청자

행정자치부장관이 인증업무를 위탁한 기관만이 인증기관 인증서를 폐지신청할 수 있다.
최상위인증기관은 4.9.1를 기준으로 인증기관 인증서를 폐지 할 수 있다.

4.9.3 인증서 폐지 절차

4.9.1를 기준으로 인증서를 폐지한다.

4.9.4 인증서 폐지 게시

인증관리센터는 인증기관 인증서 폐지 시 인증기관 폐지목록(ARL)을 갱신하고 필요시 유관 인증기관에 통보한다.

4.9.5 인증서 폐지 소요 시간

인증기관 인증서 폐지는 공문 접수 후 30일내에 처리한다. 인증기관 인증서 폐지 시 다음 인증기관 폐지목록(ARL)이 게시될 경우 공개된 저장소(디렉토리)에 반영된다.

4.9.6 인증서 폐지 확인 요구사항

인증서 검증자는 ARL을 이용하여 인증서 유효성을 확인해야 한다.

4.9.7 인증서 폐지 목록(ARL) 발행 빈도

인증기관 폐지목록(ARL)은 7일 주기로 발행한다.

4.9.8 인증서 폐지 목록(ARL) 발행 최대 소요 시간

인증기관 폐지목록(ARL) 발행은 주기적으로 자동 처리 운영된다.

4.9.9 실시간 인증서 폐지 및 상태 확인 유효성

해당사항 없음

4.9.10 실시간 인증서 폐지 확인 요구사항

해당사항 없음

4.9.11 인증서 폐지 정보 유효성 검증의 다른 방법

해당사항 없음

4.9.12 키교체 또는 키손상의 특수 요구사항

인증기관은 인증기관 행정전자서명생성키(개인키) 손상 시 최상위인증기관에 즉시 보고 후 키손상에 따른 인증기관 인증서 폐지 신청 공문을 발송한다. 최상위인증기관은 인증기관 인증서를 폐지한다.

4.9.13 인증서의 정지 사유

해당사항 없음

4.10 인증서 상태 서비스

지원하지 않음

4.11 인증 서비스 해지 및 종료

조직개편 등 인증업무의 해지 사유가 발생한 인증기관의 장은 인증관리센터와 협의하여 당해 기관의 인증업무를 행정자치부 장관이 지정하는 인증기관에 인계하여야 한다. 인증기관의 인증업무는 행정자치부 장관의 변경고시에 의해 서비스가 종료된다.

4.12 키위탁 및 복구

해당사항 없음

5. 시설 관리 및 운영 보호조치

5.1 물리적 보호조치

5.1.1 위치 및 시설

행정전자서명 인증시스템은 국가가 지정한 주요정보통신 기반시설에 위치하고 있으며, 국가의 관리 규정에 따라 운영된다.

5.1.2 물리적 접근

행정전자서명 인증시스템은 보안요원의 통제에 따라 승인된 외부인의 출입과 접근만을 허용되며 해당 출입내역은 기록된다.

5.1.3 전원 및 공조시설

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

5.1.4 침수 대비

행정전자서명 인증시스템은 침수로부터 안전하게 보호되기 위해 전산실 바닥으로부터 이격하여 설치된다.

5.1.5 화재 예방 및 보호

행정전자서명 인증시스템은 화재 탐지 및 자동 소화 설비가 설치된 공간에서 운영된다.

5.1.6 매체 저장

행정전자서명 인증시스템에 보관된 데이터의 손실, 파손의 위험으로부터 주요 정보를 보호하기 위해 백업장비를 이용하여 백업한다.

5.1.7 폐기물 처리

정부통합전산센터는 행정전자서명 인증시스템을 폐기할 경우 폐기물의 종류에 따라 안전하게 처리한다.

5.1.8 원격지 백업

행정전자서명 인증시스템의 데이터 보호를 위해 물리적으로 분리된 백업센터에 원격백업 된다.

5.2 절차적 보호조치

5.2.1 신뢰된 역할

행정전자서명 인증체계의 신뢰성을 확보하기 위해 인증관리센터 운영 책임자는 다음과 같이 신뢰성 역할을 지정하고 승인한다.
지정된 신뢰성 역할은 매년 현행화 한다.

5.2.2 주요 업무별 수행인력

- 인증업무 정책 관리자는 행정전자서명 인증업무 정책 수립, 등록, 유지 및 개정한다.
- 보안관리자는 출입통제 등 인증관리센터 보안 통제 관리한다.
- 인증업무운영 관리자는 인증 시스템의 설치 운영 및 운영유지보수의 업무를 총괄한다.
- 인증시스템 운영자는 2인 이상의 직원을 배치하여 인증시스템 운영 및 유지보수 업무를 수행한다.
- 서비스데스크는 고객 문의에 대한 상담 업무를 수행한다.
- 키 생성 담당자는 인증기관 키 생성 및 활성화 업무를 수행한다.
- 인증업무 개발자는 인증 홈페이지 등을 관리한다.

5.2.3 업무 담당자 신원 확인 및 인증

인증관리센터 업무 담당자는 신원카드 및 지문을 통하여 인증관리센터 출입을 통제한다. 인증 업무시스템 접근 시 각 개인 인증서로 접근 통제 한다.

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 신원 확인

행정전자서명 인증체계의 운영인력은 국가의 신원확인 결과 결격 사유가 없어야 한다.

5.3.3 교육 및 훈련

인증업무 수행 인력은 업무수행에 필요한 보안규정, 내부관리절차 및 기술교육을 이수 한다.

5.3.4 재교육 및 훈련

인증업무 수행 인력은 매년 보안 및 관련 기술 교육을 이수한다.

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 Independent contractor 요건

해당사항 없음.

5.3.8 직원의 문서공개

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

5.4 감사로깅(Audit logging) 절차

행정전자서명 인증시스템은 주기적인 감사를 위해 주요 이벤트에 대한 로그(Log)를 보관한다.

5.4.1 로그(Log)의 유형

응용 프로그램(RootCA)는 다음과 같은 이벤트 로그를 기록한다.

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

5.4.2 로그(Log)의 검토 주기

로그(Log)는 로그 감사자에 의해 주 1회 검토한다

5.4.3 로그(Log)의 보관 기간

로그(Log)의 보관기간은 저장 공간의 가용성과 관리의 효율성을 고려하여 유형에 따라 10년간 보관한다.

5.4.4 감사로그(Log)의 보호

감사로그의 삭제는 권한있는 관리자에 의해서만 수행된다.

5.4.5 감사로그(Log)의 백업

해당 로그는 실시간 백업 된다.

5.4.6 로그(Log) 취합 시스템

로그는 내부 시스템에 저장된다.

5.4.7 로그(Log) 대상에 대한 통지

로그를 발생시킨 개인 및 기관에게 감사수행과 관련하여 별도 통지하지 않는다.

5.4.8 취약점 측정

취약점은 인증 시스템의 기능을 유지하는데 위협이 되는 요소를 식별하고 그 가능성을 줄이기 위한 기술적 관리적 요소를 평가한다.

5.5 기록(Records)의 보관

5.5.1 기록(Records)의 종류

행정전자서명 인증서를 발급하기 위해 필요한 정보를 기록으로 관리한다.

5.5.2 기록(Records)의 보관 기간

기록의 보관 기관은 10년으로 한다.

5.5.3 기록(Records)의 보호

행정전자서명 인증서 신청기록은 변조되지 안도록 전자파일로 변환하여

정보시스템에 보관한다. 기록의 유실로부터 정보를 보호하기 위해 정보시스템은 주기적으로 백업되고 관리된다.

5.5.4 기록(Records)의 보관 절차

전자화된 기록은 백업장비를 이용하여 별도의 매체에 보관된다.

5.5.5 기록(Records)의 시점보유(Time-Stamping) 요건

해당사항 없음

5.5.6 기록(Records) 취합 시스템

관련 기록은 전자결제 시스템으로 취합한다.

5.5.7 정보의 청구 절차

행정전자서명 인증시스템과 관련된 정보는 인증관리센터와 사전협의 후 요청기관 명의의 공문을 통해 요청한다. 인증관리센터는 공문으로 접수된 요청에 대해서 공문으로 회신한다.

5.6 키 변경

행정전자서명 인증시스템의 키 유효 기간이 만료하거나 서명 키의 비밀번호 분실, 키 파손 등의 사유가 발생한 경우, 행정전자서명 인증시스템은 동일한 기능과 권한이 있는 키를 재발급 한다. 키의 재발급 절차는 키 신규발급 절차와 동일한 절차로 수행한다.

5.7 재해 복구

재난 발생시 행정전자서명 인증시스템은 물리적으로 독립된 위치에 독립된 장소에서 업무를 재개할 수 있다.

5.7.1 정보시스템 재해복구 절차

행정전자서명 인증시스템의 업무에 심각한 위험을 초래하는 재난이 발생한 경우 재해복구절차에 따라 기반시설과 전산장비를 복구하고, 행정전자서명 인증센터의 재해복구절차에 따라 인증 업무를 재개한다.

5.7.2 정보시스템 자원의 손상된 경우의 절차

재해복구 절차에 따라 소산된 키를 이용하여 인증체계를 복구한다.

5.7.3 키 소실에 대한 복구 절차

CA 서명키의 파손 또는 사용의 위험이 발생한 경우 인증관리센터는 CA 서명키를 재발급 하고 이에 따른 기관과 개인에게 발급된 모든 키를 재발급 한다.

5.7.4 업무연속성 확보

행정전자서명 인증시스템은 국가의 연속성계획에 따라 주 센터와 백업 센터체계로 운영되며, 재해로 인해 주 센터에서 인증서비스를 하지 못하는 경우 백업 센터에서 기반 인프라, 정보시스템 및 인력을 포함한 대체 운영체계를 가동한다.

5.8 CA 또는 RA의 위임 종료

인증관리센터는 최상위 인증기관으로서 인증기관의 위임 종료시 이를 공지하고 인증기관이 발급한 인증서를 재발급 한다.

인증관리센터는 인증기관으로서 등록기관의 위임 종료시 이를 공지하고 등록기관의 위임 종료시 업무공백이 발생하지 않도록 한다.

6. 기술적 보호조치

6.1 키쌍 생성 및 절차

6.1.1 키쌍 생성 절차

최상위인증기관(RootCA) 키 쌍은 키 생성 절차에 따라 생성한다. 키 생성은 FIPS 140-2 레벨 3 인증을 받은 HSM을 사용한다. 키 생성 작업은 권한이 부여된 최소 2인의 참여로 실시한다.

6.1.2 개인키 전달 절차

해당사항 없음

6.1.3 공개키 전달 절차

(최상위)인증기관은 PKCS#10형식의 CSR파일을 공문의 첨부파일로 인증관리센터에 제출한다.

6.1.4 관련자에게 최상위인증기관 공개키 제공 절차

인증관리센터 웹사이트에 최상위인증기관(RootCA) 인증서 및 지문(FingerPrint) 정보를 게시한다.

6.1.5 키 길이

안전하고 신뢰성 있는 행정전자서명 알고리즘을 사용하기 위하여 다음과 같은 크기의 키를 사용한다.

- RSA의 경우 2048비트 이상
- ECDSA의 경우 224비트 이상

6.1.6 공개키 매개변수 생성 및 품질 검사

(최상위)인증기관 인증서 신규 발급 시 및 행정전자서명검증키(공개키)가 (최상위)인증기관이 소유한 행정전자서명생성키(개인키)와 합치하는 지 확인 및 DN의 유일성 확인 및 규격준수 여부를 확인한다.

6.1.7 키 사용 용도

X.509 확장필드에 명시된 사용용도로만 사용한다. 사용용도는 본 문서의 4.5.2에 정의되어 있다.

6.2 개인키 보호 및 암호화 모듈

6.2.1 암호화 모듈의 기준

‘인증기관 시설 및 장비 등에 관한규정’ 및 FIPS-140-2 레벨 3을 만족하는 보안 모듈을 이용한다.

6.2.2 다중 통제

행정전자서명 키관리 정책의 다중 통제는 별도의 접근통제 권한을 가진 자가 수행하며, 지정된 3명 중 2명 이상 참여 하에 다중 통제를 수행한다.

6.2.3 개인키 위탁

해당사항 없음

6.2.4 개인키 백업

최상위인증기관 행정전자서명생성키(개인키)의 백업키는 하드웨어 전자서명 모듈(HSM) 백업 장비에 저장한다.

6.2.5 개인키 보관

최상위인증기관 행정전자서명생성키(개인키) 백업 장비는 별도의 안전한 장소에 보관한다.

6.2.6 개인키 추출

해당사항 없음.

6.2.7 개인키 저장

하드웨어 전자서명 모듈(HSM) 내부에 안전하게 저장된다.

6.2.8 개인키 활성화

최상위인증기관 행정전자서명생성키(개인키)는 복수의 오퍼레이터에 의해 조작키와 비밀번호를 사용하여 활성화된다.

6.2.9 개인키 비활성화

모듈은 항상 활성화 되어 있다.

6.2.10 개인키 삭제 및 파괴

최상위인증기관 키가 더 이상 필요하지 않을 경우, HSM 파티션에서 삭제된다. 또한 백업세트의 제거도 포함된다.

6.2.11 암호화 모듈 등급

이 CPS의 섹션 6.2.1을 참조

6.3 키쌍 관리

6.3.1 공개키 보관

공개키의 보관은 이 CPS의 섹션 5.5.2의 기간 동안 보관된다. 공개키는 최상위인증시스템(RootCA) 데이터베이스에 포함되어 있다.

6.3.2 인증서 운영기간 및 사용기간

최상위 인증서(Root)는 20년, 인증기관 인증서(CA)는 10년이다. 해당 인증서는 유효기간까지 사용가능한다.

6.4 활성화 데이터 (Activation Data)

활성화 데이터는 하드웨어 전자서명 모듈(HSM)을 작동 및 사용하는데 필요한 정보이다. 활성 데이터의 예로는 핀, 암호문과 키 분할 체계 등이 있다.

6.4.1 활성화 데이터 생성

활성 데이터는 하드웨어 전자서명 모듈(HSM)의 사양에 따라 생성된다. 이 하드웨어는 FIPS 140-2 인증된다.

6.4.2 활성화 데이터 보호

활성 데이터를 보호하기 위해 사용되는 절차는 데이터가 핀 번호 와 접근 인증용 키에 의존한다. 접근 인증용 키는 지정된 관리자에 의해 유지된다. 핀 번호는 인증관리센터의 암호화 정책에 적용된다.

6.4.3 활성화 데이터 추가 고려사항

규정하지 않는다.

6.5 컴퓨터 보안

관련 시스템에 대해 기술적 관리적 물리적 보안방안을 준수하며 보안점검 활동을 수행하여 안전하게 관리 한다.

6.5.1 특정 컴퓨터 보안 요건

최상위인증시스템(Root)은 엑세스 제어 기능, 작업자 식별 및 확인 기능, 감사 로그 수집 기능, CTL/ARL 생성기능을 가지고 있다.
인증시스템(CA)은 엑세스 제어 기능, 작업자 식별 및 확인 기능, 감사 로그 수집 기능, CRL 생성기능을 가지고 있다.

6.5.2 시스템 보안 요건

최상위인증시스템(RootCA) 접근 시 패스워드 및 인증서 등 2가지 이상의 보안을 요구한다. 시스템 접근 매체는 독립된 장소에서 보호되고 있다.

6.6 생명주기 보안

6.6.1 시스템 개발 통제

최상위인증시스템(RootCA)의 기능 변경, 성능 개선 시 위탁기관, 주관기관의 승인 하에 실시된다.

6.6.2 보안 관리 통제

최상위인증시스템(RootCA)에 접근하는 모든 컴퓨터에 대하여 적절한 업무분장이 되어 있으며, 접근 권한을 최소화하여 운영한다.
최상위인증시스템(RootCA) 접근을 위해서는 인증관리센터, 위탁기관, 주관기관의 승인이 필요하며, 접근 인력의 업무변경 시 주기적으로 권한변경을 한다.

6.6.3 생명주기 보안 통제

해당사항 없음

6.7 네트워크 보안

침입탐지시스템 및 침입차단시스템에 의해 네트워크가 보호되고 있다.

6.8 시점 확인

최상위인증시스템(RootCA)의 시간은 NTP를 사용한다.

7. 인증 규격

행정전자서명인증서, 인증기관 폐지목록(ARL)은 “행정전자서명 기술요건”을 준수한다.

7.1 인증서 프로파일 규격

인증관리센터는 공인전자서명인증체계 기술규격을 준수하고 X.509 V3 표준을 준용하는 행정전자서명인증서를 발급•공고한다.

7.1.1 인증서 버전

인증관리센터는 X.509 V3 인증서를 발급한다. (버전 필드 값은 숫자 2로 지정)

7.1.2 인증서 확장

인증관리센터에서 발급되는 인증서는 "행정전자서명 기술요건" 에 명시된 인증서 확장 필드를 사용한다.

7.1.3 알고리즘 개체 식별자

인증서 알고리즘 OID는 “행정전자서명 기술요건" 체계를 준수한다.

sha256WithRSA Encryption	iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(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

발급자 DN과 주체 DN은 "행정전자서명 기술요건" 체계를 준수한다.

7.1.5 이름 양식

해당사항 없음.

7.1.6 인증서 정책 개체 식별자

인증서 정책(Certificate Policies)의 정책 식별자(OID)는 "행정전자서명 기술요건" 체계를 준수한다.

7.1.7 정책 제한 확장의 사용

인증서 정책 필드(Certificate Policies)의 제한여부는 “행정전자서명 기술요건” 체계를 준수한다.

7.1.8 정책 한정자 구문 및 의미

해당사항 없음

7.1.9 주요 인증서 정책 확장에 대한 의미 처리

인증서 확장필드 내 PolicyQualifierId는 “행정전자서명 기술요건” 체계를 준수한다.

7.2 인증서 폐지목록 프로파일 규격

인증서 소유자의 조직정보가 변경되거나 비밀키의 신뢰가 손상 되었을때 인증서를 폐지할 필요가 있다 본 기술요건에서는 X.509 V2 인증서 폐지목록이 사용 된다

7.2.1 버전

행정전자서명인증서 폐지목록은 X.509 V2로 사용된다. (버전 필드 값은 숫자 1로 지정)

7.2.2 확장 필드

인증서 폐지목록의 확장필드는 “행정전자서명 기술요건” 체계를 준수한다.

7.3 실시간인증서 상태검증 프로파일 규격

해당사항 없음.

8. 감사 준수 및 기타 평가

행정전자서명 인증업무준칙의 모든 사항은 국내·외 법·제도 및 관련 기술표준을 준용하며, 독립된 제3자에 의해 정기적인 감사를 수행한다.

8.1 평가 빈도 및 환경

감사는 최대 1년을 넘지 않고, 주기적으로 수행 한다.

8.2 평가 주체 및 자격

감사는 아래와 같이 일정한 자격과 기술을 갖춘 인력이 수행 한다.

1. 피감사대상자로부터 독립적인 자
2. 국내·외 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 평가자의 관계

감사자는 피감사 대상자와 금전적으로나 사업적으로 등으로 이해관계가 없어야 한다.

8.4 평가 범위

감사의 범위는 행정전자서명 인증업무준칙의 준수여부, 인증기관 키 관리, 인증서 관리 및 최상위인증기관(RootCA) 시스템관리를 포함한다.

8.5 평가 결과 조치

감사를 통해 발견된 미비점과 특이점은 보고서에 포함되며, 감사결과에 따라 정책적, 기술적 조치를 취하게 되며, 범위는 영향도 등에 따라 결정한다.

8.6 평가 결과 공표

감사결과는 인증관리센터장에게 보고한다.

9. 기타 업무상 및 법적 사항

9.1 요금

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

9.2 재무적 책임

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

9.3 기밀 정보 보호

행정전자서명 인증센터는 인증서비스와 관련하여 취득하고 생성된 정보를 안전하게 보호한다.

9.3.1 기밀 정보의 범위

행정전자서명 인증서비스의 안전성 및 신뢰성이 저하될 우려가 있는 정보에 대해서 기밀로 관리한다.

9.3.2 기밀 정보의 범위를 벗어난 정보

행정전자서명 인증서비스의 안전성 및 신뢰성에 영향이 없는 정보에 대해서는 공개한다.

9.3.3 기밀 정보 보호의 책임

행정전자서명 인증서비스의 기밀 정보는 안전하게 보관되고 인가된 인력에 의해 관리된다.

9.4 개인 정보 보호

행정전자서명 인증센터는 인증서 신청과 관련하여 취득한 개인정보를 개인정보보호법에 따라 안전하게 관리한다.

9.5 지적재산권

행정전자서명 인증체계로부터 발생한 모든 지적 권한은 행정자치부에 있

다.

9.6 보증(Representations and Warranties)

9.6.1 CA 보증(CA Representations and Warranties)

행정전자서명 인증체계는 국내의 관련 법, 법령, 시행규칙 및 준칙을 준수한다.
행정전자서명 인증체계는 CA 업무와 관련하여 행정전자서명 인증업무준칙(CPS)를 준수한다.
행정전자서명 인증체계는 안전하고 신뢰할 수 있는 인증체계 제공을 위해 관련된 표준과 규칙을 준수한다.

9.6.2 RA 보증(RA Representations and Warranties)

최상위 인증기관은 RA 보증과 관련한 해당사항 없음.
인증기관은 RA 업무와 관련하여 행정전자서명 인증업무준칙(CPS)를 준수한다.

9.6.3 사용자 보증(Subscriber Representations and Warranties)

사용자는 행정전자서명 인증서비스의 이용을 위해서 정확한 정보를 제공하여야 한다. 인증기관은 인증서 사용자가 신뢰할 수 있는 서명키 알고리즘과 유효성 검증을 보장한다.

9.7 보증의 철회

해당사항 없음.

9.8 책임의 제한

해당사항 없음.

9.9 면책 사항

해당사항 없음.

9.10 유효기간 및 종료

해당사항 없음.

9.11 의사소통 및 통지

해당사항 없음.

9.12 개정

9.12.1 개정 절차

행전자자서명 인증업무준칙(CPS)은 변경이 필요한 경우 행정전자서명인증센터장의 승인을 받는다. 행전자자서명 인증업무준칙(CPS)의 정책과 무관한 사소한 변경이나 오류 정정 등의 사유가 있는 경우 사전 승인 없이 수정할 수 있다.

9.12.2 개정 공지

CPS의 변경이 발생한 경우 인증센터 홈페이지(www.gpki.go.kr)에 게시한다.

9.12.3 인증체계 식별명(OID)의 변경사항

해당사항 없음

9.13 분쟁해결

행전자자서명 인증체계와 관련하여 발생하는 분쟁은 행정자치부장의 결정에 따른다.

9.14 준거법

행전자자서명 인증업무준칙(CPS)는 국가의 관련법을 준수하며 상충될 경우 상위법을 따른다.

9.15 관련 법률의 준수

행전자자서명 인증업무준칙(CPS)는 전자정부법 및 관련 법령을 준수한다.

9.16 별도 부칙

해당사항 없음.

9.17 기타 조항

해당사항 없음.