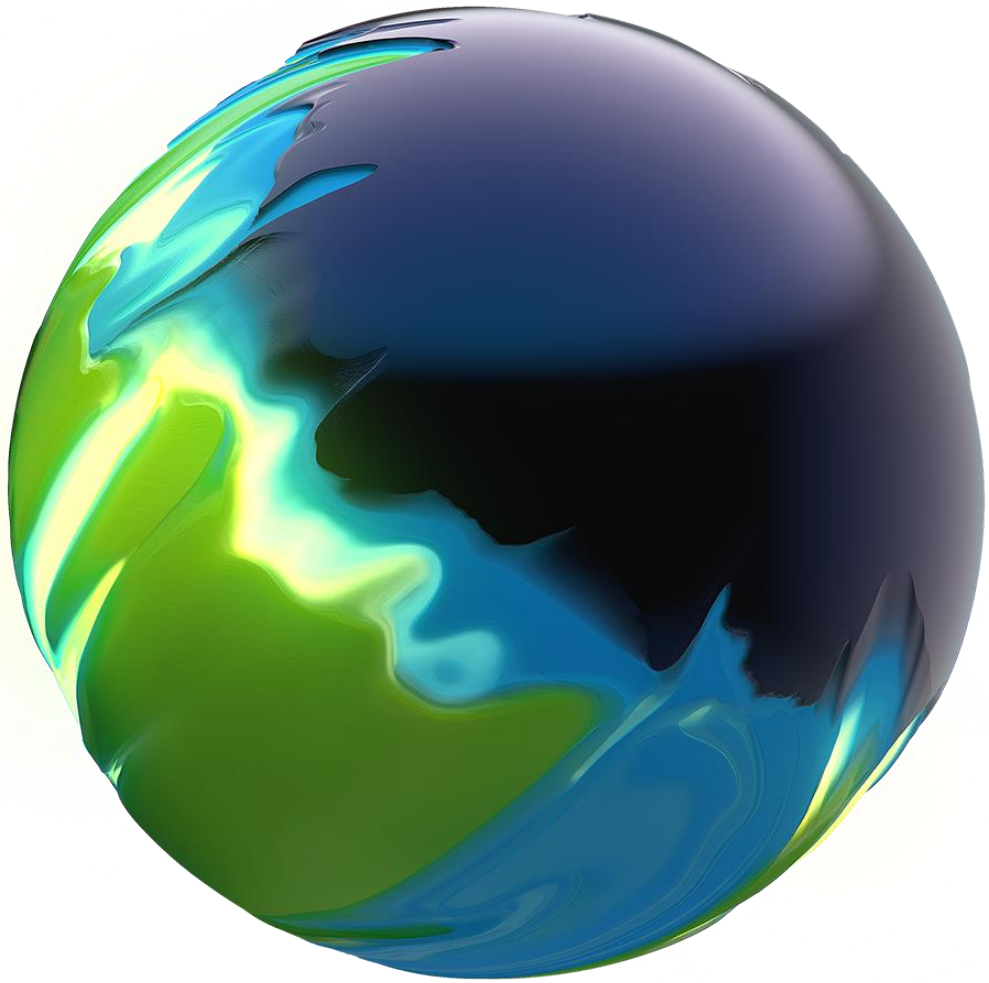
Deloitte.



딜로이트 안진회계법인

전자서명인증업무 평가 안내서

Deloitte Anjin LLC, August 2024, v1.4.0

목차

1. 개요

딜로이트 안진회계법인은 전자서명인증업무 평가신청을 희망하는 전자서명인증사업자에 전자서명인증업무 평가 (이하 "평가") 관련 전반적인 절차 등을 안내하기 위해 본 안내서를 작성하였습니다.

딜로이트 안진회계법인은 2020 년 12 월 22 일, 「전자서명법」 제 10 조제 1 항 및 같은 법 시행령 제 6 조제 4 항에 따라 과학기술정보통신부로부터 평가기관으로 선정되었습니다.

딜로이트 안진회계법인은 「전자서명법」 제 7 조부터 제 13 조에 의거하여, 평가기관으로써 전자서명인증업무 운영기준 (이하 "운영기준") 준수 여부를 평가합니다.

딜로이트 안진회계법인은 「전자서명법」 제 8 조에 따른 운영기준 준수 사실의 평가·인정을 받기 희망하는 전자서명인증사업자를 대상으로 운영기준 준수 여부를 평가합니다.

딜로이트 안진회계법인의 평가는 전자서명인증사업자가 제공하는 전자서명인증업무 및 신원 확인, 가입 신청 접수, 등록을 대행해주는 외부 업체(이하 "등록대행기관")의 전자서명인증업무를 범위로 합니다.

2. 용어 정의

전자서명인증사업자 | 「전자서명법」 제 8 조에 따른 운영기준 준수 사실을 인정받기 위해 딜로이트 안진회계법인에 평가를 신청하는 자를 말하며, 평가 신청자라고도 말합니다.

전자서명인증시스템 | 전자서명인증사업자가 전자서명인증서비스를 제공하기 위해 운영하는 시스템(예: 가입자 등록정보 관리 시스템, 전자서명생성정보 생성·관리 시스템, 인증서 생성·발급·관리 시스템, 기타 전자서명인증업무 수행과 관련된 시스템 및 설비)을 말한다.

인정기관 | 「전자서명법」 제 9 조에 따라 과학기술정보통신부 장관이 지정한 기관(한국인터넷진흥원)으로써, 전자서명인증사업자의 전자서명인증업무 운영기준 준수 인정과 관련한 업무를 수행하는 기관을 말합니다.

평가기관 | 「전자서명법」 제 10 조에 따라 과학기술정보통신부 장관이 지정한 기관으로써, 전자서명인증사업자의 운영기준 준수 여부를 평가하는 기관이며 본 안내서에서는 딜로이트 안진회계법인을 지칭합니다.

등록대행기관 | 전자서명인증사업자를 대신하여 전자서명인증서비스에 가입하려는 자의 신원을 확인하고 가입 신청을 접수·등록하는 등의 업무를 수행하는 자를 말합니다.

평가팀 | 「전자서명법」 시행령 별표 1 에 따른 요건을 갖춘 전문인력으로써, 전자서명인증사업자의 운영기준 준수 여부를 평가하는 자 또는 그룹을 말합니다.

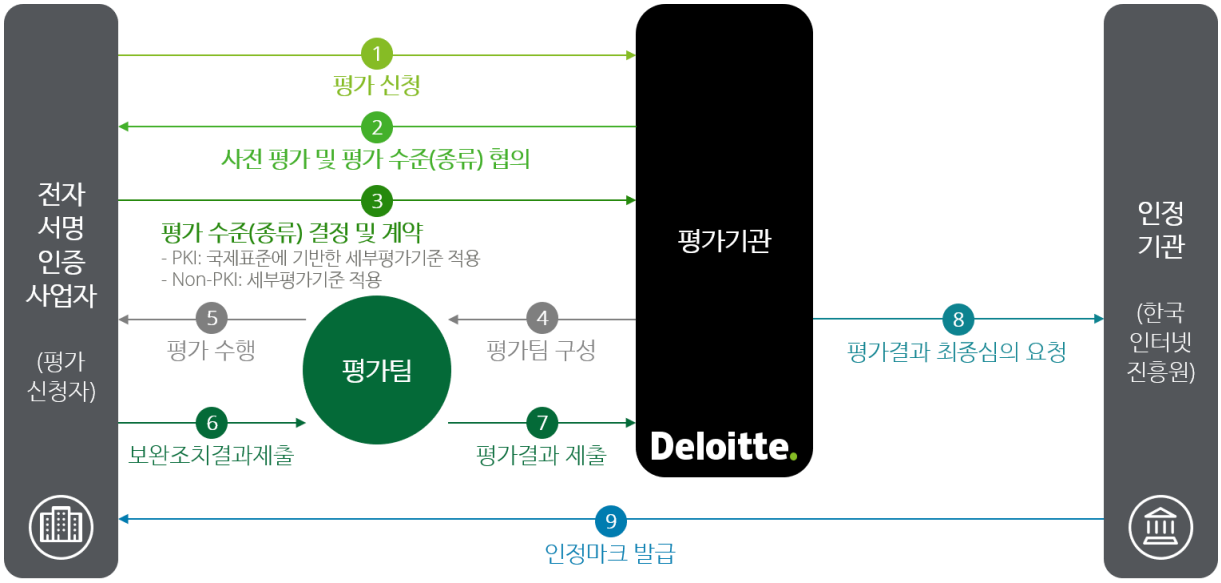
세부평가기준 | 전자서명인증사업자가 제공하는 전자서명인증업무의 운영기준 준수여부를 평가하기 위해 딜로이트 안진회계법인이 정한 평가기준을 말합니다.

발견사항 | 전자서명인증사업자가 세부평가기준의 요구사항을 충족하지 못한 사항을 말하며, 미비점이라고도 말합니다.

보완조치 | 전자서명인증사업자가 발견사항(또는 미비점)을 해결하기 위해 추가적으로 이행하는 보완 사항을 말합니다.

3. 평가 절차

평가 절차는 아래와 같다.



① 평가 신청

- 운영기준 준수 여부 평가에 대해 관심이 있거나 평가 진행을 희망하는 전자서명인증사업자는 딜로이트 안진회계법인에 전화, 전자우편(e-mail), 방문 등의 방법을 통해 평가 관련 문의를 진행할 수 있고, 평가 문의를 통해 딜로이트 안진회계법인과 평가를 진행하기로 협의한 전자서명인증사업자는 전자우편(e-mail), 우편, 방문 등의 방법을 통해 아래 제출서류들을 제출할 수 있습니다.

  ※ 제출서류:
  - 평가 신청 공문 1 부
  - 평가 신청서 1 부 [별지 1]
  - 법인사업자등록증* 1 부

  * 「전자서명법」 제 8 조제 2 항에 따라 전자서명인증사업자는 국가기관, 지방자치단체 또는 법인이어야 함

- 평가 신청자는 딜로이트 안진회계법인과 평가 일정, 대상, 범위를 사전에 협의한 후 평가 신청서에 명시합니다.

- 딜로이트 안진회계법인은 평가 신청자가 작성 및 제출한 서류가 미비하거나 누락된 경우 보완을 요청할 수 있으며, 평가 신청자는 15 일 이내에 서류를 보완 및 제출합니다.

② 사전 평가 및 평가 수준(종류) 협의

- 딜로이트 안진회계법인은 평가 신청서를 접수한 후, 평가팀을 구성하여 평가 신청자의 준비 현황*을 사전 확인합니다.

  * 전자서명인증업무 운영기준 관련 정보보호 정책, 전자서명인증업무준칙 등의 기본 문서 수립 여부, 기 신청한 평가 대상 및 범위의 적절성, 평가 대상 및 범위에 포함된 장소 등

- 딜로이트 안진회계법인은 평가 신청자의 준비 현황을 고려하여 평가 신청자와 평가 수준을 협의할 수 있으며, 평가 신청자는 최종적으로 결정한 평가 수준을 딜로이트 안진회계법인에 알려야 합니다.

- 딜로이트 안진회계법인은 평가 신청자에 대한 사전 평가 결과가 미흡한 경우 보완조치를 요청할 수 있으며, 보완 조치 및 평가 준비가 완료되지 않은 경우 기 신청된 평가 신청 사실을 취소할 수 있습니다.

③ 평가 수준(종류) 결정 및 계약

- 평가 신청자가 PKI(공개 키 기반구조) 방식을 활용하여 전자서명인증업무 및 서비스를 제공하고자 하는 경우, 국제표준에 기반한 세부평가기준에 따라 평가를 수행할 수 있습니다.

  ※ 「전자서명법」 제 11 조제 1 항 및 2 항에 따라. 과학기술정보통신부장관은 운영기준에 부합한다고 인정하는 국제적으로 통용되는 평가(이하 "국제통용평가")를 정하여 고시할 수 있으며, 전자서명인증사업자가 국제통용평가를 받은 경우에는 평가기관의 평가를 받은 것으로 간주할 수 있습니다.

- 딜로이트 안진회계법인은 평가 신청자에 대한 사전 평가 결과, 평가 신청자가 최종적으로 결정한 평가 수준에 따라 준비 현황이 충분하다고 판단되면 평가 계약을 진행할 수 있습니다.

  ※ 평가를 진행하기 위한 계약서, 평가 수수료, 평가 소요기간 등에 대한 사항은 계약 절차 진행 시 평가 신청자에 알리며, 이 때 평가 신청자는 딜로이트 안진회계법인과 협의하여 일부 조정할 수 있습니다.

- 평가 신청자는 평가 수수료를 청구 받은 날로부터 평가 수행 시작일 전 날까지 지정된 계좌번호로 납부하여야 합니다.

※ 평가 신청자는 딜로이트 안진회계법인과 협의하여 평가 수수료 납부일을 조정할 수 있습니다.

- 평가 수수료는 반납하지 않는 것이 원칙이나, 평가 기관이 귀책 사유가 있거나 이를 인정한 경우 평가 신청자와 협의하여 평가 수수료 일부 또는 전부를 반납할 수 있습니다.

④ 평가팀 구성

- 딜로이트 안진회계법인은 평가 신청자가 제공하고 있는 전자서명인증서비스 특성 및 평가 범위 등을 고려하여 평가팀을 구성하고, 구성된 평가팀은 평가 신청자에게 공유됩니다.
- 딜로이트 안진회계법인의 평가팀은 「전자서명법」 시행령 별표 1 에서 정한 자격을 충족하고, 평가팀의 평가 수행경력, 평가 품질 및 태도, 평가 신청자와의 독립성 및 이해상충 여부에 대해 검증된 전문 인력으로 구성됩니다.

⑤ 평가 수행

- 딜로이트 안진회계법인의 평가팀은 평가 신청자에 대한 평가 수행 전 착수 회의를 개최하거나, 경우에 따라 평가 계획 공유로 대체할 수 있습니다.
- 딜로이트 안진회계법인은 평가 과정에 대한 독립성, 공정성, 객관성, 신뢰성 확보를 위한 방안을 수립하고 이행합니다.
- 딜로이트 안진회계법인의 평가 방식은 서면평가와 현장평가로 구분하여 진행합니다.

서면평가	딜로이트 안진회계법인 세부평가기준 대비 평가 신청자의 운영기준 준수 및 충족 현황에 대한 평가를 평가 신청자가 수립한 전자서명인증업무준칙 및 내부 절차 문서 등을 통해 확인
현장평가	평가 신청자가 관리하고 있는 전자서명인증업무준칙 및 내부 절차 문서에 따라 운영기준의 운영 효과성을 평가하기 위해 관련 시스템 증적을 무작위로 추출(샘플링)하여 확인

- 딜로이트 안진회계법인은 다음 사항에 해당하는 경우 평가를 중단할 수 있습니다.

1. 평가 신청자가 고의로 평가의 실시를 지연 또는 방해하는 경우
2. 천재지변 및 경영환경 변화 등과 같은 불가항력적 사유로 인해 평가를 진행하기 어렵거나 불가능하다고 판단하는 경우
3. 평가 신청자가 평가 수수료를 평가 수행 시작일(또는 사전에 딜로이트 안진회계법인과 협의한 날짜)까지 납부하지 않은 경우
4. 평가 진행 중 평가의 독립성, 공정성, 객관성, 신뢰성을 훼손할 수 있는 상황이 발생한 경우

⑥ 보완조치 결과 제출

- 평가팀은 평가 진행 중 딜로이트 안진회계법인의 세부평가기준 대비 평가 신청자의 운영기준 준수 현황을 준수하지 않거나 충족하지 않은 사항을 발견한 경우, 해당 사항을 수집하여 발견사항(또는 미비점) 보고서를 작성하고 평가 신청자에게 해당 발견사항(또는 미비점) 목록에 대한 보완조치를 요청할 수 있습니다.

⑦ 평가결과 제출

- 평가팀은 평가 신청자에 대한 평가가 완료됨에 따라 전자서명인증업무 운영기준 준수 현황이 세부평가기준에 충족하다고 판단하는 경우, 해당 사실을 바탕으로 평가결과 보고서를 작성합니다.
- 딜로이트 안진회계법인은 평가 진행 중 평가 신청자에 보완조치를 요청한 경우, 해당 보완조치 결과를 검토하고 평가결과 보고서 작성 여부를 결정합니다.
- 딜로이트 안진회계법인은 평가팀이 작성한 평가결과 보고서를 내부적으로 검토한 뒤 최종적으로 이상이 없는 경우, 이 사실을 평가 신청자에게 공유하고 인정기관에 해당 평가결과를 제출하기 위해 준비합니다.

⑧ 평가결과 최종심의 요청

- 딜로이트 안진회계법인은 평가 신청자와 최종적으로 협의한 후 최종 평가결과 보고서를 인정기관이 요구하는 자료들을 포함하여 인정기관에 제출합니다.
- 딜로이트 안진회계법인은 최종 평가결과 보고서를 제출한 후 인정기관장이 필요하다고 인정하는 경우 추가적인 평가를 수행할 수 있으며, 추가 평가는 딜로이트 안진회계법인의 평가 절차를 준용하여 진행됩니다.

⑨ 인정마크 발급

- 인정기관은 평가 신청자에 대한 평가기관의 평가결과 등을 바탕으로 평가 신청자의 운영기준 준수 사실을 인정하면, 전자서명인증업무 증명서 및 인정마크를 평가 신청자에 발급합니다.

- 평가 신청자는 발급받은 인정마크 아래에 인정을 받은 사업자명, 전자서명인증 서비스명, 인정을 받은 연도, 순서를 순차적으로 기입한 후 평가 신청자 홈페이지 등에 게시할 수 있습니다.

  ※ 인정마크 게시를 통해 운영기준을 준수한다는 사실을 홍보하기 위해, 「전자서명법」 제 8 조제 2 항 및 같은 법 제 13 조제 1 항에 따른 법적 근거를 준수해야 합니다.

4. 세부평가기준

딜로이트 안진회계법인은 평가 신청자의 운영기준 준수 여부를 평가하기 위해, **전자서명 관련 준수 필요 사항**, **관리적·물리적·기술적 대책**, **개인정보보호 대책** 기준을 보유하고 있습니다.

※ 본 안내서 별첨 자료는 전자서명인증사업자가 평가 업무에 대한 이해를 돕기 위해 작성되었으며, 딜로이트 안진회계법인이 세부평가기준을 개정하면 내용이 변경될 수 있습니다.

딜로이트 안진회계법인에 평가 관련 문의 및 상담 시, 딜로이트 안진회계법인의 세부평가기준에 대한 정보를 제공해드립니다.

5. 문의처

딜로이트 안진회계법인
리스크자문본부 정보보안리스크
전자서명인증업무 평가팀

- **전화번호:** 02-6099-4675
- **이메일:** krtrustesign@deloitte.com
- FAX: 02-6674-2114
- **주소:** 서울특별시 영등포구 국제금융로 10
  서울국제금융센터 One IFC 빌딩 12 층
  (우) 07326

[첨부] 전자서명인증업무 평가 관련 세부평가기준

별첨 1. 전자서명인증업무 세부평가기준

연번	평가 항목 및 상세 평가 기준
1. 전자서명인증업무의 독립성	
1.1	전자서명인증사업자는 전자서명인증업무준칙에 인증서 이용 범위를 명확히 기술하여야 한다.
1.2	전자서명인증사업자는 전자서명인증업무를 수행함에 있어 기술적·관리적 조치를 통해 "전자서명인증업무의 독립성"을 준수하여야 한다. *[예시] 기술적 조치* *① 전자서명인증업무 관련 설비의 물리적 분리* *② 전자서명인증업무 관련 시스템의 독립적 구성* *③ 전자서명인증업무 관련 설비에 허가된 인원만 출입 가능하도록 물리적 통제* *④ 전자서명인증업무 관련 시스템에 허가된 인력만 접근이 가능하도록 통제 등* *[예시] 관리적 조치* *① 중립적으로 신뢰성 있는 자로부터 감사, 관리·감독 수행* *② 전자서명인증업무가 독립성을 유지하도록 내부 규정 마련* *③ 전자서명인증업무 수행인력의 독립성 유지 등*
2. 적정 기술의 이용	
2.1	전자서명인증서비스는 이용자가 가입자(서명자)의 신원을 식별할 수 있도록 전자서명인증업무준칙에 명시된 대로 다양한 방법으로 연계정보(CI), VID, DN, 이메일 주소 등을 사용하여 가입자(서명자)의 식별정보를 제공해야 한다. *[예시] 인증서에 가입자(서명자)의 식별정보를 넣어 발급하는 기능* *[예시] 이용자의 전자서명 생성 요청 시, 이용자에게 가입자의 전자서명과 연계정보(CI)를 전달하는 기능*
2.2	가입자의 전자서명 생성절차를 통제할 수 있어야 하고 비인가자가 비공식적인 절차를 통해 가입자의 전자서명을 생성할 수 없어야 한다. • 전자서명은 가입자(서명자)의 전자서명생성정보를 통해서만 생성될 수 있는 속성이 있는지 확인 • 전자서명인증시스템은 가입자(또는 가입자의 서명 권한을 위임 받은 자) 이외의 다른 자가 가입자의 전자서명생성정보에 접근할 수 없도록 가입자 인증 및 접근통제 기능을 제공하는지 확인 *[예시] 전자서명생성정보를 패스워드 기반으로 암호화하여 저장하며, 패스워드를 통한 가입자 인증이 성공한 경우에만 전자서명을 생성하도록 기능 제공* *[예시] 전자서명생성정보를 단말기의 Key store 에 저장하며, 생체인증을 통한 가입자 인증이 성공한 경우에만 전자서명을 생성하도록 기능 제공*

연번	평가 항목 및 상세 평가 기준
2.2	• 전자서명인증시스템은 가입자의 전자서명생성정보 이용 시마다 가입자 인증을 수행하는지 확인 • 전자서명인증시스템은 전자서명 생성 기능 수행 전 전자서명생성정보 및 인증서의 유효성을 검증하는지 확인 • 전자서명생성정보 및 인증서가 유효하지 않은 경우 전자서명을 생성하지 않는지 확인
2.3	**전자서명인증시스템은 서로 다른 전자문서에 대해 서로 다른 전자서명을 생성하여야 한다.** ※ 동일한 전자문서에 대해 서로 다른 전자서명 생성을 요구하지 아니함
2.4	**다음 절차를 통해 전자문서가 전자서명 된 후 전자문서(서명대상 원문) 또는 전자서명 값의 변경이 있는 경우 전자 문서 또는 전자서명 값이 변경되었다는 사실을 확인할 수 있어야 한다.** • 전자서명은 전자문서 및 전자서명이 변경된 경우, 이를 확인할 수 있는 속성이 있는지 확인 • 전자서명인증시스템은 전자서명 검증 수행 시 전자문서 및 전자서명의 변경여부를 확인하는지 확인 • 전자서명인증시스템은 전자문서 또는 전자서명이 변경된 경우, 검증 실패 결과를 이용자 또는 가입자가 확인할 수 있도록 관련 기능을 제공하는지 확인 *[예시] 전자서명 검증 앱에서 인증서 검증 실패 결과를 화면에 출력* *[예시] 전자서명 검증 API 에서 검증 실패 결과를 리턴*
2.5	**안전한 암호화 알고리즘을 사용하여야 한다.** • 전자서명인증시스템은 전자서명에 보안강도 112 비트 이상의 안전한 암호 알고리즘 및 키 길이를 사용하는지 확인 *[예시] 전자서명 생성/검증용 키 쌍 생성, 난수 생성, 인증서 서명, 전자서명생성정보 암호화 등* • 보안강도 112 비트 이상의 안전한 암호 알고리즘의 기준은 "KISA 암호 알고리즘 및 키 길이 이용 안내서"를 참고하여 적용하는지 확인 • "KISA 암호 알고리즘 및 키 길이 이용 안내서"에 명시되지 않은 암호 알고리즘 및 키 길이를 사용하는 경우, 전자서명인증사업자는 해당 암호 알고리즘 및 키 길이에 대한 보안강도 112 비트 이상의 안전성을 보증해야 할 책임을 가지는지 확인
2.6	**특별한 사정이 없는 한 국가 및 단체 또는 국제 표준이 있는 경우 이를 준수하여야 한다.** • 전자서명인증시스템은 전자서명에 표준 프로파일 및 프로토콜을 사용하는 경우 이를 준수하는지 확인 *[예시] 인증서 프로파일에 ITU-T X.509 표준 사용 및 준수* *[예시] 전자서명생성정보 암호화에 PKCS#5 표준 사용 및 준수* *[예시] 인증서 및 인증서폐지목록(CRL) 프로파일에 RFC 5280 표준 사용 및 준수* *[예시] 온라인 인증서 상태 확인 프로토콜(OCSP)에 RFC 6960 표준 사용 및 준수* *[예시] 인증서 관리 프로토콜 사용 시 RFC 4210(CMP) 표준 사용 및 준수* *[예시] 인증서 요청에 RFC 4211(CRMF) 및 RFC 2986(CSR) 등 표준 사용 및 준수* • 전자서명인증시스템이 전자서명에 표준 프로토콜을 사용하지 않는 경우, 전자서명인증사업자는 해당 프로토콜에 대한 안전성을 보증해야 할 책임을 가지는지 확인
3. 전자서명인증업무준칙	
3.1	**전자서명인증사업자는 법 제 15 조에 따른 전자서명인증업무준칙을 작성하여 인터넷 홈페이지 등에 게시하고, 이에 따라 전자서명인증업무를 수행하여야 한다.** • 전자서명인증사업자는 법 제 15 조에 따른 전자서명인증업무준칙을 작성하여 게시하는지 확인 • 전자서명인증사업자는 게시한 전자서명인증업무준칙에 따라 전자서명인증업무를 수행하는지 확인
3.2	**전자서명인증사업자는 전자서명인증업무준칙에 포함하여야 하는 법 제 15 조제 1 항 각 호의 사항에 변동이 생긴 경우 전자서명인증업무준칙에 해당 내용을 반영하여야 한다.**

연번	평가 항목 및 상세 평가 기준
3.3	전자서명인증사업자는 전자서명인증업무준칙의 내용을 변경하는 경우, 사전에 규정된 절차에 따라 전자서명인증업무준칙을 개정하고, 관련 당사자 모두가 개정 이전 또는 개정된 전자서명인증업무준칙을 열람할 수 있도록 한다. ※ 관련 당사자는 전자서명인증업무준칙에 명시된 “전자서명인증체계 관련자” 의미 *[예시] 개정된 전자서명인증업무준칙과 이전 전자서명인증업무준칙을 모두 홈페이지에 게시* *[예시] 개정된 전자서명인증업무준칙과 변경 직전의 전자서명인증업무준칙을 홈페이지에 게시* *[예시] 개정된 전자서명인증업무준칙과 신구비교표를 홈페이지에 게시*
3.4	전자서명인증사업자는 자신이 제공하는 전자서명인증서비스와 관련된 인증기관이 있는 경우, 해당 기관과의 정책 일관성을 위해 전자서명인증업무준칙의 제·개정시 이에 대해 협의하여야 한다. • 전자서명인증사업자가 제공하는 전자서명인증서비스와 관련된 인증기관이 있는 경우, 전자서명인증업무준칙의 "전자서명인증체계 관련자"에 이를 명시해야 하며, "제·개정 절차"에 협의 절차를 기술하는지 확인 *[예시] 전자서명인증사업자의 최상위인증기관이 존재하는 경우 전자서명인증업무준칙에 이를 명시하고, 준칙의 제·개정 절차에 협의 절차를 기술* • 전자서명인증사업자가 제공하는 전자서명인증서비스와 관련된 인증기관이 있는 경우, 전자서명인증업무준칙의 제·개정 시 해당 인증기관과 이에 대해 협의해야 하며, 협의에 대한 증거자료를 작성 및 보관하는지 확인 *[예시] 전자서명인증사업자의 전자서명인증업무준칙 제·개정 시 최상위인증기관과 이에 대해 협의한 후, 협의 결과와 전자서명인증사업자 및 최상위인증기관의 서명이 포함된 회의록을 작성 및 보관*
4. 가입자 등록	
4.1	전자서명인증사업자 또는 등록대행기관은 법 시행령 제 9 조, 시행규칙 제 5 조, 그리고 가입자 신원정보의 진위(정확성) 및 주체(소유자)가 맞는지에 대하여 확인할 수 있는 방법을 이용하여 전자서명인증서비스에 가입하려는 자의 신원을 확인하여야 한다. • 전자서명인증사업자 또는 등록대행기관은 가입자 신원확인을 위해, 신원정보의 진위 및 주체를 확인하는지 확인 • 신원확인을 위해 사용되는 신원정보는 전자서명인증사업자 또는 등록대행기관이 정하는지 **확인** ※ 단, 본인확인기관의 경우 신원정보는 실지명의를 기준으로 하되, 사전에 가입자의 신원확인을 실지명의 기준으로 확인한 경우에는 실지명의 이외의 방법으로 신원확인 가능 *[예시] 본인확인기관이 본인확인서비스 등의 제공을 위해 사전에 가입자의 주민등록증을 확인한 경우, 해당 본인확인기관은 전자서명인증서비스 제공을 위해 동일한 가입자의 신원 확인 시 해당 가입자의 주민등록증을 확인하지 않아도 됨* • 신원정보의 진위 확인은 신원정보를 발급한 기관 또는 신뢰할 수 있는 출처를 통하는지 확인 • 신원정보의 주체 확인은 주체의 얼굴을 대면 및/또는 비대면으로 확인, 주체만이 알 수 있는 정보로 확인 등 합리적인 방안으로 수행하는지 확인
4.2	전자서명인증사업자 또는 등록대행기관은 직접 대면(법 시행령 제 9 조제 1 항의 요건을 충족하는 것으로 직접 대면에 준하는 비대면 방법 포함)하여 가입자의 신원을 확인하여야 하며, 비대면으로 신원을 확인하는 경우 대면에 준하는 신원확인 수준을 갖출 수 있도록 신원확인을 위한 방안을 마련하여야 한다.

연번	평가 항목 및 상세 평가 기준
4.2	※ [참고] 금융회사 비대면 실명확인 시 신원확인 방법 - (이중확인: 필수) ① 신분증 사본 제출, ② 영상 통화, ③ 접근매체(예: OTP, 보안카드) 전달 시 확인, ④ 기존 계좌 활용, ⑤ 기타 이에 준하는 새로운 방식(생체인증 등) 중 "2 가지" 의무 적용 - (이중확인: 권고) ⑥ 타기관 확인결과 활용(휴대폰 인증 등), ⑦ 다수의 개인정보 검증까지 포함하여 ①~⑦ 중 추가 확인
4.3	전자서명인증사업자 또는 등록대행기관은 가입자를 등록하거나 인증서를 발급하기 전에 인증서의 이용범위, 전자서명의 효력 등에 대한 이용약관을 가입자와 이용자에게 알리는 절차를 마련하여야 한다. *[예시] 가입자 등록 또는 인증서 발급 전 이용약관 화면 출력*
4.4	전자서명인증사업자는 등록대행기관이 관련 규정을 준수하도록 계약서에 관련 통제방안 명시 등 방안을 수립하고, 현장방문 등을 통해 등록대행기관의 통제방안 수행여부를 관리하여야 한다.
4.5	전자서명인증사업자는 등록대행기관으로부터 정보통신망으로 가입자의 등록정보를 전송 받는 경우, 가입자의 등록정보가 위·변조 되지 않도록 조치를 취하여야 하며, 등록정보가 유출되지 않도록 대책을 마련하여야 한다. • 전자서명인증사업자는 등록대행기관으로부터 정보통신망으로 가입자의 등록정보를 전송 받는 경우, 가입자의 등록정보가 위·변조 되지 않도록 조치를 취하는지 확인 • 전자서명인증사업자는 가입자 등록정보가 유출되지 않도록 대책을 마련하는지 확인 *[예시] 가입자 등록정보를 암호화하여 저장하고, 가입자 등록정보 취급자에 대한 식별 및 인증, 접근통제를 수행* • 안전한 암호 알고리즘의 기준은 "KISA 암호 알고리즘 및 키 길이 이용 안내서"를 참고하여 적용하는지 확인 • "KISA 암호 알고리즘 및 키 길이 이용 안내서"에 명시되지 않은 암호 알고리즘 및 키 길이를 사용하는 경우, 전자서명인증사업자는 해당 암호 알고리즘 및 키 길이에 대한 안전성을 보증할 책임을 가지는지 확인
5. 인증서 발급·효력정지·효력회복 및 폐지 등	
5.1	전자서명인증사업자는 가입자에게 인증서를 발급하는 경우, 가입자 전자서명생성정보의 유일성을 확인하여야 한다. ※ 가입자 전자서명생성정보와 전자서명검증정보가 1:1 로 매핑되는 경우를 전자서명검증정보의 유일성을 확인하는 방법으로 대체할 수 있다. *[예시] 인증서 발급 전, 가입자 전자서명검증정보가 이전에 발급된 모든 전자서명검증정보와 중복되지 않음을 확인*
5.2	전자서명인증사업자는 전자서명 생성 검증 등 가입자에게 발급된 인증서를 이용자가 이용할 수 있는 방안을 마련하여 제공하여야 한다. *[예시] 소프트웨어(앱 등) 제공, API 제공, 전자서명 생성 및 검증에 필요한 절차 안내 등*
5.3	전자서명인증사업자는 인증서의 위·변조 여부를 탐지할 수 있는 기술적 방안을 마련하여야 한다. *[예시] 인증서에 대해 전자서명인증사업자의 전자서명 수행, 인증서의 블록체인 저장 등*
5.4	전자서명인증사업자는 가입자가 인증서의 효력정지, 효력회복, 폐지를 신청하는 경우, 전자서명인증업무 운영기준 제 6 조제 1 항에 따라 가입자의 신원을 확인한 경우에만 인증서의 효력을 정지 또는 회복하거나 인증서를 폐지하여야 한다. ※ 인증서의 효력정지, 효력회복, 폐지 기능을 반드시 제공해야 하는 것은 아님

연번	평가 항목 및 상세 평가 기준
5.5	**전자서명인증사업자는 인증서의 효력정지, 효력회복, 폐지 사실을 이용자가 지체 없이 확인할 수 있도록 방안을 마련하여 제공하여야 한다.** **※ "지체없이 확인"이 "즉시 확인"을 의미하지는 아니함** *[예시] 12 시간 주기로 인증서 효력정지 및 폐지목록(CRL)을 배포하는 방안을 마련하고, 12 시간 주기로 지체 없이 CRL 을 배포* *[예시] 온라인 인증서 상태 프로토콜(OCSP) 서비스를 제공하고, 인증서의 효력정지, 효력회복, 폐지 상태를 즉시 반영*
5.6	**전자서명인증사업자는 이용자가 인증서의 유효성을 확인할 수 있도록 인증서 효력정지 및 폐지목록을 생성하여 전자서명인증업무준칙에 규정한 공고 설비에 공고하거나, 이용자에게 인증서 유효성 확인 서비스를 제공할 수 있다.** *[예시] 인증서 효력정지 및 폐지목록(CRL)을 생성하여 게시* *[예시] 온라인 인증서 상태 프로토콜(OCSP) 서비스 제공*
6. 전자서명생성정보 생성	
6.1	**전자서명인증사업자는 물리적으로 안전한 환경에서 전자서명인증업무준칙에 규정된 절차에 따라 전자서명생성정보를 생성하여야 한다.** • 전자서명인증사업자가 자신의 전자서명생성정보를 물리적으로 안전한 환경에서 전자서명인증업무준칙에 규정된 절차에 따라 생성하는지 확인 • 전자서명인증사업자가 가입자의 전자서명생성정보를 생성하는 경우, 전자서명인증사업자는 가입자의 전자서명생성정보를 물리적으로 안전한 환경에서 전자서명인증업무준칙에 규정된 절차에 따라 생성하는지 확인 *[예시] 비인가자의 접근을 방지하기 위하여 출입통제 장치 및 감시시스템을 설치하고, 출입 자격을 최소 인원으로 유지한 장소에서 전자서명인증업무준칙에 규정된 절차에 따라 전자서명생성정보를 생성*
6.2	**전자서명인증사업자는 전자서명생성정보를 생성하는 경우, 관련 표준을 따라야 하고 안전한 암호 알고리즘 또는 안전한 암호화 장치를 이용하여야 한다.** • 전자서명인증사업자가 자신의 전자서명생성정보 및 가입자의 전자서명생성정보를 표준 프로토콜을 통해 생성하는 경우 해당 표준을 준수하는지 확인 • 전자서명인증사업자가 자신의 전자서명생성정보 및 가입자의 전자서명생성정보 생성에 표준 프로토콜을 사용하지 않는 경우, 전자서명인증사업자는 해당 프로토콜에 대한 안전성을 보증해야 할 책임을 가지는지 확인 • 전자서명인증사업자가 자신의 전자서명생성정보 및 가입자의 전자서명생성정보 생성에 안전한 암호 알고리즘 및 키 길이를 사용하는지 확인 • 전자서명인증사업자가 자신의 전자서명생성정보 및 가입자의 전자서명생성정보 생성 시, 안전한 암호화 장치를 이용하는지 확인 *[예시] FIPS 140-2 Level 3 이상 또는 이와 동등한 인증을 받은 전용 HSM 장비를 이용하여 전자서명 생성정보를 생성*
6.3	**전자서명인증사업자는 자신의 전자서명생성정보를 생성하는 경우, 다자인증 통제(m of N, m 은 3 명 이상)하에 전자서명생성정보를 생성하여야 한다.** *[예시] 전자서명인증사업자는 안전한 암호화 장치의 다자인증 통제 기능을 제공하며, 키 쌍 생성을 위한 다자인증 통제 설정을 '3 of 5'로 설정함. 다자인증 통제 설정(3 of 5)에 따라 인증을 수행할 수 있는 5 명 중 최소 3 명이 인증에 성공한 경우에만 키를 생성하도록 함*

연번	평가 항목 및 상세 평가 기준
6.4	**전자서명인증사업자는 가입자의 신청이 있는 경우 외에는 가입자의 전자서명생성정보를 보관하여서는 아니되며, 가입자의 신청에 의하여 그의 전자서명생성정보를 보관하는 경우 해당 가입자의 동의없이 이를 이용하거나 반출하여서는 아니된다.** • 가입자의 신청이 있는 경우 외에는 가입자의 전자서명생성정보를 보관하지 않는지 확인 • 가입자의 신청에 의하여 가입자의 전자서명생성정보를 보관하는 경우, 해당 가입자의 동의없이 이를 이용하거나 반출하지 않는지 확인 • 가입자의 신청에 의하여 가입자의 전자서명생성정보를 보관하는 경우, 가입자의 전자서명생성정보가 유출되지 않도록 암호화 및 접근통제 등의 대책을 마련하는지 확인
6.5	**전자서명인증사업자는 가입자의 전자서명생성정보를 생성하는 경우, 2 인 이상의 권한 있는 직원이 공동으로 이를 수행하여야 한다. 자동화된 설비를 이용하는 경우에는 해당 설비를 다자인증 통제 (m of N, m 은 2 명 이상) 하에 활성화하여야 한다.** • 전자서명인증사업자가 가입자의 전자서명생성정보를 생성하는 경우, 2 인 이상의 권한 있는 직원이 공동으로 이를 수행하는지 확인 **※ 관리·감독 인력은 전자서명생성정보 생성 수행 인력으로 인정되지 아니함** **(예: 1 인이 전자서명생성정보를 생성하고, 다른 1 인이 관리·감독을 수행하는 경우 해당 요구사항을 만족하지 아니함)** • 전자서명인증사업자가 가입자의 전자서명생성정보 생성을 위해 자동화된 설비를 이용하는 경우, 해당 설비를 다자인증 통제 (m of N, m 은 2 명 이상)하에 활성화하는지 확인 *[예시] HSM 장비의 활성화를 위해 '2 of 3' 다자인증 수행*
7. 전자서명생성정보 보호	
7.1	**전자서명인증사업자는 전자서명생성정보를 생성한 경우 그 전자서명생성정보를 안전하게 보호하여야 한다.** • 전자서명인증사업자는 자신의 전자서명생성정보 및 가입자의 전자서명생성정보를 생성한 경우, 전자서명생성정보를 안전하게 저장하는지 확인 *[예시] 안전한 암호 알고리즘 및 키 길이를 사용하여 전자서명생성정보 암호화 후 저장* *[예시] 안전한 암호화 장치에 전자서명생성정보 저장* • 전자서명인증사업자는 자신의 전자서명생성정보 및 가입자의 전자서명생성정보를 생성한 경우, 메모리의 전자서명생성정보를 모두 삭제하는지 확인
7.2	**전자서명인증사업자는 가입자의 전자서명생성정보를 생성한 경우, 해당 전자서명생성정보가 가입자의 통제 하에 이용될 수 있도록 안전조치를 마련하여야 한다.** • 전자서명인증사업자는 가입자의 전자서명생성정보를 생성하는 경우, 가입자의 전자서명생성정보에 대한 접근통제를 수행하는지 확인 • 전자서명인증시스템은 가입자의 전자서명생성정보를 이용 시마다 가입자 인증을 수행하는지 확인
7.3	**전자서명인증사업자는 전자서명생성정보의 분실·훼손 또는 도난·유출 등을 방지하고 전자서명인증업무를 계속하여 안정적으로 제공할 수 있도록 전자서명생성정보를 백업하여야 한다.** • 전자서명인증사업자는 자신의 전자서명생성정보의 분실·훼손 또는 도난·유출 등을 방지하는지 확인 • 전자서명인증사업자가 가입자의 전자서명생성정보를 생성하는 경우, 전자서명인증사업자는 가입자의 전자서명생성정보의 분실·훼손 또는 도난·유출 등을 방지하는지 확인 • 전자서명인증사업자는 자신의 전자서명생성정보를 백업하는지 확인 • 전자서명인증사업자가 가입자의 전자서명생성정보를 생성하는 경우, 전자서명인증사업자는 가입자의 전자서명생성정보를 백업하는지 확인

연번	평가 항목 및 상세 평가 기준
7.4	**전자서명인증사업자는 전자서명생성정보를 백업하는 경우, 백업된 전자서명생성정보를 안전하게 보호하여야 한다.** • 전자서명인증사업자가 자신의 전자서명생성정보 및 가입자의 전자서명생성정보를 백업하는 경우, 백업된 전자서명생성정보를 안전하게 저장하는지 확인 • 전자서명인증사업자가 자신의 전자서명생성정보 및 가입자의 전자서명생성정보를 백업하는 경우, 백업된 전자서명생성정보에 대한 접근통제를 수행하는지 확인
7.5	**전자서명인증사업자는 백업된 전자서명생성정보 중 1 부를 전자서명인증업무 수행 시설과는 별도의 원격지 저장설비에 안전하게 보관하여야 한다.** • 백업된 전자서명생성정보 중 1 부를 전자서명인증업무 수행 시설과는 별도의 원격지 저장설비에 안전하게 보관하는지 확인 • 원격지 저장설비에 대한 기준(예: 전자서명생성정보 저장 시스템으로부터 10km 이상 떨어진 저장설비)을 전자서명인증업무준칙에 명시하고, 해당 기준을 만족하는 원격지 저장설비에 백업된 전자서명생성정보 중 1 부를 보관하는지 확인
7.6	**전자서명인증사업자는 자신의 전자서명생성정보 및 가입자의 전자서명생성정보를 백업하거나 복구하는 경우, 2 인 이상의 권한 있는 직원이 공동으로 이를 수행하도록 하여야 한다.** ※ 관리·감독 인력은 전자서명생성정보의 백업 및 복구 수행 인력으로 인정되지 아니함 (예: 1 인이 전자서명생성정보를 백업 또는 복구하고, 다른 1 인이 관리·감독을 수행하는 경우 해당 요구사항을 만족하지 아니함)
7.7	**전자서명인증사업자는 전자서명생성정보 원본 및 백업본을 파기하는 경우, 전자서명인증업무의 보호조치를 계획하고 감독·통제하는 관리책임자와 전자서명인증업무의 보호조치를 이행하는 보안관리자의 입회 하에 안전하게 파기하여야 한다.** ※ 전자서명생성정보는 '전자서명인증사업자 및 가입자의 전자서명생성정보'를 모두 포함함 *[예시] 전자서명생성정보가 보관된 저장설비의 디가우징* *[예시] HSM 에 보관된 전자서명생성정보 덮어쓰기*
7.8	**전자서명인증사업자는 전자서명생성정보가 분실·훼손 또는 도난·유출된 경우, 해당 가입자 및 관련 당사자가 이 사실을 알 수 있도록 인터넷 홈페이지에 게시 등의 적절한 방안을 마련하여야 한다.**
8. 시설 및 자료 보호조치 등	
8.1	**전자서명인증사업자는 전자서명인증업무 관련 시설 및 자료의 보호를 위해 "별첨 2. 관리적·물리적·기술적 세부평가기준"에 따른 보호조치를 수행하여야 한다.**
8.2	**전자서명인증사업자는 관계 법령의 준수여부를 자체적으로 점검하고, 점검 결과(예: 자체 점검표)를 평가기관에 제출하여야 한다.**
9. 가입자 및 이용자 보호 대책	

연번	평가 항목 및 상세 평가 기준
9.1	**전자서명인증사업자는 법 제 15 조제 2 항, 제 3 항, 제 4 항에 따른 전자서명인증업무의 휴지·폐지 절차 및 법 제 20 조에 따른 손해배상 절차를 준수하여야 한다.** • 전자서명인증업무 휴지 시, 휴지일 30 일 전에 가입자에게 통보하고 인터넷 홈페이지에 게시할 수 있도록 내부절차를 마련하는지 확인 • 전자서명인증업무 폐지 시, 폐지일 60 일 전에 가입자에게 통보하고 인터넷 홈페이지에 게시할 수 있도록 내부절차를 마련하는지 확인 • 전자서명인증업무 휴지 및 폐지 시, 통보 및 게시하는 내용에는 요금의 반환, 가입자의 개인정보 폐기 등 가입자 보호조치를 포함하는지 확인 • 법 시행령 상의 요건을 충족하는 손해배상 보험을 가입하고, 가입자 등에게 미치는 손해발생 시 이를 해결하기 위한 절차 및 방안을 마련하는지 확인 [시행령 상 보험의 요건] [1] 보험금액: 연간 총 보상액의 한도가 10 억 원 이상의 금액 [2] 보험기간: 인정 유효기간 내에 발생한 사고를 대상으로 보장 가능
9.2	**전자서명인증사업자가 법 시행령 제 14 조에 따라 연계정보(CI)를 처리하는 경우 다음 각 항의 사항을 수행하여야 한다.** • 연계정보(CI)를 이용 및 수집하거나 이를 제 3 자에게 제공하는 경우 가입자로부터 이에 대한 별도의 동의를 얻는지 확인 • 연계정보(CI)를 저장하거나 전송하는 경우 이를 안전한 암호 알고리즘으로 암호화하는지 확인 • 연계정보(CI)를 저장하거나 전송 시, "KISA 암호 알고리즘 및 키 길이 이용 안내서"에 명시되지 않은 암호 알고리즘 및 키 길이를 사용하는 경우, 전자서명인증사업자는 해당 암호 알고리즘 및 키 길이에 대한 안전성을 보증할 책임을 가지는지 확인 • 인증서에 연계정보(CI) 값을 포함할 수 없으며 이를 가입자 단(모바일, PC, 클라우드 등) 내에도 저장을 금지하는지 확인 • 연계정보(CI) 값의 송수신 시간, 대상 등에 대한 로그를 기록하여 저장 및 보관하는지 확인 • 연계정보(CI)를 처리하는 시스템에 접근할 수 있는 관리자를 지정하고, 해당 관리자만 연계정보 처리 시스템에 접근 가능하도록 접근통제를 수행하는지 확인 • 연계정보(CI)를 개인정보의 일환으로 보호할 수 있도록 개인정보보호법 등 관련 법령에 따른 필요조치 사항을 준수하고, 전자서명인증사업자의 "별첨 3. 개인 정보보호 세부평가기준"을 준용하는지 확인
10.	**장애인 · 고령자 등의 전자서명 이용 보장**
10.1	**전자서명인증사업자는 법 제 7 조제 2 항에 따른 장애인 · 고령자 등의 전자서명 이용을 보장하기 위하여 전자서명인증 서비스가 「장애인 · 고령자 등의 정보 접근 및 이용 편의 증진을 위한 고시」를 준수함을 신뢰할 수 있는 기관을 통해 인증되어야 한다.** *[예시] 웹 접근성 경우, 과학기술정보통신부장관이 지정한 정보통신 접근성(웹 접근성) 품질인증 기관을 통한 웹 접근성 인증서 제출* *[예시] 모바일 어플리케이션의 경우, '(KS X 3253) 모바일 어플리케이션 콘텐츠 접근성 지침 2.0' 준수 여부를 확인하는 인증서 제출*
11.	**취약점 점검 및 조치**
11.1	**전자서명인증사업자는 가입자의 신원확인정보가 위변조 되지 않도록 무결성과 기밀성을 보장할 수 있는 안전한 서비스 환경을 구현하여야 한다.**

연번	평가 항목 및 상세 평가 기준
11.2	전자서명인증사업자는 전자서명인증서비스(발급, 갱신 등 모든 프로세스 및 웹, 앱 등 서비스에 직간접적으로 참여하는 응용 및 시스템) 취약점 점검을 정기적으로 수행하고, 발견된 취약점에 대해서는 신속하게 조치 후 확인하여야 한다.
12.	**인증서 부정발급 상시확인 체계**
12.1	전자서명인증사업자는 인증서의 부정발급을 방지하기 위한 모니터링 기준을 수립하여 주기적으로 점검하고, 문제 발생 시 사후조치를 적시에 수행하여야 한다. • 인증서 부정발급 모니터링 및 점검주기, 점검내용*, 점검 방법 및 절차 등을 포함하여 상시점검 체계 마련 여부 확인 **[예시] 동일 휴대폰/계좌 등으로 다수의 인증서 발급, 비정상적인 신원확인정보 저장, 신원확인 요청정보와 수신정보 상이 등* • 인증서 발급 모니터링 및 점검결과 보고 및 이상 징후 발견 시 절차에 따른 대응 여부 확인

별첨 2. 관리적·물리적·기술적 세부평가기준

연번	평가 항목	상세 평가 기준	WebTrust
1. 정보보호 정책 및 조직			
1.1	정보보호 정책 수립 및 관리		
1.1.1	정보보호 정책 수립	전자서명인증사업자는 정보보호 정책을 수립하고 이를 문서화하여야 한다. • 정보보호 정책 문서가 물리적, 관리적, 기술적 통제를 포함하여, 경영진의 승인을 얻어 전직원에게 전파되었는지 확인	● (3.1.1)
1.1.2	정보보호 정책 이행	전자서명인증사업자는 수립된 정보보호 정책이 준수될 수 있도록 관리하여야 한다. • 최고경영자는 정보보호 분야 전문성을 갖춘 인력을 확보하고, 정보보호 정책의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하고 있는지 확인	● (3.1.2)
1.1.3	정보보호 정책 내용	전자서명인증사업자는 정보보호를 포함하는 구체적인 정보보호 정책을 마련하여야 한다. • 정보보호 정책이 다음을 포함하고 있는지 확인 a) 정보 공유를 가능하도록 하는 메커니즘으로서 정보보호의 정의, 목표 및 범위와 중요성 b) 정보보호의 원칙 및 목표를 지원하기 위한 경영진의 의지 c) 조직에게 특별히 중요시되는 보안정책, 원칙, 표준, 준수 요구사항에 대한 설명 d) 보안 침해 보고를 포함하는 정보보호관리체계에서의 책임에 대한 정의 e) 정책을 지원하는 문서에 대한 목록	● (3.1.3)
1.1.4	정보보호 정책 검토	전자서명인증사업자는 정보보호 정책을 주기적으로 검토하는 절차를 마련하여 최신성을 유지하여야 한다. • 정보보호 정책 문서의 최신성을 유지하기 위한 주기적인 검토 절차가 마련되어 있는지 확인 • 정보보호 관련 정책과 시행문서는 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경변화 등에 따라 필요한 경우 제·개정하고 그 이력을 관리하는지 확인	● (3.1.4) (3.1.8)

연번	평가 항목	상세 평가 기준	WebTrust
1.1.5	제 3 자 접근보안 정책	전자서명인증사업자는 제 3 자 접근 보안정책을 수립하고 이를 이행하여야 한다. • 전자서명인증사업자 시설 및 시스템에 대한 제 3 자의 물리적 및 논리적 접근 통제가 마련되어 있는지 확인 • 전자서명인증사업자 시설 및 시스템에 대한 제 3 자의 접근은 필수적인 보안 요구 사항을 담고 있는 정식 계약을 통해 이루어지고 있는지 확인	● (3.1.9) (3.1.10) (3.1.11)
1.1.6	아웃소싱 보안 정책	전자서명인증사업자는 전자서명인증 관련 운영 및 일부 시스템을 아웃소싱 할 경우 보안요구사항을 명확히 하여야 한다. • 전자서명인증사업자가 운영 및 전자서명인증시스템에 대한 모두 또는 일부를 아웃소싱 할 경우, 양측이 합의한 계약서에 전자서명인증 사업자의 보안 요구사항을 명시하는지 확인	● (3.1.12) (3.1.13)
1.2	**정보보호 조직 구성 및 운영**		
1.2.1	정보보호 책임자 지정	최고경영자는 임원급의 고위 경영진을 정보보호 총괄 관리 책임자로 지정하여야 한다.	● (3.1.5)
1.2.2	정보보호 조직 구성	전자서명인증사업자는 정보보호 활동을 체계적으로 이행할 수 있는 실무 조직 또는 정보보호 위원회를 구성하여야 한다. • 정보보호 활동을 체계적으로 이행할 수 있는 실무 조직이 존재하는지 확인 • 전자서명인증 관련 전문가 그룹이나 관련 기관과 적절한 연계를 유지하며 활동하는지 확인	● (3.1.6)
1.2.3	정보보호 조직 운영	전자서명인증사업자는 구성된 정보보호 조직에 대해서 구성원들의 역할과 책임을 명확하게 하고 구성원간 상호 의사소통을 할 수 있도록 운영하여야 한다. • 각각의 정보자산을 보호하기 위한 책임 및 특정 보안 절차를 수행할 책임이 명확히 되어 있는지 확인 • 구성원들의 정보보호 활동을 평가할 수 있는 체계와 구성원간 상호 의사소통을 할 수 있는 체계를 수립하여 운영하고 있는지 확인	● (3.1.7)
2. 자산관리			
2.1	**정보자산 식별 및 분류**		
2.1.1	정보자산 식별 및 분류	전자서명인증사업자는 전자서명인증업무 범위 내 모든 정보 자산을 식별하여 분류한 후 관리 책임자를 지정하여야 한다. • 전자서명인증사업자가 정보자산 분류기준을 확립한 후, 이에 따라 모든 정보자산을 분류 및 식별하고 있는지 확인 • 식별된 정보자산에 대해 중요도가 산정되었는지 확인 • 식별된 모든 정보 자산에 대해서 관리 책임자를 지정하고 있는지 확인	● (3.2.1) (3.2.4)

연번	평가 항목	상세 평가 기준	WebTrust
2.2	자산 관리 및 통제		
2.2.1	자산 관리	전자서명인증사업자는 자산목록을 만들어 관리하여야 한다. • 전자서명인증사업자가 정보 및 정보 처리 시설과 연관된 자산목록을 만들어 관리하고 있는지 확인	● (3.2.2)
2.2.2	자산 통제	전자서명인증사업자는 분류된 자산 및 정보자료를 위험으로부터 적절한 수준의 보호를 받을 수 있도록 통제 절차를 마련하여야 한다. • 전자서명인증사업자가 분류된 자산 및 정보자료에 대한 위협 분석을 수행하였는지 확인 • 전자서명인증사업자가 사업의 요구사항 및 사업에 미치는 영향에 따라 조직 내에서 사용되고 있는 자산의 적절한 사용을 위한 규칙을 문서화하였는지 확인	● (3.2.3)
3. 인적 보안			
3.1	직무 적합성 검토		
3.1.1	직무 적합성 검토	전자서명인증사업자는 전자서명인증 업무에 대한 직무기술서를 명시하여야 하며, 업무 적합성 여부 등을 검토하는 절차를 마련하여야 한다. • 전자서명인증 업무를 수행하는 직무에 대한 요건, 역할, 책임 등을 기술한 직무기술서가 있는지 확인 • 전자서명인증 담당자에 대한 신원확인 등 업무 적합성 여부 검토를 위한 절차가 마련되어 있는지 확인	● (3.3.1) (3.3.2)
3.2	역할 구분		
3.2.1	신뢰된 역할 담당자	정보보호 정책 문서에 신뢰된 역할에 대한 식별과 이를 취급하는 담당자들에 대한 각별한 관리를 반영하여야 한다. • 다음과 같이 신뢰된 역할에 대한 식별이 되어 있는지 확인 a) 인증서 생성, 폐지, 휴지에 대한 승인 b) 전자서명인증시스템의 설치, 구성 및 유지보수 c) 전자서명인증시스템 및 시스템 백업·복구 장비의 운영 d) 전자서명인증시스템 아카이브 및 감사로그의 검토 및 유지관리 e) 암호화 키 생명 주기 관리 기능 f) 인증시스템 개발 • 정보보호 정책 문서에 신뢰된 역할(trusted roles)과 비 신뢰된 역할(non-trusted roles)에 요구되는 신원확인에 대해 상세히 기술되어 있는지 확인하고, 최소한 정규직 인력 채용 시에는 신원확인을 수행하는지 확인 • 신뢰된 역할 담당자가 승인을 거친 후에 시스템 및 시설에 대한 접근 또는 작업을 수행하고 있는지 확인 • 신뢰된 역할을 수행하는 계약직 직원은 최소한 정규직 직원들과 똑같은 신원확인 절차 및 인력 관리 절차를 적용 받고 있는지 확인	● (3.3.3) (3.3.4) (3.3.5) (3.3.7) (3.3.8)

연번	평가 항목	상세 평가 기준	WebTrust
3.2.2	키 관리 및 인증서 직무자	키 관리 및 인증서 관리 등과 관련된 직원들에 대해서는 주기적인 신뢰성 검토 및 검증이 이루어져야 한다. • 키 관리 및 인증서 관리 등 주요 직무를 수행하는 직원들에 대한 주기적인 신뢰성 검토 및 검증이 이루어지는지 확인	● (3.3.9)
3.2.3	징계절차 마련	보안정책 및 절차를 위반한 직원에 대한 공식적인 징계 절차가 수립되어야 한다. • 보안서약서 위반이나, 전자서명인증업무와 관련하여 승인 받지 않은 사용 및 승인 받지 않은 시스템의 사용에 대한 처벌 규정이 마련되어 있는지 확인	● (3.3.10)
3.2.4	퇴사자 관리	전자서명인증사업자는 퇴사자에 대해서는 모든 접근통제 권한을 종료시켜야 한다. • 퇴사자에 대해서 물리적·논리적 접근을 종료하고 있는지 확인	● (3.3.11) (3.3.12)
3.3	보안서약서 작성		
3.3.1	보안서약서 작성	전자서명인증사업자는 전자서명인증 업무를 수행하는 모든 직무 관련자 (임시직원이나 외부자 포함)에게 기밀 유지 등에 대한 서약서를 받아야 한다. • 전자서명인증 업무를 수행하는 모든 직무 관련자(임시직원이나 외부자 포함)에게 기밀 유지 등에 대한 서약서를 받았는지 확인	● (3.3.6)
3.4	보안 교육		
3.4.1	보안교육 절차	전자서명인증사업자는 전자서명인증업무를 수행하는 모든 직무 관련자에게 보안 정책 및 절차에 대한 교육을 실시하여야 한다. • 전자서명인증사업자는 모든 직원들(하청 용역자 포함)에게 보안 정책 및 절차에 대한 교육을 위해 다음을 마련하고 있는지 확인 a) 각자의 역할에 대한 교육훈련 요구사항 및 교육훈련 절차 b) 각자의 역할에 대한 재교육훈련 기간 및 재교육훈련 절차	● (3.3.13)
3.5	외부자 보안		
3.5.1	외부자 보안 대책	전자서명인증사업자가 업무의 일부로 외부서비스를 이용하거나 외부자에게 위탁하는 경우 이에 대한 보안대책을 명확히 하여야 한다. • 전자서명인증사업자가 업무의 일부로 외부서비스를 이용하거나 외부자에게 업무를 위탁하는 경우, 정부 요구사항을 계약서에 명시하고 명시된 요구사항 준수 여부에 대해 주기적으로 점검 또는 관리·감독하고 있는지 확인	● (3.1.10) (3.1.11)
4. 물리적 보안			
4.1	물리적 보호		

연번	평가 항목	상세 평가 기준	WebTrust
4.1.1	중요설비 보호	전자서명인증사업자는 인증서 발급 등을 수행하는 중요설비를 별도의 통제 구역에 타 시스템과 물리적으로 분리하는 등 안전한 시설에 위치하여 사고 및 재난 등을 방지할 수 있는 방안을 마련하여야 한다. • 전자서명인증 운영실이 위치한 빌딩 또는 장소는 허가된 인원만 출입 가능하도록 물리적 접근 통제를 위한 보안요원 접수나 다른 보호 수단이 구비되어 있는지 확인 • 인증서 발급 등을 수행하는 중요 시설에 대한 비인가 출입과 환경오염을 방지하기 위해 물리적 장벽이 설치되어 있는지 확인 • 통제구역에 위치한 설비는 온·습도 조절, 화재감지, 소화설비, 누수 감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영 절차를 수립·운영하고 있는지 확인	● (3.4.2) (3.4.3) (3.4.4) (3.4.5) (3.4.6)
4.1.2	장비 관리	전자서명인증사업자는 주요장비에 대해 물리적 보안 조치를 마련하고 이행하여야 한다. • 장비에 대한 재고 관리를 하고 있는지 확인 • 장비는 정전 및 기타 전기적 이상으로부터 보호되고 있는지 확인 • 전자서명인증 운영실이 있는 건물 내의 전력 및 통신선이 파손이나 도청의 위협으로부터 보호되고 있는지 확인 • 개인용 컴퓨터나 워크스테이션은 미사용 시에 로그오프 되거나, 패스워드 등을 통하여 적절히 통제되고 있는지 확인	● (3.4.16) (3.4.17) (3.4.18) (3.4.19) (3.4.20) (3.4.21) (3.4.22) (3.4.23)
4.2	출입통제 관리		
4.2.1	주요시설 출입통제	전자서명인증사업자는 인증서를 발급하는 설비 등이 있는 주요 운영시설에 대한 철저한 출입통제 정책을 수립하고 이행하여야 한다. • 전자서명인증 관련 주요 운영시설의 출입은 통제되고 있는 제한된 수의 접근 지점을 통해서만 이루어지는지 여부를 확인 • 전자서명인증 관련 주요 운영시설의 출입은 다중 신원 검증 절차를 통하여 인가된 인원에게만 접근이 가능하도록 통제되는지 여부를 확인	● (3.4.1) (3.4.9) (3.4.10)
4.2.2	출입통제 관리	전자서명인증 관련 운영시설을 출입하는 모든 인원에 대한 기록을 관리하여야 한다. • 모든 인원들은 육안으로 식별 가능한 신분 등을 패용하고, 만일 패용하지 않는 인원을 발견 시에는 직원들이 신원확인을 요구할 수 있는지 여부를 확인 • 전자서명인증 관련 운영시설을 출입하는 모든 인원에 대해 기록을 남기고 관리하는지 확인 • 제 3 의 서비스 지원인력은 필요시에만 전자서명인증 관련 운영 시설의 보안 구역 출입이 허용되어야 하며, 이 경우에도 직원과 동행하여 이루어지는지 확인 • 전자서명인증 관련 시설의 방문자에 대해서 출입날짜와 시간을 기록하는 등 감독하는 절차가 마련되어 있는지 여부를 확인 • 전자서명인증 관련 시설에 대한 접근 권한이 주기적으로 검토 및 갱신되고 있는지 확인	● (3.4.11) (3.4.13) (3.4.14) (3.4.15)

연번	평가 항목	상세 평가 기준	WebTrust
4.3	침입 감지 및 감시		
4.3.1	침입 감지 및 감시	전자서명인증사업자는 전자서명인증 관련 운영시설에 대한 물리적인 침입에 대비하는 방안을 마련하여야 하고, 이러한 시설의 출입이나 내부활동을 모니터링하여야 한다. • 전자서명인증 관련 운영건물의 모든 외부 출입문에 침입 감지 시스템이 설치되어 운영되고 있는지 확인 • 전자서명인증 관련 시설 내에 직원이 없을 때에 물리적으로 잠금이 되고 경보장치가 작동되고 있는지 확인 • 전자서명인증 관련 시설의 출입이나 내부의 활동이 CCTV 등 영상정보 처리기기를 통해 모니터링 되고 있는지 확인	● (3.4.7) (3.4.8) (3.4.12) (3.9.13)
4.4	반출입 통제		
4.4.1	반출입 통제	전자서명인증사업자는 장비, 문서, 휴대용 저장매체 등의 반출입 통제 정책을 수립하고 반출입 시 이력을 작성하고 보관하여야 한다. • 전자서명인증 관련 시설 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제절차를 수립·이행하고 주기적으로 검토하는지 확인	● (3.4.24)
5. 운영 보안			
5.1	운영 절차 수립 및 준수		
5.1.1	운영절차 수립 및 준수	전자서명인증사업자는 전자서명인증시스템 및 보안시스템 운영을 위한 절차를 수립하고 이행하여야 한다. • 전자서명인증시스템 및 보안시스템 운영절차가 각 기능영역 별로 문서화되어 관리되고 있는지 확인 • 전자서명인증시스템 및 보안시스템 관련 장비, 소프트웨어, 운영 절차상의 모든 변경 사항을 통제하기 위하여, 관리 책임자 및 절차가 존재하는지 확인 • 시스템문서는 비인가 접근으로부터 보호되고 있는지 확인	● (3.5.1) (3.5.2) (3.5.3) (3.5.5)
5.1.2	저장매체 관리	전자서명인증사업자는 운영에 필요한 저장매체 및 이동식 저장매체를 관리하는 절차를 마련하고 이를 이행하여야 한다. • 저장매체 및 이동식 저장매체 관리 절차에 다음을 포함하고 있는지 확인 a) 더 이상 필요 없을 시, 재사용 가능한 저장매체에 담겨 있던 내용물은 지우거나, 저장매체 자체를 파기한다. b) 조직의 모든 이동식 저장매체는 승인을 득하여야 하며, 해당 저장매체들에 대한 감사 증적을 위해 기록이 유지관리 되어야 한다. c) 모든 저장매체는 안전하고 보안이 적용된 환경에서 제조사의 요구 스펙에 따라 보관되어야 한다. • 저장매체를 포함하는 장비는 파기 또는 재사용 전 민감 데이터의 저장 여부를 검사하여야 하며, 민감 데이터를 담고 있는 저장매체는 파기 또는 재사용 전 물리적으로 파기하거나 안전하게 덮어쓰기를 하는지 확인 • 비인가 공개 또는 남용으로부터 정보를 보호하기 위해, 정보의 저장 및 취급절차가 존재하며 이행하는지 확인	● (3.5.14) (3.5.15) (3.5.16) (3.5.17)

연번	평가 항목	상세 평가 기준	WebTrust
5.2	시스템 및 서비스 관리		
5.2.1	시스템 및 서비스 관리	전자서명인증사업자는 전자서명인증 관련 운영 시스템을 개발 및 테스트 시스템과 분리하고 안전한 보안설정, 성능·용량·상태 모니터링, 안전한 인수 및 유지 보수 절차를 수립하고 이행하여야 한다. • 개발 및 테스트 시설이 운영 설비로부터 분리되어 있는지 확인 • 외부로부터 설비관리 서비스를 받기 전에, 위협과 관련 통제 항목들이 식별되고 계약자와 협의하여 이를 계약서에 명시하고 있는지 확인 • 용량 요구사항을 모니터링하고 적절한 처리 능력 및 저장 용량의 가용성을 보장하기 위해서 향후 용량 요구사항을 예측하고 있는지 확인 • 신규 정보시스템, 업그레이드 및 새로운 버전에 대한 승인 기준이 수립되고 승인 전 시스템에 대한 적절한 테스트가 수행되는지 확인	● (3.5.4) (3.5.6) (3.5.7)
5.3	악성코드 예방·탐지·대응		
5.3.1	악성코드 예방·탐지·대응	악성코드 예방·탐지·대응을 위한 보안 시스템을 운영하고 운영체제 및 소프트웨어의 패치와 업데이트에 대한 정책과 절차를 수립하고 이행하여야 한다. • 악성코드 예방·탐지·대응을 위한 보안 시스템을 운영하고 운영체제 및 소프트웨어의 패치와 업데이트에 대한 정책과 절차를 수립하였는지 확인 • 수립된 정책과 절차의 이행과 더불어, 직원들에 대해서 지속적인 관심을 환기하는 프로그램이 있는지 확인	● (3.5.8)
5.4	침해사고 대응		
5.4.1	침해사고 대응정책	전자서명인증사업자는 침해사고에 대응하기 위한 정책을 수립하고 이행하여야 한다. • 비상연락 체계를 포함하여 침해사고 발생 시 보고절차, 대응 및 복구 절차, 신고 절차 등 침해사고 대응 정책 문서가 있는지를 확인 • 침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하고 있는지 확인 • 하드웨어 및 소프트웨어 오동작을 보고할 수 있는 절차를 수립하고 이행하고 있는지 확인 • 보고된 침해사고에 대해서 적절히 대응하였는지 평가하는 절차를 수립하고 이행하고 있는지 확인 • 침해사고의 종류, 크기, 영향, 오작동에 대해서 문서화 및 정량화하고, 모니터링 될 수 있도록 하는 공식적인 관리 절차가 존재하는지 확인	● (3.5.10) (3.5.11) (3.5.12) (3.5.13)

연번	평가 항목	상세 평가 기준	WebTrust
6. 접근통제			
6.1	접근통제 정책		
6.1.1	접근통제 정책수립	전자서명인증사업자는 전자서명인증시스템 및 보안시스템의 접근통제 절차, 역할에 따른 접근권한, 특정 업무 수행을 위해 요구되는 인원수 등이 포함된 접근통제 정책을 수립하여야 한다. • 접근 통제에 대한 다음 요건을 반영되어 수립되었는지 확인 a) 역할 및 역할에 따른 접근 권한 b) 각 사용자에 대한 신원확인과 인증 절차 c) 업무 분장 d) 특정 전자서명인증업무 수행을 위해 요구되는 인원 수 (m of N 규칙 등) • 전자서명인증시스템과 서비스에 접근하기 위한 사용자 등록 및 등록 취소 절차가 수립되었는지 확인	● (3.6.1)
6.2	접근권한 관리		
6.2.1	접근권한 관리	전자서명인증사업자는 전자서명인증시스템 및 보안시스템, 중요정보에 접근하기 위한 공식적인 사용자 계정 및 권한의 관리절차를 마련하고 갱신하여야 한다. • 시스템에 대한 특별 권한의 사용과 할당이 제한되고 통제되었는지 확인 • 공식적인 관리 절차에 따라 패스워드 및 멀티팩터 인증 토큰의 할당이 통제되고 있는지 확인 • 전자서명인증시스템과 보안시스템 운영절차가 각 기능 영역 별로 문서화되어 관리되고 있는지 확인 • 신뢰역할을 수행하는 사용자의 접근 권한이 정기적인 주기로 검토되고 갱신되는지 확인 • 사용자로 하여금 정의된 정책과 절차에 따라 패스워드의 사용과 선택을 하도록 하고 있는지 확인 • 관리 및 슈퍼사용자 계정은 멀티팩터 인증 통제를 권고하고 있는지 확인	● (3.6.2) (3.6.3) (3.6.4) (3.6.5) (3.6.6) (3.6.7) (3.6.8)
6.2.2	네트워크 접근통제	전자서명인증사업자는 전자서명인증시스템 및 보안시스템의 네트워크 보안에 대한 절차를 마련하고 이행하여야 한다. • 사용자는 인가된 서비스에만 직접적인 접근 권한이 부여되는지 확인 • 원격지 컴퓨터 시스템으로의 접속은 인증과정을 거치는지 확인 • 진단포트로의 접근은 엄격히 통제되는지 확인 • 내부 네트워크는 외부 도메인의 비인가 접근으로부터 보호하기 위한 통제(예: 방화벽)가 적용되어 있는지 확인 • 인가된 사용자의 가용성을 확보하기 위하여 접근 통제 정책에 따라 네트워크 서비스를 제한할 수 있는 통제가 있는지 확인 • 전자서명인증사업자는 로컬 네트워크 구성요소를 물리적으로 안전한 환경에서 관리하고, 구성 요구사항에 맞추어서 주기적으로 점검하는지 확인	● (3.6.9) (3.6.10) (3.6.11) (3.6.12) (3.6.14) (3.6.15) (3.6.16) (3.6.17)

연번	평가 항목	상세 평가 기준	WebTrust
6.2.3	하이퍼바이저, 운영시스템, 데이터베이스 및 네트워크 장치 접근 통제	전자서명인증사업자는 하이퍼바이저, 운영시스템, 데이터베이스 및 네트워크 장치에 대한 별도의 운영규정을 두어 관리하여야 한다. • 하이퍼바이저, 운영시스템, 데이터베이스 및 네트워크 장치는 전자서명인증사업자의 시스템 설정 표준을 준수하여 설정되어 있으며, 주기적으로 검토 및 업데이트되는지 확인 • 하이퍼바이저, 운영시스템, 데이터베이스 및 네트워크 장치의 패치 및 업데이트는 위험 평가에 기반하여 필요하다고 여겨질 때 적시적으로 적용되어야 하며 공식적인 변경 관리 절차를 따라 진행하는지 확인	● (3.6.20) (3.6.22) (3.6.27) (3.6.28) (3.6.29)
6.3	비인가자 시스템 접근 금지		
6.3.1	비인가자 시스템 접근 금지	시스템에 대한 접속 권한은 허가된 네트워크 서비스에서 사용자 인증절차에 의해 통제되어야 하며, 비인가자가 전자서명인증 업무와 관련된 네트워크, 서버, 데이터베이스 등의 시스템에 접근할 수 없도록 하여야 한다. • 시스템 접근 시 안전한 로그인 절차가 요구되는지 확인 • 모든 직원은 고유한 식별자(user ID)를 가지고 사용함으로써, 이에 따른 모든 활동들을 추적할 수 있는지 확인 • 공유 또는 그룹 계정이 필요 시, 개인의 책임을 유지하기 위해 다른 모니터링 통제가 구현되어 있는지 확인 • 시스템 유틸리티 프로그램의 사용은 인가된 사용자로 제한하고 엄격하게 통제되고 있는지 확인 • 비활성화 터미널은 사용에 앞서 재인증을 요구하고 있는지 확인 • 민감 데이터는 비인가 사용자에게 공개되지 않도록 보호되고 있는지 확인	● (3.6.18) (3.6.19) (3.6.21) (3.6.23) (3.6.24) (3.6.25) (3.6.26)
7. 개발 보안			
7.1	비인가자 시스템 접근 금지		
7.1.1	시스템 개선 및 변경	전자서명인증사업자는 시스템 개선이나 신규 시스템 도입 시 통제 절차를 수립하여야 한다. • 신규 시스템 도입이나 시스템 개선 시 통제 절차를 마련하고 있는지 확인 • 하드웨어, 네트워크 구성요소 및 시스템 설정 변경을 위한 변경 통제 절차를 수립하고 준용하고 있는지 확인 • 테스트 데이터가 보호되고 통제되고 있는지 확인 • 운영시스템(OS)의 변경이 있을 시, 응용시스템이 검토되고 테스트 되도록 절차가 마련되어 있는지 확인	● (3.7.1) (3.7.2) (3.7.3) (3.7.4) (3.7.6)
7.1.2	소프트웨어 관리	전자서명인증사업자는 정보시스템의 오류 위험을 최소화하기 위해 소프트웨어의 변경에 대해서 엄격하게 통제하여야 한다. • 소프트웨어의 테스트 및 변경 통제 절차가 존재하는지 확인 • 소프트웨어 패키지의 수정을 제한하고 모든 변경을 엄격하게 통제하고 있는지 확인 • 소프트웨어의 구매, 사용, 변경은 통제되며, 악성코드 등의 포함 여부를 확인하는 절차가 마련되어 있는지 확인. 이러한 통제들이 아웃소싱된 소프트웨어 개발에도 동일하게 적용되는지 확인	● (3.7.7) (3.7.8) (3.7.9)

연번	평가 항목	상세 평가 기준	WebTrust
7.2	비인가자 시스템 접근 금지		
7.2.1	프로그램 소스코드 보호	전자서명인증사업자는 프로그램 소스 라이브러리에 대한 적절한 접근 통제와 형상 관리를 수행하여야 한다. • 프로그램 소스 라이브러리에 대한 접근 통제와 소스코드에 대한 형상 관리를 하고 있는지 확인	● (3.7.5)
8. 업무 연속성 관리			
8.1	업무 연속성 계획		
8.1.1	업무 연속성 계획	전자서명인증사업자는 장애 및 재해로부터 업무 연속성 확보를 위해 위험 평가에 기초한 연속성 계획을 마련하여야 한다. • 전자서명인증사업자의 업무 연속성 계획에 다음이 포함되어 있는지 확인 a) 계획 실행을 위한 조건 b) 응급 절차 c) 대체시스템 절차 d) 재개 절차 e) 계획에 대한 유지관리 일정 f) 홍보 및 교육 요건 g) 개인의 책임 h) 복구 시간 목표(RTO) 및 복구 지점 목표(RPO) i) 긴급 사태 대책에 대한 정기적인 테스트 • 업무 연속성 계획에 전자서명인증의 메인 시설 또는 원격지 시설에 대해서, 재난 발생 후 안전한 환경을 복원하기 전까지의 시설보안 절차를 포함하는지 확인 • 업무 연속성 계획에 컴퓨팅 리소스, 소프트웨어 및 (또는) 데이터가 손상되거나 손상이 의심되는 경우 사용되는 복구 절차를 다루고 있는지 확인 • 업무 연속성 계획에 인증 정책이나 전자서명인증업무준칙에 공개된 허용 가능한 시스템 정지 시간, 복구 시간, 장애 간 평균 시간이 정의되어 있는지 확인	● (3.8.1) (3.8.2) (3.8.6) (3.8.7) (3.8.8) (3.8.9)
8.1.2	업무 연속성 계획 관리	업무 연속성 계획을 정기적으로 테스트하여 변화 사항을 반영하여 갱신하여야 한다. • 업무 연속성 계획의 유효성 유지를 위하여 주기적으로 테스트하여 유효성을 유지하도록 갱신되는지 확인 • 업무 연속성 계획은 주기적으로 검토되고 갱신되고 있는지 확인	● (3.8.10) (3.8.11)
8.2	백업 및 원격지 시설		
8.2.1	백업 및 원격지	전자서명인증사업자는 장애 및 재해 발생 시 핵심 업무가 복구될 수 있도록 대체 백업 시설을 마련하여야 한다.	● (…)

연번	평가 항목	상세 평가 기준	WebTrust
8.2.1	백업 및 원격지	• 장애 및 재해 발생 시 업무가 복구될 수 있도록 마련된 대체 백업 시설이 있는지 확인 • 복구 장치와 백업 미디어는 메인 시설의 재해로부터 손상 및 피해를 피하기 위해 안전한 거리에 위치하고 있는지 확인 • 대체 백업 시설에 대한 보안 수준이 메인 시설과 동등한 수준으로 유지되는지 확인 • 필수 사업 정보의 백업 사본이 정기적으로 발생하여야 하며, 이러한 백업 사본에 대한 보안요구사항은 백업된 정보와 동일한지 여부를 확인	● (3.8.3) (3.8.4) (3.8.5)
9. 감사로그			
9.1	감사로그 생성		
9.1.1	감사로그 생성	전자서명인증사업자는 전자서명인증 서비스와 관련된 전자서명생성정보·인증서·암호화 장치 등의 감사로그를 생성하고 위험 평가 및 관계 법령에서 요구하는 특정 기간 동안 보관할 수 있도록 하여야 한다. • 모든 입력 기록이 다음 사항을 포함하는지 확인 a) 입력 날짜와 시간 b) 입력 일련 번호 (자동 입력에 대해) c) 입력의 종류 d) 입력소스 (예: 터미널, 포트, 장소, 가입자, 등) e) 입력 개체의 신원 • 전자서명인증사업자가 키의 수명관리와 관련된 다음 사항들을 기록하는지 확인 a) 전자서명인증사업자 키의 생성 b) 수동 암호화 키의 설치와 그 결과 (운영자의 신원과 함께) c) 전자서명인증사업자 키의 백업 d) 전자서명인증사업자 키의 보관 e) 전자서명인증사업자 키의 복구 f) 전자서명인증사업자 키의 escrow activities (해당 사항이 있는 경우) g) 전자서명인증사업자 키의 사용 h) 전자서명인증사업자 키의 기록(archival) i) 키와 관련된 자료의 서비스로부터의 철회 j) 전자서명인증사업자 키의 파기 k) 전자서명인증사업자 키 전송 l) 전자서명인증사업자 키 마이그레이션 m) 키 관리 활동의 승인 개체의 신원 n) 키와 관련된 자료(예를 들어, 이동식 저장매체에 보관된 키 또는 중요한 요소)를 다루는 개체의 신원 o) 키 보관 및 키를 저장하고 있는 장치 또는 매체의 보관 p) 개인키 손상	● (3.9.4) (3.10.1) (3.10.2) (3.10.3) (3.10.5) (3.10.6) (3.10.7) (3.10.8) (3.10.9)

연번	평가 항목	상세 평가 기준	WebTrust
9.1.1	감사로그 생성	• 전자서명인증사업자가 암호화 장치의 생명 주기 관리와 관련된 다음 주요 이벤트를 기록하는지 확인 a) 장치의 습득과 설치 b) 저장매체에 저장 또는 추출 c) 장치의 활성화와 사용 d) 장치의 제거 e) 서비스 또는 수리에 맡김 f) 장치의 파기 • 전자서명인증사업자가 가입자의 키 관리 서비스를 제공하는 경우, 가입자 키 관리의 생명 주기와 관련된 주요 이벤트를 기록하는지 확인 a) 키의 생성 b) 키의 배부 (해당사항이 있는 경우) c) 키의 백업 (해당사항이 있는 경우) d) 키의 위탁 (해당사항이 있는 경우) e) 키의 보관 f) 키의 복구 (해당사항이 있는 경우) g) 키의 기록 (해당사항이 있는 경우) h) 키의 파기 i) 키의 관리활동을 승인하는 주체의 신원 j) 키의 유출 • 전자서명인증사업자가 다음과 같은 인증서 신청 정보를 기록하거나 등록기관에게 기록하도록 하는지 확인 a) 가입자에게 요구사항을 만족하기 위해 적용된 신원 확인 방법 또는 사용된 정보 b) 고유 신원인증 데이터, 숫자 또는 신원 증빙 문서의 조합에 대한 기록 (예: 가입자의 운전면허번호) (해당사항이 있는 경우) c) 신청서와 신원 증빙 문서의 보관 장소 d) 신청을 수락하는 개체의 신원 e) 신원 증빙 문서를 검증하는 방법 (해당사항이 있는 경우) f) 수령하는 전자서명인증사업자 또는 제출하는 등록기관의 이름 (해당사항이 있는 경우) g) 가입자의 가입 동의서에 대한 동의 h) (개인정보보호법에서 요구되는 경우) 개인정보 기록 및 소유, 지정된 제 3 자에 제공, 인증서 발급 등에 대한 동의 내역 • 전자서명인증사업자가 다음의 인증서 생명 주기 관리와 관련된 주요 이벤트를 기록하고 있는지 확인 a) 인증서 요청의 접수 – 초기 인증서 요청, 갱신 요청, rekey 요청 포함 b) 인증을 위한 공개 키의 제출	● (3.9.4) (3.10.1) (3.10.2) (3.10.3) (3.10.5) (3.10.6) (3.10.7) (3.10.8) (3.10.9)

연번	평가 항목	상세 평가 기준	WebTrust
9.1.1	감사로그 생성	c) 개체의 소속 변경 d) 인증서 생성 e) 전자서명인증사업자의 공개키 배부 f) 인증서 폐지 요청 g) 인증서 폐지 h) 인증서 정지 요청 (해당사항이 있는 경우) i) 인증서 효력 정지와 효력 회복 j) 인증서 폐지 목록의 생성과 배포 • 전자서명인증사업자가 보안에 민감한 다음 이벤트들을 기록하는지 확인 a) 보안에 민감한 파일 또는 기록의 읽기/쓰기 (감사로그 포함) b) 보안에 민감한 데이터에 대해 행해진 모든 행위 c) 보안 프로파일 변경 내역 d) 신원 인증 메커니즘의 사용 (성공/실패 여부 및 다중 실패 시도 기록) e) 시스템 충돌, 하드웨어 에러 및 기타 비정상 이벤트 f) 신뢰행위자, 컴퓨터 운영자, 시스템 관리자, 시스템 보안 책임자 등이 수행한 행위 g) 개체의 소속 변경 h) 암호화 및 인증 절차를 우회하는 결정 i) 전자서명인증시스템 또는 관련 구성요소에 대한 접근 • 감사 기록에는 개인키를 어떠한 형태로도 포함하고 있지 않는지 확인 (예: 일반 텍스트 또는 암호화 형태) • 전자서명인증사업자 컴퓨터시스템의 시간은 정확한 기록 유지를 위해 전자서명인증업무준칙에서 정의하고 있는 타임 소스와 동기화되어 있는지 확인	● (3.9.4) (3.10.1) (3.10.2) (3.10.3) (3.10.5) (3.10.6) (3.10.7) (3.10.8) (3.10.9)
9.2	감사로그 관리		
9.2.1	감사로그 관리	전자서명인증사업자는 감사로그의 무결성 검증, 승인되지 않거나 의심되는 기록에 대해서 주기적으로 검토하고, 백업 및 접근 통제 등을 포함한 관리 절차를 마련하여야 한다. • 현재 및 보관된 감사로그는 변경, 대체, 승인되지 않은 파기 등으로부터 보호되도록 관리하고 있는지 확인 • 감사 기록의 무결성을 보호하기 위한 전자서명 등이 적용되고 있는지 확인 • 감사로그를 서명하는 키는 해당 용도로만 사용되고 다른 용도로는 사용되지 않는지 확인 • 전자서명인증정책이나 전자서명인증업무준칙에 준거하여 감사로그는 주기적으로 백업 및 보관되는지 확인 • 감사로그의 보유기간이 관련 법령과 더불어 위험 평가를 통해 지정되고 있는지 확인	● (3.9.11) (3.9.12) (3.10.10) (3.10.11) (3.10.12) (3.10.13) (3.10.14) (3.10.15) (3.10.16) (3.10.17) (3.10.18)

연번	평가 항목	상세 평가 기준	WebTrust
9.2.1	감사로그 관리	• 감사로그의 백업을 안전한 별도의 장소에 보관하여야 하며, 위험 평가 및 관련 법령에서 요구되는 특정 기간 동안 보관하고 있는지 확인 • 승인 받은 인원만이 타당한 사업 또는 보안상의 사유로 감사기록 및 보관 중인 감사기록을 열람할 수 있도록 하는지 확인 • 장애 및 재해 발생 시 업무가 복구될 수 있도록 마련된 대체 백업 시설이 있는지 확인 • 감사기록은 전자서명인증업무준칙에 준거하여 주기적으로 검토되고 있는지 확인	● (3.9.11) (3.9.12) (3.10.10) (3.10.11) (3.10.12) (3.10.13) (3.10.14) (3.10.15) (3.10.16) (3.10.17) (3.10.18)

별첨 3. 개인정보보호 세부평가기준

연번	평가 항목 및 상세 평가 기준
1. 관리체계 수립	
1.1	**최고책임자 지정** 전자서명인증사업자의 최고경영자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보보호책임자를 직위 및 자격 요건을 갖춘 자로 지정하여야 한다.
1.2	**정책 수립** 전자서명인증사업자는 개인정보보호 정책을 실행하기 위한 내부관리 계획을 수립 및 시행하여야 한다. • 내부관리계획(개인정보지침 등) 수립 및 승인 여부 확인 • 중요 변경이 있는 경우, 개정 이력을 관리하는지 확인
1.3	**주요 직무자 지정 관리** 전자서명인증사업자는 개인정보 및 중요정보의 취급이나 주요 시스템 접근 등 주요 직무의 기준과 관리방안을 수립하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다. • 업무 필요성에 따라 주요 직무자 및 개인정보취급자를 최소화하여 지정 • 개인정보 및 중요정보의 취급, 주요 시스템 접근 등 주요 직무의 기준을 명확히 정의
1.4	**직무 분리** 전자서명인증사업자는 개인정보취급자의 권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다. • 개인정보취급 업무를 포함한 직무 분리 기준을 수립하고 있는지 확인 • 직무분리가 어려운 경우 직무자간 상호 검토, 정기 모니터링 및 변경사항 승인, 책임추적성 확보 방안 등의 보완통제 마련 여부 확인
2. 관리체계 실행 및 운영	
2.1	**개인정보 식별** 전자서명인증사업자는 업무특성에 따라 개인정보 분류기준을 수립하여 관리체계 범위 내 모든 개인정보를 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다. • 개인정보 분류 기준 수립 및 목록 관리 여부 확인 • 식별된 개인정보에 대해 업무 영향도 등에 따른 중요도를 결정하고 보안등급을 부여하는지 확인
2.2	**CI 정보 식별 등** 개인정보 목록에는 연계정보(CI) 등 전자서명인증 관련 정보가 식별되어 포함되어야 한다.

연번	평가 항목 및 상세 평가 기준
2.3	**현황 및 흐름분석** 전자서명인증사업자는 개인정보보호 관리체계 내 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다. • 개인정보 처리 현황을 식별하고 개인정보 흐름을 파악하고 있는지 확인 (개인정보 또는 전자서명인증 관련 정보 흐름도) • 최신 현황으로 업데이트 되어 있는지 확인
3. 관리체계 검토 및 개선	
3.1	**관리체계 점검** 전자서명인증사업자는 개인정보보호 관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1 회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다. • 내부 관리계획 이행 실태에 대한 연 1 회 이상의 점검을 수행하고 있는지 확인 (자체/외부 점검, 내부 감사 등) • 점검 결과에 대한 경영진 승인 여부 확인
3.2	**관리체계 개선** 전자서명인증사업자는 법적 요구사항 준수 검토 및 관리체계 점검을 통해 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하며, 경영진은 개선 결과의 정확성과 효과성 여부를 확인하여야 한다. • 내부 관리계획의 이행 계획이 수립되어 있는지 확인 • 법적 요구사항 준수 여부를 검토하고 있는지 확인 • 개선 계획에 대한 경영진 승인을 받고 있는지 확인
4. 개인정보 생명주기 관리	
4.1	**개인정보 수집 제한** 전자서명인증사업자는 전자서명인증 서비스 제공을 위하여 필요한 최소한의 개인정보를 적법하고 정당하게 수집하여야 하며, 필수정보 이외의 개인정보를 수집하는 경우에는 선택항목으로 구분하여 해당 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하지 않아야 한다. • 서비스 제공 또는 법령에 근거한 처리 등을 위해 필요한 최소한의 정보만을 수집하는지 확인 • 필수/선택 항목을 구분하여 수집하고, 선택 항목 동의가 없어도 서비스가 제공되는지 확인
4.2	**개인정보 수집 동의** 전자서명인증사업자는 정보주체(이용자)의 동의를 받거나 관계 법령에 따라 개인정보를 적법하게 수집하여야 하며, 만 14 세 미만 아동의 개인정보를 수집하려는 경우에는 법정대리인의 동의를 받아야 한다. • 개인정보 수집 시 정보주체(이용자)에게 관련 내용을 명확하게 고지하고 있는지 확인 • 동의를 받는 경우 법령에서 정한 중요한 내용에 대해 명확히 표시하는지 확인 • 수집이용/제 3 자제공/목적외이용 등에 대해 각각 구분하여 동의를 받고 있는지 확인

연번	평가 항목 및 상세 평가 기준
4.3	**법정 대리인 동의** 전자서명인증사업자는 만 14 세 미만 아동의 개인정보에 대해 수집·이용·제공 등의 동의를 받는 경우 법정대리인에게 필요한 사항에 대하여 고지하고 동의를 받아야 한다. • 수집하는 경우 전자서명인증 관련 업무 필요성 여부 확인 • 법정 대리인 자격요건 확인 절차 및 동의 기록 보관 여부 확인
4.4	**주민등록번호 처리 제한** 전자서명인증사업자는 법적 근거가 있는 경우를 제외하고는 주민등록번호를 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다. • 명확한 법적 근거가 있는 경우에만 처리하고 있는지 확인 • 주민등록번호 수집이 가능한 경우에도 아이핀, 휴대폰 인증 등 주민등록번호를 대체하는 수단을 제공하고 있는지 확인
4.5	**민감정보 및 고유식별정보 처리 제한** 전자서명인증사업자는 민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체(이용자)의 별도 동의를 받아야 한다. • 수집 시 정보주체(이용자)로부터 별도의 동의를 받거나 관련 법령에 근거가 있는 경우에만 처리하고 있는지 확인
4.6	**간접수집 보호조치** 전자서명인증사업자는 정보주체(이용자) 이외로부터 개인정보를 수집하거나 제공받는 경우에는 업무에 필요한 최소한의 개인정보만 수집·이용하여야 하고 법령에 근거하거나 정보주체(이용자)의 요구가 있으면 개인정보의 수집 출처, 처리목적, 처리정지의 요구나 동의 철회 권리를 알려야 한다. • 해당되는 경우, 개인정보 수집에 대한 동의 획득 책임이 개인정보를 제공하는 자에게 있음을 계약을 통해 명시하고 있는지 확인 • 자동수집장치 등에 의해 수집·생성하는 개인정보(이용내역 등)의 경우에도 최소수집 원칙을 적용(쿠키 등 내역 확인)하고 있는지 확인 • 정보주체(이용자)의 요구가 있는 경우 즉시 필요한 사항을 정보주체(이용자)에게 알리고 있는지 확인 • 정보주체(이용자)에게 수집 출처에 대해 알린 기록을 해당 개인정보의 파기 시까지 보관·관리하고 있는지 확인
4.7	**개인정보 현황관리** 전자서명인증사업자는 개인정보 파일을 신규로 보유하거나 변경하는 경우, 개인정보파일 관리대장을 작성하거나 변경하여야 한다. • 전자서명인증업무가 포함된 개인정보 목록을 관리하고 있는지 확인 • 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하는지 확인

연번	평가 항목 및 상세 평가 기준
4.8	**개인정보 품질보장** 전자서명인증사업자는 개인정보 처리 목적에 따라 개인정보의 정확성·완전성·최신성을 보장하기 위한 관리절차를 마련하고, 이를 정보주체(이용자)에게 알려야 한다. • 수집된 개인정보는 내부 절차에 따라 안전하게 처리하도록 관리하며, 최신의 상태로 정확하게 유지하고 있는지 확인 • 정보주체(이용자)가 개인정보의 정확성, 완전성 및 최신성을 유지할 수 있는 방법을 제공하고 있는지 확인
4.9	**개인정보 표시제한 및 이용 시 보호조치** 전자서명인증사업자는 개인정보 처리 시 목적에 따라 출력 항목 최소화, 개인정보 표시 제한, 출력물 보호조치 등을 수행하여야 한다. 또한, 불필요해진 개인정보는 삭제 또는 식별할 수 없도록 조치하여야 한다. • 가입자/인증서 조회 화면 등에서 개인정보 조회 및 출력(인쇄, 화면표시, 파일생성 등) 항목 최소화 확인 • 개인정보 표시제한 보호조치의 일관성을 확보할 수 있도록 관련 기준을 수립하여 적용하는지 확인 (마스킹 정책 등) • 종이 인쇄물 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 조치 확인
4.10	**개인정보 유·노출 방지** 전자서명인증사업자는 개인정보 처리화면 및 공중망을 통한 개인정보 유·노출 등을 방지하기 위한 보호대책을 적용하여야 한다. • 개인정보 파일 다운로드 제한 조치 확인 • 개인정보 검색 시 과도한 정보가 조회되지 않도록 일치 검색 또는 두 가지 항목 이상의 검색조건 요구 확인 • 개인정보 노출 여부를 정기적으로 점검하는지 확인
4.11	**개인정보 유출 등의 통지·신고** 전자서명인증사업자는 개인정보가 분실·도난·유출 되었음을 알게 되었을 때 관계 법령에서 정한 시한 내에 정보주체에게 알리고 관련 기관에 신고하여야 한다.
4.12	**홍보 및 마케팅 목적 활용 시 조치** 전자서명인증사업자는 마케팅을 목적으로 개인정보를 수집·이용하는 경우, 그 목적을 정보주체(이용자)가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다. • 정보주체(이용자)가 명확하게 인지할 수 있도록 알리고 별도 동의를 받고 있는지 확인 • 2 년 마다 정기적으로 수신자의 수신동의를 받고 있는지 확인 • 수신자가 수신거부의사를 표시하거나 사전 동의를 철회한 경우 영리목적의 광고성 정보 전송을 중단하도록 하고 있는지 확인 • 전송자 명칭, 수신거부 방법 등을 구체적으로 밝히고 있으며, 야간시간에는 전송하지 않도록 하고 있는지 확인

연번	평가 항목 및 상세 평가 기준
4.13	**이용자 단말기 접근 보호** 전자서명인증사업자는 정보주체(이용자)의 이동통신 단말장치 내에 저장되어 있는 정보 및 이동통신 단말장치에 설치된 기능에 접근이 필요한 경우 이를 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받아야 한다. • 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받고 있는지 확인 • 해당 서비스에 반드시 필요한 접근권한이 아닌 경우, 정보주체(이용자)가 동의하지 않아도 서비스 제공을 거부하지 않도록 하고 있는지 확인 • 해당 접근 권한에 대한 정보주체(이용자)의 동의 및 철회 방법을 마련하고 있는지 확인
4.14	**개인정보 목적 외 이용 및 제공** 전자서명인증사업자는 개인정보 수집 시 정보주체(이용자)에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체(이용자)의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다. • 동의 받은 목적 또는 법령에 근거한 범위 내에서만 이용·제공하고 있는지 확인 • 수집 목적 또는 범위를 초과하여 이용하거나 제공하는 경우 별도의 동의를 받거나 법적 근거가 있는 경우로 제한하고 있는지 확인 • 목적 외의 용도로 제 3 자에게 제공하는 경우 제공받는 자에게 이용목적·방법 등을 제한하거나 안전성 확보를 위해 필요한 조치를 마련하도록 요청하고 있는지 확인 • 안전한 절차와 방법을 통해 제공하고 제공 내역을 기록하여 보관하고 있는지 확인 • 제 3 자에게 개인정보의 접근을 허용하는 경우 개인정보를 안전하게 보호하기 위한 보호절차에 따라 통제하고 있는지 확인
4.15	**개인정보 제 3 자 제공** 전자서명인증사업자는 개인정보를 제 3 자에게 제공하는 경우 법적 근거에 의하거나 정보주체(이용자)의 동의를 받아야 하며, 제 3 자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다. • 법령에 규정이 있는 경우를 제외하고는 정보주체(이용자)에게 관련 내용을 명확하게 고지하고 동의를 받고 있는지 확인 • 수집·이용에 대한 동의와 구분하여 받고 이에 동의하지 않는다는 이유로 해당 서비스의 제공을 거부하지 않도록 하고 있는지 확인 • 제공 목적에 맞는 최소한의 개인정보 항목으로 제한하고 있는지 확인
4.16	**업무 위탁에 따른 정보주체 고지** 전자서명인증사업자는 개인정보 처리업무를 제 3 자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자(재수탁자 포함) 등 관련사항을 정보주체에게 알려야 한다. • 인터넷 홈페이지 등에 위탁하는 업무의 내용과 수탁자를 현행화하여 공개하고 있는지 확인 • 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 문자전송 등의 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체(이용자)에게 알리고 있는지 확인

연번	평가 항목 및 상세 평가 기준
4.17	**업무 위탁에 따른 관리 감독** 전자서명인증사업자는 개인정보처리 업무를 위탁하는 경우 수탁자가 개인정보를 안전하게 처리하는지를 주기적으로 관리·감독하여야 한다. • 수탁사에 대한 개인정보보호 교육을 실시하는지 확인 • 수탁자 주기적으로 개인정보 처리 현황을 점검하는지 확인
4.18	**영업의 양수 등에 따른 개인정보 이전** 전자서명인증사업자는 영업의 양도·합병 등으로 개인정보를 이전하거나 이전 받는 경우 정보주체 (이용자) 통지 등 적절한 보호조치를 수립·이행하여야 한다. • 개인정보를 이전 받는 자는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제 3 자에게 제공하고 있는지 확인 • 필요한 사항을 사전에 정보주체(이용자)에게 알리고 있는지 확인 • 법적 통지 요건에 해당될 경우 개인정보를 이전 받은 사실을 정보주체(이용자)에게 지체 없이 알리고 있는지 확인
4.19	**개인정보 국외 이전** 전자서명인증사업자는 개인정보를 국외로 이전하는 경우 국외 이전에 대한 동의, 관련 사항에 대한 공개 등 적절한 보호조치를 수립·이행하여야 한다. • 정보주체(이용자)에게 필요한 사항을 모두 알리고 동의를 받는지 확인 • 국외에 처리 위탁 또는 보관하는 경우에는 동의에 갈음하여 관련 사항을 이용자에게 알리고 있는지 확인 • 정보주체의 동의 없이 개인정보를 국외 이전하는 경우, 관련 법령에서 요구하는 요건에 부합하는지 확인 • 개인정보보호 관련 법령 준수 및 개인정보보호 등에 관한 사항을 포함하여 국외 이전에 관한 계약을 체결하고 필요한 조치를 취하고 있는지 확인
4.20	**처리목적 달성 후 보유 시 조치** 전자서명인증사업자는 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 개인정보를 파기하지 아니하고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다. • 관련 법령에 따른 최소한의 기간으로 한정하여 최소한의 정보만을 보존하고, 다른 개인정보와 분리하여 저장·관리하고 있는지 확인 • 분리 보관하고 있는 개인정보에 대하여 관련 법령에서 정한 목적 범위 내에서만 처리 가능하도록 관리하고 있는지 확인 • 분리 보관하고 있는 개인정보에 대하여 접근권한을 최소한의 인원으로 제한하고 있는지 확인
4.21	**개인정보처리방침 공개** 전자서명인증사업자는 개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 개인정보처리방침을 수립하고, 이를 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화 하여야 한다. • 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지 등에 지속적으로 현행화 하여 공개하고 있는지 확인 • 관련 법령에서 요구하는 내용을 모두 포함하고 있는지 확인 • 변경되는 경우 사유 및 변경 내용을 지체없이 공지하고 정보주체가 언제든지 변경 사항을 쉽게 알아볼 수 있도록 조치하고 있는지 확인

연번	평가 항목 및 상세 평가 기준
4.22	**개인정보 파기** 전자서명인증사업자는 개인정보의 보유기간 및 파기 관련 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성, 가명정보의 처리 기간 경과 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다. 단, 법령에 의거하여 보존하여야 하는 경우에는 파기하지 않고 보존하여야 한다. • 보유기간 및 파기와 관련된 내부 정책을 수립하고 있는지 확인 • 보유기간 경과, 처리목적 달성 등 불필요하게 되었을 때 지체 없이 파기하고 있는지 확인 • 복구·재생되지 않도록 안전한 방법으로 파기하고 있는지 확인 • 파기 결과 등을 개인정보파일 파기 관리대장에 기록 및 관리하는지 확인 • 관련 법령에 의거하여 개인정보를 보존하여야 하는 경우에는 해당 개인정보를 다른 개인정보와 분리하여서 저장 및 관리하는지 확인
5. 정보주체 권리보장	
5.1	**정보주체 권리보장** 전자서명인증사업자는 정보주체가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구(이하 “열람 등”)를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체의 개인정보 처리 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다. • 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구, 삭제 요청 등 권리 행사 관련 절차를 수립하여 공지하고 있는지 확인 • 개인정보 처리 요청 발생 시, 지체없이 (또는 규정된 기간 내) 필요한 조치를 취하고 있는지 확인 • 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하여 안내하고 있는지 확인 • 요구 및 처리 결과에 대하여 기록을 남기고 있는지 확인
5.2	**이용 · 제공 내역 통지** 법적 의무 대상자에 해당하는 경우 개인정보 이용 · 제공 내역 또는 해당 내역을 확인할 수 있는 정보시스템 접속 방법 등을 주기적으로 통지하고 기록으로 남겨야 한다. • 개인정보 이용 · 제공 내역을 정보주체에게 연 1 회 이상 통지하고 그 기록을 남기고 있는지 확인 • 통지 항목은 법적 요구항목을 모두 포함하고 있는지 확인 • 서면 · 전자우편 · 전화 · 문자전송 등으로 정보주체에게 통지하는지 확인. 단, 정보시스템 접속 방법 통지는 서비스 제공 과정에서 알림창을 통해 알리는 방법으로 제공하는지 확인
6. 기술적 보호조치	
6.1	**개인정보취급자 계정 관리** 전자서명인증사업자는 개인정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 개인정보취급자의 등록·해지 및 접근권한의 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 개인정보취급자에게 개인정보 관련 책임이 있음을 규정화하고 인식시켜야 한다. • 사용자 계정 및 접근권한의 등록·변경·삭제에 관한 공식적인 절차를 수립·이행하는지 확인 • 계정 및 접근권한의 생성·등록·변경 시 직무 별 접근권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하고 있는지 확인

연번	평가 항목 및 상세 평가 기준
6.2	**개인정보취급자 책임 추적성** 개인정보처리시스템에 접속할 수 있도록 사용자 계정을 발급하는 경우, 책임추적성을 확보하여야 한다. • 개인정보취급자 별로 고유한 사용자 계정을 발급하고 있는지 확인 • 개인정보취급자 계정은 다른 개인정보취급자와 공유되지 않도록 하고 있는지 확인
6.3	**사용자 식별** 전자서명인증사업자는 사용자 계정에 대하여 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립·이행하여야 한다. • 사용자 및 개인정보취급자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자의 사용을 제한하고 있는지 확인 • 불가피한 사유로 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 보완대책을 마련하여 책임자의 승인을 받고 있는지 확인
6.4	**사용자 인증** 전자서명인증사업자는 개인정보 처리 시 개인정보취급자 및 관리자, 정보주체를 대상으로 안전한 인증방식을 적용하여야 한다. • 개인정보취급자 및 관리자, 정보주체는 권한 도용 등을 방지하기 위하여 안전한 인증방식을 적용하고 있는지 확인 • 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우, 안전한 인증수단(인증서, 보안토큰, 일회용 비밀번호)을 적용하는지 확인
6.5	**원격접속 인증** 전자서명인증사업자는 개인정보취급자가 정보통신망을 통해 외부에서 이용자가 아닌 정보주체의 개인정보처리시스템에 접속하려는 경우, 가상 사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단(인증서, 보안토큰, 일회용 비밀번호)을 적용하여야 한다.
6.6	**비밀번호 관리** 전자서명인증사업자는 법적 요구사항, 외부 위협요인 등을 고려하여 개인정보취급자와 고객, 회원 등 정보주체(이용자)가 아이디 및 비밀번호를 사용하여 인증 시에는 비밀번호 관리절차를 수립·이행하여야 한다. • 개인정보처리시스템에 대한 안전한 사용자 비밀번호 관리절차 및 작성규칙을 수립·이행하는지 확인 • 정보주체(이용자)가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성 규칙을 수립·이행하는지 확인 • 비밀번호 설정 시 최소길이(조합도 포함), 동일한 비밀번호 사용제한, 추측 가능한 문자열 포함 제한 등 조합규칙을 적용하는지 확인
6.7	**추가 인증 절차** 전자서명인증사업자는 정보주체(이용자)가 인터넷 홈페이지 등을 통해 중요한 정보 또는 화면에 접근하려는 경우에는 비밀번호 재확인, 휴대폰 인증, 공동인증서 등 본인임을 확인할 수 있는 추가적인 인증 절차를 적용하여야 한다.

연번	평가 항목 및 상세 평가 기준
6.8	**접근권한 부여 내역 관리** 전자서명인증사업자는 개인정보처리시스템의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3 년간 보관하여야 한다.
6.9	**인터넷 접속 통제** 전자서명인증사업자는 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 등을 통해 개인정보가 노출되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자 PC, 모바일 기기, 관리용 단말기 등에 보호 조치하여야 한다.
6.10	**인터넷망 차단 조치** 전자서명인증사업자는 관련 법령에 따라 인터넷망 차단 조치 의무가 부과된 경우, 개인정보에 대한 다운로드, 파기, 접근 권한 설정이 가능한 개인정보취급자의 PC 등을 대상으로 개인정보처리자가 인터넷 망 차단 조치를 적용하여야 한다.
6.11	**암호정책 적용** 전자서명인증사업자는 개인정보보호를 위하여 법적 요구사항을 반영하여 암호화를 적용하여야 한다. • 법적 요구사항을 반영한 암호화 대상, 암호강도, 암호사용 등이 포함된 암호정책을 수립하고 있는지 확인 • 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보의 저장 및 송·수신 시 암호화를 적용하는지 확인 • 개인정보를 정보통신망을 통해 인터넷망 구간으로 송·수신하는 경우 암호화하고 있는지 확인 • 인증정보(생체인식정보, 비밀번호)를 정보통신망을 통해 송·수신하는 경우 암호화하고 있는지 확인 • 이용자의 개인정보, 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조 저장매체 등에 저장하는 경우 암호화하고 있는지 확인
6.12	**암호키 관리** 관련 법령에서 요구하는 경우, 전자서명인증사업자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립 및 시행하여야 한다.
6.13	**로그 및 접속기록 관리** 전자서명인증사업자는 관련 법령에서 요구하는 바에 따라 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 관리하여야 한다. • 접속 기록에 식별자, 접속일시, 접속지 정보, 처리한 정보주체정보, 수행업무 등이 포함되는지 확인 • 접속 기록을 최소 1 년 이상 보관하는지 확인. 단, 기간통신사업자이거나 5 만명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 경우에는 2 년 이상 보관·관리하는지 확인 • 접속 기록을 월 1 회 이상 정기적으로 점검하는지 확인 • 접속 기록에 개인정보의 다운로드가 확인된 경우 사유 확인 수행하는지 확인 • 접속 기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하기 위한 조치를 적용하는지 확인

연번	평가 항목 및 상세 평가 기준
6.14	**정보자산 재사용 및 폐기** 전자서명인증사업자는 정보자산의 재사용과 폐기 과정에서 개인정보 및 중요 정보가 복구 및 재생되지 않도록 안전한 재사용 및 폐기 절차를 수립·이행하여야 한다. • 안전한 재사용 및 폐기에 대한 절차를 수립·이행하고 있는지 확인 • 재사용 및 폐기 시 관련 법령에 따라 중요 정보가 복구되지 않는 방법으로 처리하고 있는지 확인 • 외부업체를 통해 폐기할 경우 폐기 절차를 계약서에 명시하고 결과를 점검하는지 확인
6.15	**단말기 보안** 전자서명인증사업자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 단말기에 대한 안전조치를 적용하도록 계획하여야 한다. • 개인정보 유출 등 침해사고 방지를 위하여 업무용 및 관리용 단말기에 대해 안전조치를 취하고 있는지 확인 • 업무용 및 관리용 단말기의 분실·도난 등으로 개인정보가 유출되지 않도록 비밀번호 설정 등의 보호조치를 적용하고 있는지 확인
6.16	**취약점 점검 및 조치** 전자서명인증사업자는 인터넷 홈페이지 취약점으로 인한 개인정보의 유출, 변조, 훼손 등을 방지하기 위하여 웹 서버 및 응용프로그램에 대한 취약점 점검 및 대응조치를 적용하여야 한다. • 개발 및 운영 시스템에 대한 정기 취약점 진단 계획을 수립하고 이행하는지 확인 • 특히 인터넷 홈페이지를 통해 고유식별정보를 처리하는 경우 연 1 회 이상 취약점 점검을 수행하는지 확인 • 점검 대상에 중요 정보자산이 모두 포함되어 있는지 확인 • 발견 취약점에 대한 개선 계획을 수립하고, 조치를 수행하는지 확인
6.17	**시험 데이터 보안** 전자서명인증사업자는 개발환경을 통한 개인정보의 유출을 방지하기 위하여 시험(테스트) 데이터 생성·이용·파기 및 기술적 보호조치 등에 관한 대책을 적용하여야 한다. • 테스트 데이터는 실제 운용되는 개인정보가 아닌 가공된 정보로 변환하여 사용하고 있는지 확인 • 불가피하게 실 운영 데이터를 사용하는 경우, 운영 시스템과 동일한 수준의 보호조치를 적용하고, 테스트 후 해당 정보를 파기하는지 확인 • 개발에서 운영 환경으로 접속 및 이관은 통제된 절차에 따라 수행하는지 확인 • 소스프로그램에 대한 변경 및 유출에 대한 보호대책을 적용하는지 확인
6.18	**악성프로그램 방지** 전자서명인증사업자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 한다. • 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1 회 이상 업데이트를 실시하는 등 최신의 상태로 유지 • 발견된 악성프로그램 등에 대해 삭제 등 대응 조치
6.19	**보안 업데이트 및 패치** 전자서명인증사업자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.

연번	평가 항목 및 상세 평가 기준
7. 물리적 보호조치	
7.1	**영상정보처리기기 설치·운영** 전자서명인증사업자는 영상정보처리기기 운영 시 안전한 보호조치를 적용하여야 한다. • 영상정보처리기기를 설치·운영할 경우 법적으로 허용한 장소 및 목적인지 확인 • 영상정보처리기기 설치·운영 시 정보주체가 쉽게 인식할 수 있도록 필요한 조치를 하고 있는지 확인 • 영상정보처리기기 운영·관리 방침을 마련하여 시행하고 있는지 확인 • 영상정보의 보관 기간을 정하고 있으며, 보관 기간 만료 시 지체 없이 삭제하고 있는지 확인 • 외부 위탁하는 경우 개인정보 보호조치가 포함된 위탁 계약을 체결하고 있는지 확인
7.2	**보조 저장매체 관리** 전자서명인증사업자는 개인정보가 포함된 서류, 보조 저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고, 개인정보가 포함된 보조 저장매체의 반출입 통제를 위한 보호대책을 마련하여야 한다.
8. 공공기관 관련 사항	
8.1	**개인정보 파기** 전자서명인증사업자가 공공기관이면서 개인정보파일을 파기하는 경우, 관련 법령에 따라 안전하게 관리하여야 한다. • 개인정보파일 파기 관리대장을 작성하여 관리하고 있는지 확인 • 개인정보 보호위원회에 등록된 개인정보파일 목록 등도 함께 삭제될 수 있도록 하고 있는지 확인
8.2	**영상정보처리기기 운영** 공공기관이 공개된 장소에 고정형, 이동형 영상정보처리기기를 설치·운영 시, 법령에 명시된 절차 및 요구사항을 준수하여야 한다. • 공청회·설명회 개최 등 법령에 따른 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하는지 확인 • 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 경우, 문서에 법적 요구사항이 명시되고 안내판 등에 위탁받는 자의 명칭 및 연락처를 포함하는지 확인
8.3	**공공시스템운영기관의 안전조치 기준 적용** 전자서명인증사업자가 공공기관이면서 개인정보보호법에 의거하여 공공시스템운영기관, 공공시스템이용기관으로서 추가 안전성 확보 조치 의무 이행 대상인 경우 안전한 보호조치를 적용하여야 한다. • 각 공공시스템 별로 내부 관리계획을 수립하여 시행하는지 확인 • 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소 시 인사정보와 연계 여부 확인 • 접근 권한 부여, 변경 또는 말소 내역 등을 반기별 1 회 이상 점검 • 공공시스템 접속기록 등을 자동화된 방식으로 분석하여 불법적인 행위 · 시도 탐지 및 그 사유 소명 • 공공시스템운영기관의 경우 공공시스템이용기관에 소관 개인정보취급자의 접속기록 점검 기능 제공

연번	평가 항목 및 상세 평가 기준
9. 신기술 관련 개인정보보호	
9.1	**RFID** • 전자서명인증사업자는 RFID 태그에 기록된 개인정보를 수집하는 경우 정보주체(이용자)에게 통지하거나 알아보기 쉽게 표시하는지 확인 • 전자서명인증사업자는 RFID 태그의 물품정보 등과 개인정보를 연계하는 경우 그 사실을 이용자에게 통지하거나 알기 쉽게 표기되는지 확인 • 전자서명인증사업자는 RFID 태그의 물품정보 등과 개인정보를 연계하여 생성된 정보를 수집 목적 외로 이용하거나 제 3 자에게 제공할 경우 이용자의 동의를 얻고 있는지 확인 • 전자서명인증사업자는 RFID 태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우 설치 사실을 이용자가 인식하기 쉽게 표기하는지 확인 • 전자서명인증사업자는 구입 및 제공받은 물품에 RFID 태그가 내장 및 부착되어 있을 경우 부착 위치, 기록정보 및 기능에 대해 표시하는지 확인 • 전자서명인증사업자는 RFID 태그가 내장 및 부착되어 있는 경우 판매 혹은 제공하는 자로부터 태그 기능을 제거할 수 있는 방법 또는 수단을 제공하고 있는지 확인 • 전자서명인증사업자는 이용자의 신체에 RFID 를 지속적으로 착용하지 않는지 확인
9.2	**위치정보** 전자서명인증사업자는 개인위치정보 수집 시 정보주체(이용자) 또는 위치정보 수집장치 소유자에 대해 사전고지와 명시적 동의를 거치도록 하여야 한다. • 전자서명인증사업자는 개인위치정보를 정보주체(이용자)가 지정하는 제 3 자에게 제공하는 경우에는 개인위치정보 주체에게 제공받는 자, 제공일시 및 제공목적을 통보하는지 확인
9.3	**클라우드 보안** • 전자서명인증사업자는 클라우드 서비스에 대하여 격리 실패 현상을 방지하고 있는지 확인 • 전자서명인증사업자는 클라우드 서비스 제공자의 관리 인터페이스에 대하여 보안 관리하고 있는지 확인 • 전자서명인증사업자는 클라우드 이용자의 데이터 삭제 요청에 따라 적절한 데이터 삭제를 통해 개인정보 재사용을 방지하고 있는지 확인 • 전자서명인증사업자는 클라우드 특성을 고려한 모니터링을 수행하고 있는지 확인
9.4	**생체인식정보** • 전자서명인증사업자는 수집된 생체인식정보의 원본정보와 제공자를 알 수 있는 신상정보(성명, 연락처 등)를 별도로 분리하고 있는지 확인 • 전자서명인증사업자는 생체인식정보의 원본정보를 특징정보 생성 후 지체 없이 파기하여 복원할 수 없는지 확인 • 전자서명인증사업자는 생체인식정보의 불법 유출, 위·변조 등을 방지하기 위한 기술적·관리적 보호조치를 취하고 있는지 확인 • 전자서명인증사업자는 위·변조된 생체인식정보의 수집 및 입력에 대한 대책을 마련하고 있는지 확인 • 전자서명인증사업자는 생체인식정보의 수집 및 입력 시, 전송구간을 보호하는지 확인 • 전자서명인증사업자는 저장 및 송·수신 단계에서 생체인식정보에 대한 암호화 조치를 취하는지 확인 • 전자서명인증사업자는 생체인식정보의 저장 및 이용 단계에서 안전한 매체를 활용하여 처리할 수 있도록 하는지 확인
9.5	**블록체인** 전자서명인증사업자는 퍼블릭 블록체인의 익명성을 보장하기 위한 기술적 대책을 적용하여야 한다.

[별지] 전자서명인증업무 운영기준 평가 신청서

별지 1. 평가 신청서

■ 평가 신청자 관련 정보

회사명 사업자등록번호

대표이사	전화번호	전자우편 (e-mail)

■ 평가 대상 정보

평가 구분 ☐ 최초평가 ☐ 갱신평가 (최초평가 이후의 평가)

전자서명인증사업자 총괄책임	*기관명*	최상위 인증서 (필수)	*명칭(개수)*
전자서명인증사업자 정책업무	*기관명*	인증서 경로	*예) 최상위 – 중계 – 가입자 등*
전자서명인증사업자 관리업무	*기관명*	가입자 인증서 용도	*전자서명, 인증 등*
전자서명 물리적센터	*메인 및 백업 운영 환경 (외부 IDC 포함)*	전자서명 알고리즘	*RSA 등*
등록대행기관	*내·외부 등록대행기관명 작성*	유효성 검증	*CRL, OCSP 운영 여부 작성*
인증서 프로파일	*RFC 5280 등*	가입자 키 쌍 생성	*CA 또는 가입자 환경 여부 작성*
		가입자 키 쌍 보관	*CA 또는 가입자 환경 여부 작성*
		기타 서비스	*평가 범위 포함 여부에 따라 작성*
기타 필요사항			

■ 평가 신청 사실 확인

「전자서명법」 제8조제1항 및 제2항, 제9조제1항에 따라 위와 같이 전자서명인증사업자의 운영기준 준수 여부에 대한 평가를 신청합니다.

년 월 일

평가 신청자 (대표이사) (서명 또는 인)

딜로이트 안진회계법인 귀하

Deloitte.