AMR-VII-2020-②-204

금융보안원
전자서명인증평가 안내서

2020. 12.

금융미래를 열어가는 금융보안파트너

금융보안원
FINANCIAL SECURITY INSTITUTE

목 차

금융보안원 전자서명인증평가 안내서

1. 개요 ····· 2

2. 용어 정의 ····· 3

3. 평가 절차 ····· 4

4. 세부평가 기준 ····· 11

5. 기타 ····· 12

6. 문의처 ····· 13

[첨부] 전자서명인증평가 세부평가 기준 ····· 14

[별지] 전자서명인증평가 관련 서식 ····· 45

[별지 1] 전자서명인증 평가 신청서
[별지 2] 평가 표준 계약서
[별지 3] 평가 약관
[별지 4] 보완조치 내역서
[별지 5] 보완조치 완료 확인서
[별지 6] 보완조치 요약서
[별지 7] 평가절차 중단 확인서
[별지 8] 이의신청서

1 개요

❒ **(목적)** 금융보안원*이 수행하는 전자서명인증평가(이하 “평가”) 업무와 관련한 세부 방법 및 절차 등을 안내하기 위함

* 금융보안원은 과학기술정보통신부로부터 「전자서명법」 제10조에 따른 평가기관으로 지정(20.12.22.)

❒ **(법적 근거)** 「전자서명법」 제7조 ~ 제13조

❒ **(평가 대상)** 「전자서명법」 제8조에 따른 「전자서명인증업무 운영기준」(이하 “운영기준”) 준수 사실의 인정을 받기 위해, 운영기준 준수 여부에 대한 평가를 받고자 하는 전자서명인증사업자

〈 전자서명인증평가 제도 〉

❒ **(평가 범위)** 전자서명인증사업자의 전자서명인증 업무 및 등록대행기관이나 외부주문기관 등을 통한 전자서명인증 업무

※ 본 안내서는 금융보안원 홈페이지(www.fsec.or.kr) ‘자료마당→전자서명인증평가’ 메뉴에서 다운로드 가능

2 용어 정의

❒ **(인정기관)** 전자서명인증사업자의 운영기준 준수 사실의 인정에 관한 업무를 수행하는 기관으로 과학기술정보통신부 장관이 「전자서명법」 제9조에 따라 지정한 기관(한국인터넷진흥원)을 말한다.

❒ **(신청인)** 「전자서명법」 제8조에 따른 운영기준 준수 사실을 인정받기 위해 금융보안원에 평가를 신청하는 자를 말한다.

❒ **(평가원)** 「전자서명법 시행령」 별표 1에서 정한 평가기관 전문인력 요건을 갖춘 자로 평가에 참여하는 자를 말한다.

❒ **(세부평가기준)** 운영기준의 준수여부를 평가하기 위해 금융보안원이 정한 세부기준을 말한다.

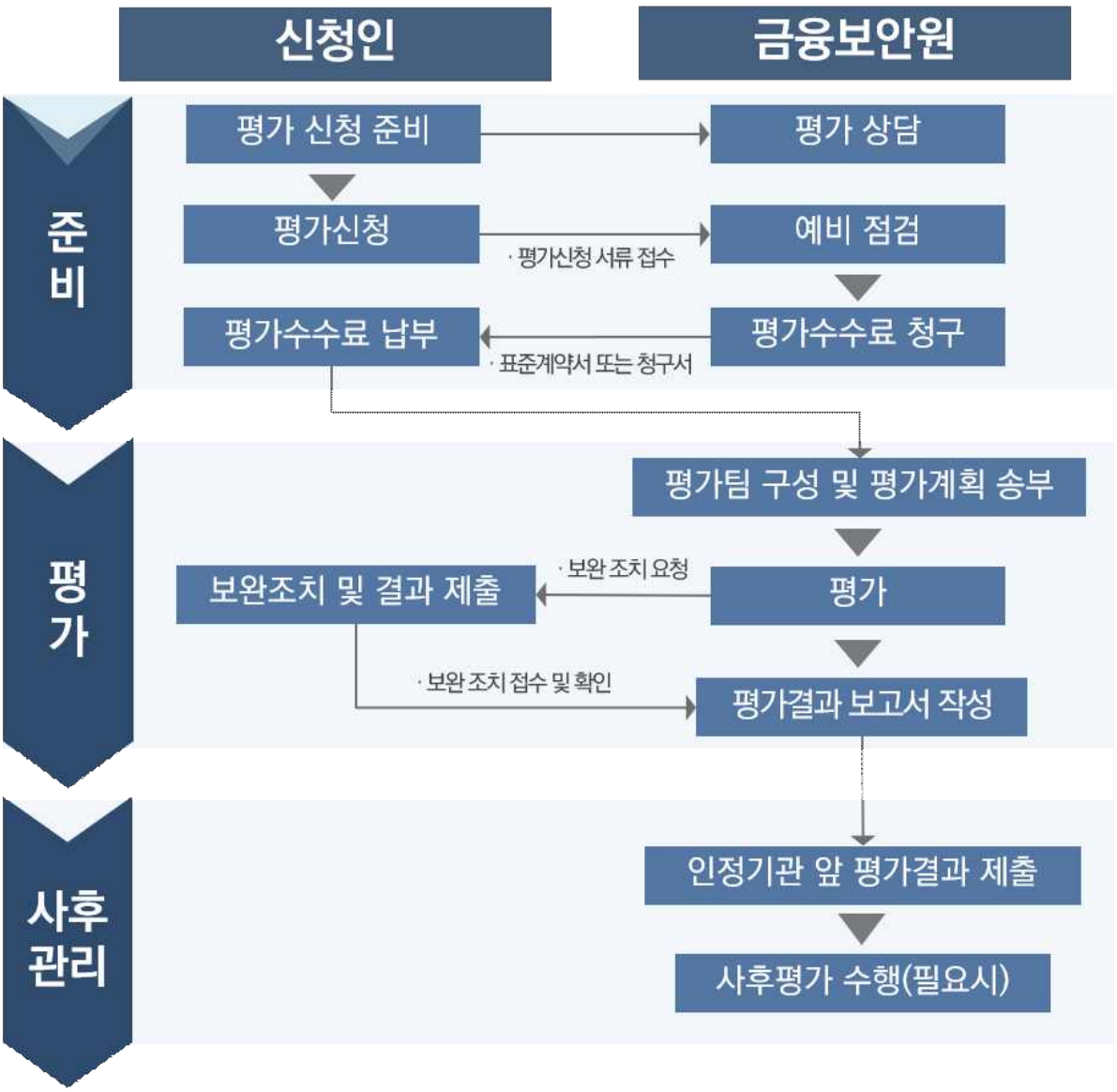
❒ **(결함)** 세부평가기준의 요구사항을 충족하지 못한 사항을 말한다.

❒ **(보완조치)** 신청인이 결함의 해결을 위해 추가적인 조치를 수행하는 것을 말한다.

3 평가 절차

❒ 평가절차는 준비단계, 평가단계, 사후관리단계로 구분되며, 세부 절차는 아래와 같음

〈 전자서명인증평가 절차도 〉



가. 준비단계

① **(평가 상담)** 평가를 희망하거나 평가에 관심 있는 전자서명인증사업자는 전화, 이메일, 방문 등의 방법으로 평가상담을 접수하고 금융보안원 전담직원과 평가 신청과 관련한 세부 사항을 상담

② **(평가 신청)** 신청인은 평가를 신청하고자 할 경우 「전자서명인증 평가 신청서〈별지 1〉」, 세부평가기준에 따른 운영기준명세서, 법인등기사항증명서 또는 고유번호증을 금융보안원에 제출

- 신청인은 평가신청 전 평가범위 및 일정 등을 금융보안원과 사전 협의
- 금융보안원은 신청인이 제출한 서류가 미비하거나 누락된 경우 보완을 요청할 수 있으며, 이 경우 신청인은 10일 이내에 서류를 보완하여 제출

※ 금융보안원은 평가신청 서류가 허위로 작성된 경우 평가신청을 취소할 수 있으며, 취소일자로부터 1년 동안 해당 신청인의 평가신청 접수 거부 가능

③ **(예비점검)** 금융보안원은 평가 신청 접수 후 신청인의 평가를 담당할 평가원을 배정하고, 신청인의 평가 준비사항을 확인*

* 평가관련 기본자료 구비 여부, 평가범위의 적절성, 운영기준명세서의 적절성, 평가장의 물리적 위치, 그 밖에 평가 준비를 위해 필요한 사항

※ 금융보안원은 예비점검 결과 평가준비가 미비한 경우 보완조치를 요청할 수 있으며, 6개월 이내에 평가준비가 완료되지 않은 경우 평가신청 취소 가능

④ **(평가수수료 산정)** 금융보안원은 아래의 세부 산정기준에 따라 평가수수료를 산정

※ 금융보안원은 필요한 경우 신청인과 협의를 통해 수수료 일부를 조정 가능

〈 평가 수수료 세부 산정 기준 〉

1. 평가 수수료 산정방식 : 직접인건비 + 제경비 + 기술료 + 직접경비

- 직접인건비 : 평가 소요기간 × 평가원 일 평균 임금*

* 「통계법」 제27조에거 한국소프트웨어산업협회에서 공표하는 S/W기술자 평균 임금 中 정보보호 컨설턴트 일평균 임금을 적용

- 제경비 : 직접인건비의 120% 적용
- 기술료 : (직접인건비+제경비)의 40% 적용
- 직접경비 : 교통비, 숙박비, 식대 등 평가업무에 소요되는 경비 산정

2. 평가 소요기간(일)

- 전자서명인증업무 평가범위 등을 고려하여 결정

⑤ **(평가수수료 청구)** 금융보안원은 평가수수료 청구를 위해 「평가수수료 청구서」및 「평가 표준계약서〈별지 2〉*」을 신청인에게 전달

* 표준계약서 내용은 금융보안원과 신청인 간 합의에 따라 일부 변경 가능

※ 신청인 요청시 별도 계약을 맺지 않고 평가수수료 청구서 및 평가 약관을 전달하는 방식으로 평가 수수료 청구 가능

⑥ **(평가수수료 납부)** 신청인은 평가수수료 청구를 받은 날로부터 15일 이내에 평가수수료를 지정된 계좌번호로 납부*

* 금융보안원은 신청인과 협의하여 평가수수료 납부일 조정 가능

- 평가수수료는 반납하지 않는 것이 원칙이나, 금융보안원이 귀책사유가 있어 이를 인정한 경우, 신청인과 협의하여 평가수수료 전부 또는 일부를 반납

나. 평가단계

① **(평가팀 구성 및 평가계획 송부)** 금융보안원은 신청인의 서비스 및 업무 특성, 평가 범위 등을 고려하여 평가팀을 구성하고, 평가계획*을 수립하여 신청인에게 송부

* 금융보안원은 신청인과 협의하여 평가계획의 일부를 조정 가능

〈 평가팀 구성시 고려사항 〉

1. 「전자서명법 시행령」별표1에서 정한 자격
2. 평가원의 전자서명인증 및 정보보호 기술, 법률 등 분야별 전문성
3. 평가원의 평가 수행경력
4. 평가원의 평가 품질, 자질, 태도
5. 신청인과의 이해관계(평가의 독립성 확보) : 신청인에 소속(근무)되어 있거나 과거 3년 동안 소속된 경력이 있는 자, 신청인의 보안컨설팅, 위탁업무 등 관련 업무를 과거 3년 동안 수행한 경력이 있는 자, 신청인과 동종업계 종사자 등 배제

② **(평가 시작)** 금융보안원은 필요시 평가 착수회의를 개최할 수 있으며, 평가의 공정성, 객관성, 신뢰성, 독립성 확보를 위해 평가 시작일에 「업무수행 윤리강령」 및 「보안서약서」를 작성하여 신청인에게 제출

③ **(평가 수행)** 평가원은 서면평가와 현장평가를 병행하여 평가 수행

〈 서면평가 및 현장평가 개요 〉

서면평가	신청인의 전자서명인증 운영현황이 세부평가기준에 적합한지 여부에 대해 운영기준명세서 및 증빙자료 등을 확인
현장평가	서면평가 결과의 실제 이행여부를 확인하기 위해 담당자 면담, 관련 시스템 등을 확인 * 금융보안원은 현장평가 시 취약점 분석·평가가 필요하다고 판단한 경우 신청인과 사전 협의하여 이를 수행 가능

- 금융보안원은 아래의 사항에 하나 이상 해당하는 경우 평가를 중단할 수 있으며, 이 경우 금융보안원과 신청인은 「평가절차 중단 확인서〈별지 7〉」를 작성

  * 신청인은 평가절차 중단 사유가 해소된 경우 평가 재신청 가능

〈 평가절차 중단 사유 〉

1. 신청인이 평가 관련 자료의 열람 또는 제공을 거부하는 등 고의로 평가를 지연 또는 방해하거나 신청인의 귀책사유로 인하여 평가를 계속 진행하기가 곤란하다고 평가기관이 판단하는 경우
2. 천재지변 및 경영환경 변화 등으로 인하여 평가진행이 불가능하다고 평가기관이 판단하는 경우
3. 신청인이 전자서명인증 서비스와 관련된 업무를 평가범위에서 누락한 사실을 평가기관이 발견한 경우
4. 신청인이 평가절차 진행 중에 평가의 신뢰성을 훼손할 만한 사회적 물의를 일으키거나 신청인에게서 중대한 정보보호 침해사고 및 개인정보 유출사고가 발생한 경우

④ **(보완조치 접수 및 확인)** 평가 수행 과정에서 세부평가기준에 적합하지 않은 사항이 발견되는 경우 금융보안원은 「결함 보고서」 및 「보완조치 요청서」를 작성하여 신청인에 결함에 대한 보완을 요청

- 신청인은 결함에 대한 보완조치 요청을 받은 날로부터 40일 이내에 보완조치를 수행하고 「보완조치 내역서〈별지 4〉」 및 「보완조치 완료 확인서〈별지 5〉」를 작성하여 금융보안원에 제출

- 금융보안원은 보완조치 결과가 미흡하거나 신청인이 보완조치 기간 연장을 요청*할 경우 최대 60일까지 보완조치 기간을 연장

  * 신청인은 보완조치 연장 요청문서와 함께 「보완조치 요약서〈별지 6〉」을 금융보안원에 제출

- 금융보안원은 필요 시 현장을 방문하여 보완조치 결과를 확인할 수 있으며, 신청인이 최대 100일 이내(연장기간 60일 포함)에 보완조치를 이행하지 못한 경우 부적합으로 판단하고 인정기관에 평가결과서를 제출

⑤ **(평가결과 보고서 작성)** 평가원은 서면평가 및 현장평가를 통하여 발견된 결함에 대해 신청인이 제출한 보완조치 내역을 확인하고 그 결과를 바탕으로 평가 결과 보고서를 작성

다. 사후관리 단계

① **(인정기관 앞 평가결과 제출)** 금융보안원은 평가기관은 평가결과 및 평가처리절차 준수에 대한 검토·승인 후 인정기관에 평가결과서(인정기관이 요구하는 자료 포함)를 제출

※ 금융보안원은 인정기관 요청 시 평가결과에 대한 세부사항 설명 가능

② **(사후평가 수행)** 금융보안원은 아래의 사항에 해당하는 경우 사후평가를 추가 수행할 수 있으며, 사후평가는 기존 평가절차를 준용

〈 사후평가 수행 요건 〉

1. 신청인의 전자서명인증 관련 서비스 운영에 중대한 변경이 발생한 경우
2. 신청인의 평가범위에서 정보보호 침해사고 또는 개인정보 유출사고가 발생한 경우
3. 그 밖에 인정기관장이 필요하다고 인정하는 경우

③ **(증명서 발급)** 인정기관은 평가결과 등을 토대로 운영기준 준수 사실의 인정을 하여 증명서를 발급하며, 인정기관의 인터넷 홈페이지에서 증명서의 발급 내용 확인 가능

4 세부 평가기준

❒ 운영기준 준수여부를 평가하기 위한 세부기준으로 전자서명 관련 준수필요 사항뿐만 아니라 신청인의 관리적·물리적·기술적 대책과 개인정보보호 관련 기준이 포함

* 세부평가기준은 평가상황 등에 따라 일부 조정 가능

❒ 금융보안원은 세부평가기준 내 항목이 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에 따른 인증기준 내 항목과 중복되는 경우, 해당 항목의 평가를 생략 가능

※ 세부평가기준은 금융보안원 홈페이지(www.fsec.or.kr) '자료마당→전자서명 인증 평가' 메뉴에서 다운로드 가능

☞ **[첨부]** 전자서명인증평가 세부평가 기준 참고

5 기타

❒ **(이의제기 절차)** 신청인은 다음에 해당하는 경우 「이의 신청서 〈별지 8〉」를 작성하여 금융보안원에 이의 신청 가능

〈 이의신청 요건 〉

1. 평가결과에 대하여 동의할 수 없는 경우
2. 정당한 사유 없이 평가 신청이 거부되었을 경우
3. 평가과정에서 평가원이 평가 관련 법령 및 윤리사항을 준수하지 않아 유·무형의 피해가 발생하였거나 예상되는 경우
4. 기타 평가기관의 업무처리에 불만족한 경우

- 이의신청 요건 중 1번에 해당되는 경우 신청인은 관련 사항을 통보받은 후 15일 이내에 이의신청서를 제출

- 신청인이 이의신청 요건 중 1번과 2번의 사유로 이의신청을 한 경우 금융보안원은 그 처리결과를 신청인에게 통지

❒ **(사고 대응)** 금융보안원은 화재발생에 따른 평가자료 유실, 평가자료의 도난 및 분실, 기타 비상상황이라 판단하는 경우 해당 사실을 신청인에게 통보

- 상기 사유로 인해 신청인에 피해발생 시 금융보안원은 협의를 통해 적절히 보상

6 문의처

❒ **금융보안원 보안연구부 전자서명인증평가TF**

- **(이메일)** eid@fsec.or.kr
- **(전화번호)** 02-3495-9777
- **(FAX)** 02-3495-9799

첨부 전자서명인증평가 세부평가 기준

항목		상세 내용
1. 전자서명 인증업무 독립성		
1.1	업무 독립성 유지	· 인정사업자는 전자서명인증업무 준칙에 인증서 이용범위를 명확히 기술해야 한다. · 인정사업자가 제공하는 "전자서명이용서비스"는 인증서 이용범위에 포함할 수 없다. ☞ [예시] A은행이 발급한 인증서의 이용범위에 "A은행의 자금조회, 이체 등 은행 업무"를 포함할 수 없다.
2. 적정기술의 이용		
2.1	가입자의 신원 식별정보 제공	· 전자서명인증서비스는 이용자가 가입자(서명자)의 신원을 식별할 수 있도록 가입자(서명자)의 식별정보를 제공해야 한다. · 가입자(서명자)의 식별정보로는 연계정보, VID, DN, 이메일주소 등이 사용될 수 있다. · 가입자(서명자)의 식별정보는 다양한 방법으로 제공할 수 있다. ☞ [예시] - 인증서에 가입자 DN 및 VID를 넣어 발급하는 기능 제공 - 이용자의 전자서명 생성 요청 시, 이용자에게 가입자의 전자서명과 연계정보를 전달하는 기능 제공
2.2	가입자의 전자서명 통제	· 전자서명은 가입자(서명자)의 전자서명생성정보를 통해서만 생성될 수 있어야 한다. · 전자서명인증서비스는 가입자(또는 가입자의 서명 권한을 위임받은 자) 이외의 다른 자가 가입자의 전자서명생성정보에 접근할 수 없도록 가입자 인증 및 접근통제 기능을 제공해야 한다. ☞ [예시] - 전자서명생성정보를 패스워드 기반으로 암호화하여 저장하며, 패스워드를 통한 가입자 인증이 성공한 경우에만 전자서명을 생성하도록 기능 제공 - 전자서명생성정보를 단말기의 Keystore에 저장하며, 생체인증을 통한 가입자 인증이 성공한 경우에만 전자서명을 생성하도록 기능 제공 · 전자서명인증서비스는 가입자의 전자서명생성정보 이용 시마다 가입자 인증을 수행해야 한다. · 전자서명인증서비스는 전자서명 생성 기능 수행 전 전자서명생성정보 및 인증서의 유효성을 검증해야 하며, 전자서명생성정보 및 인증서가 유효하지 않은 경우 전자서명을 생성하지 않아야 한다.

항목		상세 내용
2.3	전자서명 재사용 방지	· 전자서명인증서비스는 서로 다른 전자문서에 대해 서로 다른 전자서명을 생성해야 한다. ※ 동일한 전자문서에 대해 서로 다른 전자서명 생성을 요구하지 않는다.
2.4	전자서명 변경 여부 검증	· 전자서명은 전자문서(서명 대상 원문) 및 전자서명이 변경되었을 때 이를 확인할 수 있는 속성을 가져야 한다. · 전자서명인증서비스는 전자서명 검증 수행 시 전자문서 및 전자서명의 변경 여부를 확인해야 한다. · 전자서명인증서비스는 전자문서 또는 전자서명이 변경된 경우, 검증 실패 결과를 이용자 또는 가입자가 확인할 수 있도록 관련 기능을 제공해야 한다. ☞ [예시] - 전자서명 검증 앱에서 인증서 검증 실패 결과를 화면에 출력 - 전자서명 검증 API에서 검증 실패 결과를 리턴
2.5	안전한 암호 알고리즘 사용	· 전자서명인증서비스는 보안 강도 112비트 이상의 안전한 암호 알고리즘 및 키 길이를 사용해야 한다. ☞ [예시] - 전자서명에 암호 알고리즘 사용 예 : 전자서명 생성/검증용 키쌍 생성, 난수 생성, 인증서 서명, 전자서명생성정보 암호화 등) · 보안강도 112비트 이상의 안전한 암호알고리즘의 기준은 "KISA 암호 알고리즘 및 키 길이 이용 안내서"를 참고하여 적용한다. · "KISA 암호 알고리즘 및 키 길이 이용 안내서"에 명시되지 않은 암호알고리즘 및 키 길이를 사용하는 경우, 인정사업자는 해당 암호알고리즘 및 키 길이에 대한 보안강도 112비트 이상의 안전성을 보증해야 할 책임을 갖는다. ※ 이하, 세부평가기준 내 안전한 암호알고리즘에 대한 기준은 본 기준을 준용한다.
2.6	전자서명 관련 표준 준수	· 전자서명인증서비스는 전자서명에 표준 프로파일 및 프로토콜을 사용하는 경우 이를 준수해야 한다. ☞ [예시] - 인증서 프로파일에 ITU-T X.509 표준 사용 및 준수 - 전자서명생성정보 암호화에 PKCS#5 표준 사용 및 준수 - 인증서 폐지목록 프로파일에 RFC 5280 표준 사용 및 준수 - 인증서 관리 프로토콜에 RFC 4210 표준 사용 및 준수 - 실시간 인증서 상태 확인 프로토콜에 KCAC.TS.OCSP, RFC 6960 등 기술규격 사용 및 준수 · 전자서명인증서비스가 전자서명에 표준 프로토콜을 사용하지 않는 경우, 인정사업자는 해당 프로토콜에 대한 안전성을 보증해야 할 책임을 갖는다.

항목		상세 내용
3. 전자서명 인증업무 준칙		
3.1	준칙 작성 및 준수	· 인정사업자는 법 제15조에 따른 전자서명인증업무준칙을 작성하여 게시해야 한다. · 인정사업자는 게시한 전자서명인증업무준칙에 따라 전자서명인증업무를 수행해야 한다.
3.2	업무 관련 변동시 준칙 반영	· 인정사업자는 1.전자서명인증서비스의 종류, 2.전자서명인증서비스의 요금, 이용범위 및 유효기간 등 이용조건, 3.전자서명인증업무의 수행방법 및 절차, 4.그 밖에 전자서명인증업무의 수행에 필요한 사항에 변동이 생긴 경우, 전자서명인증업무 준칙 내 이를 반영하여야 한다.
3.3	준칙 변경시 기준	· 인정사업자는 인증업무준칙의 내용을 변경하는 경우, 사전에 규정된 절차에 따라 인증업무준칙을 개정해야 한다. · 인정사업자는 인증업무준칙을 개정한 경우, 관련 당사자가 개정된 인증업무준칙과 개정 이전의 인증업무준칙을 열람할 수 있도록 해야 한다. ☞ [예시] - 개정된 인증업무준칙과 이전 인증업무준칙을 모두 홈페이지에 게시 - 개정된 인증업무준칙과 변경 직전의 인증업무준칙을 홈페이지에 게시 - 개정된 인증업무준칙과 신구버전 비교표를 홈페이지에 게시 · "관련 당사자"는 인증업무준칙에 명시된 "전자서명인증체계 관련자"를 의미한다.
3.4	준칙 제·개정시 협의	· 인정사업자는 인정사업자가 제공하는 전자서명인증서비스와 관련된 인증기관이 있는 경우, 인증업무준칙의 "전자서명인증체계 관련자"에 이를 명시해야 하며, "준칙의 제·개정 절차"에 협의 절차를 기술해야 한다. ☞ [예시] - 인정사업자의 최상위인증기관이 존재하는 경우 인증업무준칙에 이를 명시하고, 준칙의 제·개정 절차에 협의 절차를 기술 · 인정사업자는 인정사업자가 제공하는 전자서명인증서비스와 관련된 인증기관이 있는 경우, 인증업무준칙의 제·개정 시 해당 인증기관과 이에 대해 협의해야 하며, 협의에 대한 증적을 작성 및 보관해야 한다. ☞ [예시] - 인정사업자의 인증업무준칙 제·개정 시 최상위인증기관과 이에 대해 협의한 후, 협의 결과와 인정사업자 및 최상위인증기관의 서명이 포함된 회의록을 작성 및 보관

항목		상세 내용
4. 가입자 등록		
4.1	가입자의 신원 확인	· 인정사업자는 또는 등록대행기관은 가입자의 신원확인을 위하여, 신원정보의 진위 및 신원정보 주체를 확인하여야 한다. · 신원확인을 위해 사용되는 신원정보는 인정사업자 또는 등록대행기관이 정할 수 있다. · 단, 본인확인기관의 경우 신원정보는 실지명의를 기준으로 하되, 사전에 가입자의 신원확인을 실지명의를 기준으로 확인한 경우에는 실지명의 이외의 방법으로 신원확인 수행을 할 수 있다. ☞ [예시] – 본인확인기관이 본인확인서비스 등의 제공을 위해 사전에 가입자의 주민등록증을 확인한 경우, 해당 본인확인기관이 전자서명인증서비스 제공을 위해 동일한 가입자의 신원을 확인시에는 주민등록증을 확인하지 않아도 됨 · 신원정보의 진위확인은 신원정보를 발급한 기관 혹은 신뢰할 수 있는 출처를 통하여야 한다. · 신원정보 주체확인은 주체의 얼굴을 대면/비대면으로 확인, 주체만이 알 수 있는 정보로 확인 등 합리적인 방안으로 수행하여야 한다.
4.2	비대면 신원확인	· 인정사업자는 비대면으로 신원을 확인하는 경우, 대면에 준하는 신원확인 수준을 갖출 수 있도록 신원확인을 위한 합당한 방안을 마련하여야 한다. ※ (참고) 금융회사 비대면 실명확인 시 신원확인 방법 – (이중확인 : 필수) ①신분증 사본 제출, ② 영상통화, ③접근매체(보안카드, OTP 등) 전달시 확인, ④기존계좌 활용, ⑤기타 이에 준하는 새로운방식(바이오인증 등) 중 "2가지" 의무 적용 – (다중확인 : 권고) ⑥타기관 확인결과 활용(휴대폰인증 등), ⑦다수의 개인정보 검증까지 포함하여 ①~⑦ 중 추가 확인
4.3	이용약관 공지	· 인정사업자 또는 등록대행기관은 가입자 등록 혹은 인증서 발급 전, 가입자에게 이용범위, 전자서명의 효력 등이 명시된 이용약관을 알릴 수 있도록 절차를 마련하여야 한다.
4.4	등록정보 위·변조 방지	· 인정사업자는 등록대행기관으로부터 정보통신망으로 가입자의 등록정보를 전송받는 경우, 전송 中 가입자의 등록정보가 위·변조 및 유·노출되지 않도록 방안을 마련하여야 한다. · 인정사업자는 등록대행기관으로부터 정보통신망으로 가입자의 등록정보를 전송받는 경우, 전송 後 가입자의 등록정보가 유출되지 않도록 안전한 암호 알고리즘이 적용된 암호화 조치 등의 방안을 마련하여야 한다. * [예시] – 다수의 등록대행기관이 가입자 등록정보를 등록하더라도, 타 등록대행기관이 등록한 가입자의 등록정보는 조회할 수 없도록 암호화 적용

항목		상세 내용
5. 인증서 발급·효력정지·효력회복 및 폐지 등		
5.1	전자서명생성정보의 유일성 확인	· 인정사업자는 가입자에게 인증서를 발급하는 경우, 가입자 전자서명생성정보가 유일함을 확인해야 한다. ※ 가입자 전자서명생성정보와 전자서명검증정보가 1:1로 매핑되는 경우, 전자서명검증정보의 유일함을 확인하는 방법으로 대체할 수 있다. * [예시] - 인증서 발급 전, 가입자 전자서명검증정보가 이전에 발급된 모든 전자서명검증정보와 중복되지 않음을 확인
5.2	인증서 이용 방안 마련	· 인정사업자는 가입자가 전자서명 생성에 필요한 방안을 마련하여야 한다. · 인정사업자는 이용자가 전자서명 검증에 필요한 방안을 마련하여야 한다. · 인정사업자는 기타 인증서 이용에 필수적으로 판단되는 기능이 있다면 이를 제공할 수 있는 방안을 마련하여야 한다. * [예시] - 소프트웨어(앱 등) 제공, API제공, 전자서명 생성 및 검증에 필요한 절차 안내 등
5.3	인증서 위·변조 방지	· 인정사업자는 인증서의 위변조 여부를 탐지할 수 있는 기술적 방안을 마련하여야 한다. * [예시] - 인증서에 대해 인정사업자의 전자서명 수행, 인증서의 블록체인 저장 등
5.4	인증서 폐지시 신원확인	· 가입자의 신청에 의거 효력정지, 회복, 폐지가 진행될 경우, 운영기준 제6조제1항에 따른 가입자의 신원확인을 수행하여야 한다.
5.5	인증서 폐지 확인 방안 마련	· 인정사업자는 이용자에게 인증서의 효력 정지, 회복, 폐지를 확인할 수 있는 방안을 마련하여야 한다. * [예시] - 이용자가 인증서 효력 정지, 회복, 폐지를 확인할 수 있도록 인증서 유효성 검증(CRL, OCSP) 제공 등
5.6	인증서 유효성 확인 서비스 제공	· 인정사업자가 인증서의 효력정지 및 폐지목록 생성이 필요한 경우, 이를 인증업무준칙 내 공고한 설비에 공고하거나, 인증서 효력정지 및 폐지목록 등을 확인할 수 있는 서비스를 제공할 수 있다.
6. 전자서명생성정보 생성		
6.1	안전한 환경 마련, 준칙 내 절차 준수	· 인정사업자는 자신 및 가입자의 전자서명생성정보를 생성하는 경우, '[별첨1] 전자서명인증업무 관리적 물리적 기술적 세부평가기준'을 만족하는 안전한 환경에서 해당 정보를 생성하여야 한다. · 인정사업자는 자신 및 가입자의 전자서명생성정보를 생성하는 경우, 인증업무 준칙 내 절차에 따라 전자서명생성정보를 생성하여야 한다.

항목		상세 내용
6.2	전자서명생성정보 생성시 기준	· 인정사업자는 전자서명생성정보 생성 시 관련 표준에 따라 전자서명생성정보를 생성하여야 한다. · 전자서명생성정보 생성 시 안전한 암호 알고리즘 또는 안전한 암호화 장치를 이용하여야 한다. * [예시] - 인정사업자는 KCMVP검증을 받은 HSM을 사용하여 전자서명생성정보 생성 · 인정사업자는 암호화 장치에 대한 안전성을 보증해야 할 책임을 갖는다.
6.3	다자인증 통제 적용	· 인정사업자는 자신의 전자서명생성정보를 생성하는 경우, 최소 3인 이상이 통제할 수 있도록 설정된 다자인증을 통해 생성하여야 한다. * [예시] - 인정사업자는 HSM의 m of N(m은 3명 이상) 기능을 사용하여 자신의 전자서명생성정보 생성
6.4	전자서명 생성정보 유출 방지	· 인정사업자는 가입자의 신청이 있는 경우가 아니면 가입자의 전자서명생성정보를 보관해서는 안된다. · 인정사업자는 가입자의 동의없이 가입자의 전자서명생성정보를 이용해서는 안된다. · 인정사업자가 가입자의 전자서명생성정보를 보관하는 경우, 해당 전자서명생성정보의 유출 방지를 위한 방안을 마련하여야 한다. * [예시] - 가입자 인증정보의 안전한 암호알고리즘을 이용한 암호화 조치 등
6.5	전자서명정보 생성시 공동 수행	· 인정사업자는 가입자의 전자서명생성정보를 생성하는 경우, 사업자가 전자서명생성 업무를 위해 지정한 최소 2인 이상이 공동으로 수행하여야 한다. * [예시] - 인정사업자는 가입자의 전자서명생성정보 생성 업무 담당자 2명을 지정하고, 감독관의 감독 下에 해당 업무 담당자 2인이 공동으로 전자서명생성정보 생성 · 인정사업자는 자동화된 설비를 이용하여 가입자의 전자서명생성정보를 생성하는 경우, 최소 2인 이상이 통제할 수 있도록 설정된 다자인증을 통해 생성하여야 한다. * [예시] - 인정사업자는 HSM의 m of N(m은 2명 이상) 기능을 사용하여 가입자의 전자서명생성정보 생성

항목		상세 내용
7. 전자서명생성정보 보호		
7.1	전자서명 생성정보 보호 방안	· 인정사업자는 자신 및 가입자의 전자서명생성정보를 생성하는 경우, 해당 전자서명생성정보를 안전하게 보호할 수 있는 방안을 마련하여야 한다. * [예시] – 전자서명생성정보 저장 시 안전한 암호알고리즘을 이용한 암호화 조치, KCMVP검증을 받은 HSM 내 전자서명생성정보 저장, 메모리 내 전자서명생성정보 저장 금지 등
7.2	전자서명생성정보 통제 및 안전조치	· 인정사업자가 가입자의 전자서명생성정보를 생성한 경우, 가입자의 통제 하에 전자서명생성정보가 이용될 수 있도록 방안을 마련하여야 한다. * [예시] – 가입자만이 전자서명생성정보를 이용할 수 있도록 접근통제 방안 마련 등
7.3	전자서명생성정보 백업	· 인정사업자는 자신 및 관리하고 있는 가입자의 전자서명생성정보의 백업을 위해, 내부적으로 백업주기, 백업절차, 백업방식 등이 포함된 백업정책을 수립하고 이를 준수하여야 한다. · 전자서명생성정보 백업시에는 원본정보가 분실·훼손, 도난·유출 시에도 백업본을 이용할 수 있도록 방안을 마련하여야 한다. * [예시] – 전자서명생성정보 백업본을 원본과 다른 별도의 서버에 보관 등
7.4	전자서명생성정보 백업본 안전 보관	· 인정사업자는 자신 및 관리하고 있는 가입자의 전자서명생성정보의 백업본이 안전하게 보관될 수 있도록 방안을 마련하여야 한다. * [예시] – 전자서명생성정보 백업본에 대한 접근통제 및 안전한 암호알고리즘을 이용한 암호화 조치 등
7.5	전자서명생성정보 소산	· 인정사업자는 백업된 전자서명생성정보 1부를 원격지 저장설비에 안전하게 소산하기 위한 내부정책을 수립하고 이를 준수하여야 한다. * [예시] – 내부 업무연속성 매뉴얼 내 전자서명인증업무 수행 시설과 10km이상의 원격지 건물에서 백업된 전자서명생성정보를 소산하도록 되어 있는 경우, 매뉴얼대로 준수 필요
7.6	전자서명생성정보 백업 및 복구 공동 수행	· 인정사업자는 전자서명생성정보를 백업하거나 복구하는 경우, 사업자가 전자서명 백업 혹은 복구 업무를 위해 지정한 최소 2인 이상이 공동으로 수행하여야 한다. * [예시] – 인정사업자는 가입자의 전자서명생성정보 백업·복구 업무 담당자 2명을 지정하고, 감독관의 감독 下에 해당 업무 담당자 2인이 공동으로 전자서명생성정보 백업·복구

항목		상세 내용
7.7	전자서명생성정보의 안전한 파기	· 인정사업자는 전자서명생성정보의 원본 및 백업본을 파기하는 경우, 전자서명인증업무 감독·통제에 대한 관리책임자 및 보안관리자의 감독 下에 수행하여야 한다. · 인정사업자는 전자서명생성정보의 원본 및 백업본을 파기 시 안전한 방법으로 파기할 수 있도록 방안을 마련하여야 한다. * [예시] - HSM장비 불능조치, HSM내 저장된 전자서명생성정보 덮어쓰기, 디스크 디가우징, 디스크 파기 등
7.8	전자서명생성정보 유출시 조치	· 인정사업자는 전자서명생성정보가 분실·훼손 또는 도난·유출된 경우, 해당 가입자 및 관련 당사자에게 해당 사실을 알 수 있도록 내부절차를 마련하고 이를 준수하여야 한다. · 인정사업자는 전자서명생성정보와 개인정보가 함께 도난·유출된 경우 개인정보보호법 등 관련 법령을 준수할 수 있도록 하여야 한다.
8. 시설 및 자료 보호 조치 등		
8.1	시설 및 자료 보호 조치 기준	· 인정사업자는 '[별첨1] 전자서명인증업무 관리적 물리적 기술적 세부평가기준'을 만족하여야 한다. · 인정사업자는 '[별첨2] 전자서명인증업무 개인정보 세부평가기준'을 만족하여야 한다.
8.2	관계 법령 준수	· 인정사업자는 관계 법령의 준수를 위해 준수해야하는 법령에 대해 자체적으로 점검하고, 점검 결과(예: 자체점검표)를 평가기관에 제출해야 한다. ※ 단, '[별첨1] 전자서명인증업무 관리적 물리적 기술적 세부평가기준' 및 '[별첨2] 전자서명인증업무 개인정보 세부평가기준'과 중복되는 법령에 대해서는 중복하여 점검하지 않을 수 있다.

9. 가입자 및 이용자 보호대책		
9.1	**업무 폐지시 절차 준수 및 손해배상 방안 마련**	· 인정사업자는 전자서명인증업무 휴지시, 휴지일 30일 전에 가입자에게 통보하고 인터넷 홈페이지에 게시할 수 있도록 내부절차를 마련하여야 한다. · 인정사업자는 전자서명인증업무 폐지 시, 폐지일 60일 전에 가입자에게 통보하고 인터넷 홈페이지에 게시할 수 있도록 내부절차를 마련하여야 한다. · 전자서명인증업무 휴지 및 폐지 시 통보 및 게시하는 내용에는 요금의 반환, 가입자의 개인정보 폐기 등 가입자 보호조치가 포함되어야 한다. · 인정사업자는 시행령 상의 요건을 충족하는 손해배상 보험을 가입하고, 가입자 등에게 미치는 손해발생 시 이를 해결하기 위한 절차 방안을 마련하여야 한다. ※시행령 상 보험의 요건 1. 보험금액 : 건당 1억 원 이상, 총 한도보상액 10억 원 이상의 금액 2. 보험기간 : 인정의 유효기간 내에 발생한 사고에 대한 보장이 가능할 것
9.2	**연계정보 처리 기준**	· 인정사업자가 연계정보(이하, CI)를 이용 및 수집하거나 이를 제3자에게 제공하는 경우 가입자로부터 이에 대한 별도의 동의를 얻어야 한다. · 인정사업자가 CI를 저장하거나 전송하는 경우 이를 안전한 암호알고리즘이 적용된 암호화 조치를 하여야 한다. · 인정사업자가 CI를 이용하는 경우 이는 전자서명서비스와는 분리된 단순 식별자 용도로만 사용해야 한다. 즉, 인증서 내 CI값을 포함할 수 없으며, 이를 가입자 단(모바일, PC, 클라우드 등)내에도 저장시킬 수 없다. · 인정사업자는 CI값의 송수신 시간, 송수신 대상 등에 대한 로그를 기록하여 저장하여 보관하여야 한다. · 인정사업자는 CI를 처리하는 시스템에 접근할 수 있는 관리자를 지정하고, 해당 관리자만 CI 처리 시스템에 접근가능하도록 접근통제를 수행하여야 한다. * [예시] - ID/패스워드, OTP 등 · 기타 인정사업자는 CI를 개인정보의 일환으로 보호할 수 있도록 '[별첨2] 전자서명인증업무 개인정보 세부평가기준'을 만족하여야 한다.

[별첨1] 전자서명인증업무 관리적·물리적·기술적 세부평가기준

(O : 해당, △ : 일부 다른 부분)

1. 정보보호 정책 및 조직

항목		세부항목		평가 기준	ISMS-P
1.1	정보보호 정책 수립 및 관리	1.1.1	정보보호 정책 수립	o 전자서명인증사업자는 정보보호 정책을 수립하고 이를 문서화 하여야 한다. - 정보보안 정책 문서가 물리적, 인적, 기술적 통제를 포함하여, 경영진의 승인을 얻어 전직원에게 전파되었는지 확인	○
		1.1.2	정보보호 정책 이행	o 전자서명인증사업자는 수립된 정보보호 정책이 준수될 수 있도록 책임있는 관리를 하여야한다. - 최고경영자는 정보보호 분야 전문성을 갖춘 인력을 확보하고, 정보 보호 정책의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하고 있는지 확인	○
		1.1.3	정보보안 정책 내용	o 전자서명인증사업자는 정보보호를 포함하는 구체적인 정보보안 정책을 마련하여야 한다. - 정보보안정책이 다음을 포함하고 있는지 확인 a) 정보 공유를 가능하도록 하는 메커니즘으로서의 정보보안의 정의, 목표 및 범위와 중요성 b) 정보보안의 원칙 및 목표를 지원하기 위한 경영진의 의지; c) 조직에게 특별히 중요시 되는 보안정책, 원칙, 표준, 준수 요구사항에 대한 설명; d) 보안 침해 보고를 포함하는 정보보안 관리에서의 책임에 대한 정의; e) 정책을 지원하는 문서에 대한 목록	○
		1.1.4	정보보안 정책의 검토	o 전자서명인증사업자는 정보보안 정책을 주기적으로 검토하는 절차를 마련하여 최신성을 유지하여야 한다. - 정보보안 정책 문서의 최신성을 유지하기 위한 주기적인 검토 프로세스 절차가 마련되어 있는지 확인 - 정보보안 관련 정책과 시행문서는 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경 변화 등에 따라 필요한 경우 제•개정하고 그 이력을 관리하는지 확인	○
		1.1.5	제3자 접근보안 정책	o 전자서명인증사업자는 제 3자 접근 보안정책을 수립하고 이를 이행하여야 한다. - 전자서명인증사업자 시설 및 시스템에 대한 제 3자의 물리적 및 논리적 접근 통제가 마련되어 있는지 확인 - 전자서명인증사업자 시설 및 시스템에 대한 제 3자의 접근은 필수적인 보안 요구 사항을 담고 있는 정식 계약을 통해 이루어지고 있는지 확인	△

		1.1.6	아웃소싱 보안 정책	o 전자서명인증사업자는 전자서명 관련 운영 및 일부 시스템을 아웃소싱 할 경우 보안요구사항을 명확히 하여야 한다. - 전자서명인증사업자가 운영 및 전자서명 시스템의 대한 모두 또는 일부 아웃소싱 할 경우, 양측이 합의한 계약서에 전자서명인증사업자의 보안 요구사항을 명시하는지 확인	△
1.2	정보보호 조직 구성 및 운영	1.2.1	정보보호 책임자 지정	o 최고경영자는 임원급의 고위 경영진을 정보보호 총괄 관리 책임자로 지정하여야 한다. - 최고경영자가 정보보호 활동을 위하여 예산·인력 등 자원을 할당할 수 있는 임원급으로 정보보호 책임자를 지정하였는지 확인 - 최고경영자가 정보보호 총괄 관리 책임자를 통하여 정보보호 관련 보고 및 의사결정 체계를 수립하여 운영하는지 확인	○
		1.2.2	정보보호 조직 구성	o 전자서명인증사업자는 정보보호 활동을 체계적으로 이행할 수 있는 실무 조직 또는 정보보안 위원회를 구성하여야 한다. - 정보보호 활동을 체계적으로 이행할 수 있는 실무 조직이 존재 하는지 확인 - 전자서명관련 전문가 그룹이나 관련 기관과 적절한 연계를 유지하며 활동하는지 확인	△
		1.2.3	정보보호 조직의 운영	o 전자서명인증사업자는 구성된 정보보호 조직에 대해서 구성원들의 역할과 책임을 명확하게 하고 구성원간 상호 의사소통할 수 있도록 운영해야 함 - 각각의 정보자산을 보호하기 위한 책임 및 특정 보안 절차를 수행할 책임이 명확히 되어 있는지 확인 - 구성원들의 정보보호 활동을 평가할 수 있는 체계와 구성원간 상호 의사소통할 수 있는 체계를 수립하여 운영하고 있는지 확인	△

2. 자산 관리

항목		세부항목		평가 기준	ISMS-P
2.1	정보자산 식별 및 분류	2.1.1	정보자산 식별 및 분류	o 전자서명인증사업자는 전자서명 인증 업무 법위 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 모든 정보 자산에 대해서 관리 책임자를 지정하고 있는지 확인	O
2.2	자산 관리 및 통제	2.2.1	자산 관리	o 전자서명인증사업자는 자산목록을 만들어 관리하여야 한다. - 전자서명인증사업자가 정보 및 정보 처리 시설과 연관된 자산목록을 만들어 관리하고 있는지 확인	○

		2.2.2	자산 통제	o 전자서명인증사업자는 분류 된 자산 및 정보자료를 위험으로 부터 적절한 수준의 보호를 받을 수 있도록 통제 절차를 마련하여야 한다. - 전자서명인증사업자가 분류된 자산 및 정보자료에 대한 위협 분석을 수행 하였는지 확인 - 전자서명인증사업자가 사업의 요구사항 및 사업에 미치는 영향에 따라 조직 내에서 사용되고 있는 자산의 적절한 사용을 위한 규칙을 문서화 하였는지 확인	△

3. 인적보안

항목		세부항목		평가 기준	ISMS-P
3.1	직무 적합성 검토	3.1.1	직무적합성 검토	o 전자인증사업자는 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	△
3.2	역할 구분	3.2.1	신뢰된 역할 담당자	o 정보보안 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) 인증시스템의 설치, 구성 및 유지보수 c) 인증시스템 및 시스템 백업 및 복구 장비의 운영 d) 인증시스템 아카이브 및 감사 로그의 검토 및 유지 관리 e) 암호화 키 생명 주기 관리 기능 f) 인증 시스템 개발 - 정보보안 정책 문서에 신뢰된 역할(trusted roles)과 비신뢰된 역할(non-trusted roles)에 요구되는 신원확인에 대해 상세히 기술되어 있는지 확인. 최소한, 정규직 인력 채용 시에는 신원확인을 수행하는지 확인. - 신뢰된 역할 담당자가 승인을 거친 후에 시스템/시설에 대한 접근 또는 작업을 수행하고 있는지 확인 - 신뢰된 역할 수행 계약직 인력은 최소한 정규직 직원들과 똑같은 신원확인 절차 및 인력 관리 절차를 적용받고 있는지 확인	X
		3.2.2	키 관리 및 인증서 업무자	o 키 관리 및 인증서 관리 등과 관련된 직원들에 대해서는 주기적인 신뢰성 검토 및 검증이 이루어져야 한다. - 키 관리 및 인증서 관리 등 주요 직무 수행 직원들에 대한 주기적인 신뢰성 검토 및 검증이 이루어지는지 확인	X
		3.2.3	징계절차 마련	o 보안정책 및 절차를 위반한 직원에 대한 공식적인 징계 절차가 수립되어야 한다. - 보안서약서 위반이나, 전자서명업무와 관련하여 승인 받지 않은 사용 및 승인 받지 않은 시스템의 사용에 대한 처벌 규정이 마련되어 있는지 확인	O

		3.2.4	퇴사자 관리	o 전자서명인증사업자는 퇴사자에 대해서는 모든 접근통제 권한을 종료시켜야 한다. - 퇴사자에 대해서 물리적, 논리적 접근을 종료하고 있는지 확인	O
3.3	보안 서약서 작성	3.3.1	보안서약서 작성	o 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	O
3.4	보안 교육	3.4.1	보안교육 절차	o 전자서명인증사업자는 전자인증업무를 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	O
3.5	외부자 보안	3.5.1	외부자 보안 대책	o 전자서명인증사업자가 업무의 일부로 외부서비스를 이용하거나 외부자에게 위탁하는 경우 이에 대한 보안대책을 명확히 해야 한다 - 전자서명인증사업자가 업무의 일부로 외부서비스를 이용하거나 외부자에게 업무를 위탁하는 경우, 정부 요구 사항을 계약서에 명시하고, 명시된 요구사항을 준수하고 있는 주기적으로 점검 또는 관리 감독하고 있는지 확인	O

4. 물리적 보안

항목		세부항목		평가 기준	ISMS-P
4.1	물리적 보호	4.1.1	중요설비 보호	o 전자서명인증사업자는 인증서 발급 등 중요설비는 별도의 통제 구역에 타 시스템과 물리적으로 분리되는 등 안전한 시설에 위치되고 사고 및 재난 등을 방지할 수 있는 방안을 마련하여야한다. - 전자서명인증 운영실이 위치한 빌딩 또는 장소는 허가된 인원만 출입 가능하도록 물리적 접근 통제를 위한 보안 요원 접수나 다른 수단이 구비되어 있는지 확인 - 인증서 제조 시설에 대한 비인가 출입과 환경오염을 방지하기 위해 물리적 장벽이 설치되어 있는지 확인 - 통제구역에 위치한 설비는 온도·습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영절차를 수립·운영하고 있는지 확인	△
		4.1.2	장비 관리	o 전자서명인증사업자는 주요장비에 대해 물리적 보안 조치를 마련하고 이행하여한 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 위험으로 보터 보호 되고 있는지 확인 - 개인용 컴퓨터나 워크스테이션은 미사용 시에 로그오프 되거나, 패스워드 등을 통하여 적절히 통제 되고 있는지 확인	
4.2	출입통제	4.2.1	주요시설 출입통제	o 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 다중신원검증 절차를 통하여 인가된 인원에게만 접근이 가능하도록 통제 되는지 여부를 확인	△
		4.2.2	출입통제 관리	o 전자서명인증관련 운영시설을 출입하는 모든 인원에 대한 기록을 관리하여야 한다. - 모든 인원들은 육안으로 식별 가능한 신분 등을 패용하고, 만일 패용하지 않는 인원을 발견 시에는 직원들이 신원 확인을 요구할 수 있는지 여부를 확인 - 전자서명인증 관련 운영시설을 출입하는 모든 인원에 대해 기록을 남기고 관리하는지 확인 - 제3의 서비스 지원인력은 필요시에만 전자인증관련 운영시설의 보안 구역 출입이 허용되어야하며, 이 경우에도 직원과 동행하여 이루어지는지 확인 - 전자서명인증 관련 시설을 방문자에 대해서 출입날짜와 시간을 기록하는 등 감독하는 절차가 마련되어 있는지의 여부를 확인 - 전자서명인증 관련 시설에 대한 접근 권한이 주기적으로 검토되고 갱신되고 있는지 확인	△
4.3	침입 감지 및 감시	4.3.1	침입 감지 및 감시	o 전자서명인증사업자는 운영시설이 있는 모든 건물에 대한 물리적인 침입 대비 방안을 마련하여야 하고, 이러한 시설의 출입이나 내부활동을 모니터링하여야 한다. - 전자서명인증 관련 운영건물의 모든 외부 출입문에 침입자 감지 시스템이 설치되어 운영되고 있는지 확인 - 전자서명인증 관련 시설 내에 직원이 없을 때에 물리적으로 잠금되고 경보장치가 작동되고 있는지 확인 - 전자서명인증 관련 시설의 출입이나 내부의 활동이 CCTV 등 카메라를 통해 모니터링 되는지 확인	△
4.4	반출입 통제	4.4.1	반출입 통제	o 전자서명인증사업자는 장비, 문서, 휴대용 저장매체 등의 반출입 통제 정책을 수립하고 반출입시 이력을 작성하고 보관하여 한다. - 전자서명인증 관련 시설 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제절차를 수립·이행하고 주기적으로 검토하는지 확인	O

5. 운영 보안

항목		세부항목		평가 기준	ISMS-P
5.1	운영 절차 수립 및 준수	5.1.1	운영절차 수립 및 준수	o 전자서명인증사업자는 전자서명인증시스템 및 보안시스템 운영을 위한 절차를 수립하고 이행하여야 한다. - 전자서명인증시스템과 보안시스템 운영절차가 각 기능 영역 별로 문서화되어 관리되고 있는지 확인 - 전자서명인증시스템과 보안시스템 관련 장비, 소프트웨어, 운영 절차상의 모든 변경 사항을 통제하기 위하여, 관리 책임자 및 절차가 존재하는지 확인 - 시스템문서는 비인가 접근으로부터 보호되고 있는지 확인	△
		5.1.2	저장매체 관리	o 전자서명인증사업자는 운영에 필요한 저장매체 및 이동식 저장매체를 관리하는 절차를 마련하고 이를 이행하여야 한다. - 이동식저장매체 관리 절차에 다음을 포함하고 있는지 확인 a) 더 이상 필요 없을 시, 재사용 가능한 매체에 담겨 있던 내용물은 지우거나, 매체 자체를 파기 한다; b) 조직의 모든 이동식저장매체는 승인을 득하여야 하며, 해당 매체들에 대한 감사 증적을 위해 기록이 유지관리 되어야 한다; c) 모든 매체는 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 겹쳐 쓰기를 하는지 확인 - 비인가 공개 또는 남용으로부터 정보를 보호하기 위해, 정보의 저장 및 취급절차가 존재하며 이행하는지 확인	△
5.2	시스템 및 서비스 관리	5.2.1	시스템 및 서비스 관리	o 전자서명인증사업자는 운영시스템을 개발 및 테스트 시스템과 분리하고 안전한 보안설정, 성능·용량·상태 모니터링, 안전한 인수 및 유지 보수 절차를 수립하고 이행하여야 한다. - 개발 및 테스트 시설이 운영설비로부터 분리되어 있는지 확인 - 외부로 부터 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	△
5.3	악성코드 예방·탐지·대응	5.3.1	악성코드 예방·탐지·대응	o 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	△

5.4	침해사고 대응	5.4.1	침해사고 대응 정책	o 전자서명인증사업자는 침해사고에 대응하기 위한 정책을 수립하고 이행하여야 한다. - 비상연락 체계를 포함하여 침해사고 발생 시 보고절차, 대응 및 복구 절차, 신고 절차 등을 포함한 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 반영하여야 한다. - 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 문서화하고, 정량화하고, 모니터될 수 있도록 하는 공식적인 관리 절차가 존재하는지 확인	△

6. 접근통제

항목		세부항목		평가 기준	ISMS-P
6.1	접근통제 정책	6.1.1	접근통제 정책수립	o 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	△
6.2	접근권한 관리	6.2.1	접근권한 관리	o 전자서명인증사업자는 전자서명인증시스템 및 보안시스템, 중요정보에 접근하기 위한 공식적인 사용자 계정 및 권한의 관리절차를 마련하고 업데이트하여야 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 업데이트 되는지 확인 - 사용자로 하여금 정의된 정책과 절차에 따라 패스워드의 사용과 선택을 하도록 하고 있는지 확인 - 신뢰역할을 수행하는 사용자의 접근 권한이 정기적인 주기로 검토되고 업데이트 되는지 확인 - 관리 및 슈퍼사용자 계정은 멀티팩터 인증 통제를 권고하고 있는지 확인	△

		6.2.2	**네트워크 접근통제**	o 전자서명인증사업자는 전자서명인증시스템 및 보안시스템의 네트워크 보안에 대한 절차를 마련하고 이행하여야 한다. - 직원은 사용이 허가된 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 - 인정사업자는 로컬 네트워크 구성요소를 물리적으로 안전한 환경에서 관리하고, 구성 요구사항에 맞추어서 주기적으로 점검하는지 확인	△
		6.2.3	**하이퍼 바이저, 운영시스템, 데이터 베이스 및 네트워크 장치 접근통제**	o 전자서명인증사업자는 하이퍼바이저, 운영시스템, 데이터베이스 및 네트워크 장치에 대한 별도의 운영규정을 두어 관리하여야 한다. - 하이퍼바이저, 운영 시스템, 데이터베이스 및 네트워크 장치는 인정기관의 시스템 설정 표준을 준수하여 설정되어 있으며, 주기적으로 검토 및 업데이트되는지 확인 - 하이퍼바이저, 운영 시스템, 데이터베이스 및 네트워크 장치 패치 및 업데이트는 위험 평가에 기반하여 필요하다고 여겨질 때 적시적으로 적용되어야 하며 공식적인 변경 관리 절차를 따라 진행하는지 확인	△
6.3	**비인가자 시스템 접근 금지**	6.3.1	**비인가자 시스템 접근 금지**	o 시스템에 대한 접속 권한은 허가된 네트워크 서비스에서 사용자 인증절차에 의해 통제되어야 하며, 비인가자가 전자서명인증업무와 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 사용함으로서, 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 제한되고 엄격하게 통제되고 있는지 확인 - 비활성화 터미널은 사용에 앞서 재인증을 요구하고 있는지 확인 - 민감 데이터는 비인가 사용자에게 공개되지 않도록 보호되고 있는지 확인	O

7. 개발 보안

항목		세부항목		평가 기준	ISMS-P
7.1	시스템 변경 관리	7.1.1	시스템 개선 및 변경	o 전자서명인증사업자는 시스템 개선이나 신규시스템 도입 시 통제 절차를 수립하여야 한다. - 신규시스템 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	O
		7.1.2	소프트웨어 관리	o 전자서명인증사업자는 정보시스템의 오류 위험을 최소화하기 위해 소프트웨어의 변경에 대해서 엄격하게 통제하여야 한다. - 소프트웨어 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	O
7.2	프로그램 소스코드 보호	7.2.1	프로그램 소스코드 보호	o 전자인증사업자는 프로그램 소스 라이브러리에 대한 적절한 접근 통제와 형상 관리를 하여야 한다. - 프로그램 소스 라이브러리에 대한 접근 통제 장치와 소스코드에 대한 형상 관리를 하고 있는지 확인	O

8. 업무 연속성 관리

항목		세부항목		평가 기준	ISMS-P
8.1	업무 연속성 계획	8.1.1	업무연속성 계획	o 전자서명인증사업자는 장애 및 재해로 부터 업무연속성 확보를 위해 위험평가에 기초한 연속성 계획을 마련해야 한다. - 전자서명인식사업자의 업무연속성 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 복구지점 목표(RPO) i) 긴급 사태 대책에 대한 정기적인 테스트	O

				- 사업연속성계획에 전자서명인증 시설에 대해서, 재난 발생 후 그리고 메인 시설 또는 원격지의 안전한 환경을 복원하기 전까지의 시설보안 절차를 포함 하는지 확인 - 업무연속성 계획에 컴퓨팅 리소스, 소프트웨어 및 (또는) 데이터가 손상되거나 손상이 의심되는 경우 사용되는 복구 절차를 다루고 있는지 확인 - 사업연속성 계획에 인증 정책이나 인증업무 준칙에 공개된 허용 가능한 시스템 정지 시간, 복구 시간, 장애 간 평균 시간이 정의되어 있는지 확인	
		8.1.2	**업무연속성 계획 관리**	o 업무연속성 계획을 정기적으로 테스트하여 변화사항을 반영하여 업데이트 하여야 한다. - 업무연속성 계획의 유효성 유지를 위하여 주기적으로 테스트하여 유효성을 유지하도록 업데이트 되는지 확인 - 업무연속성 계획은 주기적으로 검토되고 업데이트 되고 있는지 확인	O
8.2	**백업 및 원격지 시설**	8.2.1	**백업 및 원격지**	o 전자서명인증사업자는 장애 및 재해 발생 시 핵심 업무가 복구될 수 있도록 대체 백업 시설을 마련해야 한다. - 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 유지되는 지 확인 - 필수 사업정보의 백업 사본이 정기적으로 발생하여야 하며, 이러한 백업 사본에 대한 보안요구사항은 백업된 정보와 동일한지 여부를 확인	O

9. 감사 로그

항목		세부항목		평가 기준	ISMS-P
9.1	**감사로그 생성**	9.1.1	**감사로그 생성**	o 전자서명인증사업자는 전자서명생성정보·인증서·암호화 장치 등과 관련된 감사 로그를 생성하고 위험 평가 및 관계 법령에서 요구하는 특정한 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) 입력을 개체의 신원 - 전자서명인증사업자가 키의 수명관리와 관련된 다음 사항들을 기록하는지 확인 a) 인정기관(CA) key의 생성 b) 수동 암호화 key의 설치와 그 결과 (운영자의 신원과 함께)	X

				c) CA key의 백업 d) CA key의 보관 e) CA key의 복구 f) CA key 의 escrow activities (해당 사항이 있는 경우) g) CA key의 사용 h) CA key 의 기록(archival) i) key 와 관련된 자료의 서비스로 부터의 철회 j) CA key 의 파기 k) CA key 전송 l) CA key 마이그레이션 m) Key 관리 활동의 승인 개체의 신원 n) key와 관련된 자료(예를 들어, 이동저장매체에 보관된 key 또는 중요한 요소)를 다루는 개체의 신원 o) Key 보관 및 Key를 저장하고 있는 장치 또는 매체의 보관; p) 개인 키 손상 - 인정 기관이 다음 암호화 장치의 생명 주기 관리의 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 Key 관리 서비스를 제공하는 경우, 가입자 Key 관리의 생명 주기와 관련된 주요 이벤트를 기록하는지 확인 a) key의 생성 b) key의 배부 (해당사항이 있는 경우) c) key의 백업 (해당사항이 있는 경우) d) key의 위탁 (해당사항이 있는 경우) E) key의 보관 f) key의 복구 (해당사항이 있는 경우) g) key의 기록 (해당사항이 있는 경우) h) key의 파기 i) key의 관리활동을 승인하는 주체의 신원 j) key의 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 CA 또는 제출하는 RA 의 이름 (해당사항이 있는 경우); g) 가입자의 가입 동의서에 대한 동의; h) (개인정보보호법에서 요구되는 경우) 개인정보 기록 및 소유, 지정된 제3자에 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 c) 개체의 소속 변경 d) 인증서 생성 e) 인정기관의 공개 키 배부 f) 인증서 폐지 요청 g) 인증서 폐지 h) 인증 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 (감사 로그 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/인증 프로세스 또는 절차를 우회하는 결정 i) 전자서명인증시스템 또는 관련 구성요소에 대한 접근 - 감사 기록에는 개인 키를 어떠한 형태로도 포함하고 있지 않는지(예: 일반 텍스트 또는 암호화 형태) 확인 - 전자서명인증사업자 컴퓨터시스템의 시간은 정확한 기록 유지를 위해 전자서명인증준칙에서 정의하고 있는 타임 소스와 동기화되어 있는지 확인	

9.2	**감사로그 관리**	9.2.1	**감사로그 관리**	o 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 - 감사 로그를 서명하는 키는 해당 용도로만 사용되고 다른 용도로는 사용되지 않는지 확인 - 전자서명인증정책이나 전자서명인증 준칙에 준거하여 감사로그는 주기적으로 백업 및 보관되는지 확인 - 감사 로그의 보유기간을 관련 법령과 더불어 위험평가를 통해 지정되고 있는지 확인 - 감사 로그의 백업을 안전한 별도의 장소에 보관하여야 하며, 위험 평가 및 법령에서 요구되는 특정 기간 동안 보관하고 있는지 확인 - 승인받은 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 전자서명인증준칙에 준거하여 주기적으로 검토되고 있는지 확인	△

[별첨2] 전자서명인증업무 개인정보보호 세부평가기준

세부항목	평가 기준	ISMS-P
1. 최고책임자의 지정	1.1 전자서명인증사업자의 최고경영자는 개인정보보호업무를 총괄하는 개인정보보호책임자를 입원급 이상으로 지정하여야 한다.	O
2. 조직 구성	2.1 전자서명인증사업자의 최고경영자는 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있도록 개인정보보호 담당자 및 관련 업무 담당자들로 구성된 협의체 (혹은 위원회)를 구성하여 운영하여야 한다.	O
3. 정책 수립	3.1 전자서명인증사업자는 개인정보보호 정책을 실행하기 위한 내부관리 계획을 수립 및 시행하여야 한다.	
4. 주요 직무자 지정 및 관리	4.1 전자서명인증사업자는 개인정보 및 중요정보의 취급이나 주요 시스템 접근 등 주요 직무의 기준과 관리방안을 수립하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다.	O
	4.2 전자서명인증사업자는 개인정보취급자를 대상으로 역할 및 책임 부여, 개인정보보호 교육, 개인정보보호 서약서 작성 등의 관리 및 감독을 하여야 한다.	
5. 직무 분리	5.1 전자서명인증사업자는 개인정보취급자의 권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다.	O
6. 개인정보 식별	6.1 전자서명인증사업자는 업무특성에 따라 개인정보 분류기준을 수립하여 관리체계 범위 내 모든 개인정보를 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.	O
7. 현황 및 흐름분석	7.1 전자서명인증사업자는 개인정보보호 관리체계 내 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.	O
8. 위험 평가	8.1 전자서명인증사업자는 대내외 환경분석을 통해 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.	O
9. 보호대책 선정	9.1 전자서명인증사업자는 위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 개인정보보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립한다. 경영진은 이행계획을 검토 및 승인하여야 한다.	O

10. 보호대책 구현	10.1 전자서명인증사업자는 이행계획에 따라 개인정보보호대책을 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.	O
11. 관리체계 점검	11.1 전자서명인증사업자는 개인정보보호 관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다.	O
	11.2 전자서명인증사업자의 개인정보보호책임자는 연 1회 이상으로 내부 관리 계획의 이행 실태를 점검·관리하여야 한다.	
12. 관리체계 개선	12.1 전자서명인증사업자는 법적 요구사항 준수검토 및 관리체계 점검을 통해 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하며, 경영진은 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.	O
13. 개인정보 수집 제한	13.1 전자서명인증사업자는 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.	O
14. 개인정보 수집 동의	14.1 전자서명인증사업자는 정보주체(이용자)의 동의를 받거나 관계 법령에 따라 개인정보를 적법하게 수집하여야 하며, 만 14세 미만 아동의 개인정보를 수집하려는 경우에는 법정대리인의 동의를 받아야 한다.	O
15. 주민등록번호 처리 제한	15.1 전자서명인증사업자는 법적 근거가 있는 경우를 제외하고는 주민등록번호를 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.	O
16. 민감정보 및 고유식별정보의 처리 제한	16.1 전자서명인증사업자는 민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체(이용자)의 별도 동의를 받아야 한다.	O
17. 간접수집 보호조치	17.1 전자서명인증사업자는 정보주체 이외로부터 개인정보를 수집하거나 제공받는 경우에는 업무에 필요한 최소한의 개인정보만 수집·이용하여야 하고 법령에 근거하거나 정보주체의 요구가 있으면 개인정보의 수집 출처, 처리목적, 처리정지의 요구 권리를 알려야한다.	O
18. 개인정보 현황관리	18.1 전자서명인증사업자는 수집·보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 하여야 한다.	O

	18.2 전자서명인증사업자는 개인정보 파일을 신규로 보유하거나 변경하는 경우, 개인정보파일 대장을 작성하거나 변경해야 한다.	
19. 개인정보 품질보장	19.1 전자서명인증사업자는 개인정보 처리 목적에 따라 개인정보의 정확성·완전성·최신성을 보장하기 위한 관리절차를 마련하고, 이를 정보주체에게 알려야 한다.	O
20. 개인정보 표시제한 및 이용시 보호조치	20.1 전자서명인증사업자는 개인정보 처리 시 목적에 따라 출력 항목 최소화, 개인정보 표시제한, 출력물 보호조치 등을 수행하여야 한다. 또한, 불필요해진 개인정보는 삭제 또는 식별할 수 없도록 조치하여야 한다.	O
	20.2 전자서명인증사업자는 개인정보 처리화면을 통한 개인정보 유·노출 등을 방지하기 위한 보호대책을 적용하여야 한다.	
21. 출력·복사 시 보호조치	21.1 전자서명인증사업자는 개인정보를 종이로 출력할 경우 출력·복사물에 대하여 출력자·출력일시 표시 등의 보호대책을 적용해야한다.	
22. 홍보 및 마케팅 목적 활용 시 조치	22.1 전자서명인증사업자는 마케팅을 목적으로 개인정보를 수집·이용하는 경우, 그 목적을 정보주체가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다.	O
23. 이용자 단말기 접근 보호	23.1 전자서명인증사업자는 정보주체의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 접근이 필요한 경우 이를 명확하게 인지할 수 있도록 알리고 정보주체의 동의를 받아야 한다.	O
24. 개인정보 목적 외 이용 및 제공	24.1 전자서명인증사업자는 개인정보 수집 시 정보주체에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.	O
25. 개인정보 제3자 제공	25.1 전자서명인증사업자는 개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.	O
26. 업무 위탁에 따른 정보주체 고지	26.1 전자서명인증사업자는 개인정보 처리업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자 등 관련사항을 정보주체에게 알려야 한다.	O
27. 영업의 양수 등에 따른 개인정보의 이전	27.1 전자서명인증사업자는 영업의 양도·합병 등으로 개인정보를 이전하거나 이전받는 경우 정보주체 통지 등 적절한 보호조치를 수립·이행하여야 한다.	O

28. 개인정보의 국외이전	28.1 전자서명인증사업자는 개인정보를 국외로 이전하는 경우 국외 이전에 대한 동의, 관련 사항에 대한 공개 등 적절한 보호조치를 수립·이행하여야 한다.	O
29. 처리목적 달성 후 보유 시 조치	29.1 전자서명인증사업자는 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.	O
30. 휴면 이용자 관리	30.1 전자서명인증사업자는 일정기간 동안 서비스를 이용하지 않는 이용자의 개인정보를 보호하기 위하여 휴면 처리 사실을 통지하고, 개인정보의 파기 또는 분리보관 등 적절한 보호조치를 이행하여야 한다.	O
31. 개인정보처리방침 공개	31.1 전자서명인증사업자는 개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 개인정보처리방침을 수립하고, 이를 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화하여야 한다.	O
32. 개인정보의 파기	32.1 전자서명인증사업자는 개인정보의 보유기간 및 파기 관련 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.	O
33. 개인정보의 파기	33.1 전자서명인증사업자는 개인정보파일을 파기하는 경우 파기 결과 등을 '개인정보파일 파기 관리대장'에 기록 및 관리하여야 한다.	
34. 정보주체 권리보호	34.1 전자서명인증업무의 수행과 관련하여 가입자 또는 이용자에게 손해배상 책임이 있는 경우 해당 손해를 배상할 수 있도록 법령에 따른 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.	
35. 정보주체 권리보호	35.1 전자서명인증사업자는 정보주체가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체의 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.	O
36. 이용내역 통지	36.1 전자서명인증사업자는 개인정보의 이용내역 등 정보주체에게 통지하여야 할 사항을 파악하여 그 내용을 주기적으로 통지하여야 한다.	O

37. 개인정보취급자 계정 관리	37.1 전자서명인증사업자는 개인정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 개인정보취급자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 개인정보취급자에게 개인정보 관련 책임이 있음을 규정화하고 인식시켜야 한다.	O
38. 개인정보취급자 계정 관리	38.1 전자서명인증사업자는 개인정보취급자별로 책임추적성이 확보될 수 있도록 개별 계정을 부여해야 한다.	
39. 사용자 식별	39.1 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.	O
40. 사용자 인증	40.1 전자서명인증사업자는 개인정보취급자 및 관리자를 대상으로 강화된 인증방식이 적용하여야 한다.	
	40.2 전자서명인증사업자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상 사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용해야 한다.	
41. 비밀번호 관리	41.1 전자서명인증사업자는 법적 요구사항, 외부 위협요인 등을 고려하여 개인정보취급자와 고객, 회원 등 정보주체가 사용하는 비밀번호 관리 절차를 수립·이행하여야 한다.	O
	41.2 전자서명인증사업자는 개인정보취급자와 정보주체가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성규칙을 적용하여야 한다.	
	41.3 전자서명인증사업자는 정보주체가 비밀번호 변경 등 중요 정보 접근 시 비밀번호 재확인 등 추가적인 인증이 적용하여야 한다.	
42. 계정 및 권한 관리	42.1 전자서명인증사업자는 개인정보 관리 등 특수목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제해야 한다.	O
	42.2 전자서명인증사업자는 개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위하여 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하여야 한다.	
	42.3 전자서명인증사업자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무 처리를 하지 않는 경우에는 자동으로 시스템 접속을 차단하여야 한다.	

	42.4 전자서명인증사업자는 개인정보처리시스템에 대한 비정상적인 접근을 방지하기 위하여 장기 미접속시 계정 잠금, 동시 접속 제한, 관리자 로그인 알림 등 보호 대책이 적용하여야 한다.	
	42.5 전자서명인증사업자는 개인정보처리시스템의 접근권한을 부여, 변경 또는 말소한 내역을 최소 5년간 보관하여야 한다.	
	42.6 전자서명인증사업자는 개인정보처리시스템의 접근권한을 부여, 변경 또는 말소한 내역을 기록하여야 한다.	
	42.7 전자서명인증사업자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고를 방지할 수 있도록 접근통제 시스템을 설치 및 운영하도록 계획하여야 한다.	
43. 인터넷 접속 통제	43.1 전자서명인증사업자는 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 등을 통해 개인정보가 노출되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자 PC, 모바일 기기, 관리용 단말기 등에 보호 조치하여야 한다.	
44. 암호정책 적용	44.1 전자서명인증사업자는 개인정보보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보의 저장·송·수신 시 암호화를 적용하여야 한다.	O
	44.2 전자서명인증사업자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립 및 시행하여야 한다.	
	44.3 전자서명인증사업자는 고유식별정보, 바이오정보, 비밀번호 등 중요 개인정보를 정보통신망을 통해 송·수신하거나 보조저장매체 등을 통해 전달하는 경우 암호화하여야 한다.	
45. 로그 및 접속기록 관리	45.1 전자서명인증사업자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록을 월 1회 이상 정기적으로 점검하여야 한다.	
	45.2 전자서명인증사업자는 개인정보처리시스템에 접속한 기록을 최소 1년 이상 보관하고 위변조 및 도난, 분실되지 않도록 별도 저장장치 등에 백업 보관하도록 계획하여야 한다.	
46. 정보자산의 재사용 및 폐기	46.1 전자서명인증사업자는 정보자산의 재사용과 폐기 과정에서 개인정보 및 중요정보가 복구 및 재생되지 않도록 안전한 재사용 및 폐기 절차를 수립·이행하여야 한다.	O

47. 단말기 보안	47.1 전자서명인증사업자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대한 안전 조치를 적용하도록 계획하여야 한다.	
	47.2 전자서명인증사업자는 개인정보를 처리하는 업무용 모바일기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일기기에 비밀번호 설정 등의 보호조치를 계획하여야 한다.	
48. 취약점 점검 및 조치	48.1 전자서명인증사업자는 인터넷 홈페이지 취약점으로 인한 개인정보의 유출, 변조, 훼손 등을 방지하기 위하여 웹서버 및 응용프로그램에 대한 취약점 점검 및 대응조치를 적용하여야 한다.	
49. 시험 데이터 보안	49.1 전자서명인증사업자는 개발환경을 통한 개인정보의 유출을 방지하기 위하여 시험(테스트)데이터 생성·이용·파기 및 기술적 보호조치 등에 관한 대책을 적용하여야 한다.	
50. 백업 및 복구관리	50.1 전자서명인증사업자는 재해, 재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.	
51. 보호구역 지정	51.1 전자서명인증사업자는 개인정보처리시스템 및 개인정보를 보관하고 있는 물리적 장소를 보호구역으로 지정하고 물리·환경적인 위협에 대응할 수 있도록 영상정보처리기기, 출입통제 장치, 화재경보기 등 보호설비를 설치·운영해야 한다.	
52. 보조저장매체 관리	52.1 전자서명인증사업자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고, 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보호대책을 마련해야 한다.	
53. 영상정보처리기기 설치·운영	53.1 전자서명인증사업자는 영상정보처리기기를 공개된 장소에 설치·운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항(안내판 설치 등)을 준수하고, 적절한 보호대책을 수립·이행하여야 한다.	O
	53.2 전자서명인증사업자는 영상정보처리기기 설치시 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.	
	53.3 전자서명인증사업자는 영상정보처리기기 사용 시 임의조작 및 음성녹음을 사용할 수 없도록 하여야 한다.	
	53.4 전자서명인증사업자는 영상정보처리기기 운영 시 영상정보처리기기에 대한 운영 및 관리방침을 수립하여야 한다.	
	53.5 전자서명인증사업자는 영상정보처리기기 관리 위탁 시 개인정보보호에 필요한 전문장비 및 기술을 갖춘 기관을 선정하도록 하여야 한다.	

54. RFID	54.1 전자서명인증사업자는 RFID 태그에 기록된 개인정보를 수집하는 경우 이용자에게 통지하거나 알아보기 쉽게 표시하여야 한다.	
	54.2 전자서명인증사업자는 RFID 태그의 물품정보 등과 개인정보를 연계하는 경우 그 사실을 이용자에게 통지하거나 알기 쉽게 표기되도록 하여야 한다.	
	54.3 전자서명인증사업자는 RFID 태그의 물품정보 등과 개인정보를 연계하여 생성된 정보를 수집 목적 외로 이용하거나 제3자에게 제공할 경우 이용자의 동의를 얻어야 한다.	
	54.4 전자서명인증사업자는 RFID태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우 설치 사실을 이용자가 인식하기 쉽게 표기하여야 한다.	
	54.5 전자서명인증사업자는 구입 및 제공받은 물품에 RFID태그가 내장 및 부착 되어 있을 경우 부착 위치, 기록정보 및 기능에 대해 표시하여야 한다.	
	54.6 전자서명인증사업자는 RFID 태그가 내장 및 부착되어 있는 경우 판매 혹은 제공하는 자로부터 태그 기능을 제거할 수 있는 방법 또는 수단을 제공하여야 한다.	
	54.7 전자서명인증사업자는 이용자의 신체에 RFID를 지속적으로 착용하지 않아야 한다.	
55. 위치정보	55.1 전자서명인증사업자는 개인위치정보 수집 시 정보주체 또는 위치정보 수집장치 소유자에 대해 사전고지와 명시적 동의를 거치도록 하여야 한다.	
	55.2 전자서명인증사업자는 개인위치정보를 정보주체가 지정하는 제3자에게 제공하는 경우에는 개인위치 정보주체에게 제공받는 자, 제공일시 및 제공목적을 통보하여야 한다.	
56. 클라우드 보안	56.1 전자서명인증사업자는 클라우드 서비스에 대하여 격리 실패 현상을 방지하여야 한다.	
	56.2 전자서명인증사업자는 클라우드 서비스 제공자의 관리 인터페이스에 대하여 보안 관리하여야 한다.	
	56.3 전자서명인증사업자는 클라우드 이용자의 데이터 삭제 요청에 따라 적절한 데이터 삭제를 통해 개인정보 재사용을 방지하여야 한다.	
	56.4 전자서명인증사업자는 클라우드 특성을 고려한 모니터링을 수행하여야 한다.	

57. 바이오 정보	57.1 전자서명인증사업자는 수집된 바이오 원본정보와 제공자를 알 수 있는 신상정보(성명, 연락처 등)를 57.2 별도로 분리하여야 한다.	
	57.3 전자서명인증사업자는 원본정보의 경우 특징정보 생성 후 지체 없이 파기하여 복원할 수 없도록 하여야 한다.	
	57.4 전자서명인증사업자는 바이오정보의 불법 유출·위변조 등을 방지하기 위한 기술적·관리적 보호조치를 취하여야 한다.	
	57.5 전자서명인증사업자는 위·변조된 바이오정보 수집 및 입력에 대한 대책을 마련하여야 한다.	
	57.6 전자서명인증사업자는 바이오정보 수집 및 입력 시, 전송구간을 보호하여야 한다.	
	57.7 전자서명인증사업자는 저장 및 송·수신 단계에서 바이오정보에 대한 암호화 조치를 취하여야 한다.	
	57.8 전자서명인증사업자는 저장 및 이용 단계에서 기기 내 안전한 매체를 활용하여 처리할 수 있도록 하여야 한다.	
58. 블록체인	58.1 전자서명인증사업자는 퍼블릭 블록체인의 익명성을 보장하기 위한 기술적 대책을 적용하여야 한다.	

[별지]

전자서명인증평가 관련 서식

<별지 1> 전자서명인증 평가 신청서

전자서명인증 평가 신청서

※ 색상이 어두운 난은 신청인이 작성하지 아니하며, [ ]에는 해당되는 곳에 √표를 합니다.

접수번호	접수일시	처리기간

신청인	업체명	사업자등록번호
	대표자	전화번호
	주소	
	전자우편(e-mail)	

평가 구분	[ ] 최초 평가 [ ] 인정 후 평가 (인정 시 평가기관명 :)
전자서명인증 서비스명	
평가범위	

「전자서명법」 제8조에 따라 위와 같이 전자서명인증 평가를 신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

금융보안원장 귀하

첨부서류	1.「전자서명인증업무 운영기준」준수 사실을 증빙하기 위한 세부평가기준에 따른 운영기준 명세서 2. 법인등기사항증명서 또는 고유번호증

처 리 절 차

신청서 작성	→	접수 및 예비점검	→	수수료 납부	→	평가 실시	→	보완조치	→	평가결과 보고서 제공
신청인		평가기관		신청인		평가기관		신청인		평가기관

<별지 2> 평가 표준 계약서

<table>
<tr><td colspan="6">평가 계약서</td></tr>
<tr><td colspan="2">계약번호</td><td colspan="4"></td></tr>
<tr><td colspan="2">계약명</td><td colspan="4">전자서명인증사업자(사업자명 :)에 대한 평가</td></tr>
<tr><td colspan="2">계약금액</td><td colspan="4">원</td></tr>
<tr><td colspan="6">본 계약은"신청인"과 "평가기관"이 상호 기명날인한 날로부터 그 효력이 발생하며, 이를 증명하기 위하여 계약서 2부를 작성하여 각각 1부씩 보관하기로 한다.

20 년 월 일</td></tr>
<tr><td rowspan="6">계
약
자</td><td rowspan="3">"신청인"</td><td>주소</td><td colspan="3"></td></tr>
<tr><td>상호</td><td></td><td>전화
번호</td><td></td></tr>
<tr><td>대표자</td><td colspan="3">(인)</td></tr>
<tr><td rowspan="3">"평가기관"</td><td>주소</td><td colspan="3"></td></tr>
<tr><td>기관명</td><td>사단법인 금융보안원</td><td>전화
번호</td><td></td></tr>
<tr><td>대표자</td><td colspan="3">(인)</td></tr>
<tr><td colspan="2">첨부</td><td colspan="4">- 평가 표준계약서 1부</td></tr>
<tr><td colspan="2">특이사항</td><td colspan="4"></td></tr>
</table>

평가 표준계약서

사단법인 금융보안원(이하 “평가기관”이라 한다)과 ○○○○○(이하 “신청인”이라 한다)는 다음과 같이 전자서명인증 평가 계약을 체결한다.

제1조(목적) 본 계약은 “평가기관”이 “신청인”의 전자서명인증 평가업무를 수행함에 있어 필요한 사항을 정함을 목적으로 한다.

제2조(평가범위) “평가기관”이 수행하여야 할 평가의 범위는 “신청인”의 ‘_____’로 하며 평가범위의 내용은 “신청인”이 제출한 전자서명인증평가 신청서를 기반으로 한다.

제3조(평가일정 및 평가원) ① “평가기관”이 수행하여야 할 평가업무는 서면평가와 현장평가로 구분되며 평가일정은 “신청인”과 “평가기관”간 협의를 통해 결정한다.

② “평가기관”은 제1항과 제2항의 사항을 포함하는 평가계획서를 작성하여 “신청인”에게 제출한다.

③ 평가일정 및 평가원은 “신청인”과 “평가기관”간 협의를 통해 변경할 수 있다.

제4조(신의성실의무) ① “평가기관”은 공정하고 객관적인 방법으로 평가를 성실하게 수행하여야 한다.

② “신청인”은 “평가기관”의 평가가 원만히 이루어질 수 있도록 본 계약의 내용을 성실히 이행하여야 한다.

제5조(평가준비 및 자료제공) ① “신청인”은 “평가기관”이 평가를 원활히 이행할 수 있도록 필요한 장소 제공 및 기타 제반사항 준비에 협조하여야 한다.

② “평가기관”은 평가에 필요한 자료의 열람이나 제공을 요구할 수 있으며, “신청인”은 특별한 사유가 없는 경우에는 이에 협조하여야 한다.

제6조(평가 수수료 산정) 평가 수수료는 “평가기관”의 「전자서명인증 평가업무 수행지침」에 따라 산정한다.

제7조(평가 수수료 납부) “신청인”은 제6조에 따라 산정한 평가 수수료를 “평가기관”이 청구한 날로부터 15일 이내에 납부하여야 한다. 다만, “평가기관”은 “신청인”과 협의하여 납부일을 조정할 수 있다.

제8조(평가 수수료의 반환) 평가 수수료는 반환하지 않음을 원칙으로 한다. 다만, “평가기관”의 귀책사유로 인하여 평가를 수행하지 못한 경우에는 “평가기관”은 평가 수수료의 전액 또는 일부를 “신청인”에게 반환한다.

제9조(평가 중단) “평가기관”은 다음 각 호의 어느 하나에 해당하는 경우에는 평가를 중단할 수 있다.

1. “신청인”이 평가 관련 자료의 열람 또는 제공을 거부하는 등 고의로 평가를 지연 또는 방해하거나 “신청인”의 귀책사유로 인하여 평가를 계속 진행하기가 곤란하다고 평가기관이 판단하는 경우
2. 천재지변 및 경영환경 변화 등으로 인하여 평가 진행이 불가능하다고 평가기관이 판단하는 경우
3. “신청인”이 전자서명인증 서비스와 관련된 업무를 평가범위에서 누락한 사실을 평가기관이 발견한 경우
4. “신청인”이 평가절차 진행 중에 평가의 신뢰성을 훼손할 만한 사회적 물의를 일으키거나 신청인에게 중대한 정보보호 침해사고 및 개인정보 유출사고가 발생한 경우

제10조(해지) ① “신청인”은 다음 각 호의 어느 하나에 해당하는 경우에는 서면 통지로써 본 계약을 해지할 수 있다.

1. “평가기관”이 정당한 이유 없이 약정한 착수기일을 경과하고도 평가를 수행하지 아니한 경우
2. “평가기관”이 지정 취소, 파산, 해산 등으로 인하여 평가를 진행할 수 없는

경우

② “평가기관”은 다음 각 호의 어느 하나에 해당하는 경우에는 서면 통지로써 본 계약을 해지할 수 있다.

1. “신청인“이 파산, 해산 등으로 인하여 평가를 진행할 수 없는 경우
2. “신청인”이 평가 신청 또는 과정에서 제출된 서류가 허위로 인정되는 경우
3. “신청인”이 평가 수수료를 납부하지 않은 경우

제11조(비밀의 엄수) “평가기관”은 평가를 통하여 얻은 “신청인”의 정보 또는 기밀사항을 외부에 누설하지 아니한다. 다만, 관련 법령에 의한 정보의 공개 요청 시에는 예외로 한다.

제12조(책임) “신청인”이 전자서명인증 업무의 운영에 대한 유지·관리를 소홀히 하여 발생한 문제에 대해서는 “평가기관”은 어떠한 책임도 지지 아니한다.

제13조(관련 법령 및 지침 준수 등) “평가기관”은 평가관련 법령 및 내부 지침을 준수하여야 한다.

제14조(해석 및 분쟁의 해결) 본 계약에서 정하지 아니한 사항 또는 본 계약의 해석에 대하여 이견이 있거나, 분쟁이 발생한 경우에는 원만한 해결을 위하여 상호 노력하며,「국가를 당사자로 하는 계약에 관한 법률」등 기타 계약에 관한 법령을 따른다.

<별지 3> 평가 약관

평가 약관

제1조(목적) 본 약관은 사단법인 금융보안원(이하 "평가기관"이라 한다)이 _____(이하 "신청인"이라 한다)의 전자서명인증 평가업무를 수행함에 있어 필요한 사항을 정함을 목적으로 한다.

제2조(약관 등의 명시·설명 및 개정) ① "평가기관"은 이 약관의 내용과 상호 및 대표자 성명, 소재지, 연락처(전화, 팩스, 이메일 등) 등을 이용자가 쉽게 알 수 있도록 "평가기관" 홈페이지에 게시한다.

② "평가기관"은 「약관의 규제에 관한 법률」 등 관련 법령을 위배하지 않는 범위에서 이 약관을 개정할 수 있다.

③ "평가기관"은 약관을 개정하는 경우 적용일자 및 개정사유를 명시하여 현행 약관과 함께 "평가기관" 홈페이지에 그 적용 일자 7일 전부터 적용 일자 전일까지 공지한다. 다만, "신청인"에게 불리하게 약관 내용을 변경하는 경우에는 최소한 30일 이상의 사전 유예기간을 두고 공지한다. 이 경우 "평가기관"은 "평가기관" 홈페이지에 개정 전 내용과 개정 후 내용을 명확하게 비교하여 알기 쉽도록 표시한다.

④ 이 약관에서 정하지 아니한 사항과 이 약관의 해석에 관하여는 「약관의 규제 등에 관한 법률」 등 관련 법령 또는 일반적인 거래관행에 따른다.

제3조(평가범위) "평가기관"이 수행하여야 할 평가의 범위는 "신청인"의 '_____'로 하며 평가범위의 내용은 "신청인"이 제출한 전자서명인증평가 신청서를 기반으로 한다.

제4조(평가일정 및 평가원) ① "평가기관"이 수행하여야 할 평가업무는 서면평가와 현장평가로 구분되며 평가일정은 "신청인"과 "평가기관"간 협의를 통해 결정한다.

② "평가기관"은 제1항과 제2항의 사항을 포함하는 평가계획서를 작성하여

“신청인”에게 제출한다.

③ 평가일정 및 평가원은 “신청인”과 “평가기관”간 협의를 통해 변경할 수 있다.

제5조(신의성실의무) ① “평가기관”은 공정하고 객관적인 방법으로 평가를 성실하게 수행하여야 한다.

② “신청인”은 “평가기관”의 평가가 원만히 이루어질 수 있도록 본 계약의 내용을 성실히 이행하여야 한다.

제6조(평가준비 및 자료제공) ① “신청인”은 “평가기관”이 평가를 원활히 이행할 수 있도록 필요한 장소 제공 및 기타 제반사항 준비에 협조하여야 한다.

② “평가기관”은 평가에 필요한 자료의 열람이나 제공을 요구할 수 있으며, “신청인”은 특별한 사유가 없는 경우에는 이에 협조하여야 한다.

제7조(평가 수수료 산정) 평가 수수료는 “평가기관”의 「전자서명인증 평가업무 수행지침」에 따라 산정한다.

제8조(평가 수수료 납부) “신청인”은 제6조에 따라 산정한 평가 수수료를 “평가기관”이 청구한 날로부터 15일 이내에 납부하여야 한다. 다만, “평가기관”은 “신청인”과 협의하여 납부일을 조정할 수 있다.

제9조(평가 수수료의 반환) 평가 수수료는 반환하지 않음을 원칙으로 한다. 다만, “평가기관”의 귀책사유로 인하여 평가를 수행하지 못한 경우에는 “평가기관”은 평가 수수료의 전액 또는 일부를 “신청인”에게 반환한다.

제10조(평가 중단) “평가기관”은 다음 각 호의 어느 하나에 해당하는 경우에는 평가를 중단할 수 있다.

1. “신청인”이 평가 관련 자료의 열람 또는 제공을 거부하는 등 고의로 평가를 지연 또는 방해하거나 “신청인”의 귀책사유로 인하여 평가를 계속 진행하기가 곤란하다고 평가기관이 판단하는 경우

2. 천재지변 및 경영환경 변화 등으로 인하여 평가 진행이 불가능하다고 평가기관이 판단하는 경우
3. “신청인”이 전자서명인증 서비스와 관련된 업무를 평가범위에서 누락한 사실을 평가기관이 발견한 경우
4. “신청인”이 평가절차 진행 중에 평가의 신뢰성을 훼손할 만한 사회적 물의를 일으키거나 신청인에게 중대한 정보보호 침해사고 및 개인정보 유출사고가 발생한 경우

제11조(해지) ① “신청인”은 다음 각 호의 어느 하나에 해당하는 경우에는 서면 통지로써 본 계약을 해지할 수 있다.

1. “평가기관”이 정당한 이유 없이 약정한 착수기일을 경과하고도 평가를 수행하지 아니한 경우
2. “평가기관”이 지정 취소, 파산, 해산 등으로 인하여 평가를 진행할 수 없는 경우

② “평가기관”은 다음 각 호의 어느 하나에 해당하는 경우에는 서면 통지로써 본 약관을 해지할 수 있다.

1. “신청인“이 파산, 해산 등으로 인하여 평가를 진행할 수 없는 경우
2. “신청인”이 평가 신청 또는 과정에서 제출된 서류가 허위로 인정되는 경우
3. “신청인”이 평가 수수료를 납부하지 않은 경우

제12조(비밀의 엄수) “평가기관”은 평가를 통하여 얻은 “신청인”의 정보 또는 기밀사항을 외부에 누설하지 아니한다. 다만, 관련 법령에 의한 정보의 공개 요청 시에는 예외로 한다.

제13조(책임) “신청인”이 전자서명인증 업무의 운영에 대한 유지·관리를 소홀히 하여 발생한 문제에 대해서는 “평가기관”은 어떠한 책임도 지지 아니한다.

제14조(관련 법령 및 지침 준수 등) “평가기관”은 평가관련 법령 및 내부 지침을 준수하여야 한다.

<별지 4> 보완조치 내역서

보완조치 내역서

신청인		신청인 확인자	부서		
			직급		
			서명		(인)
평가명					
평가범위					
보완조치 결과확인	확인자	(인)	확인일	년 월 일	

관련 세부 평가기준	
조치내역 및 재발방지대책	**◇ (결함내역)** **◇ (조치내역)** **◇ (재발방지대책)** *※ 보완내역을 상세하게 작성하고 필요 시 증적 자료(실행 화면, 문서, 사진 등)를 첨부, 여러 페이지 작성 가능* *※ 관련 문서 또는 시스템이 있는 경우 작성*

<별지 5> 보완조치 완료 확인서

보완조치 완료 확인서

신 청 인	
평가명	
평가범위	

결함내역 건 보완조치 건

※ 보완조치내역서 별도 첨부

평가결함 사항에 대한 보완조치 내역을 제출합니다.

년 월 일

신청인 확인자 (인)

평가결함 사항에 대해 보완조치가 완료되었음을 확인하였습니다.

년 월 일

금융보안원 평가팀장 (인)

1. 이 평가는 샘플링 평가기법에 의하여 수행된 것으로 발견되지 않은 결함이 존재할 수 있습니다.
2. 이 보고서의 내용은 비밀로 취급되며 신청인의 사전 동의 없이는 공개되지 않습니다. 다만 법원의 요구가 있거나 법률로 정한 경우 예외로 합니다.

<별지 6> 보완조치 요약서

보완조치 요약서

신청인	
평가명	
평가범위	

□ 보완조치 내역

(1) 완료 내역

- 총 결함 건 중 건 완료

결함	건	완료	건	미완료	건

(2) 미완료 상세내역

세부평가기준 항목	미완료 내역	완료예정일

※ 위의 표는 **보완조치 미완료 항목**에 대한 진행상황 및 구체적인 일정계획 작성

<별지 7> 평가절차 중단 확인서

평가절차 중단 확인서

신청인	
평가명	
평가범위	

□ 평가 중단 사유

위와 같은 사유로 인하여 평가절차를 중단합니다.

년 월 일

금융보안원 평가 센터장 (인)

위 내용을 확인하였습니다.

년 월 일

신청인 확인자 (인)

1. 신청인의 귀책사유로 인해 평가절차가 중단된 경우 평가 중단 전까지 소요된 모든 비용에 대한 책임은 신청인에 있습니다.
2. 평가범위 변경으로 인한 평가중단인 경우에는 재신청시 평가를 처음부터 진행합니다.
3. 이 보고서의 내용은 비밀로 취급되며 신청인의 사전 동의 없이는 공개되지 않습니다. 다만 법원의 요구가 있거나 법률로 정한 경우 예외로 합니다.

<별지 8> 이의신청서

이의 신청서

접수번호	접수일시	처리기간

신청인	업체명	사업자등록번호
	대표자	전화번호
	주소	
	전자우편(e-mail)	
이의신청 사유		

위와 같이 이의신청합니다.

년 월 일

신청인(대표자) (서명 또는 인)

금융보안원장 귀하

첨부서류	이의신청 내용을 확인할 수 있는 증빙 자료

금융보안원 전자서명인증평가 안내서

2020년 12월 인쇄

2020년 12월 발행

발행인 : 김 영 기

발행처 : 금융보안원

경기도 용인시 수지구 대지로 132

전 화 : (02) 3495-9000

〈비 매 품〉

금융보안원 전자서명인증평가 안내서

금융보안원
FINANCIAL SECURITY INSTITUTE

(본원) 경기도 용인시 수지구 대지로 132 금융보안원
(교육센터) 서울특별시 영등포구 의사당대로 143 금투센터 8층
TEL 02-3495-9000 **FAX** 02-3495-9799