삼정 KPMG

[별첨] 전자서명인증 세부 평가 기준

v1.5

전자서명인증 평가팀

■ 문서 개정 이력

문서명		[별첨] 전자서명인증 세부 평가 기준	
버전	날짜명	내용	작성자
v1.0	2022.04.18	최초 작성	전자서명인증 평가팀
v1.1	2022.05.11	기준 수정 - 부가 서비스 보안	전자서명인증 평가팀
v1.2	2023.03.27	오탈자 수정, 용어 통일 및 중복 통제 삭제	전자서명인증 평가팀
v1.3	2024.02.20	개인정보보호법 및 ISMS-P 개정에 따른 평가 기준 일부 수정	전자서명인증 평가팀
v1.4	2024.07.24	인증서비스 안전성 강화 평가방안 추가 및 개인정보 관련 법률에 따른 평가 기준 일부 수정	전자서명인증 평가팀
v1.5	2026.02.25	가입자 신원확인 방안 고지와 지능정보화 기본법의 개정에 따른 평가기준 일부 수정	전자서명인증 평가팀

A. 전자서명인증업무 운영기준

항목		세부항목	내용
1. 전자서명인증업무 독립성			
1.1	업무 독립성 유지	1.1.1	ㅇ 전자서명인증사업자는 전자서명인증 서비스의 업무 범위, 인증서의 종류 및 이용 목적 등이 명확하게 수립되어야 하며, 경영진의 검토 및 승인 절차를 거쳐야 한다.
		1.1.2	ㅇ 전자서명인증사업자는 전자서명인증업무를 수행함에 있어 기술적·관리적 조치를 통해 전자서명인증업무의 독립성을 준수해야 한다. [예시] 기술적 조치 ① 전자서명인증업무 관련 설비의 물리적으로 분리 ② 전자서명인증업무 관련 시스템의 독립적 구성 ③ 전자서명인증업무 관련 설비에 인가된 인원만 출입 가능하도록 물리적 통제 ④ 전자서명인증업무 관련 시스템에 인가된 인원만 접근이 가능하도록 통제 [예시] 관리적 조치 ① 중립적으로 신뢰성 있는 자로부터 감사 및 관리·감독 수행 ② 전자서명인증업무를 독립적으로 수행하기 위한 별도 조직 구성 ③ 전자서명인증업무 수행 인력에 대한 독립성 유지방안(독립성 준수 서약서 징구 등) 마련
2. 적정기술의 이용			
2.1	가입자 신원 식별	2.1.1	ㅇ 전자서명인증 서비스는 이용자가 가입자의 신원을 식별할 수 있도록 가입자 식별정보(연계정보, VID, DN 등)를 제공하여야 한다. - VID(Virtual ID, 가상 식별번호) : VID = h(h(IDN, R), 여기서 IDN은 개인을 식별할 수 있는 식별번호이며, 사용되는 해시 함수는 모두 동일한 해시 함수를 사용함 - DN(Distinguished Name, 식별 이름) : ITUT-X.500 디렉터리에 정하는 이름 형식으로, 개체를 인식하기 위해 국가, 지역, 기관, 이름 등 개체의 속성으로 구성되어 있음 [예시] ① 인증서에 가입자 식별정보를 포함하여 발급 ② 이용자의 가입자 전자서명 검증 요청 시, 이용자에게 가입자의 전자서명과 연계정보(CI)를 전달하는 기능 제공 등
2.2	가입자 전자서명 통제	2.2.1	ㅇ 전자서명은 가입자의 전자서명생성정보를 통해서만 생성될 수 있어야 한다. - 공개키 기반 기술(PKI) 등과 같은 기술을 이용하여 가입자의 전자서명생성정보를 통해서만 생성될 수 있는 속성을 가져야 함
		2.2.2	ㅇ 가입자(또는 가입자의 서명 권한을 위임받은 자) 이외의 자가 가입자의 전자서명생성정보에 접근할 수 없도록 가입자 인증 및 접근통제 기능을 제공하여야 한다. [예시] ① 전자서명생성정보를 패스워드 기반으로 암호화하여 저장하며, 패스워드를 통한 가입자 인증이 성공한 경우에만 전자서명 생성 ② 전자서명생성정보를 단말기 내 보안 영역에 저장하며, 생체인증 등을 통한 가입자 인증이 성공한 경우에만 전자서명 생성 등
		2.2.3	ㅇ 가입자의 전자서명생성정보 이용 시마다 가입자 인증을 수행하여야 한다.
		2.2.4	ㅇ 전자서명인증사업자는 가입자가 전자서명을 생성하기 전에 가입자의 전자서명생성정보 및 인증서의 유효성을 검증해야 하며, 전자서명생성정보 및 인증서가 유효하지 않은 경우 전자서명을 생성하지 않아야 한다.
2.3	전자서명 구별	2.3.1	ㅇ 전자서명인증 서비스는 서로 다른 전자문서(원문)에 대해 서로 다른 전자서명을 생성하여야 한다. - 동일한 전자문서에 대해 서로 다른 전자서명 생성은 미 요구
2.4	전자서명 변경 여부 검증	2.4.1	ㅇ 전자서명은 서명 대상 원문 및 변경에 대한 정보를 확인할 수 있는 속성을 가져야 하며, 전자서명의 검증 수행 후 검증 실패 시, 검증 실패 결과를 이용자 및 가입자가 확인할 수 있도록 하여야 한다. [예시] ① (가입자) 전자서명 모바일 앱에서 검증 실패 결과를 화면에 출력 ② (이용자) 전자서명 검증 API를 통해 검증 실패 결과를 이용자에게 전달
		2.4.2	ㅇ 전자서명생성정보를 통해 생성된 전자서명은 전자서명검증정보로 검증되어야 하며, 이를 통해 전자서명의 변경 여부를 확인할 수 있어야 한다.

2.5	안전한 암호 알고리즘 사용	2.5.1	ㅇ 전자서명생성정보 및 전자서명검증정보 생성, 전자서명 생성, 난수 생성, 전자서명생성정보 암호화 등과 같은 업무에서 암호 알고리즘을 사용하는 경우, 「KISA 암호 알고리즘 및 키 길이 이용 안내서」를 참고하여 보안강도 112비트 이상의 안전한 암호 알고리즘을 적용한다.
		2.5.2	ㅇ 「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 112비트 이상의 안전성을 보증해야 할 책임을 가진다.
2.6	관련 표준 준수	2.6.1	ㅇ 전자서명인증 서비스는 전자서명에 표준 프로파일 및 프로토콜을 사용하는 경우 이를 준수하여야 한다. [예시] ① [인증서 프로파일] ITU-T X.509 표준(RFC 5280) ② [전자서명생성정보 암호화] PKCS#5 표준 ③ [전자서명생성정보 저장] PKCS#8 표준 ④ [CRL] RFC 5280 ⑤ [OCSP] RFC 6960 ⑥ [인증서 서명값 전달] CMS(RFC 5652) ⑦ [인증서 발급 요청] CRMF(RFC 4211), CSR(RFC 2986) ⑧ [인증서 관리] CMP(RFC 4210)
		2.6.2	ㅇ 전자서명에 표준 프로파일 및 프로토콜을 사용하지 않는 경우, 전자서명인증사업자는 표준에서 요구하는 안전성 보장을 위한 방안을 제시하여야 한다.
3. 전자서명인증업무준칙			
3.1	준칙에 따른 업무 수행	3.1.1	ㅇ 전자서명인증사업자는 「전자서명법」 제15조에 따른 전자서명인증업무준칙을 작성하여 게시해야 한다.
		3.1.2	ㅇ 전자서명인증사업자는 게시한 전자서명인증업무준칙에 따라 전자서명인증업무를 수행해야 한다.
3.2	법 개정 시 준칙 반영	3.2.1	ㅇ 전자서명인증사업자는 전자서명인증업무준칙에 포함하여야 하는 「전자서명법」 제15조제1항의 아래 사항이 변동되는 경우 전자서명인증업무준칙 내 해당 내용을 반영하여야 한다. - 전자서명인증 서비스의 종류 - 전자서명인증 서비스의 요금, 이용범위 및 유효기간 등 이용조건 - 전자서명인증 업무의 수행 방법 및 절차 - 그 밖에 전자서명인증업무의 수행에 필요한 사항
3.3	준칙 변경 시 절차	3.3.1	ㅇ 전자서명인증사업자는 전자서명인증업무준칙의 내용을 변경하는 경우 사전에 규정된 절차에 따라 전자서명인증업무준칙을 개정해야 한다.
		3.3.2	ㅇ 전자서명인증업무준칙 개정 시 관련 당사자(전자서명인증업무준칙에 명시된 전자서명인증체계 관련자)가 개정 이전의 전자서명인증업무준칙을 열람할 수 있어야 한다. [예시] ① 이전의 모든 제·개정 전자서명인증업무준칙을 웹페이지에 게시 ② 개정 전자서명인증업무준칙과 개전 전 전자서명인증업무준칙을 웹페이지에 게시 ③ 개정 전자서명인증업무준칙에 대한 신구 비교표를 웹페이지에 게시 등
3.4	준칙 제·개정시 협의	3.4.1	ㅇ 전자서명인증업무와 관련된 인증기관(최상위인증기관 등)이 있는 경우, 전자서명인증업무준칙의 "전자서명인증체계 관련자"에 이를 명시해야 하며, "제·개정 절차"에 협의 절차를 명시하여야 한다.
		3.4.2	ㅇ 전자서명인증업무와 관련된 인증기관(최상위인증기관 등)이 있는 경우 전자서명인증업무준칙의 제·개정 시 해당 인증기관과 이에 대해 협의해야 하며, 협의에 대한 증적을 작성 및 보관해야 한다. [예시] 협의 결과에 대해 전자서명인증사업자 및 인증기관(최상위인증기관 등)의 서명이 포함된 회의록 작성 등

4. 가입자 등록			
4.1	가입자 신원확인**(대면)**	4.1.1	ㅇ 전자서명인증사업자 또는 등록대행기관은 가입자의 신원확인을 위하여「전자서명법 시행령」제9조,「전자서명법 시행규칙」제5조에 따라 신원정보의 진위(정확성) 및 신원정보의 주체(소유자)를 확인하여야 한다. - 신원확인에 사용되는 신원정보는 전자서명인증사업자 또는 등록대행기관이 지정 가능 ※ 본인확인기관인 경우 신원정보를 실지명의로 확인하되, 사전에 가입자 신원을 실지명의로 확인한 경우 실지명의 외의 방법도 가능 - 신원정보의 진위 확인은 신원정보를 발급한 기관 혹은 신뢰할 수 있는 출처를 통해 확인 - 신원정보의 주체 확인은 주체의 얼굴을 대면/비대면으로 확인하거나 주체만이 알 수 있는 정보로 확인하는 등 합리적인 방법을 강구
4.2	신원확인 방법**(비대면)**	4.2.1	ㅇ 전자서명인증사업자 또는 등록대행기관이 비대면으로 신원을 확인하는 경우「전자서명 인증업무 운영기준」제6조에 따라 직접 대면(제1항의 요건을 충족하는 것으로 직접 대면에 준하는 비대면 방법 포함)하여 가입자의 신원을 확인한다. ※ [참고] 전자서명인증서비스_가입자_신원확인_방안_V1.0 ① 개인사업자 비대면 대표자 신원확인 1호 : 실명확인증표+본인확인서비스+영상통화+계좌점유인증 중 3개 / 2호 : 본인확인서비스+계좌점유인증 사업자 신원확인 1호,2호 : 사업자등록증명원 등을 발행기관으로부터 직접 수신 or 사업자등록증명원 사본(대표자의 인증서로 전자서명하여 직접 수신) ② 법인 및 단체 비대면 대표자 신원확인 1호 : 실명확인증표+ 영상통화 or 셀카인증+본인확인서비스 사업자 신원확인 1호 : 사업자등록증명원 등을 발행기관으로부터 직접 수신 or 사업자등록증명원 사본(대표자의 인증서로 전자서명하여 직접 수신) ③개인 비대면
4.3	이용약관 공지	4.3.1	ㅇ 전자서명인증사업자 또는 등록대행기관은 인증서의 이용 범위, 전자서명의 효력 등이 명시된 이용약관을 마련하여야 한다.
		4.3.2	ㅇ 전자서명인증사업자 및 등록대행기관은 가입자를 등록하거나 인증서를 발급하기 전에 가입자와 이용자에게 이용약관을 알릴 수 있는 절차를 마련하여야 한다.
4.4	등록대행기관 관리	4.4.1	ㅇ 전자서명인증사업자는 등록대행기관에 신원확인 및 등록대행 업무를 위임할 경우, 등록대행기관이「전자서명인증업무 운영기준」제6조의 가입자 등록 규정을 준수하도록 관리하여야 한다. - 업무 위임 계약서 등에 규정 준수와 관련한 통제방안 명시 - 정기적인 실태 점검 등을 통해 등록대행기관의 통제방안 준수 여부 관리 등
4.5	등록정보 위·변조 방지	4.5.1	ㅇ 전자서명인증사업자는 등록대행기관으로부터 정보통신망으로 가입자의 등록 정보를 전송받는 경우, 전송 중 가입자의 등록정보가 위·변조 및 유·노출되지 않도록 방안을 마련하여야 한다.
		4.5.2	ㅇ 전자서명인증사업자는 가입자의 등록정보를 전송받은 후 가입자의 등록정보가 유출되지 않도록 안전한 암호 알고리즘이 적용된 암호화 조치 등의 방안을 마련하여야 한다. - 안전한 암호 알고리즘의 기준은「KISA 암호 알고리즘 및 키 길이 이용 안내서」를 참고하여 적용 -「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 갖음 [예시] 다수의 등록대행기관이 가입자 등록정보를 등록하더라도, 자사 외 타 등록대행기관이 등록한 정보를 조회할 수 없도록 암호화 적용
5. 인증서 발급·효력정지·효력회복 및 폐지 등			
5.1	전자서명 생성정보의 유일성 확인	5.1.1	ㅇ 전자서명인증사업자는 인증서를 발급하는 경우 가입자의 전자서명생성정보가 유일함을 확인하여야 한다. - 가입자의 전자서명생성정보와 전자서명검증정보가 1:1로 매핑되는 경우 전자서명검증정보의 유일성을 확인하는 방법으로 대체 가능 [예시] 인증서 발급 전 가입자의 전자서명검증정보가 이전에 발급된 모든 가입자의 전자서명검증정보와 중복되지 않는지 확인
5.2	인증서 이용 방안 마련	5.2.1	ㅇ 전자서명인증사업자는 전자서명 생성·검증 등 가입자에게 발급된 인증서를 이용자가 이용할 수 있는 방안을 마련하여 제공해야 한다. [예시] 전자서명 검증에 필요한 SDK(Software Development Kit) 제공, 전자서명 검증을 위한 API(Application Programming Interface) 제공 등
5.3	인증서 위·변조 방지	5.3.1	ㅇ 전자서명인증사업자는 가입자 인증서의 위·변조를 방지(무결성 검증) 및 탐지할 수 있는 기술적 방안을 마련하여야 한다. [예시] 가입자 인증서에 대해 전자서명인증사업자가 전자서명을 수행, 인증서의 블록체인 저장 등
		5.3.2	ㅇ 전자서명인증사업자는 인증서 이용 시마다 가입자 인증서의 위·변조 여부를 확인하여야 한다.

5.4	인증서 폐지 등 처리 시 신원확인	5.4.1	ㅇ 전자서명인증사업자는 가입자의 신청이 있는 경우, 전자서명 인증업무 운영기준 제6조제1항에 따라 가입자의 신원을 확인 한 후 인증서의 효력을 정지하거나 회복 또는 폐지할 수 있다. ※ 전자서명 인증업무 운영기준 제6조제1항 1. 가입자 신원정보의 진위(정확성)를 확인할 수 있을 것 2. 신원정보와 주체(소유자)가 맞는지 확인할 수 있을 것
5.5	인증서 폐지 등 확인 방안 마련	5.5.1	ㅇ 전자서명인증사업자는 인증서의 효력을 정지하거나 회복 또는 폐지하는 경우 이용자가 지체 없이 그 사실을 확인할 수 있는 방안을 마련하여 제공해야 한다. [예시] 인증서 유효성 검증서비스(CRL - 인증서폐지목록(Certificate Revocation List, OCSP - 온라인 인증서 상태 프로토콜(Online Certificate Status Protocol) 제공 등
5.6	인증서 유효성 확인 서비스 제공	5.6.1	ㅇ 전자서명인증사업자는 이용자가 인증서의 유효성을 확인할 수 있도록 인증서 효력 정지 및 폐지목록(CRL)을 전자서명인증업무준칙에 규정한 공고 설비에 공고하거나, 온라인 인증서 상태 프로토콜(OCSP)을 제공할 수 있다.

6. 전자서명생성정보 생성			
6.1	안전한 환경 마련, 준칙 내 절차 준수	6.1.1	ㅇ 전자서명인증사업자는 물리적으로 안전한 환경('[별첨] A. 전자서명인증업무 운영기준' 충족)에서 자신 및 가입자의 전자서명생성정보를 생성하여야 한다.
		6.1.2	ㅇ 전자서명인증사업자는 전자서명인증업무준칙 내 절차에 따라 자신 및 가입자의 전자서명생성정보를 생성하여야 한다. [예시] ① 전자서명인증사업자의 전자서명생성정보를 생성하는 시설은 여타 업무 시설과 물리적으로 분리하고 다중 출입통제 대책 등을 적용 ② 가입자의 전자서명생성정보를 가입자 단말기에서 생성하는 경우 단말기 내 안전한 보안영역을 활용 등
6.2	전자서명 생성정보 생성 시 기준	6.2.1	ㅇ 전자서명인증사업자는 자신 혹은 가입자의 전자서명생성정보 생성 시 표준 프로토콜을 이용할 시 해당 표준을 준수해야 하며, 표준 프로토콜을 사용하지 않는 경우 전자서명인증사업자는 해당 프로토콜에 대한 안전성을 보증해야 한다.
		6.2.2	ㅇ 전자서명인증사업자는 전자서명생성정보 생성 시 안전한 암호 알고리즘 또는 안전한 암호화 장치를 사용하여야 한다. [예시] FIPS 140-3 Level 3 인증을 받은 전용 암호화 장치(HSM, Hardware Security Module)를 이용하여 전자서명생성정보 생성 등
6.3	다자인증 통제 적용	6.3.1	ㅇ 전자서명인증사업자의 전자서명생성정보를 생성하는 경우, 다자인증 통제(m of N, m은 3명 이상) 하에 전자서명생성정보를 생성하여야 한다. - 전자서명생성정보를 생성하는 경우 정의된 키 생성 절차서(Key Generation Script)에 따라 수행하고 기록(video record, written log)을 남겨야 함 [예시] 전자서명인증사업자는 전자서명생성정보 생성 시 암호화 장치(HSM)는 다자인증 통제 기능을 제공하며, 전자서명생성정보 생성을 위한 다자인증 통제 설정을 '3 of N'로 설정함. HSM의 다자인증 통제 설정(3 of N)에 따라 인증을 수행할 수 있는 N명 중 최소 3명이 인증에 성공한 경우에만 키를 생성하도록 함
6.4	가입자 전자서명 생성정보 유출 방지	6.4.1	ㅇ 전자서명인증사업자는 가입자의 신청이 있는 경우가 아니면 가입자의 전자서명생성정보를 보관해서는 아니된다.
		6.4.2	ㅇ 전자서명인증사업자는 가입자의 신청에 의해 가입자의 전자서명생성정보를 보관하는 경우 전자서명생성정보 유출 방지를 위한 방안을 마련하여야 한다. [예시] 가입자 전자서명생성정보를 안전한 암호 알고리즘을 이용하여 암호화, 접근통제, 무결성 유지 등
		6.4.3	ㅇ 전자서명인증사업자는 가입자의 신청에 의해 가입자의 전자서명생성정보를 보관하는 경우 가입자의 동의 없이 이를 이용하거나 유출하여서는 아니된다.
6.5	가입자 전자서명 생성정보 생성 시 공동 수행	6.5.1	ㅇ 전자서명인증사업자는 가입자의 전자서명생성정보를 생성하는 경우 전자서명생성 업무를 위해 지정한 최소 2인 이상이 공동으로 수행하여야 한다. [예시] 전자서명생성정보 생성 업무담당자 2명을 지정하고, 감독관의 감독하에 해당 2인이 공동으로 전자서명생성정보를 생성함
		6.5.2	ㅇ 전자서명인증사업자는 자동화된 설비를 이용하여 가입자의 전자서명생성정보를 생성하는 경우 최소 2인 이상이 통제할 수 있도록 설정된 다자인증을 통해 생성하여야 한다. [예시] 암호화 장치(HSM)의 m of N(m은 2명 이상) 기능을 사용하여 가입자의 전자서명생성정보를 생성함
7. 전자서명생성정보 보호			
7.1	전자서명 생성정보 보호	7.1.1	ㅇ 전자서명인증사업자는 전자서명생성정보를 생성한 경우 이를 안전하게 보호할 수 있는 방안을 마련하여야 한다. [예시] ① 전자서명생성정보를 안전한 암호 알고리즘으로 암호화하여 저장 ② FIPS 140-3 Level 3 이상의 인증을 받은 암호화 장치(HSM) 내 전자서명생성정보 저장 ③ 메모리 내 전자서명생성정보 저장 금지 등
7.2	전자서명 생성정보 통제 및 안전조치	7.2.1	ㅇ 전자서명인증사업자는 가입자의 전자서명생성정보를 생성한 경우 가입자의 통제하에 전자서명생성정보가 이용될 수 있도록 방안을 마련하여야 한다. - 가입자의 전자서명생성정보 이용 시마다 가입자 인증을 통해 가입자 본인만이 이용할 수 있도록 접근통제를 적용하여야 함
7.3	전자서명 생성정보 백업	7.3.1	ㅇ 전자서명인증사업자의 전자서명생성정보는 기술적·물리적 통제 및 암호화를 통하여 안전하게 관리하여야 하며, 분실·훼손 또는 도난·유출을 방지하고 전자서명인증업무를 계속하여 안정적으로 제공할 수 있도록 백업 체계(백업 정책 수립 등)를 구축하여야 한다. - 백업 정책 수립 시 백업 주기, 백업 절차, 백업 방식, 복구 방법 등을 포함
		7.3.2	ㅇ 전자서명인증사업자는 원본정보가 분실·훼손, 도난·유출 시에도 백업본을 이용할 수 있도록 방안을 마련하여야 한다. [예시] 전자서명생성정보 백업본을 원본과 다른 별도의 서버에 보관 등

7.4	전자서명 생성정보 백업본 안전 보관	7.4.1	ㅇ 전자서명인증사업자의 전자서명생성정보 백업본이 안전하게 보관될 수 있도록 방안을 마련하여야 한다. [예시] ① 전자서명생성정보 백업본에 대한 접근통제 및 안전한 암호 알고리즘으로 암호화 조치 ② 전자서명생성정보 백업본은 원본과 동일하거나 높은 보안 수준 유지 등
		7.4.2	ㅇ 전자서명인증사업자는 가입자의 전자생성정보를 백업하는 경우 가입자의 전자생성정보의 백업본을 안전하게 보관될 수 있도록 방안을 마련하여야 한다. [예시] 전자서명생성정보 백업본에 대한 접근통제 및 안전한 암호 알고리즘으로 암호화 조치
7.5	전자서명 생성정보 소산	7.5.1	ㅇ 전자서명인증사업자는 백업된 전자서명생성정보 중 1부는 원격 저장설비(10Km 이상 떨어진 원격지)에 소산하여야 하며, 소산 정책 수립 시 다음의 사항을 고려하여야 한다. - 원격 저장설비 내 물리적 보호조치(물리적으로 분리된 격실, 내화금고 등) - 원격 저장설비에 대한 내부 출입통제 및 감시설비를 통한 모니터링 - 소산 시 잠금장치가 있는 하드케이스에 보관 후 운반 - 소산 시 담당자 및 운영자 통제를 위한 출입/작업 이력 관리
7.6	전자서명 생성정보 백업 및 복구 공동 수행	7.6.1	ㅇ 전자서명인증사업자는 전자서명생성정보의 백업 및 복구 시 지정된 2인 이상의 직원이 공동으로 업무를 수행하여야 하며, 별도의 관리·감독자를 지정하여야 한다. [예시] 전자서명인증사업자는 가입자의 전자서명생성정보 백업·복구 업무 담당자 2명을 지정하고, 감독관의 감독 하에 해당 업무 담당자 2인이 공동으로 전자서명생성정보 백업·복구
7.7	전자서명 생성정보 안전한 파기	7.7.1	ㅇ 전자서명인증사업자는 전자서명생성정보의 원본 및 백업본을 파기하는 경우 전자서명인증업무 관리책임자 및 보안관리자의 감독하에 수행하여야 한다. - 전자서명인증사업자의 전자서명생성정보를 파기할 경우 정의된 키 파기 절차서(Key Destruction Script)에 따라 수행하고 기록을 남겨야 함
		7.7.2	ㅇ 전자서명인증사업자는 전자서명생성정보 파기 시 복구가 불가능하도록 안전한 방법으로 파기하여야 한다. [예시] 암호화 장치(HSM) 장비 불능 조치, 암호화 장치(HSM) 내 저장된 전자서명생성정보 덮어쓰기, 디가우징, 디스크 파쇄 등
7.8	전자서명 생성정보 유출 시 조치	7.8.1	ㅇ 전자서명인증사업자는 전자서명생성정보가 분실·훼손 또는 도난·유출된 경우 가입자 및 관련 당사자에게 해당 사실을 알릴 수 있도록 내부 절차를 마련하고 이를 준수하여야 한다. [예시] 분실·훼손 또는 도난·유출된 사실을 인터넷 홈페이지에 게시하는 절차 마련 등
8. 시설 및 자료 보호조치 등			
8.1	시설 및 자료 보호조치 기준	8.1.1	ㅇ 전자서명인증사업자는 '[별첨] B. 시설 및 자료의 보호조치'을 만족하여야 한다.
		8.1.2	ㅇ 전자서명인증사업자는 '[별첨] C. 개인정보 보호조치'을 만족하여야 한다.
8.2	관계 법령 준수	8.2.1	ㅇ 전자서명인증사업자는「정보통신망법」,「개인정보보호법」,「정보통신기반보호법」등 준수해야 하는 법령이 있는 경우 이를 준수하여야 한다. - 준수해야 하는 법령이 있는 경우 전자서명인증사업자가 자체 점검하고 점검결과(예: 자체 점검표)를 평가기관에 제출 ※ 단, '[별첨] B. 시설 및 자료의 보호조치' 및 '[별첨] C. 개인정보 보호조치'과 중복되는 사항은 생략 가능
9. 가입자 및 이용자 보호대책			
9.1	업무 휴지·폐지 시 절차 준수 및 손해배상	9.1.1	ㅇ 전자서명인증사업자는 전자서명인증업무 휴지 시, 휴지기간을 정하여 휴지하려는 날의 30일 전에 가입자에게 관련 사실을 통보하고 이를 인터넷 홈페이지 등에 게시하는 절차를 마련하여야 한다.
		9.1.2	ㅇ 전자서명인증사업자는 전자서명인증업무 폐지 시, 폐지 60일 전에 가입자에게 관련 사실을 통보하고 이를 인터넷 홈페이지 등에 게시하는 절차를 마련하여야 한다.
		9.1.3	ㅇ 전자서명인증업무 휴지 및 폐지 시 통보·게시하는 내용에는 요금의 반환, 가입자의 개인정보 폐기 등 가입자 보호조치가 포함되어야 한다.
		9.1.4	ㅇ 전자서명인증사업자는「전자서명법 시행령」상의 요건을 충족하는 손해배상 보험을 가입하고 가입자 등에 미치는 손해 발생 시 이를 해결하기 위한 절차를 마련하여야 한다. ※ 시행령 상 손해배상 보험 요건 1. 보험 금액 : 연간 총 한도보상액 10억원 이상 금액 2. 보험 기간 : 인정의 유효기간 내에 발생한 사고에 대한 보장이 가능할 것

9.2	연계정보 처리 기준	9.2.1	ㅇ 전자서명인증사업자가 연계정보(CI)를 수집·이용하거나 제3자에게 제공하는 경우 가입자로부터 별도 동의를 얻어야 한다.
		9.2.2	ㅇ 전자서명인증사업자가 연계정보(CI)를 저장하거나 전송하는 경우 안전한 암호 알고리즘으로 암호화하여야 한다.
		9.2.3	ㅇ 전자서명인증사업자가 연계정보(CI)를 이용하는 경우 전자서명과 분리된 단순 식별자 용도로만 사용하여야 한다. - 인증서 내 연계정보(CI)를 포함할 수 없으며, 가입자 단말기에도 연계정보(CI) 저장 금지
		9.2.4	ㅇ 전자서명인증사업자는 연계정보(CI)의 송수신 시간, 송수신 대상 등에 대한 로그를 기록하여 저장·보관하여야 한다.
		9.2.5	ㅇ 전자서명인증사업자는 연계정보(CI)를 처리하는 시스템에 접근할 수 있는 관리자를 지정하고, 해당 관리자만 연계정보(CI) 처리시스템에 접근하도록 통제하여야 한다.
		9.2.6	ㅇ 전자서명인증사업자는 연계정보(CI)를 개인정보의 일환으로 보호하여야 하며 '[별첨] C. 개인정보 보호조치'을 만족하여야 한다.
10. 장애인・고령자 등의 전자서명 이용 보장			
10.1	전자서명 이용 보장	10.1.1	ㅇ 전자서명인증사업자는 장애인·고령자 등의 전자서명인증서비스 접근 및 이용 보장을 위하여 「지능정보화 기본법」 제46조 및 46조의2에 따라 접근성을 보장하며 정보 접근 및 이용 편의를 증진하기 위한 조치를 하여야 한다. [예시] ① 웹 접근성 : 과학기술정보통신부장관이 지정한 정보통신 접근성(웹 접근성) 품질인증 기관을 통한 웹 접근성 인증 ② 앱 접근성 : '(KS X 3253) 모바일 어플리케이션 콘텐츠 접근성 지침 2.0' 준수 여부 인증 ③ 소프트웨어 접근성 : '(TTAS.KO-10.0213) 소프트웨어 접근성 지침 1.0' 준수 여부 인증
11. 인증서비스 안전성 제공			
11.1	신원확인정보의 안전한 처리환경 마련	11.1.1	ㅇ 인정사업자는 가입자의 신원확인정보가 위변조 되지 않도록 무결성과 기밀성을 보장할 수 있는 안전한 서비스 환경을 구현하여야 한다.
		11.1.2	ㅇ 인정사업자는 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.
11.2	인증서 부정발급 상시 확인 체계 운영	11.2.1	ㅇ 인정사업자는 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

B. 시설 및 자료의 보호조치

항목		세부항목		내용	ISMS-P	WebTrust for CA
1. 정보보호 정책 수립 및 조직						
1.1	정보보호 정책 수립 및 관리	1.1.1	정보보호 정책 수립	o 전자서명인증사업자는 정보보호 정책을 수립하고 이를 문서화하여야 한다. - 정보보호 정책 문서가 물리적, 인적, 기술적 통제를 포함 - 정보보호 정책 문서가 경영진의 승인을 얻어 전직원에게 전파	1.1.5	3.1.1
		1.1.2	정보보호 정책 이행	o 전자서명인증사업자는 수립된 정보보호 정책이 준수될 수 있도록 책임 있는 관리에 의해 구현하고 준수하여야 한다. - 최고경영자는 정보보호 분야 전문성을 갖춘 인력을 확보 - 정보보호 정책의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당	1.1.6	3.1.2
		1.1.3	정보보안 정책 내용	o 전자서명인증사업자는 정보보호를 포함하는 구체적인 정보보호 정책을 마련하여야 한다. - 정보보호 정책이 다음을 포함 a) 정보 공유를 가능하도록 하는 메커니즘으로서의 정보보호의 정의, 목표 및 범위와 중요성 b) 정보보호의 원칙 및 목표를 지원하기 위한 경영진의 의지 c) 조직에게 특별히 중요시 되는 보안정책, 원칙, 표준, 준수 요구사항에 대한 설명 d) 보안 침해 보고를 포함하는 정보보호 관리에서의 책임에 대한 정의 e) 정책을 지원하는 문서에 대한 목록	-	3.1.3
		1.1.4	정보보안 정책의 검토	o 전자서명인증사업자는 정보보호 정책을 주기적으로 검토하는 절차를 마련하여 최신성을 유지하여야 한다. - 정보보호 정책 문서의 최신성을 유지하기 위한 주기적인 검토 프로세스 절차 마련 - 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 관리	2.1.1	3.1.4 3.1.8
1.2	정보보호 조직 구성 및 운영	1.2.1	정보보호 책임자 지정	o 최고경영자는 정보보호 총괄 관리책임자를 임원급으로 지정하여야 한다. - 최고경영자가 정보보호 활동을 위하여 예산·인력 등 자원을 할당 권한을 보유한 임원급으로 정보보호책임자를 지정 - 최고경영자가 정보보호 총괄 관리 책임자를 통하여 정보보호 관련 보고 및 의사결정 체계를 수립하여 운영	1.1.2 1.1.6	3.1.5
		1.2.2	정보보호 조직 구성	o 전자서명인증사업자는 정보보호 활동을 체계적으로 이행 할 수 있는 실무 조직 또는 정보보호 위원회를 구성하여 운영하여야 한다. - 정보보호 활동을 체계적으로 이행할 수 있는 실무 조직이 존재 - 전자서명관련 전문가 그룹이나 관련 기관과 적절한 연계를 유지하며 활동	1.1.3	3.1.6
		1.2.3	정보보호 조직의 운영	o 전자서명인증사업자는 구성된 정보보호 조직에 대해서 구성원들의 역할과 책임을 명확하게 지정하여야하고 구성원 간 상호 의사소통할 수 있도록 운영하여야 한다. - 각각의 정보자산을 보호하기 위한 책임 및 특정 보안 절차를 수행할 책임이 명확 - 구성원들의 정보보호 활동을 평가할 수 있는 체계와 구성원간 상호 의사소통할 수 있는 체계를 수립하여 운영	2.1.2	3.1.7
2. 자산 관리						
2.1	정보자산 식별 및 분류	2.1.1	정보자산 식별 및 분류	o 전자서명인증사업자는 전자서명인증업무 법위 내 모든 정보 자산을 식별하여 분류한 후 내역을 문서화하여 최신으로 관리하여야 한다. - 전자서명인증사업자가 정보자산 분류기준을 확립한 후 이에 따라, 모든 정보자산을 분류 및 식별 - 식별된 정보자산에 대해 중요도 산정	1.1.4 1.2.1	3.2.1
		2.1.2	정보자산 관리 책임자 지정	o 전자서명인증사업자는 전자서명인증업무 정보자산별로 관리책임자를 지정하여야 한다. - 식별된 모든 정보 자산에 대해서 관리 책임자를 지정	2.1.3	3.2.4
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 관리	1.2.1	3.2.2
		2.2.2	자산 통제	o 전자서명인증사업자는 분류된 자산 및 정보자료를 위험으로부터 보호를 받을 수 있도록 적절한 통제절차를 마련하여야 한다. - 전자서명인증사업자가 분류된 자산 및 정보자료에 대한 위협 분석을 수행 - 전자서명인증사업자가 사업의 요구사항 및 사업에 미치는 영향에 따라 조직 내에서 사용되고 있는 자산의 적절한 사용을 위한 규칙을 문서화	1.2.3	3.2.3

3. 인적 보안						
3.1	직무 적합성 검토	3.1.1	직무 적합성 검토	o 전자서명인증사업자는 전자서명인증업무에 대한 직무기술서를 명시하여야 하며, 담당자에 대한 신원확인 등 업무 적합성 여부 등을 검토하는 절차를 마련하여야 한다. - 전자서명인증업무를 수행하는 직무에 대한 요건, 역할, 책임 등을 기술한 직무기술서 - 전자서명인증업무 관련 담당자에 대한 신원확인 등 업무 적합성 여부 검토를 위한 절차 마련 - 전자서명인증업무 관련 담당자 및 신뢰된 역할을 수행하는 계약직 인력은 최소한 정규직 직원들과 동일한 신원확인 절차 및 인력 관리 절차를 적용	2.1.2 2.2.1	3.3.1 3.3.2
3.2	역할 구분	3.2.1	신뢰된 역할 담당자	o 정보보호 정책 문서에, 신뢰된 역할에 대한 식별과 이를 취급하는 담당자들에 대한 각별한 관리를 반영하여야 한다. - 다음과 같이 신뢰된 역할에 대한 식별 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 유지관리 e) 암호화 키 생명 주기 관리 기능 f) 인증 시스템 개발 - 정보보호 정책 문서에 신뢰된 역할(trusted roles)과 비 신뢰된 역할(non-trusted roles)에 요구되는 신원확인에 대해 상세히 기술 - 신뢰된 역할 담당자가 승인을 거친 후에 시스템/시설에 대한 접근 또는 작업을 수행 - 신뢰된 역할 수행 계약직 인력은 정규직 직원들과 동일한 신원확인 절차 및 인력 관리 절차를 적용받고 있는지 확인	-	3.3.3 3.3.4 3.3.5 3.3.7 3.3.8
		3.2.2	키 관리 및 인증서 업무자	o 전자서명생성정보 및 인증서 관리 등과 관련된 직원들에 대해서는 권한 오남용, 고의적 행위 등을 할 수 없도록 주기적인 신뢰성 검토 및 검증이 이루어져야 한다. - 전자서명생성정보 및 인증서 관리 등 주요 직무 수행 직원들에 대한 주기적인 신뢰성 검토 및 검증	-	3.3.9
		3.2.3	징계 절차 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 마련	2.2.6	3.3.10
		3.2.4	퇴사자 관리	o 전자서명인증사업자는 퇴사자에 대해서는 모든 접근통제 권한을 종료시켜야 한다. - 퇴사자에 대해서 물리적, 논리적 접근을 종료 - 퇴사자 권한 회수 이력 관리	2.2.5	3.3.11 3.3.12
3.3	보안 서약서 작성	3.3.1	보안 서약서 작성	o 전자서명인증사업자는 전자서명인증업무를 수행하는 모든 직무 관련자(임시직원이나 외부자 포함)에게 기밀 유지 등에 대한 서약서를 받아야 한다. - 전자서명인증업무를 수행하는 모든 직무 관련자(임시직원이나 외부자 포함)에게 기밀 유지 등에 대한 서약서 수령	2.2.3	3.3.6
3.4	보안 교육	3.4.1	보안 교육 절차	o 전자서명인증사업자는 전자서명인증업무를 수행하는 모든 직무관련자에게 보안 정책 및 절차에 대한 교육을 실시하여야 한다. - 전자서명인증사업자는 모든 직원들(하청 용역자 포함)에게 보안 정책 및 절차에 대한 교육을 위해 다음을 마련 a) 각자의 역할에 대한 교육훈련 요구사항 및 교육훈련 절차 b) 각자의 역할에 대한 재교육훈련 기간 및 재교육훈련 절차	2.2.4	3.3.13
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. - 전자서명인증업무 시설 및 시스템에 대한 제3자의 물리적 및 논리적 접근 통제 마련 - 전자서명인증사업자가 업무의 일부로 외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우, 정보보호 요구사항을 계약서에 명시	2.3.1 2.3.2	3.1.10 3.1.11
		3.5.2	외부자 보안 관리	o 업무 수탁자 등의 정보보호 요구사항 준수 여부를 주기적으로 점검 또는 관리·감독하여야 한다. - 명시된 요구사항을 준수하고 있는 주기적으로 점검 또는 관리 감독	2.3.3	3.1.10 3.1.11

4. 물리적 보안						
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 마련하여야 한다. - 전자서명인증 운영실이 위치한 빌딩 또는 장소는 허가된 인원만 출입 가능하도록 물리적 접근 통제를 위한 보안요원 접수나 다른 수단 구비 - 인증서 제조 시설에 대한 비인가 출입과 환경오염을 방지하기 위해 물리적 장벽 설치 - 통제구역에 위치한 설비는 온·습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영절차를 수립·운영	2.4.1 2.4.2 2.4.3 2.4.4	3.4.2 3.4.3 3.4.4 3.4.5 3.4.6
		4.1.2	장비 관리	o 전자서명인증사업자는 주요장비에 대해 물리적 보안 조치를 마련하고, 사고 및 재난 등을 방지할 수 있는 방안이 마련되어 있어야 한다. - 장비에 대한 재고 관리 - 장비는 정전 및 기타 전기적 이상으로부터 보호 - 전자서명인증업무 운영시설이 있는 건물 내의 전력 및 통신선이 파손이나 도청의 위험으로부터 보호 - 개인용 컴퓨터나 워크스테이션은 미사용 시에 로그오프 되거나, 패스워드 등을 통하여 적절히 통제	2.4.3	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	4.2.1	주요시설 출입통제	o 전자서명인증사업자는 인증서를 발급하는 설비 등이 있는 주요 운영시설에 대한 철저한 출입통제 정책을 수립하고 이행하여야 한다. - 전자서명인증업무 관련 주요 운영시설의 출입은 통제되고 있는 제한된 수의 접근 지점을 통해서만 이루어지는지 여부 - 전자서명인증업무 관련 주요 운영시설의 출입은 다중신원검증 절차 (예 : IC 카드 + 지문)를 통하여 인가된 인원에게만 접근이 가능하도록 통제	2.4.2	3.4.1 3.4.9 3.4.10
		4.2.2	출입통제 관리	o 전자서명인증업무 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 여부 - 전자서명인증업무 관련 운영시설을 출입하는 모든 인원에 대해 기록을 남기고 관리 - 제3의 서비스 지원인력은 필요시에만 전자서명인증업무 관련 운영시설의 보안 구역 출입이 허용되어야 하며, 이 경우에도 직원과 동행 여부 - 전자서명인증업무 관련 시설을 방문자에 대해서 출입날짜와 시간을 기록하는 등 감독하는 절차 마련되어 있는 지의 여부 - 전자서명인증업무 관련 시설에 대한 접근 권한은 주기적으로 검토 및 갱신	2.4.2	3.4.11 3.4.13 3.4.14 3.4.15
4.3	침입 감지 및 감시	4.3.1	침입 감지 및 감시	o 전자서명인증사업자는 운영시설이 있는 모든 건물에 대한 물리적인 침입 감지 및 감시 방안을 마련하여야 하고, 이러한 시설의 출입이나 내부활동을 모니터링하여야 한다. - 전자서명인증업무 관련 운영건물의 모든 외부 출입문에 침입자 감지 시스템이 설치되어 운영 - 전자서명인증업무 관련 시설 내에 직원이 없을 때에 물리적으로 잠금 되고 경보장치 작동 - 전자서명인증업무 관련 시설의 출입이나 내부의 활동이 CCTV 등 카메라를 통해 사각지대 없이 상시 모니터링	2.4.4	3.4.7 3.4.8 3.4.12 3.9.13
4.4	반출입 통제	4.4.1	반출입 통제	o 전자서명인증사업자는 장비, 문서, 휴대용 저장매체 등의 반출입 통제 정책을 수립하고 반출입시 이력을 작성하고 보관하여야 한다. - 전자서명인증업무 관련 시설 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제절차를 수립·이행하고 주기적으로 검토	2.4.6	3.4.24
5. 운영 보안						
5.1	운영절차 수립 및 준수	5.1.1	운영절차 수립 및 준수	o 전자서명인증사업자는 전자서명인증업무 관련 시스템 및 보안시스템 운영을 위한 절차를 수립하고 이행하여야 한다. - 전자서명인증업무 관련 시스템과 보안시스템 운영절차가 각 기능영역 별로 문서화되어 관리 - 전자서명인증업무 관련 시스템과 보안시스템 관련 장비, 소프트웨어, 운영 절차상의 모든 변경 사항을 통제하기 위하여, 관리 책임자 및 절차가 존재 - 시스템 관련 문서는 비인가 접근으로부터 보호	2.10.1	3.5.1 3.5.2 3.5.3 3.5.5
		5.1.2	저장매체 관리	o 전자서명인증사업자는 운영에 필요한 저장매체 및 이동식 저장매체를 관리하는 절차를 마련하고 이를 이행하여야 한다. - 이동식저장매체 관리 절차에 다음을 포함 a) 더 이상 필요 없을 시, 재사용 가능한 매체에 담겨 있던 내용물은 지우거나, 매체 자체를 파기한다. 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 쓰기 - 비인가 공개 또는 남용으로부터 정보를 보호하기 위해, 정보의 저장 및 취급절차가 존재하며 이행	2.10.7	3.5.14 3.5.15 3.5.16 3.5.17

5.2	시스템 및 서비스 관리	5.2.1	시스템 및 서비스 관리	o 전자서명인증사업자는 운영시스템을 개발 및 테스트 시스템과 분리하여야 한다. - 개발 및 테스트 시설이 운영설비로부터 분리 - 신규 정보시스템, 업그레이드 및 새로운 버전에 대한 승인 기준이 수립되고 승인 전 시스템에 대한 적절한 테스트가 수행	2.8.2 2.8.3	3.5.4
		5.2.2	성능 및 용량 관리	o 전자서명인증업무 관련 시스템에 대해 보안 설정, 성능·용량·상태 모니터링, 안전한 인수 및 유지보수 절차를 수립·이행하여야 한다. - 성능·용량·상태 모니터링하고 적절한 처리능력 및 가용성을 보장하기 위해 향후 용량 요구사항을 예측 - 외부로부터 설비관리 서비스를 받기 전에, 위협과 관련 통제 항목들이 식별되고 계약자와 협의하여 이를 계약서에 명시	2.4.4 2.9.2	3.5.6 3.5.7
5.3	악성코드 예방·탐지·대응	5.3.1	악성코드 예방·탐지·대응	o 전자서명인증사업자는 악성코드 예방·탐지·대응을 위한 보안시스템을 운영하여야 한다. - 악성코드 예방·탐지·대응을 위한 보안 시스템을 운영 - 수립된 정책과 절차의 이행과 더불어, 직원들에 대해서 지속적인 관심을 환기하는 프로그램 여부	2.10.9	3.5.8
		5.3.2	패치 관리	o 전자서명인증사업자는 운영체제 및 소프트웨어에 대한 패치·업데이트 정책과 절차를 수립·이행하여야 한다. - 운영체제 및 소프트웨어의 패치와 업데이트에 대한 정책과 절차를 수립	2.10.8	3.5.8
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 반영 - 하드웨어 및 소프트웨어 오동작을 보고할 수 있는 절차를 수립하고 이행 - 보고된 침해사고에 대해서 적절히 대응하였는지 평가하는 절차를 수립하고 이행 - 침해사고의 종류, 크기, 영향, 오작동에 대해서 문서화하고, 정량화하고, 모니터링 될 수 있도록 하는 공식적인 관리 절차가 존재	2.11.1 2.11.5	3.5.10 3.5.11 3.5.12 3.5.13
6. 접근통제						
6.1	접근통제 정책	6.1.1	접근통제 정책 수립	o 전자서명인증사업자는 전자서명인증업무 관련 시스템 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 수립 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) - 전자서명인증업무 관련 시스템과 서비스에 접근하기 위한 사용자 등록 및 등록 취소 절차가 수립	2.10.1	3.6.1
6.2	접근권한 관리	6.2.1	접근권한 관리	o 전자서명인증업무 관련 시스템 및 보안시스템, 중요 정보에 접근하기 위한 사용자 계정 및 권한관리 절차를 마련하여야 한다. - 사용자 계정 및 권한의 등록과 삭제 절차가 수립 - 시스템에 대한 특별 권한의 사용과 할당이 제한되고 통제 - 공식적인 관리 절차에 따라 패스워드 및 멀티팩터 인증 토큰의 할당이 통제 - 전자서명인증업무 관련 시스템과 보안시스템 운영절차가 각 기능영역 별로 문서화되어 관리 - 사용자로 하여금 정의된 정책과 절차에 따라 패스워드의 사용과 선택 - 관리 및 슈퍼사용자 계정은 멀티팩터 인증 통제를 권고	2.5.1 2.5.5	3.6.2 3.6.3 3.6.4 3.6.6 3.6.7 3.6.8
		6.2.2	접근권한 검토	o 사용자 계정 및 권한관리 절차는 정기적으로 검토하여 업데이트 되어야 한다. - 신뢰 역할을 수행하는 사용자의 접근 권한이 정기적인 주기로 검토되고 갱신	2.5.6	3.6.5

6.3	비인가자 시스템 접근 금지	6.3.1	비인가자 시스템 접근 금지	o 전자서명인증사업자는 접근통제 정책에 따라 비인가자가 시스템에 접근할 수 없도록 통제하여야 한다. - 접근통제 정책의 접근권한이 시스템에 반영 - 시스템 접근 시 안전한 로그인 절차가 요구 - 모든 직원은 1인 1계정 발급을 원칙으로 하여 고유한 식별자(user ID)를 가지고 사용함으로써, 이에 따른 모든 활동들을 추적 - 공유 또는 그룹 계정이 필요 시, 개인의 책임을 유지하기 위해 다른 모니터링 통제 구현 - 시스템 유틸리티 프로그램의 사용은 인가된 사용자로 제한되고 엄격하게 통제 - 비활성화 터미널은 사용에 앞서 재인증을 요구 - 민감 데이터는 비인가 사용자에게 공개되지 않도록 보호	2.5.2 2.5.3	3.6.18 3.6.19 3.6.21 3.6.22 3.6.23 3.6.24 3.6.25 3.6.26
		6.3.2	네트워크 접근통제	o 전자서명인증사업자는 전자서명인증업무 관련 시스템 및 보안시스템의 네트워크에 대한 접근통제 대책을 마련하고 이행하여야 한다. - 원격 접속 시 허가된 관리자(운영자)에게만 접근권한이 부여 - 원격 접속 시 인증 과정 존재 - 내부 네트워크는 외부 도메인의 비인가 접근으로부터 보호하기 위한 통제(예: 방화벽) 적용 여부 - 진단포트로의 접근은 엄격히 통제 - 인가된 사용자의 가용성을 확보하기 위하여 접근 통제 정책에 따라 네트워크 서비스를 제한할 수 있는 통제 - 전자서명인증사업자는 로컬 네트워크 구성요소를 물리적으로 안전한 환경에서 관리하고, 구성 요구사항에 맞추어서 주기적으로 점검	2.6.1 2.6.6	3.6.9 3.6.10 3.6.11 3.6.12 3.6.14 3.6.15 3.6.16 3.6.17
		6.3.3	데이터베이스 접근통제	o 전자서명인증사업자는 전자서명인증업무 관련 시스템의 데이터베이스에 대한 접근통제 대책을 마련하고 이행하여야 한다. - 데이터베이스의 테이블 목록 등 저장·관리되고 있는 정보를 식별 - 데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근통제 정책에 따라 통제 - 데이터베이스에 직접 접근 시 접근권한 구분 및 안전한 로그인 절차 이행	2.6.4	3.6.20 3.6.22 3.6.27 3.6.28 3.6.29
		6.3.4	정보시스템 접근통제	o 전자서명인증사업자는 정보시스템(하이퍼바이저, OS, DBMS, 네트워크 장비 등)에 대한 별도의 운영규정을 두어 관리하여야 한다. - 정보시스템은 전자서명인증사업자의 시스템 설정 표준을 준수하여 설정되어 있으며, 주기적으로 검토 및 업데이트 - 정보시스템의 패치 및 업데이트는 위험 평가에 기반하여 필요하다고 여겨질 때 적시적으로 적용되어야 하며 공식적인 변경 관리 절차를 따라 진행	-	3.6.20 3.6.22 3.6.27 3.6.28 3.6.29
7. 개발 보안						
7.1	시스템 개선 및 변경	7.1.1	시스템 개선 및 변경	o 전자서명인증사업자는 시스템 개선이나 신규 시스템 도입 시 통제 절차를 수립하여야 한다. - 신규 시스템 도입이나 시스템 개선 시 통제 절차를 마련 - 하드웨어, 네트워크 구성요소 및 시스템 설정 변경을 위한 변경 통제 절차를 수립하고 준용 - 테스트 데이터가 보호되고 통제 - 운영시스템(OS)의 변경이 있을 시, 응용시스템이 검토되고 테스트 되도록 절차 마련	2.8.1	3.7.1 3.7.2 3.7.3 3.7.4 3.7.6
		7.1.2	소프트웨어 변경 관리	o 전자서명인증사업자는 정보시스템의 오류 위험을 최소화하기 위해 소프트웨어의 변경에 대해서 엄격하게 통제하여야 한다. - 소프트웨어 테스트 및 변경 통제 절차가 존재 - 소프트웨어 패키지의 수정을 제한하고 모든 변경을 엄격하게 통제	2.8.1 2.9.1	3.7.7 3.7.8 3.7.9
		7.1.3	보안성 검토	o 시스템 및 소프트웨어의 변경사항 적용 시 테스트 실시, 보안성 확인 등 안전성을 검증하여야 한다. - 소프트웨어의 구매, 사용, 변경은 통제되며, 악성코드 등의 포함 여부를 확인하는 보안성 검토 절차 마련. 이러한 통제들이 아웃소싱된 소프트웨어 개발에도 동일하게 적용	2.8.2	3.7.6
7.2	프로그램 소스코드 보호	7.2.1	프로그램 소스코드 접근통제	o 프로그램 소스 라이브러리에 대한 접근통제를 수행하여야 한다. - 프로그램 소스 라이브러리에 대한 접근통제	2.8.5	3.7.5
		7.2.2	프로그램 소스코드 형상관리	o 프로그램 소스 라이브러리에 대한 형상관리를 수행하여야 한다. - 프로그램 소스 라이브러리에 대한 형상관리	2.8.5	

8. 업무 연속성 관리						
8.1	업무 연속성 계획	8.1.1	업무 연속성 계획	o 전자서명인증사업자는 장애 및 재해로부터 업무 연속성 확보를 위해 위험평가에 기초한 연속성 계획을 마련하여야 한다. - 전자서명인증사업자의 업무 연속성 계획에 다음이 포함 a) 대체시스템 가동 절차 b) 복구 및 재개 절차 c) 업무분장, 책임 및 역할 d) 비상연락체계 e) 복구 시간 목표(RTO) 및 복구지점 목표(RPO) f) 계획 실행을 위한 조건 g) 응급 절차 h) 계획에 대한 유지관리 일정 i) 홍보 및 교육 요건 j) 개인의 책임 k) 긴급 사태 대책에 대한 정기적인 테스트 - 업무 연속성 계획에 전자서명인증업무 관련 시설에 대해서, 재난 발생 후 그리고 메인 시설 또는 원격지의 안전한 환경을 복원하기 전까지의 시설보안 절차 포함 - 업무 연속성 계획에 컴퓨팅 리소스, 소프트웨어 및 (또는) 데이터가 손상되거나 손상이 의심되는 경우 사용되는 복구 절차	2.12.1	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	o 업무 연속성 계획을 정기적으로 테스트하여 변화 사항을 반영하여 갱신하여야 한다. - 업무 연속성 계획의 유효성 유지를 위하여 주기적으로 테스트하여 유효성을 유지하도록 갱신 - 업무 연속성 계획은 주기적으로 검토되고 갱신	2.12.2	3.8.10 3.8.11
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 마련하여야 한다. - 장애 및 재해 발생 시 업무가 복구될 수 있도록 마련된 대체 백업 시설 존재(단, 내부 절차에는 물리적 공간 확보, 시스템 장비 마련 및 복구 절차, 물리적/논리적 보안 조치 방안 등이 포함되어야 하며 절차에 따른 타당한 목표 복구 시간이 설정되어야 함) - 복구 장치와 백업 미디어는 메인 시설의 재해로부터 손상 및 피해를 피하기 위해 안전한 거리에 위치 - 대체 백업 시설에 대한 보안 수준이 메인 시설과 동등한 수준으로 유지 - 필수 사업 정보의 백업 사본이 정기적으로 발생하여야 하며, 이러한 백업 사본에 대한 보안요구사항은 백업된 정보와 동일한지 여부	2.9.3	3.8.3 3.8.4 3.8.5
9. 감사 로그						
9.1	감사로그 생성	9.1.1	감사로그 생성	o 전자서명인증사업자는 전자서명생성정보·인증서·암호화 장치(HSM) 등과 관련된 감사로그를 생성하고 위험평가 및 관계 법령에서 요구하는 특정한 기간 동안 보관할 수 있도록 하여야 한다. - 모든 입력 기록이 다음 사항을 포함 a) 입력 날짜와 시간 b) 입력 일련번호 (자동 입력에 대해) c) 입력의 종류 d) 입력소스 (예, 터미널, 포트, 장소, 가입자, 등) e) 입력을 개체의 사용		
				- 전자서명인증사업자가 키의 생명 주기 관리와 관련된 주요 이벤트를 기록 a) 인증기관 key의 생성 b) 인증기관 key 백업 c) 인증기관 key(백업key) 보관 d) 인증기관 key 복구 e) 인증기관 key escrow activities (해당 사항이 있는 경우) f) 인증기관 key 사용 g) 인증기관 key 파기 h) 인증기관 key 전송(해당 사항이 있는 경우) i) 인증기관 key 마이그레이션(해당 사항이 있는 경우) j) 암호화 장치(HSM) Key(또는 토큰) 사용(반출) 및 보관(반입) k) 암호화 장치(HSM) 관리		

				- 전자서명인증사업자가 다음 암호화 장치(HSM)의 생명 주기와 관련된 주요 이벤트를 기록 a) 암호화 장치(HSM)의 습득과 설치 b) 저장매체에 저장 또는 추출 c) 암호화 장치(HSM)의 활성화 d) 암호화 장치(HSM)의 파기 및 제거 e) 서비스 또는 수리에 맡김		
				- 전자서명인증사업자가 가입자의 Key 관리 서비스를 제공하는 경우, 가입자 Key의 생명 주기와 관련된 주요 이벤트를 기록 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	2.9.4 2.9.6	3.10.1 3.10.2 3.10.3 3.10.5 3.10.6 3.10.7 3.10.8 3.10.9
				- 전자서명인증사업자 또는 등록대행기관에서 인증서 신청 정보를 기록 a) 신원확인 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) 신원 증빙 문서를 검증하는 방법 (해당사항이 있는 경우) e) 수령하는 CA 또는 제출하는 RA의 이름 (해당사항이 있는 경우) f) 가입자의 서비스 이용/가입 동의 g) 개인정보 기록 및 소유, 지정된 제3자에 제공, 인증서 발급 등에 대한 동의 내역		
				- 전자서명인증사업자가 인증서 생명 주기와 관련된 주요 이벤트를 기록 a) 인증서 요청의 접수 - 인증서 발급 요청, 갱신 요청, 재발급 요청 포함 b) 가입자의 공개키 제출 c) 가입자 정보 변경 d) 인증서 발급 e) 인정기관의 공개키 배부 f) 인증서 폐지 요청 g) 인증서 폐지 h) 인증서 효력 정지 요청 (해당사항이 있는 경우) i) 인증서 효력 정지 j) 인증서 효력 회복 k) 인증서 갱신		
				- 전자서명인증사업자가 보안에 민감한 이벤트를 기록 a) 보안에 민감한 파일 또는 기록의 조회(감사기록 포함) b) 보안에 민감한 데이터에 대해 행해진 모든 행위 c) 보안 프로파일 변경 내역 d) 신원 인증 메커니즘의 사용 e) 시스템 충돌, 하드웨어 에러 및 기타 비정상 이벤트 f) 신뢰 행위자, 컴퓨터 운영자, 시스템 관리자, 시스템 보안 책임자 등이 수행한 행위 g) 개체의 소속 변경 h) 인증시스템 또는 관련 구성요소에 대한 접근 - 감사로그에는 개인키를 어떠한 형태로도 포함하지 않는지 여부(예: 일반 텍스트 또는 암호화 형태)		

9.2	감사로그 관리	9.2.1	감사로그 무결성 검증	o 전자서명인증사업자는 감사로그를 변경, 대체, 승인되지 않은 파기 등으로부터 보호되도록 관리하고 무결성 검증하여야 한다. - 현재 및 보관된 감사로그는 변경, 대체, 승인되지 않은 파기 등으로부터 보호되도록 관리 - 감사로그의 무결성을 보호하기 위한 전자서명 등이 적용되고 있는지 여부 - 감사로그를 서명하는 키는 해당 용도로만 사용되고 다른 용도로는 사용되지 않는지 여부 - 감사로그의 보유기간이 관련 법령과 더불어 위험평가를 통해 지정	2.9.4	3.10.10 3.10.11 3.10.12 3.10.13 3.10.14 3.10.15 3.10.16 3.10.17
		9.2.2	감사로그 검토	o 전자서명인증사업자는 감사로그의 승인되지 않거나 의심되는 기록 등에 대해 주기적으로 검토하여야 한다. - 감사로그는 전자서명인증업무준칙에 준거하여 주기적으로 검토되고 있는지 여부	2.9.5 2.11.3	3.10.8
		9.2.3	감사로그 백업	o 감사로그에 대한 백업 및 접근통제 절차를 수립 이행하여야 한다. - 전자서명인증업무 관련 정책이나 전자서명인증업무준칙에 준거하여 감사로그는 주기적으로 백업 및 보관 - 감사로그의 백업을 안전한 별도의 장소에 보관하여야 하며, 위험평가 및 법령에서 요구되는 특정 기간 동안 보관 - 승인된 인원만이 타당한 사업 또는 보안상의 사유로 감사로그 및 보관 중인 감사로그를 열람 여부 - 장애 및 재해 발생 시 업무가 복구될 수 있도록 마련된 대체 백업 시설이 있는지 여부	2.9.4	3.10.14 3.10.17

C. 개인정보 보호조치

항목		세부항목		내용	ISMS-P
1. 관리체계 수립 및 운영					
1.1	관리체계 기반 마련	1.1.1	최고책임자의 지정	o 전자서명인증사업자는 개인정보보호업무를 총괄하는 개인정보 보호책임자를 지정하여야 한다.	1.1.2
		1.1.2	정책 수립	o 전자서명인증사업자는 개인정보보호 정책을 실행하기 위한 내부 관리계획을 수립 및 시행하여야 한다.	-
		1.1.3	주요 직무자 지정 및 관리	o 전자서명인증사업자는 개인정보 및 중요정보의 취급이나 주요 시스템 접근 등 주요 직무의 기준과 관리방안을 수립 하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다.	2.2.1
		1.1.4	직무 분리	o 전자서명인증사업자는 개인정보취급자의 권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다.	2.2.2
1.2	위험 분석	1.2.1	개인정보 식별	o 전자서명인증사업자는 업무특성에 따라 개인정보 분류기준을 수립하여 관리체계 범위 내 모든 개인정보를 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.	1.2.1
		1.2.2	현황 및 흐름 분석	o 전자서명인증사업자는 개인정보보호 관리체계 내 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.	1.2.2
1.3	관리체계 운영	1.3.1	관리체계 점검	o 전자서명인증사업자는 내부 관리계획이 효과적으로 운영되고 있는지 확인하기 위해 연 1회 이상 내부 관리계획의 이행 실태를 점검·관리하고 개인정보 보호책임자에게 보고하여야 한다. - 식별된 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행 - 개선 결과의 정확성과 효과성 여부를 확인	-
2. 개인정보 처리 단계별 요구사항					
2.1	개인정보 수집 시 보호조치	2.1.1	개인정보 수집 제한	o 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.	3.1.2
		2.1.2	개인정보 수집 동의	o 전자서명인증사업자는 정보주체(가입자)의 동의를 받거나 관계 법령에 따라 개인정보를 적법하게 수집하여야 하며, 만 14세 미만 아동의 개인정보를 수집하려는 경우에는 법정대리인의 동의를 받아야 한다.	3.1.1
		2.1.3	주민등록번호 처리 제한	o 전자서명인증사업자는 법적 근거가 있는 경우를 제외하고는 주민등록번호를 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.	3.1.3
		2.1.4	민감정보 및 고유식별정보 처리 제한	o 전자서명인증사업자는 민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체(가입자)의 별도 동의를 받아야 한다.	3.1.4
		2.1.5	간접수집 보호조치	o 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 및 동의 철회 권리를 알려야 한다.	3.1.5
2.2	개인정보 보유 및 이용 시 보호조치	2.2.1	개인정보 현황 관리	o 전자서명인증사업자는 수집·보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 한다.	3.2.1
		2.2.2	개인정보 품질 보장	o 전자서명인증사업자는 개인정보 처리 목적에 따라 개인정보의 정확성·완전성·최신성을 보장하기 위한 관리절차를 마련하고, 이를 정보주체에게 알려야 한다.	3.2.2
		2.2.3	개인정보 표시제한 및 이용자 보호조치(1)	o 전자서명인증사업자는 개인정보 처리 시 목적에 따라 출력 항목 최소화, 개인정보 표시제한, 출력물 보호조치 등을 수행하여야 한다. - 불필요해진 개인정보는 삭제 또는 식별할 수 없도록 조치 - 개인정보를 종이로 출력하는 경우 출력·복사물에 대하여 출력자·출력일시 표시 등의 보호대책 적용	2.6.3
		2.2.4	개인정보 표시제한 및 이용자 보호조치(2)	o 전자서명인증사업자는 개인정보 처리화면을 통한 개인정보 유·노출 등을 방지하기 위한 보호대책을 적용하여야 한다. - 개인정보 조회 시 강화된 검색조건 적용 - 개인정보 파일 다운로드 제한, 사유 입력 등의 보호대책 적용	2.6.3

		2.2.5	홍보 및 마케팅 보호조치	o 전자서명인증사업자는 마케팅을 목적으로 개인정보를 수집·이용하는 경우, 그 목적을 정보주체가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다.	3.1.7
		2.2.6	이용자 단말기 접근 보호	o 전자서명인증사업자는 정보주체의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 접근이 필요한 경우 이를 명확하게 인지할 수 있도록 알리고 정보주체의 동의를 받아야 한다.	3.2.3
2.3	개인정보 제공 시 보호조치	2.3.1	개인정보의 목적 외 이용 및 제공	o 전자서명인증사업자는 개인정보 수집 시 정보주체에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려 는 때에는 정보주체의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.	3.2.4
		2.3.2	개인정보의 제3자 제공	o 전자서명인증사업자는 개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정 에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.	3.3.1
		2.3.3	업무 위탁에 따른 정보주체 고지	o 전자서명인증사업자는 개인정보 처리 업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자(재수탁자 포함) 등 관련사항을 정보주체에게 알려야 한다. - 개인정보 처리 업무를 위탁 받은 수탁자가 관련 업무를 제3자에게 재위탁 하는 경우 위탁자 동의	3.3.2
		2.3.4	업무 위탁에 따른 관리 감독	o 전자서명인증사업자는 개인정보 처리 업무를 위탁하는 경우 수탁자가 개인정보를 안전하게 처리하는지를 주기적으로 관리·감독하여야 한다. - 수탁자에 대한 개인정보보호 교육 실시 - 수탁자 개인정보 처리 현황 점검	2.3.1
		2.3.5	영업의 양수 등에 따른 개인정보의 이전	o 전자서명인증사업자는 영업의 양도·합병 등으로 개인정보를 이전하거나 이전 받는 경우 정보주체 통지 등 적절한 보호조치를 수립·이행하여야 한다.	3.3.3
		2.3.6	개인정보의 국외 이전	o 전자서명인증사업자는 개인정보를 국외로 이전하는 경우 국외 이전에 대한 동의, 관련 사항에 대한 공개 등 적절한 보호조치를 수립·이행하여야 한다.	3.3.4
2.4	개인정보 파기 시 보호조치	2.4.1	개인정보 파기	o 전자서명인증사업자는 개인정보의 보유기간 및 파기 관련 정책을 수립하고 개인정보의 보유기간 경과, 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다. - 다만, 기술적 특성으로 파기하는 것이 현저히 곤란한 경우 더 이상 개인을 알아볼 수 없는 정보로 처리하여 복원이 불가능하도록 조치	3.4.1
		2.4.2	처리 목적 달성 후 보유 시 조치	o 전자서명인증사업자는 개인정보의 보유기간 경과, 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.	3.4.2
2.5	정보주체 권리보호	2.5.1	개인정보처리방침 공개	o 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.	3.5.1
		2.5.2	정보주체 권리보호	o 전자서명인증사업자는 정보주체가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의 철회 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.	3.5.2
		2.5.3	이용 내역 통지	o 전자서명인증사업자는 5만명 이상의 민감정보 또는 고유식별정보를 처리하거나 100만명 이상의 개인정보를 처리하는 경우, 개인정보의 이용·제공 내역이나 이용·제공 내역을 확인할 수 있는 정보시스템에 접속하는 방법 등을 주기적으로 정보주체에게 통지하여야 한다.	3.5.3
		2.5.4	개인정보 유출 등의 통지·신고	o 전자서명인증사업자는 전자서명인증사업자는 개인정보가 분실·도난·유출 되었음을 알게 되었을 때 관계 법령에서 정한 시한 내에 정보주체에게 알리고 관련 기관에 신고하여야 한다.	3.5.3
3. 보호대책 요구사항					
3.1	인증 및 권한 관리	3.1.1	개인정보취급자 계정 관리	o 전자서명인증사업자는 개인정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 개인정보처리시스템의 개인정보취급자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 개인정보취급자에게 개인정보 관련 책임이 있음을 규정화하고 인식시켜야 한다.	2.5.1 2.5.6
		3.1.2	개인정보취급자 식별	o 전자서명인증사업자는 개인정보취급자별로 책임추적성이 확보될 수 있도록 개인정보처리시스템의 개별 계정을 부여해야 하며, 계정을 공유하여 사용하는 경우 그 타당성을 검토하고 책임추적성 확보를 위한 대책을 수립하여야 한다. - 유일하게 구분할 수 있는 식별자 사용, 추측 가능한 식별자 사용 제한 - 계정 공유 시 타당성 검토 결과에 대한 책임자의 승인 및 책임추적성 확보 방안 마련	2.5.2

		3.1.3	개인정보취급자 인증(1)	o 전자서명인증사업자는 개인정보취급자 및 관리자를 대상으로 강화된 인증방식이 적용하여야 한다.	2.5.3
		3.1.4	개인정보취급자 인증(2)	o 전자서명인증사업자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 안전한 인증수단을 적용하여야 한다.	2.5.3
		3.1.5	비밀번호 관리(1)	o 전자서명인증사업자는 법적 요구사항, 외부 위협요인 등을 고려하여 개인정보취급자와 고객, 회원 등 정보주체가 사용하는 비밀번호 관리절차를 수립·이행하여야 한다. - 개인정보취급자와 정보주체가 안전한 비밀번호를 설정하여 사용할 수 있도록 비밀번호 작성 규칙을 적용	2.5.4
		3.1.6	비밀번호 관리(2)	o 전자서명인증사업자는 정보주체(가입자)가 비밀번호 변경 등 중요 정보 접근 시 비밀번호 재확인 등 추가적인 인증이 적용하여야 한다.	-
		3.1.7	계정 및 권한 관리	o 전자서명인증사업자는 개인정보처리시스템의 접근권한을 부여, 변경 또는 말소한 내역을 전자적으로 기록하고, 최소 3년간 보관하여야 한다.	2.5.6
3.2	시스템 및 서비스 보안관리	3.2.1	인터넷 접속 통제	o 전자서명인증사업자는 인터넷 홈페이지, P2P, 공유설정 등을 통해 개인정보가 노출되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 보호 조치하여야 한다.	2.6.7
		3.2.2	망분리	o 전자서명인증사업자는 관련 법령에 따라 인터넷 망분리 의무가 부과된 경우 망분리 대상자를 식별하여 안전한 방식으로 망분리를 적용하여야 한다.	2.6.7
		3.2.3	암호정책 적용(1)	o 전자서명인증사업자는 개인정보보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고, 중요 정보 또는 개인정보를 저장하거나 송·수신하는 경우 안전한 암호 알고리즘으로 암호화하여야 한다.	2.7.1
		3.2.4	암호정책 적용(2)	o 전자서명인증사업자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립 및 시행하여야 한다.	2.7.2
		3.2.5	로그 및 접속기록 관리	o 전자서명인증사업자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록을 보관·관리하여야 한다. - 최소 1년 이상 보관(다만, 5만명 이상 개인정보를 처리하거나 민감정보 또는 고유식별정보를 처리하는 경우 최소 2년 이상 보관) - 위변조 및 도난, 분실되지 않도록 별도 저장장치 등에 백업 보관 - 월 1회 이상 정기적으로 점검 - 접속기록에 필수 포함 항목 : 식별자, 접속일시, 접속지 정보, 처리한정보주체정보, 수행업무 - 접속기록의 위변조 방지조치 - 다운로드 사유 확인	2.9.5
		3.2.6	정보자산의 재사용 및 폐기	o 전자서명인증사업자는 정보자산의 재사용과 폐기 과정에서 개인정보 및 중요정보가 복구 및 재생되지 않도록 안전한 재사용 및 폐기 절차를 수립·이행하여야 한다.	2.9.7
		3.2.7	악성프로그램 등 방지(1)	o 전자서명인증사업자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며, 다음의 사항을 준수하여야 한다. - 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지 - 발견된 악성프로그램 등에 대해 삭제 등 대응 조치	2.10.9
		3.2.8	악성프로그램 등 방지(2)	o 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.	2.10.8
		3.2.9	관리용 단말기 보안	o 전자서명인증사업자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기(개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기)에 대한 안전조치를 하여야 한다. - 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 - 본래 목적 외로 사용되지 않도록 조치 - 악성프로그램 감염 방지 등을 위한 보안조치 적용	2.10.6
		3.2.10	취약점 점검 및 조치	o 전자서명인증사업자는 인터넷 홈페이지 취약점으로 인한 개인정보의 유출, 변조, 훼손 등을 방지하기 위하여 웹서버 및 응용프로그램에 대한 취약점 점검 및 대응조치를 적용하여야 한다.	-
		3.2.11	시험 데이터 보안	o 전자서명인증사업자는 개발환경을 통한 개인정보의 유출을 방지하기 위하여 시험(테스트)데이터 생성·이용·파기 및 기술적 보호조치 등에 관한 대책을 적용하여야 한다.	-
		3.2.12	보조저장매체 관리	o 전자서명인증사업자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고, 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보호대책을 마련해야 한다.	2.10.7

3.3	물리 보안	3.3.1	영상정보처리기기 설치 운영(1)	o 전자서명인증사업자는 고정형 영상정보처리기기를 공개된 장소에 설치·운영하는 경우 설치 목적 및 위치에 따라 법적 요구 사항(안내판 설치 등)을 준수하고, 적절한 보호대책을 수립·이행하여야 한다.	3.1.6
		3.3.2	영상정보처리기기 설치 운영(2)	o 전자서명인증사업자는 고정형 영상정보처리기기를 공개된 장소에 설치·운영하는 경우 영상정보처리기기를 임의 조작하거나 녹음 기능을 사용하여서는 안 된다.	-
		3.3.3	영상정보처리기기 설치 운영(3)	o 전자서명인증사업자는 고정형 영상정보처리기기를 공개된 장소에 설치·운영하는 경우 영상정보처리기기에 대한 운영 및 관리방침을 수립하여야 한다.	3.1.6
		3.3.4	영상정보처리기기 설치 운영(4)	o 전자서명인증사업자는 고정형 영상정보처리기기를 공개된 장소에 설치·운영하는 경우 영상정보처리기기 관리 위탁 시 개인정보보호에 필요한 전문장비 및 기술을 갖춘 기관을 선정하도록 하여야 한다.	3.1.6
3.4	부가 서비스 보안	3.4.1	RFID(1)	o 전자서명인증사업자는 RFID 태그에 기록된 개인정보를 수집하는 경우 이용자에게 통지하거나 알아보기 쉽게 표시하여야 한다.	-
		3.4.2	RFID(2)	o 전자서명인증사업자는 RFID 태그의 물품정보 등과 개인정보를 연계하는 경우 그 사실을 이용자에게 통지하거나 알기 쉽게 표기되도록 하여야 한다.	-
		3.4.3	RFID(3)	o 전자서명인증사업자는 RFID 태그의 물품정보 등과 개인정보를 연계하여 생성된 정보를 수집 목적 외로 이용하거나 제3자에게 제공할 경우 이용자의 동의를 얻어야 한다.	-
		3.4.4	RFID(4)	o 전자서명인증사업자는 RFID태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우 설치 사실을 이용자가 인식하기 쉽게 표기하여야 한다.	-
		3.4.5	RFID(5)	o 전자서명인증사업자는 구입 및 제공받은 물품에 RFID태그가 내장 및 부착 되어 있을 경우 부착 위치, 기록정보 및 기능에 대해 표시하여야 한다.	-
		3.4.6	RFID(6)	o 전자서명인증사업자는 RFID 태그가 내장 및 부착되어 있는 경우 판매 혹은 제공하는 자로부터 태그 기능을 제거할 수 있는 방법 또는 수단을 제공하여야 한다.	-
		3.4.7	RFID(7)	o 전자서명인증사업자는 이용자의 신체에 RFID를 지속적으로 착용하지 않아야 한다.	-
		3.4.8	위치정보(1)	o 전자서명인증사업자는 개인위치정보 수집 시 정보주체 또는 위치정보 수집장치 소유자에 대해 사전고지와 명시적 동의를 거치도록 하여야 한다.	-
		3.4.9	위치정보(2)	o 전자서명인증사업자는 개인위치정보를 정보주체가 지정하는 제3자에게 제공하는 경우에는 개인위치 정보주체에게 제공받는 자, 제공일시 및 제공목적을 통보하여야 한다.	-
		3.4.10	클라우드 보안(1)	o 전자서명인증사업자는 클라우드 서비스에 대하여 격리 실패 현상을 방지하여야 한다.	-
		3.4.11	클라우드 보안(2)	o 전자서명인증사업자는 클라우드 서비스 제공자의 관리 인터페이스에 대하여 보안 관리하여야 한다.	-
		3.4.12	클라우드 보안(3)	o 전자서명인증사업자는 클라우드 이용자의 데이터 삭제 요청에 따라 적절한 데이터 삭제를 통해 개인정보 재사용을 방지하여야 한다.	-
		3.4.13	클라우드 보안(4)	o 전자서명인증사업자는 클라우드 특성을 고려한 모니터링을 수행하여야 한다.	-
		3.4.14	생체인식정보(1)	o 전자서명인증사업자는 수집된 생체인식 원본정보와 제공자를 알 수 있는 신상정보(성명, 연락처 등)를 별도로 분리하여야 한다.	-
		3.4.15	생체인식정보(2)	o 전자서명인증사업자는 생체인식 원본정보의 경우 특징정보 생성 후 지체 없이 파기하여 복원할 수 없도록 하여야 한다.	-
		3.4.16	생체인식정보(3)	o 전자서명인증사업자는 생체인식정보의 불법 유출·위변조 등을 방지하기 위한 기술적·관리적 보호조치를 취하여야 한다.	-
		3.4.17	생체인식정보(4)	o 전자서명인증사업자는 위·변조된 생체인식정보 수집 및 입력에 대한 대책을 마련하여야 한다.	-
		3.4.18	생체인식정보(5)	o 전자서명인증사업자는 생체인식정보 수집 및 입력 시, 전송구간을 보호하여야 한다.	-
		3.4.19	생체인식정보(6)	o 전자서명인증사업자는 저장 및 송·수신 단계에서 생체인식정보에 대한 암호화 조치를 취하여야 한다.	-
		3.4.20	생체인식정보(7)	o 전자서명인증사업자는 생체인식정보의 저장 및 이용 단계에서 기기 내 안전한 매체를 활용하여 처리할 수 있도록 하여야 한다.	-
		3.4.21	블록체인	o 전자서명인증사업자는 퍼블릭 블록체인의 익명성을 보장하기 위한 기술적 대책을 적용하여야 한다.	-