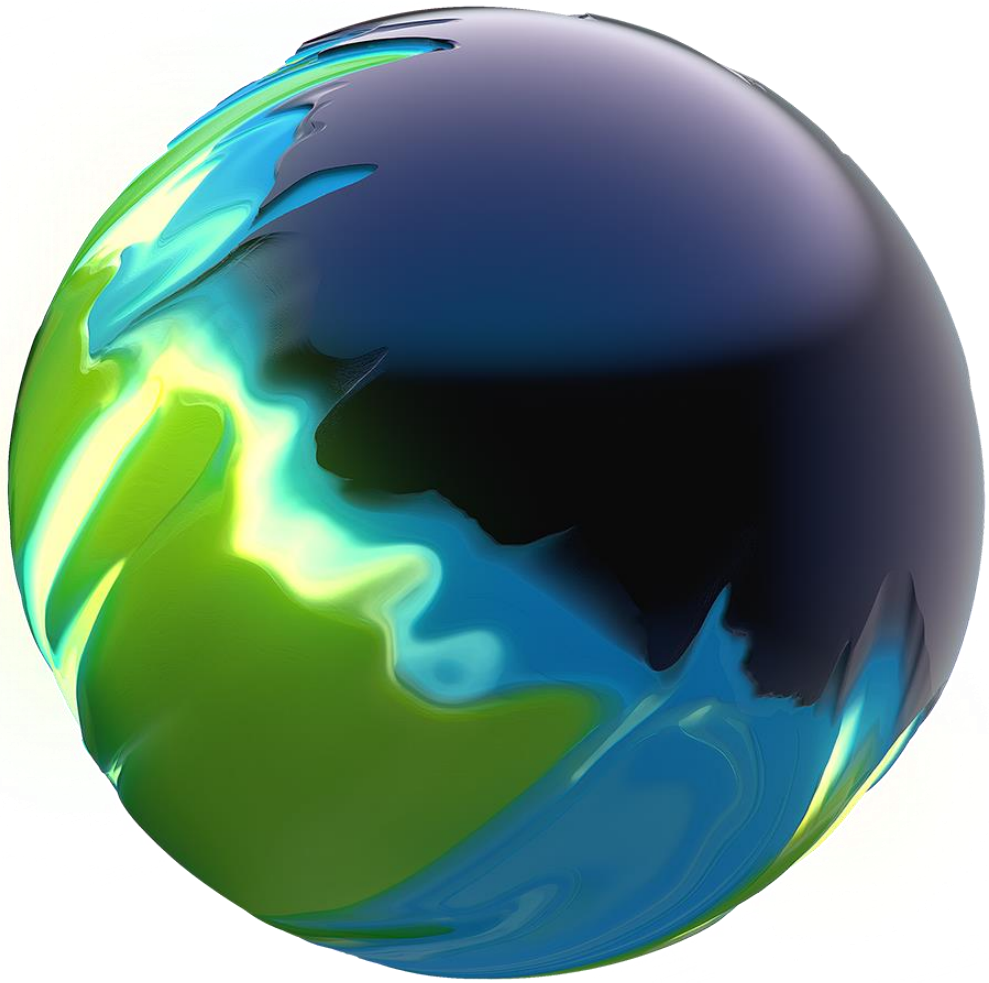
Deloitte.



딜로이트 안진회계법인

전자서명인증업무 평가 안내서 개정이력

Deloitte Anjin LLC, July 2024, v1.4.0

목차

1. 전자서명인증업무 평가 안내서(v1.4.0) 개정이력

구분	v1.3.6 (2024 년 3 월)		v1.4.0 (2024 년 7 월)	
[첨부] 별첨 1	신규		11.1	전자서명인증사업자는 가입자의 신원확인 정보가 위변조 되지 않도록 무결성과 기밀성을 보장할 수 있는 안전한 서비스 환경을 구현하여야 한다.
	신규		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.
	신규		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
[첨부] 별첨 3	1.1	최고책임자 지정 전자서명인증사업자의 최고경영자는 개인정보보호 업무를 총괄하는 개인정보보호책임자를 지정하여야 한다. • 개인정보보호책임자의 자격 요건, 업무 및 역할을 확인 (전자서명인증 관련 업무 포함) • 개인정보보호책임자가 내부 인사 발령 등 공식적인 절차를 통해 지정되었는지 확인	1.1	최고책임자 지정 전자서명인증사업자의 최고경영자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보보호책임자를 직위 및 자격 요건을 갖춘 자로 지정하여야 한다.

구분	v1.3.6 (2024 년 3 월)		v1.4.0 (2024 년 7 월)	
[첨부] 별첨 3	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 요구권리를 알려야 한다.** (생략)	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.** (생략)
	4.17	업무 위탁에 따른 정보주체 고지 전자서명인증사업자는 개인정보 처리업무를 제 3 자에게 위탁하는 경우 위탁하는 업무의 내용과 **수탁자 등 관련사항을 정보주체(이용자)에게 알려야 한다.** • 인터넷 홈페이지 등에 위탁하는 업무의 내용과 수탁자를 현행화하여 공개하고 있는지 확인 **• 동의가 필요한 경우 처리 위탁을 받은 자와 위탁하는 업무의 내용을 알리고 동의를 받고 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	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
	4.18	업무 위탁에 따른 관리 감독 **전자서명인증사업자는 업무 위탁 시, 수탁사의 관리/감독 활동을 계획하고 이행하고 있는지 확인하여야 한다.** **• 수탁사에 대한 주기적인 관리 현황 검토 여부 확인** **• 수탁자가 위탁 받은 업무를 제 3 자에게 재위탁하는 경우 위탁자의 사전 동의 여부 확인**	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**

구분	v1.3.6 (2024 년 3 월)		v1.4.0 (2024 년 7 월)	
[첨부] 별첨 3	4.23	개인정보 파기 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. 단, 법령에 의거하여 보존하여야 하는 경우에는 파기하지 않고 보존하여야 한다. (생략)	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. (생략)
	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 이용자 정보주체의 개인정보처리시스템에 접속하려는 경우, 안전한 인증수단(인증서, 보안토큰, 일회용 비밀번호)을 적용하는지 확인 • 개인정보취급자가 정보통신망을 통해 외부에서 이용자가 아닌 정보주체의 개인정보처리시스템에 접속하려는 경우, 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단(인증서, 보안토큰, 일회용 비밀번호)을 적용하는지 확인	6.4	사용자 인증 전자서명인증사업자는 개인정보 처리 시 개인정보취급자 및 관리자를 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.
	6.9	망분리 전자서명인증사업자는 관련 법령에 따라 인터넷 망분리 의무가 부과된 경우 망분리 대상자를 식별하여 안전한 방식으로 망분리를 적용하여야 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.

구분	v1.3.6 (2024 년 3 월)		v1.4.0 (2024 년 7 월)	
[첨부] 별첨 3	6.10	암호정책 적용 (생략) • 인터넷 등 공개된 정보통신망을 통해 개인정보를 송·수신하는 경우 암호화하고 있는지 확인 • 생체인식정보, 비밀번호를 정보통신망을 통해 개인정보를 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	6.11	암호정책 적용 (생략) • 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	로그 및 접속기록 관리 전자서명인증사업자는 관련 법령에서 요구하는 바에 따라 접속기록을 관리하여야 한다. • 개인정보처리시스템의 접속기록을 월 1 회 이상 정기적으로 점검하는지 확인 • 개인정보 다운로드, 과도한 개인정보 조회 등 위험 행위에 대한 점검을 수행하는지 확인 • 접속 기록을 최소 1 년 이상 보관하고 위·변조 및 도난, 분실되지 않도록 별도 저장장치에 백업 등 조치를 적용하는지 확인 • 기간통신사업자이거나 5 만명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2 년 이상 보관·관리하는지 확인	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 • 접속기록을 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

구분	v1.3.6 (2024 년 3 월)		v1.4.0 (2024 년 7 월)	
[첨부] 별첨 3	6.14	단말기 보안 전자서명인증사업자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 단말기에 대한 안전조치를 적용하도록 계획하여야 한다. • 개인정보 유출 등 침해사고 방지를 위하여 **관리용 단말기**에 대해 안전조치를 취하고 있는지 확인 • **관리용** 단말기의 분실·도난 등으로 개인정보가 유출되지 않도록 비밀번호 설정 등의 보호조치를 적용하고 있는지 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

2. 전자서명인증업무 평가 안내서(v1.3.6) 개정이력

구분	v1.3.5 (2024 년 3 월)		v1.3.6 (2024 년 7 월)	
[첨부] 별첨 2	2.2.2	자산 통제 전자서명인증사업자는 분류된 자산 및 정보자료를 위협으로부터 적절한 수준의 보호를 받을 수 있도록 통제 절차를 마련하여야 한다. • 전자서명인증사업자가 분류된 자산 및 정보자료에 대한 위험 분석을 수행하였는지 확인 • 전자서명인증사업자가 사업의 요구사항 및 사업에 미치는 영향에 따라 조직 내에서 사용되고 있는 자산의 적절한 사용을 위한 규칙을 문서화하였는지 확인	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
[첨부] 별첨 3	8.1	개인정보 파기 전자서명인증사업자가 공공기관이면서 개인정보파일을 파기하는 경우, 관련 법령에 따라 안전하게 관리하여야 한다. • 개인정보파일 파기 관리대장을 작성하여 관리하고 있는지 확인 • 행정안전부에 등록된 개인정보파일 목록 등도 함께 삭제될 수 있도록 하고 있는지 확인	8.1	개인정보 파기 전자서명인증사업자가 공공기관이면서 개인정보 파일을 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

3. 전자서명인증업무 평가 안내서(v1.3.5) 개정이력

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 1	**공통**	평가 항목의 연변 기준 3 단계	**공통**	평가 항목의 연변 기준 2 단계
	2.1.1 2.1.2 2.1.3	-	2.1	전자서명인증서비스는 이용자가 가입자 (서명자)의 신원을 식별할 수 있도록 전자서명 인증업무준칙에 명시된 대로 다양한 방법으로 연계정보(CI), VID, DN, 이메일 주소 등을 사용하여 가입자 (서명자)의 식별정보를 제공해야한다. *[예시] 인증서에 가입자(서명자)의 식별 정보를 넣어 발급하는 기능* *[예시] 이용자의 전자서명 생성 요청 시, 이용자에게 가입자의 전자서명과 연계정보 (CI)를 전달하는 기능*
	2.2.1 2.2.2 2.2.3 2.2.4	-	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* • 전자서명인증시스템은 가입자의 전자서명 생성정보 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

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 1	2.4.1 2.4.2 2.4.3	-	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*
	2.5.1 2.5.2 2.5.3	-	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

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 1	2.6.1 2.6.2	-	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
	3.1.1 3.1.2	-	3.1	전자서명인증사업자는 법 제 15 조에 따른 전자서명 인증업무준칙을 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

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 1	3.3.1 3.3.2 3.3.3	-	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*
	3.4.1 3.4.2	-	3.4	전자서명인증사업자는 자신이 제공하는 전자서명 인증서비스와 관련된 인증기관이 있는 경우, 해당 기관과의 정책 일관성을 위해 전자서명인증 업무준칙의 제·개정시 이에 대해 협의하여야 한다. • 전자서명인증사업자가 제공하는 전자서명 인증서비스와 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 전자서명 인증서비스와 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*

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 1	4.1.1 4.1.2 4.1.3 4.1.4 4.1.5	-	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
	4.2.1	-	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. ※ [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

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 1	4.5.1 4.5.2 4.5.3 4.5.4	-	4.5	전자서명인증사업자는 등록대행기관으로부터 정보통신망으로 가입자의 등록정보를 전송받는 경우, 가입자의 등록정보가 위·변조되지 않도록 조치를 취하여야 하며, 등록정보가 유출되지 않도록 대책을 마련하여야 한다. • 전자서명인증사업자는 등록대행기관으로부터 정보통신망으로 가입자의 등록정보를 전송받는 경우, 가입자의 등록정보가 위·변조되지 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
	5.4.1 5.4.2	-	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

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 1	6.1.1 6.1.2	-	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 출입통제장치 및 감시시스템을 설치하고, 출입 자격을 최소 인원으로 유지한 장소에서 전자서명인증업무준칙에 규정된 절차에 따라 전자서명생성정보를 생성*
	6.2.1 6.2.2 6.2.3 6.2.4	-	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 전자서명생성정보를 생성*

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 1	6.4.1 6.4.2 6.4.3	-	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
	6.5.1 6.5.2	-	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*

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 1	7.1.1 7.1.2	-	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
	7.2.1 7.2.2	-	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
	7.3.1 7.3.2 7.3.3 7.3.4	-	7.3	전자서명인증사업자는 전자서명생성정보의 분실·훼손 또는 도난·유출 등을 방지하고 전자서명인증 업무를 계속하여 안정적으로 제공할 수 있도록 전자서명생성정보를 백업하여야 한다. • 전자서명인증사업자는 자신의 전자서명생성정보의 분실·훼손 또는 도난·유출 등을 방지하는지 확인 • 전자서명인증사업자가 가입자의 전자서명생성정보를 생성하는 경우, 전자서명인증 사업자는 가입자의 전자서명생성정보의 분실·훼손 또는 도난·유출 등을 방지하는지 확인 • 전자서명인증사업자는 자신의 전자서명생성정보를 백업하는지 확인 • 전자서명인증사업자가 가입자의 전자서명생성정보를 생성하는 경우, 전자서명인증 사업자는 가입자의 전자서명생성정보를 백업하는지 확인

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 1	7.4.1 7.4.2	-	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
	7.5.1 7.5.2	-	7.5	전자서명인증사업자는 백업된 전자서명생성 정보 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 저장 설비에 백업된 전자서명생성정보 중 1 부를 보관하는지 확인
	9.1.1 9.1.2 9.1.3 9.1.4	-	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

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 1	9.2.1 9.2.2 9.2.3 9.2.4 9.2.5 9.2.6 9.2.7	-	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 세부평가 기준"을 준용하는지 확인
	10.1 10.1.1	-	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*

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 3	**공통**	-	**공통**	개인정보보호법 개정 사항 반영 별첨 2 및 별첨 3 중복 통합
	1.1	최고책임자의 지정 전자서명인증사업자의 최고경영자는 개인 정보보호업무를 총괄하는 **개인정보보호 책임자를 임원급 이상으로 지정**하여야 한다. • 개인정보보호책임자의 업무 및 역할을 확인 (전자서명인증 관련 업무 포함) • 개인정보보호책임자가 내부 인사 발령 등 공식적인 절차를 통해 지정되었는지 확인	1.1	최고책임자의 지정 전자서명인증사업자의 최고경영자는 개인정보보호업무를 총괄하는 **개인정보보호 책임자를 지정**하여야 한다. • 개인정보보호책임자의 자격 요건, 업무 및 역할을 확인 (전자서명인증 관련 업무 포함) • 개인정보보호책임자가 내부 인사 발령 등 공식적인 절차를 통해 지정되었는지 확인
	1.2	조직 구성 전자서명인증사업자의 최고경영자는 개인 정보보호 관련 주요 사항을 검토 및 의결할 수 있도록 개인정보보호 담당자 및 관련 업무 담당자들로 구성된 협의체(혹은 위원회)를 구성하여 운영하여야 한다.	**삭제**	
	1.5	취급자 관리 감독 전자서명인증사업자는 개인정보취급자를 대상으로 역할 및 책임 부여, 개인정보보호 교육, 개인정보보호 서약서 작성 등의 관리 및 감독을 수행하여야 한다.	**삭제**	
	2.4	위험 평가 전자서명인증사업자는 대내외 환경분석을 통해 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1 회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.	**삭제**	

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 3	2.5	보호대책 선정 전자서명인증사업자는 위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 개인정보보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립한다.	삭제	
	2.6	보호대책 구현 전자서명인증사업자는 이행계획에 따라 개인정보보호대책을 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.	삭제	
	4.10	개인정보 유•노출 방지 전자서명인증사업자는 개인정보 처리화면(개인정보취급자 및 정보주체의 단말기)을 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 검색조건을 요구하는지 확인	4.10	개인정보 유•노출 방지 전자서명인증사업자는 개인정보 처리화면 및 공중망을 통한 개인정보 유·노출 등을 방지하기 위한 보호대책을 적용하여야 한다. • 개인정보파일 다운로드 제한 조치하는지 확인 • 개인정보 검색 시 과도한 정보가 조회되지 않도록 일치 검색 또는 두 가지 항목 이상의 검색조건을 요구하는지 확인 • 개인정보 노출여부를 정기적으로 점검하는지 확인
	신규		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.
	4.11	개인정보 비식별화 개인정보를 비식별화하여 이용·제공 시 재식별화의 위험을 최소화할 수 있도록 적절한 방법으로 비식별 조치를 수행하여야 한다. • 가명정보 처리 관련 규정 수립 여부 확인 • 재사용 방지, 암호화 등 안정성 확보 조치 여부 확인	4.12	개인정보 비식별화 개인정보를 비식별화하여 이용·제공 시 재식별화의 위험을 최소화할 수 있도록 적절한 방법으로 비식별 조치를 수행하여야 한다. • 가명정보 처리 관련 규정 수립 여부 확인 • 재사용 방지, 암호화 등 안정성 확보 조치 여부 확인 • 가명정보 처리 기록을 작성하여 보관하는지 확인 • 가명정보 파기한 경우, 파기한 날로부터 3 년이상 보관하는지 확인

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 3	4.20	개인정보의 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 • 개인정보보호 관련 법령 준수 및 개인정보보호 등에 관한 사항을 포함하여 국외 이전에 관한 계약을 체결하고 필요한 조치를 취하고 있는지 확인	4.20	개인정보의 국외 이전 전자서명인증사업자는 개인정보를 국외로 이전하는 경우 국외이전에 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
	4.21	휴면 이용자 관리 전자서명인증사업자는 일정기간 동안 서비스를 이용하지 않는 이용자의 개인정보를 보호하기 위하여 휴면 처리 사실을 통지하고, 개인정보의 파기 또는 분리 보관 등 적절한 보호조치를 이행하여야 한다.	삭제	
	4.22	개인정보처리방침 공개 전자서명인증사업자는 개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 개인정보 처리방침을 수립하고, 이를 정보주체 (이용자)가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화 하여야 한다. • 정보주체(이용자)가 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 정보주체(이용자)가 언제든지 변경 사항을 쉽게 알아볼 수 있도록 조치하고 있는지 확인	4.22	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

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 3	4.23	개인정보의 파기 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. • 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	4.23	개인정보의 파기 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. **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**
	5.1	정보주체 권리보장 전자서명인증사업자는 **정보주체(이용자)**가 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, **정보주체(이용자)**의 개인정보 처리 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 **정보주체(이용자)**의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다. (이하 생략)	5.1	정보주체 권리보장 전자서명인증사업자는 **정보주체**가 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, **정보주체**의 개인정보 처리 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 **정보주체**의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다. (이하 생략)

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 3	5.2	이용 내역 통지 법적 의무 대상자에 해당하는 경우 개인정보 이용내역을 주기적으로 통지하고 기록으로 남겨야 한다. • 개인정보 이용 내역을 정보주체(이용자)에게 통지하고 그 기록을 남기고 있는지 확인 • 통지 항목은 법적 요구항목을 모두 포함하고 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 방법을 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
	6.4	사용자 인증 전자서명인증사업자는 개인정보 처리 시 개인정보취급자 및 관리자를 대상으로 강화된 인증방식이 적용하여야 한다. • 개인정보취급자 및 관리자는 권한 도용 등을 방지하기 위하여 강화된 인증방식을 적용하고 있는지 확인 • 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우, 가상 사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하는지 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 이용자 정보주체의 개인정보처리시스템에 접속하려는 경우, 안전한 인증수단(인증서, 보안토큰, 일회용 비밀번호)을 적용하는지 확인 • 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 적용하는지 확인

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 3	6.5	비밀번호 관리 전자서명인증사업자는 법적 요구사항, 외부 위협요인 등을 고려하여 개인정보취급자와 고객, 회원 등 정보주체(이용자)가 사용하는 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	6.5	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	특수 권한 관리 전자서명인증사업자는 개인정보처리시스템에 대한 계정 및 권한을 안전하게 적용 및 관리하여야 한다.	삭제	
	6.8	불법 접근 제한 전자서명인증사업자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위한 조치를 적용하여야 한다.	삭제	
	6.9	접근권한 부여 내역 관리 전자서명인증사업자는 개인정보처리시스템의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3 년간 보관하여야 한다. (정보통신서비스제공자의 경우 5 년이상 보관)	6.9	접근권한 부여 내역 관리 전자서명인증사업자는 개인정보처리시스템의 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3 년간 보관하여야 한다.

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 3	6.12	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 • 고유식별정보, 생체인식정보, 비밀번호를 정보통신망을 통하여 송·수신하거나, 보조 저장매체 등을 통하여 전달하는 경우 암호화하고 있는지 확인 • 인터넷 등 공개된 정보통신망을 통해 개인정보를 송·수신하는 경우 암호화하고 있는지 확인	6.10	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 • 생체인식정보, 비밀번호를 정보통신망을 통해 개인정보를 송·수신하는 경우 암호화하고 있는지 확인 • 이용자의 개인정보, 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장하는 경우 암호화하고 있는지 확인
	6.13	암호키 관리 전자서명인증사업자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립 및 시행하여야 한다.	6.11	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.
	6.14	로그 및 접속기록 관리 전자서명인증사업자는 관련 법령에서 요구하는 바에 따라 접속기록을 관리하여야 한다. • 개인정보처리시스템의 접속기록을 월 1 회 이상 정기적으로 점검하는지 확인 • 대량 개인정보 다운로드, 과도한 개인정보 조회 등 위험 행위에 대한 점검을 수행하는지 확인 • 접속 기록을 최소 1 년 이상 보관하고 위·변조 및 도난, 분실되지 않도록 별도 저장장치에 백업 등 조치를 적용하는지 확인 • 기간통신사업자이거나 5 만명 이상의 정보주체(이용자)에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리 시스템의 경우에는 2 년 이상 보관· 관리하는지 확인	6.12	로그 및 접속기록 관리 전자서명인증사업자는 관련 법령에서 요구하는 바에 따라 접속기록을 관리하여야 한다. • 개인정보처리시스템의 접속기록을 월 1 회 이상 정기적으로 점검하는지 확인 • 개인정보 다운로드, 과도한 개인정보 조회 등 위험 행위에 대한 점검을 수행하는지 확인 • 접속 기록을 최소 1 년 이상 보관하고 위·변조 및 도난, 분실되지 않도록 별도 저장장치에 백업 등 조치를 적용하는지 확인 • 기간통신사업자이거나 5 만명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2 년 이상 보관·관리하는지 확인

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 3	6.15	정보자산의 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 중요 정보가 복구되지 않는 방법으로 처리하고 있는지 확인 • 외부업체를 통해 폐기할 경우 폐기 절차를 계약서에 명시하고 결과를 점검하는지 확인	6.13	정보자산의 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
	6.16	단말기 보안 전자서명인증사업자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 단말기에 대한 안전 조치를 적용하도록 계획하여야 한다. • 개인정보 유출 등 침해사고 방지를 위하여 관리용 단말기에 대해 안전조치를 취하고 있는지 확인 • 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 비밀번호 설정 등의 보호조치를 적용하고 있는지 확인	6.14	단말기 보안 전자서명인증사업자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 단말기에 대한 안전 조치를 적용하도록 계획하여야 한다. • 개인정보 유출 등 침해사고 방지를 위하여 관리용 단말기에 대해 안전조치를 취하고 있는지 확인 • 관리용 단말기의 분실·도난 등으로 개인정보가 유출되지 않도록 비밀번호 설정 등의 보호조치를 적용하고 있는지 확인
	신규		6.17	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

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 3	신규		6.18	보안 업데이트 및 패치 전자서명인증사업자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.
	6.19	백업 및 복구관리 전자서명인증사업자는 재해, 재난 발생 시를 대비한 계획을 마련하여야 한다.	삭제	
	7.1	보호구역 지정 전자서명인증사업자는 개인정보처리시스템 및 개인정보를 보관하고 있는 물리적 장소를 보호구역으로 지정하고 물리·환경적인 위협에 대응할 수 있도록 영상정보처리기기, 출입통제 장치, 화재경보기 등 보호설비를 설치·운영하여야한다.	삭제	
	7.2	영상정보처리기기 설치·운영 전자서명인증사업자는 영상정보처리기기 운영 시 안전한 보호조치를 적용하여야 한다. • 공개된 장소에 영상정보처리기기를 설치·운영할 경우 법적으로 허용한 장소 및 목적인지 확인 • 영상정보처리기기 설치·운영 시 정보주체(이용자)가 쉽게 인식할 수 있도록 안내판 설치 등 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	7.1	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

구분	v1.3.4 (2023 년 12 월)		v1.3.5 (2024 년 2 월)	
[첨부] 별첨 3	8.2	영상정보처리기기 운영 공공기관이 공개된 장소에 영상정보처리기기를 설치·운영하려는 경우 공청회·설명회 개최 등의 법령에 따른 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.	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
	신규		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

4. 전자서명인증업무 평가 안내서(v1.3.4) 개정이력

구분	v1.3.3 (2023 년 8 월)		v1.3.4 (2023 년 12 월)	
[첨부] 별첨 3	6.6	추가 인증 절차 전자서명인증사업자는 정보주체(이용자)가 인터넷 홈페이지 등을 통해 중요한 정보 또는 화면에 접근하려는 경우에는 비밀번호 재확인, 휴대폰 인증, 공인인증서 등 본인임을 확인할 수 있는 추가적인 인증 절차를 적용하여야 한다.	6.6	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.

5. 전자서명인증업무 평가 안내서(v1.3.3) 개정이력

구분	v1.3.2 (2023 년 4 월)		v1.3.3 (2023 년 8 월)	
[첨부] 별첨 1	4.2.1	⑤기타 이에 준하는 새로운 방식(바이오 인증 등) 중 "2 가지" 의무 적용	4.2.1	[참고] 금융회사 비대면 실명확인 시 신원확인방법 '⑤' 변경 ⑤기타 이에 준하는 새로운 방식(생체인증 등) 중 "2 가지" 의무 적용
	9.2	전자서명인증사업자가 법 시행령 제 13 조에 따라 연계정보(CI)를 처리하는 경우 다음 각 항의 사항을 수행하여야 한다.	9.2	전자서명인증사업자가 법 시행령 제 14 조에 따라 연계정보(CI)를 처리하는 경우 다음 각 항의 사항을 수행하여야 한다.
[첨부] 별첨 3	6.12	고유식별정보, 바이오정보, 비밀번호를 정보통신망을 통하여 송·수신하거나, 보조저장매체 등을 통하여 전달하는 경우 암호화하고 있는지 확인	6.12	고유식별정보, 생체인식정보, 비밀번호를 정보통신망을 통하여 송·수신하거나, 보조저장매체 등을 통하여 전달하는 경우 암호화하고 있는지 확인
	9.4	바이오 정보 • 전자서명인증사업자는 수집된 바이오 원본정보와 제공자를 알 수 있는 신상정보(성명, 연락처 등)를 별도로 분리하여야 한다. • 전자서명인증사업자는 원본정보의 경우 특징정보 생성 후 지체 없이 파기하여 복원할 수 없도록 하여야 한다. • 전자서명인증사업자는 바이오정보의 불법 유출·위변조 등을 방지하기 위한 기술적·관리적 보호조치를 취하여야 한다. • 전자서명인증사업자는 위·변조된 바이오정보 수집 및 입력에 대한 대책을 마련하여야 한다. • 전자서명인증사업자는 바이오정보 수집 및 입력 시, 전송구간을 보호하여야 한다. • 전자서명인증사업자는 저장 및 송·수신 단계에서 바이오정보에 대한 암호화 조치를 취하여야 한다. • 전자서명인증사업자는 저장 및 이용 단계에서 기기 내 안전한 매체를 활용하여 처리할 수 있도록 하여야 한다.	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

6. 전자서명인증업무 평가 안내서(v1.3.2) 개정이력

구분	v1.3.1 (2022 년 5 월)		v1.3.2 (2023 년 4 월)	
용어 정의	세부 평가 기준	운영기준 준수여부를 평가하기 위해 딜로이트 안진회계법인이 정한 평가기준을 말합니다.	세부 평가 기준	전자서명인증사업자가 제공하는 전자서명인증업무의 운영기준 준수여부를 평가하기 위해 딜로이트 안진회계법인이 정한 평가기준을 말합니다.
	발견 사항	평가 신청자가 세부평가기준의 요구사항을 충족하지 못한 사항을 말하며, 미비점이라고도 말합니다.	발견 사항	전자서명인증사업자가 세부평가기준의 요구사항을 충족하지 못한 사항을 말하며, 미비점이라고도 합니다.
세부 평가 기준	-	딜로이트 안진회계법인의 세부평가기준은 딜로이트 안진회계법인에 평가 관련 문의 및 상담 시 기준에 대한 정보를 제공해드립니다.	-	딜로이트 안진회계법인에 평가 관련 문의 및 상담 시, 딜로이트 안진회계법인의 세부평가기준에 대한 정보를 제공해드립니다.
문의처	이메일	krdeloitteracni@deloitte.com	이메일	krtrustesign@deloitte.com
[첨부] 별첨 1	공통	인증사업자	공통	전자서명인증사업자
	공통	인증업무준칙	공통	전자서명인증업무준칙
	공통	연계정보	공통	연계정보(CI)
	6.2.3	※ 안전한 암호 알고리즘 및 키 길이에 대한 요구사항은 본 세부평가기준 제 5 조제 5 항을 참고	6.2.3	삭제
	6.4.3	인정사업자는 가입자의 신청에 의하여 가입자의 전자서명생성정보를 보관하는 경우, 해당 가입자의 동의없이 이를 이용해서는 아니된다.	6.4.3	전자서명인증사업자는 가입자의 신청에 의하여 가입자의 전자서명생성정보를 보관하는 경우, 해당 가입자의 동의없이 이를 이용하거나 반출해서는 아니된다.
	8.1	인정사업자는 전자서명인증업무 관련 시설 및 자료의 보호를 위해 “별첨 2. 전자서명인증업무 관리적·물리적·기술적 세부평가기준”에 따른 보호조치를 수행하여야 한다.	8.1	전자서명인증사업자는 전자서명인증업무 관련 시설 및 자료의 보호를 위해 “별첨 2. 관리적·물리적·기술적 세부평가기준”에 따른 보호조치를 수행하여야 한다.
	9.1.4	[1] 보험금액: 건당 1 억 원 이상, 총 한도 보상액 10 억 원 이상의 금액	9.1.4	[1] 보험금액: 연간 총 한도 보상액의 한도가 10 억 원 이상의 금액

구분	v1.3.1 (2022 년 5 월)		v1.3.2 (2023 년 4 월)	
[첨부] 별첨 1	9.2.7	기타 인정사업자는 연계정보를 개인정보의 일환으로 보호할 수 있도록 **개인정보보호법에** 따른 필요조치 사항을 준수하여야 하며, 또한 전자서명인증 사업자의 **개인정보보호 세부평가기준을** 준용하여야 한다.	9.2.7	기타 전자서명인증사업자는 연계정보(CI)를 개인정보의 일환으로 보호할 수 있도록 개인정보보호법 등 관련 법령에 따른 필요조치 사항을 준수하여야 하며, 또한 전자서명인증사업자의 "별첨 3. 개인정보보호 세부평가기준"을 준용하여야 한다.
[첨부] 별첨 2	1.1.1	전자서명인증사업자는 **정보보호정책을 포함하는** 정보보호 정책을 수립하고 이를 문서화하여야 한다.	1.1.1	전자서명인증사업자는 정보보호정책을 수립하고 이를 문서화하여야 한다.
	1.1.2	전자서명인증사업자는 수립된 정보보호 정책을 **책임 있는 관리에 의해 구현하고 준수**하여야 한다.	1.1.2	전자서명인증사업자는 수립된 정보보호정책이 준수될 수 있도록 관리하여야 한다.

7. 전자서명인증업무 평가 안내서(v1.3.1) 개정이력

구분	v1.2.2 (2021 년 9 월)		v1.3.1 (2022 년 5 월)	
[첨부] 별첨 1	2.6.1	-	2.6.1	[예시] 인증서 요청에 RFC 4211 (CRMF) 및 RFC 2986 (CSR) 등 표준 사용 및 준수
	4.1.3	단, 본인확인기관의 경우 신원정보는 실지명의를 기준으로 하되, 사전에 가입자의 신원확인을 실지명의를 기준으로 확인한 경우에는 실지명의 이외의 방법으로 신원확인 수행을 할 수 있다.	4.1.3	단, 본인확인기관의 경우 신원정보는 실지명의를 기준으로 하되, 사전에 가입자의 신원확인을 실지명의 기준으로 확인한 경우에는 실지명의 이외의 방법으로 신원확인 수행을 할 수 있다.
	6.2.4	FIPS 140-2 Level2 이상 또는 이와 동등한 인증을 받은 전용 HSM 장비를 이용하여 전자서명생성정보를 생성	6.2.4	FIPS 140-2 Level3 이상 또는 이와 동등한 인증을 받은 전용 HSM 장비를 이용하여 전자서명생성정보를 생성
	-	-	7.8	**전자서명생성정보의 분실 · 훼손 또는 도난 · 유출 방안 관련 평가 항목 신설** 인정사업자는 전자서명생성정보가 분실 · 훼손 또는 도난 · 유출된 경우, 해당 가입자 및 관련 당사자가 이 사실을 알 수 있도록 인터넷 홈페이지에 게시하는 등의 적절한 방안을 마련하여야 한다.
[첨부] 별첨 1	9.1.1	인정사업자는 전자서명인증업무 휴지 시, 휴지일 30 일 전에 가입자에게 통보하고 인터넷 홈페이지에 게시할 수 있도록 내부절차를 마련한다.	9.1.1	인정사업자는 전자서명인증업무 휴지 시, 휴지일 30 일 전에 가입자에게 통보하고 인터넷 홈페이지에 게시할 수 있도록 내부절차를 마련하여야 한다.
	9.1.2	인정사업자는 전자서명인증업무 폐지 시, 폐지일 60 일 전에 가입자에게 통보하고 인터넷 홈페이지에 게시할 수 있도록 내부절차를 마련한다.	9.1.2	인정사업자는 전자서명인증업무 폐지 시, 폐지일 60 일 전에 가입자에게 통보하고 인터넷 홈페이지에 게시할 수 있도록 내부절차를 마련하여야 한다.
	9.1.3	전자서명인증업무 휴지 및 폐지 시, 통보 및 게시하는 내용에는 요금의 반환, 가입자의 개인정보 폐기 등 가입자 보호조치를 포함한다.	9.1.3	전자서명인증업무 휴지 및 폐지 시, 통보 및 게시하는 내용에는 요금의 반환, 가입자의 개인정보 폐기 등 가입자 보호조치를 포함하여야 한다.

구분	v1.2.2 (2021 년 9 월)		v1.3.1 (2022 년 5 월)	
[첨부] 별첨 1	9.1.4	인정사업자는 시행령 상의 요건을 충족하는 손해배상 보험을 가입하고, 가입자 등에게 미치는 손해발생 시 이를 해결하기 위한 절차 및 방안을 마련한다.	9.1.4	인정사업자는 시행령 상의 요건을 충족하는 손해배상 보험을 가입하고, 가입자 등에게 미치는 손해발생 시 이를 해결하기 위한 절차 및 방안을 마련하여야 한다.
	-	-	10.1.1	**장애인 · 고령자 등의 전자서명 이용을 보장하기 위한 전자서명인증 관련 평가 항목 신설** 인정사업자는 전자서명인증 서비스 관련 웹, 모바일 어플리케이션, 소프트웨어 등이 [장애인 · 고령자 등의 정보 접근 및 이용 편의 증진을 위한 고시]를 준수함에 있어 신뢰할 수 있는 기관을 통해 인증되어야 한다.
[첨부] 별첨 2	1.2.3	구성원들의 정보보호 활동을 평가할 수 있는 체계와 구성원간 상호 의사소통할 수 있는 체계를 수립하여 운영하고 있는지 확인	1.2.3	구성원들의 정보보호 활동을 평가할 수 있는 체계와 구성원간 상호 의사소통을 할 수 있는 체계를 수립하여 운영하고 있는지 확인
	4.2.2	- 제 3 의 서비스 지원인력은 필요시에만 전자인증 관련 운영 시설의 보안 구역 출입이 허용되어야 하며, 이 경우에도 직원과 동행하여 이루어지는지 확인	4.2.2	- 제 3 의 서비스 지원인력은 필요시에만 전자서명인증 관련 운영 시설의 보안 구역 출입이 허용되어야 하며, 이 경우에도 직원과 동행하여 이루어지는지 확인
	4.2.2	- 전자서명인증 관련 시설을 방문자에 대해서 출입날짜와 시간을 기록하는 등 감독하는 절차가 마련되어 있는지 여부를 확인	4.2.2	- 전자서명인증 관련 시설의 방문자에 대해서 출입날짜와 시간을 기록하는 등 감독하는 절차가 마련되어 있는지 여부를 확인
	4.3.1	전자서명인증사업자는 운영시설이 모든 건물에 대한 물리적인 침입에 대비하는 방안을 마련하여야 하고, 이러한 시설의 출입이나 내부활동을 모니터링하여야 한다. - 전자서명인증 관련 시설 내에 직원이 없을 때에 물리적으로 잠금되고 경보장치가 작동되고 있는지 확인	4.3.1	전자서명인증사업자는 운영시설에 대한 물리적인 침입에 대비하는 방안을 마련하여야 하고, 이러한 시설의 출입이나 내부활동을 모니터링하여야 한다. - 전자서명인증 관련 시설 내에 직원이 없을 때에 물리적으로 잠금이 되고 경보장치가 작동되고 있는지 확인
	5.4.1	- 침해사고의 종류, 크기, 영향, 오작동에 대해서 문서화하고, 정량화하고, 모니터될 수 있도록 하는 공식적인 관리 절차가 존재하는지 확인	5.4.1	- 침해사고의 종류, 크기, 영향, 오작동에 대해서 문서화 및 정량화하고, 모니터링 될 수 있도록 하는 공식적인 관리 절차가 존재하는지 확인

구분	v1.2.2 (2021 년 9 월)		v1.3.1 (2022 년 5 월)	
[첨부] 별첨 2	6.2.3	- 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	6.2.3	- 하이퍼바이저, 운영 시스템, 데이터베이스 및 네트워크 장치의 패치 및 업데이트는 위험 평가에 기반하여 필요하다고 여겨질 때 적시적으로 적용되어야 하며 공식적인 변경 관리 절차를 따라 진행하는지 확인
	6.3.1	- 모든 직원은 고유한 식별자(user ID)를 가지고 **사용함으로서**, 이에 따른 모든 활동들을 추적할 수 있는지 확인 - 시스템 유틸리티 프로그램의 사용은 인가된 사용자로 **제한되고** 엄격하게 통제되고 있는지 확인	6.3.1	- 모든 직원은 고유한 식별자(user ID)를 가지고 사용함으로써, 이에 따른 모든 활동들을 추적할 수 있는지 확인 - 시스템 유틸리티 프로그램의 사용은 인가된 사용자로 제한하고 엄격하게 통제되고 있는지 확인
	8.1.1	업무 연속성 계획에 **전자서명인증 시설에 대해서, 재난 발생 후 그리고 메인 시설 또는 원격지의** 안전한 환경을 복원하기 전까지의 시설보안 절차를 포함하는지 확인	8.1.1	업무 연속성 계획에 전자서명인증의 메인 시설 또는 원격지 시설에 대해서, 재난 발생 후 안전한 환경을 복원하기 전까지의 시설보안 절차를 포함하는지 확인
	9.1.1	e) **입력을** 개체의 신원	9.1.1	e) 입력 개체의 신원
[첨부] 별첨 3	**공통**	평가 항목 연변 기준 3 단계	**공통**	평가 항목의 연변 기준 2 단계로 변경
	1.4	업무 필요성에 따라 주요 직무자 및 개인정보취급자를 **업무상 필요에 따라** 최소화하여 지정	1.4	업무 필요성에 따라 주요 직무자 및 개인정보취급자를 최소화하여 지정
	4.3	**법적 대리인** 자격요건 확인 절차 및 동의 기록 보관 여부 확인	4.3	법정 대리인 자격요건 확인 절차 및 동의 기록 보관 여부 확인
	4.16	인터넷 홈페이지 등에 위탁하는 업무의 내용과 수탁자를 현행화하여 공개하고 **있는진** 확인	4.16	인터넷 홈페이지 등에 위탁하는 업무의 내용과 수탁자를 현행화하여 공개하고 있는지 확인
	6.6	전자서명인증사업자는 **정보주제**가 인터넷 홈페이지 등을 통해 중요한 정보 또는 화면에 접근하려는 경우에는 비밀번호 재확인, 휴대폰 인증, 공인인증서 등 본인임을 확인할 수 있는 추가적인 인증 절차를 적용하여야 한다.	6.6	전자서명인증사업자는 정보주체가 인터넷 홈페이지 등을 통해 중요한 정보 또는 화면에 접근하려는 경우에는 비밀번호 재확인, 휴대폰 인증, 공인인증서 등 본인임을 확인할 수 있는 추가적인 인증 절차를 적용하여야 한다.
	7.2	외부 위탁하는 경우 개인정보 보호조치가 포함된 **위착 계약**을 체결하고 있는지 확인	7.2	외부 위탁하는 경우 개인정보 보호조치가 포함된 위탁 계약을 체결하고 있는지 확인

8. 전자서명인증업무 평가 안내서(v1.2.2) 개정이력

구분	v1.2.1 (2021 년 6 월)		v1.2.2 (2021 년 9 월)	
전체	-	없음	**없음**	개정이력 추가

9. 전자서명인증업무 평가 안내서(v1.2.1) 개정이력

구분	v1.2.0 (2021 년 3 월)		v1.2.1 (2021 년 6 월)	
[첨부] 별첨 1	9.2.2	인정사업자가 연계정보를 저장하거나 전송하는 경우 이를 안전한 암호 알고리즘으로 암호화하여야 하며, 안전한 암호 알고리즘의 기준은 본 기준의 제 5 조제 5 항을 참고하여 적용한다.	9.2.2	인정사업자가 연계정보를 저장하거나 전송하는 경우 이를 안전한 암호 알고리즘으로 암호화하여야 한다.
[첨부] 별첨 3	6.1.9	법적 의무 대상자에 해당하는 경우 개인정보 이용내역을 주기적으로 정보주체(이용자)에게 통지하고 그 기록을 남기고 있는가?	6.1.9	삭제
[첨부] 별첨 3	6.1.10	개인정보 이용내역 통지 항목은 법적 요구항목을 모두 포함하고 있는가?	6.1.10	삭제

Deloitte.