전자서명인증업무 운영기준

[시행 2022. 4. 20.] [과학기술정보통신부고시 제2022-5호, 2022. 2. 8., 일부개정]

과학기술정보통신부(정보보호기획과), 044-202-6445, 6449

제1조(목적) 이 운영기준은 「전자서명법」(이하 "법"이라 한다) 제7조제2항에 따라 전자서명인증업무의 안정성과 신뢰성 확보 및 가입자・이용자 보호 등을 위하여 법 제8조에 따른 운영기준 준수사실의 인정을 받았거나 받으려는 전자서명인증사업자가 전자서명인증업무를 수행함에 있어 지켜야 할 구체적인 사항을 정하는 것을 목적으로 한다.

제2조(정의) 이 운영기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "인정사업자"란 법 제8조에 따라 운영기준 준수사실의 인정을 받은 전자서명인증사업자를 말한다.
2. "전자서명인증시스템"이란 인정사업자가 전자서명인증서비스를 제공하기 위해 운영하는 다음 각 호의 시스템을 말한다.
   가. 가입자의 등록정보를 관리하기 위한 시스템
   나. 전자서명생성정보를 생성・관리하기 위한 시스템
   다. 인증서를 생성・발급・관리하기 위한 시스템
   라. 기타 전자서명인증업무의 수행과 관련된 시스템 및 설비
3. "등록대행기관"이란 인정사업자를 대신하여 전자서명인증서비스에 가입하려는 자의 신원을 확인하고 가입 신청을 접수・등록하는 등의 업무를 수행하는 자를 말한다.
4. "가입자등록정보"란 전자서명인증서비스에 가입하려는 자가 인정사업자에게 제출한 신청서, 신원확인을 위해 제출한 서류 및 증명서 등의 사본 그리고 기타 신청에 필요한 전자적 기록 등을 말한다.
5. "가입자"란 전자서명생성정보에 대하여 전자서명인증사업자로부터 전자서명인증을 받은 자를 말한다.
6. "이용자"란 전자서명인증사업자가 제공하는 전자서명인증서비스를 이용하는 자를 말한다.

제3조(전자서명인증업무의 독립성) 인정사업자는 인증업무를 신뢰성 있게 수행하기 위하여 자신이 발급한 인증서를 이용하는 가입자와의 관계에 있어서 독립성을 유지하여야 한다.

제4조(적정 기술의 이용) 인정사업자는 다음 각 호의 요건을 충족하는 기술을 이용하여 전자서명인증서비스를 제공한다.

1. 전자문서에 전자서명을 한 서명자의 신원을 알 수 있도록 할 것
2. 가입자의 전자서명은 가입자 본인의 통제 아래에서만 생성할 수 있어야 하고, 가입자의 통제를 벗어나 가입자 이외의 다른 자가 가입자의 전자서명을 생성할 수 없도록 할 것
3. 서로 다른 전자문서에 사용된 전자서명은 구별될 수 있도록 하여, 하나의 전자문서에 사용된 전자서명이 다른 전자문서에 재사용될 수 없도록 할 것

4. 전자문서가 전자서명된 후 해당 전자문서 및 전자서명의 변경여부를 확인할 수 있을 것
5. 안전한 암호알고리즘을 사용할 것
6. 특별한 사정이 없는 한 국가・단체 또는 국제 표준이 있는 경우 이를 준수할 것

제5조(전자서명인증업무준칙) ① 인정사업자는 법 제15조에 따른 전자서명인증업무준칙(이하 "인증업무준칙"이라 한다)을 작성하여 인터넷 홈페이지 등에 게시하고, 이에 따라 전자서명인증업무를 수행한다.

② 인정사업자는 인증업무준칙에 포함하여야 하는 법 제15조제1항 각 호의 사항에 변동이 생긴 경우 인증업무준칙에 해당 내용을 반영한다.

③ 인정사업자는 인증업무준칙의 내용을 변경하는 경우, 사전에 규정된 절차에 따라 인증업무준칙을 개정하고 관련 당사자 모두가 변경본을 열람할 수 있도록 한다.

④ 인정사업자가 제공하는 전자서명인증서비스와 관련된 인증기관이 있는 경우, 해당 기관과의 정책 일관성을 위해 인증업무준칙의 제・개정 시 이에 대해 협의한다.

제6조(가입자 등록) ① 인정사업자 또는 등록대행기관은 법 시행령 제9조・시행규칙 제5조 및 다음 각 호의 요건을 충족하는 방법을 이용하여 전자서명인증서비스에 가입하려는 자의 신원을 확인한다.

1. 가입자 신원정보의 진위(정확성)를 확인할 수 있을 것
2. 신원정보의 주체(소유자)가 맞는지 확인할 수 있을 것

② 인정사업자 또는 등록대행기관은 직접 대면(제1항의 요건을 충족하는 것으로 직접 대면에 준하는 비대면 방법 포함)하여 가입자의 신원을 확인한다.

③ 인정사업자 또는 등록대행기관은 가입자를 등록하거나 인증서를 발급하기 전에 인증서의 이용범위, 전자서명의 효력 등에 대한 이용약관을 가입자와 이용자에게 알리는 절차를 마련한다.

④ 인정사업자는 계약에 의해 가입자의 신원 확인 및 등록 업무를 등록대행기관에 위임하는 경우, 등록대행기관이 제6조의 규정을 준수하도록 관련 통제 절차를 수립・유지・관리하고 해당 절차에 따라 업무를 수행하는지 관리・감독한다.

⑤ 인정사업자는 등록대행기관으로부터 정보통신망으로 가입자의 등록정보를 전송받는 경우, 가입자의 등록정보가 위조・변조 되지 않도록 조치를 취하여야 하며 안전한 암호 알고리즘이 적용된 암호화 조치 등을 통해 등록정보가 유출되지 않도록 대책을 마련한다.

제7조(인증서 발급・효력정지・효력회복 및 폐지 등) ① 인정사업자는 가입자에게 인증서를 발급하는 경우, 가입자의 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인한다.

② 인정사업자는 전자서명 생성・검증 등 가입자에게 발급된 인증서를 이용자가 이용할 수 있는 방안을 마련하여 제공한다.

③ 인정사업자는 자신이 발급하는 인증서가 위조・변조되지 않도록 시스템 구축 등 다양한 방법으로 필요한 조치를 마련한다.

④ 인정사업자는 가입자의 신청이 있는 경우, 제6조제1항에 따라 가입자의 신원을 확인한 후 인증서의 효력을 정지하거나 회복 또는 폐지할 수 있다.

⑤ 인정사업자는 제4항에 따라 인증서의 효력을 정지하거나 회복 또는 폐지하는 경우 이용자가 지체 없이 그 사실을 확인할 수 있는 방안을 마련하여 제공한다.

⑥ 인정사업자는 이용자가 인증서의 유효성을 확인할 수 있도록 인증서 효력정지 및 폐지목록을 생성하여 인증업무준칙에 규정한 공고 설비에 공고하거나, 이용자에게 인증서 유효성 확인 서비스를 제공할 수 있다.

제8조(전자서명생성정보 생성) ① 인정사업자는 물리적으로 안전한 환경에서 인증업무준칙에 규정된 절차에 따라 전자서명생성정보를 생성한다.

② 인정사업자는 전자서명생성정보를 생성하는 경우, 관련 표준을 따라야 하고 안전한 암호 알고리즘 또는 안전한 암호화 장치를 이용한다.

③ 인정사업자는 자신의 전자서명생성정보를 생성하는 경우, 다자인증 통제(m of N, m은 3명 이상)하에 전자서명생성정보를 생성한다.

④ 인정사업자는 가입자의 신청이 있는 경우 외에는 가입자의 전자서명생성정보를 보관하여서는 아니되며, 가입자의 신청에 의하여 그의 전자서명생성정보를 보관하는 경우 해당 가입자의 동의없이 이를 이용하거나 유출하여서는 아니된다.

⑤ 인정사업자는 가입자의 전자서명생성정보를 생성하는 경우, 2인 이상의 권한 있는 직원이 공동으로 이를 수행한다. 자동화된 설비를 이용하는 경우에는 해당 설비를 다자인증 통제(m of N, m은 2명 이상)하에 활성화한다.

제9조(전자서명생성정보 보호) ① 인정사업자는 전자서명생성정보를 생성한 경우 그 전자서명생성정보를 안전하게 보호한다.

② 인정사업자는 가입자의 전자서명생성정보를 생성한 경우, 해당 전자서명생성정보가 가입자의 통제 아래 이용될 수 있도록 안전조치를 마련한다.

③ 인정사업자는 전자서명생성정보의 분실·훼손 또는 도난·유출 등을 방지하고 전자서명인증업무를 계속하여 안정적으로 제공할 수 있도록 전자서명생성정보를 백업한다.

④ 인정사업자는 전자서명생성정보를 백업하는 경우, 백업된 전자서명생성정보를 안전하게 보호한다.

⑤ 인정사업자는 백업된 전자서명생성정보 중 1부를 전자서명인증업무 수행 시설과는 별도의 원격지 저장설비에 안전하게 보관한다.

⑥ 인정사업자는 전자서명생성정보를 백업하거나 복구하는 경우, 2인 이상의 권한 있는 직원이 공동으로 이를 수행한다.

⑦ 인정사업자는 전자서명인증업무의 보호조치를 계획하고 감독·통제하는 관리책임자와 전자서명인증업무의 보호조치를 이행하는 보안관리자의 입회 하에 백업된 전자서명생성정보와 그 원본을 안전하게 파기한다.

⑧ 인정사업자는 전자서명생성정보가 분실·훼손 또는 도난·유출된 경우, 해당 가입자 및 관련 당사자가 이 사실을 알 수 있도록 인터넷 홈페이지에 게시하는 등의 적절한 방안을 마련한다.

제10조(시설 및 자료 보호조치 등) ① 인정사업자는 전자서명인증업무 관련 시설 및 자료의 보호를 위해 별표에 따른 보호조치를 수행한다.

② 인정사업자는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」,「개인정보 보호법」,「정보통신기반 보호법」등 관계 법령을 준수한다.

제11조(가입자 및 이용자 보호 대책) ① 인정사업자는 법 제15조제2항, 제3항, 제4항에 따른 전자서명인증업무 휴지·폐지 절차 및 법 제20조에 따른 손해배상 절차를 준수한다.

② 인정사업자가 법 시행령 제14조에 따라 연계정보를 처리하는 경우 다음 각 호의 사항을 수행한다.

1. 연계정보를 이용·수집하거나 제3자에게 제공하는 경우 가입자로부터 별도의 동의를 받을 것
2. 연계정보를 저장하거나 전송하는 경우 안전한 암호알고리즘에 따른 암호화 조치를 할 것
3. 연계정보를 이용하는 경우 전자서명과는 분리된 별도 방식을 통해 이용자에게 연계정보를 전송할 것
4. 연계정보를 전송하거나 수신한 시간 등 로그를 기록·저장할 것
5. 권한 있는 관리자만이 연계정보 처리 시스템에 접근할 수 있는 접근통제를 갖출 것
6. 그밖에「개인정보 보호법」에 따른 개인정보 보호조치사항을 준수할 것

제12조(장애인·고령자 등의 전자서명 이용 보장) 인정사업자는 장애인·고령자 등의 전자서명인증서비스 접근 및 이용 편의 증진을 위하여「지능정보화 기본법」제46조제6항에 따른 고시를 준수한다.

제13조(재검토기한) 과학기술정보통신부 장관은 이 고시에 대하여「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제394호)에 따라 2021년 1월 1일 기준으로 매3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <제2022-5호,2022.2.8.>

이 고시는 2022년 4월 20일부터 시행한다.