<별지> 행정전자서명 인증기관 구성요건

# 행정전자서명 인증기관 구성요건

# 1. 개요

본 기준은 행정전자서명인증체계 내 인증기관의 시설 및 장비에 관한 구체적인 사항을 정의한다.

일반적으로 인증기관 또는 등록기관을 지정하기 위해서는 다음의 사항을 만족해야 하나, 구체적인 기준 등은 행정전자서명인증관리센터와 협의하여 정할 수 있다.

# 2. 시스템 구성 요건

## 2.1 가입자 등록정보 관리 시스템(등록 시스템)

| | | |
|---|---|---|
| **가입자 등록정보 관리 기능** | 가입자 식별기능 | o 인증서 DN 체계에 따라서 DN을 부여하는 기능<br>- DN의 유일성 보장 기능<br>- 갱신 등록시, DN의 유일성 또는 동일성을 확인하는 기능 |
| | 가입자 등록정보 관리 기능 | o 등록정보를 입력, 열람, 변경, 삭제하는 기능<br>o 네트워크를 통해 전송되는 등록정보에 대한 암호화 및 전자서명 기능 |
| | 감사 및 보안 기능 | o 등록정보를 입력, 접근, 변경, 삭제한 사실, 시각, 행위자에 관한 내역에 대한 감사기록을 생성·보존하는 기능<br>o 감사기록의 위·변조 및 삭제 위협에 대처하는 기능<br>o 권한없는 자가 감사기록을 삭제할 수 없도록 하는 보호기능<br>o 등록정보에 대한 접근통제 및 등록정보 위·변조, 삭제 및 유출 위협에 대처하는 기능<br>o 등록정보 관리 소프트웨어의 위·변조 및 삭제 위협에 대처하는 기능 및 형상관리 기능<br>o 등록정보 관리 소프트웨어 운영관리자 및 감사관리자에 대한 역할 구분 및 접근통제 기능 |
| **암호 알고리즘** | 전자서명 알고리즘 | o 행정전자서명기술요건(이하,기술요건)에 명시된 전자서명 알고리즘 지원<br>o 전자서명 알고리즘을 이용한 전자서명 생성 및 검증 기능 |
| | 해쉬 알고리즘 | o 기술요건에 명시된 해쉬 알고리즘 지원 |
| | 암호 알고리즘 | o 기술요건에 명시된 암호 알고리즘 지원 |
| **등록기관 키 생성·관리 기능** | 키 생성 기능 | o 기술요건에서 규정한 전자서명 알고리즘의 키 생성기능<br>o 알고리즘 종류, 키 길이, 용도와 같은 키 생성 관련 정보를 설정·확인할 수 있는 기능<br>o 키 생성시 보안성을 손상시키지 않는 절차를 통하여 키를 생성하는 기능 |
| | 키 저장 기능 | o 전자서명 키 및 암호키를 안전하게 저장하는 기능<br>o 키 입력 및 출력시 안전한 방법으로 키를 입출력하는 기능 |
| | 감사 및 보안 기능 | o 서명용 개인키 및 암호용 개인키의 생성·접근·파기 및 전자서명에 관한 내역에 대한 감사기록을 생성·보존·검색하는 기능<br>o 감사기록의 위·변조 및 삭제 위협에 대처하는 기능<br>o 관리자 접근통제 기능<br>o 행정전자서명생성키(비밀키) 생성·관리 소프트웨어의 위조·변조 및 삭제 위협 등 불법적인 사용에 대처하는 기능 |

| | | |
|---|---|---|
| | | o 행정전자서명생성키(비밀키) 생성·관리 소프트웨어의 형상관리 기능 |

## 2.2 인증서 생성·발급·관리 시설

| | | |
|---|---|---|
| **인증서 생성·발급·관리 기능** | 인증서 발급 기능 | o 기술요건의 인증서 프로파일을 준수하는 인증서 생성 및 발급 기능<br>- 설정된 인증서 정책에 따라서 인증서 생성<br>- 가입자 행정전자서명검증키(공개키)의 유일성 확인 기능<br>- 가입자 행정전자서명검증키(공개키)가 가입자에게 속한다는 사실 확인<br>- 인증서를 DER(X.690) 형식으로 발급하는 기능<br>o 인증서의 키 위탁 기능<br>o 인증서의 일련번호를 유일하게 부여하는 기능<br>o 인증서 내에 주입하는 본인확인 정보의 내용, 형식 및 주입 위치 등은 기술요건 준수<br>o 기술요건의 전자서명 기능을 이용하여 인증서를 생성하는 기능<br>o 인증서 발급요청시 기술요건 중 인증서관리 프로토콜을 준수하여 처리하는 기능<br>- 인증서 요청형식을 준수하여 처리하는 기능<br>- 인증서 요청형식에 대한 응답 메시지 생성 기능<br>- 응답 메시지 생성시, DER 또는 Base64 코딩형식을 지원하는 기능 |
| | 인증서 생성정책 설정 기능 | o 전자서명 알고리즘, 암호 알고리즘, 인증서 용도/이용범위, 인증서 유효기간, 인증서 확장 필드 설정 기능 |
| | 인증서 조회 기능 | o 전자서명 알고리즘, 암호 알고리즘, 가입자 및 발급자 DN, 이용범위 및 용도, 인증서 확장필드 및 인증서 폐지여부 조회기능 |
| **암호 알고리즘** | 전자서명 알고리즘 | o 기술요건에 명시된 전자서명 알고리즘 지원<br>o 전자서명 알고리즘을 이용한 전자서명 생성 및 검증 기능 |
| | 해쉬 알고리즘 | o 기술요건에 명시된 해쉬 알고리즘 지원 |
| | 암호 알고리즘 | o 기술요건에 명시된 암호 알고리즘 지원 |
| **인증서 폐지목록 생성·관리 기능** | 인증서 폐지 요청 처리 기능 | o 인증서 관리프로토콜을 준수하여 인증서 폐지 요청, 처리 기능<br>o 폐지의 구분, 요청일자, 사유 등을 기록하는 기능<br>o 대상 인증서의 상태가 요청처리에 적절한지 확인하는 기능 |
| | 인증서 폐지목록 발급 기능 | o 기술요건 중 인증서 폐지목록 프로파일을 준수하는 인증서 폐지목록 발급 기능<br>o 인증서 폐지목록을 DER(X.690) 형식으로 발급하는 기능 |
| | 인증서 폐지목록 생성정책 설정 기능 | o 전자서명 알고리즘, 다음 발급일자, 인증서 폐지목록 확장 필드, 다음 발급일자 이전 자동갱신 또는 알림기능 등의 설정 기능 |
| | 인증서 폐지목록생성 기능 | o 설정된 생성정책에 따라 인증서 폐지목록을 생성하는 기능<br>o 전자서명 기능을 이용하여 인증서 폐지목록을 생성하는 기능<br>o 전자서명 생성 키의 무결성 검사 수행기능<br>o 폐지 일자는 반드시 당일의 정확한 시간으로 자동으로 입력하는 기능<br>o 인증서 폐지목록 생성시 DER 코딩형식을 지원하는 기능 |
| | 인증서 폐지목록 조회 기능 | o 전자서명 알고리즘, 발급일자 및 다음 발급일자, 폐지된 인증서 일련번호, 폐지된 인증서 폐지일시, 사유, 인증서 폐지목록 확장필드 등에 대한 조회 기능 |

| | | |
|---|---|---|
| **가입자 인증서 보관** | 가입자의 인증서와 그 폐지에 관한 기록 보관 | o 보관된 기록에 대한 백업 및 안전한 장소에 복사본 저장 |
| **감사 및 보안 기능** | 감사기록 생성·보존 기능 | o 인증서 발급, 폐지, 정책설정에 관한 내역에 대한 감사기록 생성, 보존 기능<br>o 감사기록 식별자, 사건의 유형, 일자 및 시각, 행위자 등에 대한 감사기록을 생성·보존하는 기능<br>o 감사기록을 검색할 수 있는 기능 |
| | 보안 기능 | o 감사기록의 위·변조 및 삭제 위협에 대처하는 기능<br>o 관리자 접근통제 기능<br>o 인증서 생성·관리 소프트웨어의 위·변조 및 삭제 위협에 대처하는 기능<br>o 인증서 생성·관리 소프트웨어의 불법적인 사용에 대처하는 기능 |
| **인증서 공고·유효성 확인 설비** | 인증서, 인증서 폐지목록 관리 기능 | o DN을 이용하여 인증서, 인증서 폐지목록을 등록 및 삭제하는 기능 |
| | 인증서, 인증서 폐지목록 검색지원 기능 | o 기술요건 중 LDAP 프로토콜을 준수하여 사용자 인증서 등을 DN으로 검색하는 기능<br>o 기술요건 중 LDAP 프로토콜을 준수하여 인증서 폐지목록 검색하는 기능 |
| | 감사 및 보안 기능 | o 인증서, 인증서 폐지목록을 등록·관리에 대한 감사기록을 생성·보존하는 기능<br>o 감사기록의 위·변조 및 삭제 위협에 대처하는 기능<br>o 인증서, 인증서 폐지목록의 삭제 위협에 대처하는 기능<br>o 인증서, 인증서 폐지목록 공고 소프트웨어의 위·변조 및 삭제 위협 등에 대처하는 기능<br>o 디렉토리 시스템 관리자 접근 통제 기능 |
| **인증서 실시간 유효성 확인 기능** | OCSP | o 기술요건을 준수하여 OCSP 기능 제공<br>o OCSP 서버용 인증서 요청형식을 올바르게 생성하는 기능<br>o 발급된 OCSP 서버용 인증서를 올바르게 설치하고 이를 확인할 수 있는 기능<br>o 단기 인증서 OCSP 서버용 인증서를 이용할 경우, 인증서 유효기간이 인증서 폐지목록 갱신주기보다 짧게 설정하는 기능 |
| | 감사 및 보안 기능 | o 인증서 유효성 확인을 한 사실, 시각, 요청자에 관한 내역에 대한 감사기록을 생성·보존하는 기능<br>o 감사기록의 위·변조 및 삭제 위협에 대처하는 기능<br>o 인증서 유효성확인 소프트웨어의 위·변조 및 삭제 위협 등에 대처하는 기능<br>o 관리자 접근 통제 기능 |
| **시점확인 기능** | 시각 수신 기능 | o 시각확인 프로토콜에 따라 시각을 수신하는 기능<br>o 천분의 일초까지 시간을 표현하는 기능<br>o 시각수신장치에 문제가 발생하였을 경우 이를 관리자에게 알리는 기능 |
| | TSA 시간 보정 기능 | o 시각수신장치에서 제공하는 시간을 이용하여 TSA 시각 보정 기능<br>o 시각보정기능에 오류가 발생한 경우 이에 대한 오류 메시지 출력기능 |
| | 시점확인 서비스 기능 | o 시점확인 프로토콜을 준수하여 시점확인서비스를 제공하는 기능<br>o 사용자가 수신한 시점확인토큰에 기록된 시각이 발급기록시간과 일치 |

| | | |
|---|---|---|
| | | 하는지를 확인하는 기능<br>o 전자서명 기능을 이용하여 시점확인서비스 제공 |
| | 감사 및 보안 기능 | o 다음의 사항에 대한 감사기록을 생성·보존하는 기능<br>- 시각보정 내용에 대한 기록<br>- 시점확인사실, 시각, 행위자, 신청자<br>- 시각비동기 등 문제발생 사실, 시각<br>- 시점확인서비스 제공 지연 사실, 시각, 신청자<br>o 감사기록의 위·변조 및 삭제 위협에 대처하는 기능<br>o 시점확인 소프트웨어의 위·변조 및 삭제 위협 등에 대처하는 기능 |
| **암호키 위탁 관리 설비** | 암호키 위탁 기능 | o 암호키 위탁 신청·승인·복구 신청·복구 기능<br>o 감사기록의 위·변조 및 삭제 위협에 대처하는 기능 |
| | 감사 및 보안 기능 | o 행정전자서명 암호용키 위탁 및 복구에 대한 감사기록을 생성·보존하는 기능<br>o 다음의 사항에 대한 감사기록을 생성·보존하는 기능<br>- 암호키 위탁 신청, 승인, 복구 신청자 및 승인자, 시각<br>- 암호키 위탁, 승인, 복구 거부시 거부 사유 및 거부자, 시각<br>- 암호키 복구 관련 오류 발생시 그 사유 및 시각<br>o 감사기록의 위·변조 및 삭제 위협에 대처하는 기능 |

## 2.3 보호 설비

| | | |
|---|---|---|
| **네트워크·시스템 보안 설비** | 네트워크 장비 | o 네트워크 장비 및 시스템에서 생성하는 네트워크 관련 주요 감사기록의 보존 기능 |
| | 네트워크 보안 설비 | o 침입차단시스템 운영<br>- CC인증을 필한 침입차단소프트웨어의 사용<br>- 인증업무에 한정된 접근통제규칙을 설정하여 사용<br>o 침입탐지시스템 운영<br>- CC인증을 필한 침입탐지시스템의 사용<br>- 서비스 방해 공격 탐지 기능<br>- 모든 트래픽에 대한 점검 및 침입탐지 기능<br>- 새로운 패턴의 침입유형에 대한 추가 기능<br>- 침입이 탐지되었을 경우 이를 관리자에게 알리는 기능 |
| | 네트워크 및 시스템 관리설비 | o 실시간으로 네트워크 및 시스템의 상태를 점검을 할 수 있는 시스템 또는 장비의 운영<br>o 인증업무와 관련된 주요 프로그램 또는 프로세스의 동작 여부를 점검할 수 있는 시스템 또는 장비의 운영 |
| **시스템 보안 기능** | 인증시스템의 운영 | o 관리자별로 계정 분리 설정 및 접근통제<br>o 필요한 최소한의 사용자 등록<br>o 인증업무에 필요한 소프트웨어만 설치·운영<br>o 인증업무에 필요한 프로그램 또는 프로세스만 실행<br>o 프로그램 및 운영체제에 대한 패치 수행<br>o 인증시스템 운영에 대한 감사 생성, 보존 기능<br>- 인증시스템 시작과 종료<br>- 루트 및 사용자의 로그인/아웃<br>- 사용자 계정의 추가/삭제, 권한변경 사실, 시각, 행위자 등에 관한 내역<br>- 관리자 권한의 변경 사실<br>- 기타 인증시스템 관리자의 주요 활동 내역 |
| **물리적 보안 설비** | 인증시스템 운영실 | o 인증시스템을 안전하게 운영할 수 있는 별도의 통제구역 설치 |
| | 다중출입 통제장치 | o 인증시스템 운영실에 대한 다중 출입 통제 기능<br>- 지문인식 등 생체특성기반 및 신원확인 카드 등 소지기반 신원확인 기능을 결합한 출입 통제 장치<br>o 출입통제장치는 다음의 정보에 대한 감사기록<br>- 사건의 유형, 성공/실패 여부 및 실패 시 원인<br>- 일자 및 시각, 행위자<br>o 무게감지장치<br>o 정전시에도 출입통제 및 감사기록 가능하도록 하는 기능 |
| | 침입감지·경보 및 감시·통제 장치 | o 물리적인 침입감지 및 경보 기능<br>- 운영실내에 진동감지장치, 음향감지장치 등의 침입감지장치 설치<br>- 침입감지장치에 이상이 발생했을 때 이를 감지하는 기능<br>- 침입감지장치가 침입을 감지하였을 경우 관리자에게 즉각 알리는 기능<br>o 침입감시 기능<br>- CCTV시스템은 모든 출입행위에 대하여 녹화하는 기능<br>- CCTV시스템에 대한 접근통제기능<br>o 다중출입통제장치로부터의 출입현황정보 확인 기능<br>- 정당한 관리자만이 감사기록을 조회<br>- 출입통제시스템 감사기록 저장공간 소진에 대한 대책<br>- 출입통제시스템에 대한 접근통제 기능 |

| | | |
|---|---|---|
| | 물리적 잠금장치 | o 통제구역 내의 인증시스템, 침입차단시스템 및 네트워크설비 등에 대한 접근을 물리적으로 통제하는 보안캐비닛<br>o 중요 자료 및 주요 시스템 백업매체에 대한 접근을 물리적으로 통제하는 내화금고 |
| | 재해 예방설비 | o 화재 발생시 이를 조기에 감지하고 진화하는 설비<br>o 수재 예방설비<br>o 정전 발생시 지속적인 인증업무의 수행이 가능토록 일정기간 전원을 공급하여 주는 전원 공급설비<br>o 온도 및 습도를 일정하게 유지하기 위한 항온항습장치 설치<br>o 각종 전원장비에 대한 접지시설<br>o 비상시를 대비한 전지역의 유도등 및 유도표지 설치 |

## 2.4 가입자 소프트웨어

| | | |
|---|---|---|
| **키 관리 기능** | 키 생성기능 | o 기술요건에 정의한 전자서명알고리즘 및 암호 알고리즘에 사용되는 키 생성 기능 |
| | 키 저장기능 | o 기술요건을 준수하여 키를 PKCS#5로 암호화하는 기능<br>o PKCS#5로 암호화된 키를 기술요건을 준수하여 PKCS#8로 저장하는 기능<br>o 키를 생성하여 별도의 저장장치에 저장한 후 키를 즉시 memory 또는 임시파일에서 삭제하는 기능 |
| **인증서 관리 기능** | 인증서 관리프로토콜 기능 | o 기술요건 중 인증서 요청 형식을 준수<br>o 기술요건 중 인증서 관리 프로토콜을 준수<br>o 인증기관으로부터 수신한 응답 메시지를 처리할 수 있는 기능 |
| | 인증서 저장 기능 | o 가입자 인증서 저장과 관련된 사항은 기술요건 준수 |
| | 인증서 조회기능 | o 인증서를 조회하는 기능은 기술요건 준수<br>o 인증서임을 표시하는 기능은 기술요건 준수<br>o 인증서 폐지목록을 조회하는 기능은 기술요건 준수 |
| | 인증서 전달 기능 | o 행정전자서명생성키(비밀키)와 인증서를 PKCS#12 형식으로 내보내기 기능<br>o 행정전자서명생성키(비밀키)와 인증서를 PKCS#12 형식으로 가져오기 기능 |
| | 최상위 인증기관 인증서 신뢰여부 확인기능 | o 기술요건 준수 |
| **전자서명 및 인증서 검증 기능** | 인증서 검증 기능 | o 인증서 경로구축 기능은 기술요건 준수<br>o 인증서 상태확인 기능은 기술요건 준수 |
| | 전자서명 생성 및 검증 기능 | o 전자서명 기능(PKCS#7 등)<br>o 전자서명을 검증하는 기능 |
| **시점 확인 기능 (신청시)** | 시점확인서비스 이용기능 | o 기술요건을 준수하여 시점확인서비스를 요청하는 기능<br>o 해당 요청에 대한 시점확인토큰을 수신하는 기능<br>o 시점확인토큰을 검증하는 기능 |

| | | |
|---|---|---|
| | | o 원본 파일과 시점확인 토큰을 보관, 검색할 수 있는 기능<br>- 시점확인토큰을 원본 파일과 연결하여 검색할 수 있는 기능 |

## 3. 지침 등 내부 절차

인증기관은 인증업무를 수행함에 있어 다음 사항에 해당하는 시설 및 장비의 관리·운영절차 및 방법을 마련하여야 한다.

| | |
|---|---|
| 인증기관의 행정전자서명 비밀키 관리에 관한 사항 | o 행정전자서명 비밀키 생성/백업/파기에 관한 사항<br>o 행정전자서명 비밀키 분실/훼손 시 대응에 관한 사항 |
| 인증서 관리에 관한 사항 | o 가입자 등록 절차 및 신원확인을 위한 서류 제출 등<br>o 가입자 등록 정보 및 제출 서류의 관리에 관한 사항<br>o 인증서 발급/재발급/갱신/폐지 및 인증서 공고에 관한 사항<br>o 인증서 폐지 정보의 생성 및 공고에 관한 사항 |
| 시설 및 장비의 관리에 관한 사항 | o S/W, 시스템, 네트워크, 물리적 설비 등의 접근 통제에 관한 사항<br>o S/W, 시스템, 네트워크, 물리적 설비 등의 변경 및 유지보수에 관한 사항<br>o 감사기록의 생성·백업·관리에 관한 사항<br>o 인증업무 관련 정보의 생성·백업·관리에 관한 사항 |
| 재해 복구에 관한 사항 | o 장애 및 재해발생 시 비상계획<br>o 운영 데이터, S/W, 시스템, 설비에 대한 백업 및 복구 계획 |
| 인원 통제에 관한 사항 | o 업무 담당자별 역할 정의 및 업무 분리에 관한 사항<br>o 담당자 신원조회, 자격, 경력 등의 조회에 관한 사항<br>o 업무 담당자의 의무사항 및 인증업무 등에 대한 교육 계획 |