정부 웹보안인증서
인증업무준칙(CPS)

2024. 8.

행정안전부

개 정 이 력

버전	작성일	변경내용	작성자	승인자
1.0	2023. 2. 9	최초 제정	최의열	한창윤
1.1	2023. 4. 14	키 세레모니 결과 반영 및 용어 통일 등 수정보완	최의열	한창윤
1.2	2024. 2. 6	OCSP 인증서 유효기간 변경	신동화	한창윤
1.3	2024. 3. 29	최신 CA/Browser Forum TLS BRs 반영 - 9.4.6, 인증서 프로파일 및 기타 내용 수정 - 용어 및 오탈자 수정	신동화	한창윤
1.4	2024. 6. 25	CA/Browser Forum의 네트워크 보안 요구사항 준용 - 6.7. 네트워크 보안 항목 내용 추가	정의성	한태근
1.5	2024. 8. 22	최신 CA/Browser Forum TLS BRs 반영 - 3.1, 한글 도메인의 Punycode 변환 지원 내용 추가 - 3.4, 4.9.2, 4.9.12, 키 손상의 경우 관련기관의 인증서 폐지 요청 허용 내용 추가	성지은	박병호

<목 차>

1. 전 문

1.1. 개요

행정안전부 정부 웹보안인증서 인증체계는 TLS 인증서 발급에 특화된 PKI 체계로서 전자정부 및 공공기관 웹서비스의 무결성과 기밀성 제공을 그 목적으로 한다. 본 문서는 행정안전부 정부 웹보안인증서 인증기관 운영에 대한 인증정책, 운영관리 절차를 정의한다.

본 문서는 RFC 3647(X.509 PKI 인증정책/인증업무 프레임워크)에 따라 작성되었으며, 행정안전부 정부 웹보안인증서(GSSL(Government SSL))를 발급하는 인증기관은 CA/Browser Forum(www.cabforum.org)에서 작성된 Baseline Requirement for the Issuance and Management of Publicly-Trusted TLS Server Certificate를 준수한다.

본 문서와 TLS BRs 간 내용 충돌이 발생할 경우 TLS BRs을 우선적으로 따르기로 한다.

1.2. 문서명 및 식별

본 문서명은 정부 웹보안인증서 인증업무준칙(CPS) (이하 인증업무준칙(CPS))이며 최상위 인증기관인 GSSL Root CA와 인증기관인 GSSL Sub CA (이하, GSSL Root CA와 함께 통칭하여 GSSL 인증기관)의 운영 및 관리에 대한 정책을 기술한다. 세부적으로 신뢰당사자 및 가입자를 대상으로 인증서의 발급 승인, 발급, 재발급, 관리, 사용, 유효성 검증, 폐지를 포함하는 인증 서비스를 제공하기 위한 법적, 기술적 요건을 명시한다.

1.3. PKI 참여자

1.3.1. 인증기관

최상위 인증기관은 다음과 같은 업무를 수행한다.

- 인증기관의 신원확인
- 인증업무준칙(CPS), 이용약관, 개인정보처리 방침의 제 개정

- 인증기관 인증서의 발급, 갱신, 폐지 및 인증기관 인증서 폐지 목록(ARL)의 게시
- 최상위 인증기관에서 발급한 인증기관 인증서의 유효성 확인
- 인증업무에 관한 기록의 안전한 보관·관리
- 인증업무의 안전성과 신뢰성을 확보하기 위한 인증기관의 인증업무 운영 실태점검

인증기관은 다음과 같은 업무를 수행한다.

- 가입자 인증서의 발급, 갱신, 폐지 및 인증서 폐지 목록(CRL)의 게시
- 해당 인증기관에서 발급한 인증서의 유효성 확인
- 인증업무에 관한 기록의 안전한 보관·관리
- 인증업무의 안전성과 신뢰성을 확보하기 위한 인증업무 운영 실태점검

1.3.2. 등록기관

등록기관은 사용자인증서 발급, 갱신, 재발급, 폐지 신청을 검토/등록 처리하는 기관이다. GSSL 인증기관은 등록기관으로서, 신청자와 신청기관의 신원을 확인하고, 신청서를 검토하며, 외부 등록기관은 운영하지 않는다.

1.3.3. 가입자

가입자는 인증기관이 발급한 TLS 인증서(이하 가입자 인증서)의 사용이 허가되어 가입자 인증서 생성 키(개인 키)를 사용할 수 있는 행정/공공기관으로 가입자는 가입자 인증서를 보유한다. 가입자는 3.2 (최초 신원확인) 항목을 거쳐 가입되며, 인증서 사용을 위해서는 인증서 발급 이전에 이용약관에 기술된 책임과 의무사항에 동의하여야 한다.

1.3.4. 신뢰당사자

신뢰당사자는 인증기관이 발급한 가입자 인증서를 이용하여 전자서명 검증 또는 암호화된 문서나 메시지를 복호화하는 개인이나 기관이다.

1.3.5. 기타 참여자

1.3.5.1. 행정안전부

행정안전부는 정부 웹보안인증서 인증체계의 감독 기관으로 다음과 같은 업무를 수행한다.

- 정부 웹보안인증서 인증체계의 구축 및 운영
- 최상위 인증기관/인증기관의 인증업무 운영 실태점검 및 시정조치 요구
- 인증업무준칙(CPS)의 개정

1.3.5.2. 국가정보자원관리원

국가정보자원관리원은 정부 기관의 주요정보통신기반시설을 운영하는 국가기관이다.

정부 웹보안인증서 인증체계의 모든 시스템은 국가정보자원관리원의 자산으로 위탁되어 있으며, 국가의 주요정보통신기반시설 운영 절차에 따라 운영된다. 인증관리 업무와 관련하여 인증시스템에 대한 물리적 보안, 시스템에 대한 접근 통제 및 승인 업무를 주관한다.

1.3.5.3 한국지역정보개발원

한국지역정보개발원은 행정안전부 장관으로부터 최상위 인증기관 및 인증기관 운영업무를 위탁받은 기관이다.

운영센터는 정부 웹보안인증서 인증관리체계의 최상위 인증기관 및 인증기관 업무를 수행하는 전문조직이다.

운영센터는 다음과 같은 업무를 수행한다.

- 인증기관 인증서 발급 · 관리 등 인증업무
- 인증기관 시설 및 장비 기준 제정
- 인증기관의 시설 및 장비의 안전 운영 여부 점검 또는 이에 상응하는 조치
- 인증기관의 인증서와 인증서 폐지 목록 게시
- 인증기관이 생성한 모든 인증서와 인증서 폐지 목록의 보관
- 인증기관 관리에 관련된 정보 및 기록의 유지
- 정부 웹보안인증서 인증관리체계에 속하는 임직원에 대한 인증업무 관련 교육
- 기타 인증업무와 관련하여 필요하다고 인정되는 업무

1.4. 인증서의 용도

1.4.1. 인증서 종류 및 용도

인증업무준칙(CPS)에 따라 발급된 가입자 인증서는 인증서 내 확장 키 사용(Extended Key Usage) 필드의 정의에 따라 서버 인증과 클라이언트 인증 용도로 사용된다. 인증기관은 조직 유효성 검사(OV) 인증서를 발급한다.

1.4.2. 인증서 이용 제한

인증서는 발급받은 목적과 용도에 맞게 사용하여야 하며 이용 범위와 용도를 벗어나 부정하게 사용하는 것을 금지한다. 또한, 유효기간이 만료 또는 폐지된 인증서를 사용하여서는 안된다.

인증서는 거래 상대측의 신뢰성, 준법성, 거래의 안전성을 담보하지 않으며, 인증서 발급 시점 기준으로 인증서 내 정보가 정확하게 검증되었다는 사실만을 입증한다. 인증서의 용도는 3.2 (최초 신원확인) 항목, 4.2 (인증서 신청처리) 항목에 따라 검증된 가입자의 웹사이트와 접속 브라우저 간 전송 정보의 암호화에 한정하여 사용한다.

1.5. 인증업무준칙(CPS) 관리

1.5.1. 인증업무준칙(CPS) 제정 및 개정

행정안전부는 인증업무준칙(CPS)을 제정하고 인증업무준칙(CPS)의 일관성을 유지하기 위해 CA/Browser Forum 최신 요구사항을 확인하여 최소 연 1회 본 인증업무준칙(CPS)을 개정한다.

1.5.2. 인증업무준칙(CPS)의 담당

인증업무준칙(CPS)과 관련된 담당자의 연락처는 다음과 같다.

전화번호 : 1661-9088(내선 2)
팩　　스 : 02)2031-9363
웹사이트 : ssl.gpki.go.kr
이 메 일 : gssl@klid.or.kr
주　　소 : (03923) 서울 마포구 성암로 301, 한국지역정보개발원

1.5.3. 인증업무준칙(CPS)의 책임

인증업무준칙(CPS)의 제정 및 개정의 책임은 행정안전부 장관에게 있다. 인증업무준칙(CPS) 개정 이력은 인증업무준칙(CPS) 버전 및 사유 등을

기재한다.

1.5.4. 인증업무준칙(CPS)의 개정 승인 절차

인증기관은 기술적 또는 절차적인 변경 등의 사유가 발생할 때 행정안전부 장관의 승인을 받아 인증업무준칙(CPS)을 개정한다. 개정된 모든 내용은 2.(게시 및 저장소 책임)에 기술된 위치에 게시한다. 개정에 따른 가입자에 대한 중대한 영향의 발생 가능성이 있는 경우, 가입자에게 웹사이트를 통해 통지할 수 있다.

1.6. 정의 및 약어

1.6.1. 정의

- 가입자 : 인증기관으로부터 인증서를 발급받은 기관, 법인 및 단체를 말한다.
- 가입자 인증서 : 전자정부법 제2조 제9호에 해당하는 법인·기관 및 단체에 발급하고, 전자정부 웹사이트와 이용자 브라우저 간에 전송되는 정보를 안전하게 보호하기 위해 암·복호화 용도로 사용되는 전자적 정보를 말한다.
- 가입자 인증서 생성 키(개인 키, private key) : 가입자 인증서를 생성하기 위하여 이용하는 전자적 정보로 가입자가 보유하는 정보를 말한다.
- 가입자 인증서 검증 키(공개 키, public key) : 가입자 인증서를 검증하기 위하여 이용하는 전자적 정보로 인증서 내에 포함되는 정보를 말한다.
- 객체 식별자(OID) : 가입자 인증서 내에는 가입자(DN), 발급자, 버전 등 기본정보 외에 알고리즘, 인증서 정책, 키 용도, 인증서 속성 등이 포함되며, 정보들이 표현하는 대상을 객체(Object)라 한다. 이러한 객체들을 유일하게 중복되지 않고 식별하기 위해서는 각 객체에 고유번호를 부여하는 방법이 사용되며, 이것을 객체 식별자(OID, Object Identifier)라 한다.
- 고유식별 이름(DN) : 소유자 객체를 명확히 구별할 수 있도록 부여하는 고유한 이름을 말한다.
- 국제인터넷주소관리기구(ICANN) : 국제인터넷주소관리기구는 1998년에

설립된 인터넷의 비즈니스, 기술계, 학계 및 사용자 단체 등으로 구성된 기관으로 인터넷 DNS의 기술적 관리, IP 주소 공간 할당, 프로토콜 파라미터 지정, 루트 서버 시스템 관리 등의 업무를 조정하는 역할을 한다.

- 국가정보원: 대한민국 정부/공공기관 대상의 최상위 국가 사이버 보안 관리기관을 말한다.
- 온라인 인증서 상태 검증 프로토콜(OCSP) : 인증서 폐지 목록(CRL)을 획득하지 않고도 실시간으로 인증서의 상태를 검증할 수 있도록 하는 인증서 상태 실시간 검증 프로토콜을 말한다.
- 신청기관 : 가입자 인증서를 발급받기 위해 인증서를 신청한 법인·기관 및 단체를 말한다.
- 신청자 : 가입자 인증서를 발급받기 위한 신청기관을 대표하는 개인을 말한다.
- 소유자(Subject) : 인증서 내에 기재된 소유자의 고유한 명칭을 말한다.
- 인증 : 가입자 인증서 생성 키가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명해 주는 행위를 말한다.
- 인증기관(CA) : 전자서명 인증서를 발급하는 신뢰 기관으로 인증서 폐지 목록(CRL)을 주기적으로 발행하며, 웹사이트에 인증기관 인증서와 인증서 폐지 목록(CRL)을 게시 등의 인증업무를 담당한다.
- 인증업무 : 인증서 발급·갱신·폐지, 가입자 정보등록·변경, 인증서·인증서 폐지 목록(CRL)의 공고 등 인증서 및 인증 관련 기록의 관리 등의 업무를 말한다.
- 인증서 폐지 목록(CRL) : 인증서 효력이 상실된 인증서들의 목록으로 인증기관에서 주기적으로 발급하는 전자적 정보를 말한다.
- 인증서 투명성(Certificate Transparency) : 인증서의 발급을 모니터링하고 감사하기 위해 공개 로그 시스템에 모든 인증서를 기록하여 식별할 수 있도록 하는 인터넷 보안 표준을 말한다.
- 조직 유효성 검사(OV) 인증서 : 신청기관 신원 검증과 도메인 소유권 심사를 통해 발급되고, 검증된 정보가 인증서에 표시되어, 사이트의 소유권을 확인할 수 있는 인증서를 말한다.
- 해시 함수(Hash Function) : 임의의 길이의 문자열을 고정된 길이의 이진 문자열로 매핑하여 주는 함수. 데이터를 자르고, 치환하거나 위치를 바꾸는 방법들로 결과를 만들어 내며, 이 결과를 해시값(hash value)이라 한다. 해시 함수는 데이터의 무결성, 인증, 부인방지 등에서 응용되는 중요한 함수 가운데 하나이다.

- CA/Browser Forum : 국제 인증기관이 충족해야 하는 요구사항을 설정하고 관리하는 인증기관 및 브라우저로 구성된 국제 그룹이다.
- CSPRNG(Cryptographically Secure Pseudo-Random Number Generator) : 암호학적으로 안전한 의사 난수 생성기 또는 암호화된 의사 난수 생성기를 말한다.

1.6.2. 약어

- ARL: Authority Revocation List
- CA: Certificate Authority or Certification Authority
- CAA: Certification Authority Authorization
- CABF: CA/Browser Forum
- CPS: Certification Practice Statement
- CRL: Certificate Revocation List
- CSR: Certificate Signing Request
- CT: Certificate Transparency
- DN: Distinguished Name
- DNS: Domain Name System or Domain Name Service
- FIPS: (US Government) Federal Information Processing Standard
- FQDN: Fully Qualified Domain Name
- HSM: Hardware Security Module
- HTTP: Hypertext Transfer Protocol
- ICANN: Internet Corporation for Assigned Names and Numbers
- IETF: Internet Engineering Task Force
- NTP: Network Time Protocol
- OCSP: Online Certificate Status Protocol
- OID: Object Identifier
- OV: Organization Validation
- PKCS: Public Key Cryptography Standard
- PKI: Public Key Infrastructure
- PKIX: IETF Working Group on Public Key Infrastructure
- RA: Registration Authority
- RFC: Request for Comments (IETF.org)
- SCT: Signed Certificate Timestamp

- SHA: Secure Hashing Algorithm
- SSL: Secure Sockets Layer
- TLS: Transport Layer Security
- URL: Uniform Resource Locator
- UTC: Coordinated Universal Time

2. 게시 및 저장소 책임

국문/영문 인증업무준칙(CPS)은 인증기관 웹사이트(ssl.gpki.go.kr)에 게시한다. 인증업무준칙(CPS)의 변경사항 및 개정 이력을 5.4 (감사 로깅(Audit logging) 절차) 항목에 따라 기록・보관한다.

2.1. 저장소

인증기관은 저장소에 인증업무준칙(CPS)을 포함하여 다음 정보를 게시한다.

- 인증업무준칙(CPS)
- 가장 최근에 발급된 가입자 인증서 폐지 목록(CRL)
- 가장 최근에 발급된 인증기관 인증서 폐지 목록(ARL)
- 최상위 인증기관 및 인증기관 인증서
- 그 밖에 공개가 필요하다고 판단되는 기타 문서 또는 정보

인증기관은 인증업무준칙(CPS)의 개정 후 7일 이내에 공개된 저장소에 개정된 인증업무준칙(CPS)를 게시한다.

2.2. 정보공개 채널

인증기관은 인증서 발급 및 관리 정보를 누구나 쉽게 이용할 수 있도록 웹사이트에 게시한다.

웹사이트 : ssl.gpki.go.kr
전자메일 : gssl@klid.or.kr
우　　편 : (03923) 서울 마포구 성암로 301
전　　화 : +82 1661-9088(Ext. 2)
팩　　스 : +82 02)2031-9363

2.3. 정보공개 주기

가입자 인증서의 인증서 폐지 목록(CRL)은 매일 갱신되며, 인증기관 인증서의 인증서 폐지 목록(ARL)은 최소 364일마다 갱신된다. 인증기관은 최신 CA/Browser Forum의 규정에 따라 인증업무준칙(CPS)을 최소 연

1회 개정한다.

2.4. 접근 통제

인증기관 웹사이트에 게시된 정보는 누구나 열람할 수 있도록 읽기 전용으로 공개되어 있다. 인증기관은 물리적·논리적으로 보안을 통제하여 저장소가 무단으로 수정되거나 삭제되지 않도록 보호한다.

3. 식별 및 인증

3.1. 인증서의 명칭 및 DN 체계

가입자 인증서의 명칭 및 DN 체계는 ITU X.509 표준을 준수한다. 인증기관은 한글 도메인 이름에 대해 Punycode 인코딩 방식을 지원한다.

3.1.1. 인증서 DN의 종류

가입자 조직 유효성 검사(OV) 인증서의 DN은 다음 체계를 준수한다.

- CN=웹사이트 URL
- O=기관명
- L=시명
- S=시도명
- C=국가명

3.1.2. 명칭 의미

인증기관은 가입자 고유식별 이름(Subject DN)과 발급자 고유식별 이름(Issuer DN) 모두에 의미 있는 명칭을 부여하고 소유자와 발급자를 각각 식별해야 한다.

3.1.3. 신청인의 식별이 불가능한 익명의 인증서 발급

인증기관은 익명 또는 가명 인증서를 발급하지 않는다.

3.1.4. 인증서 DN 규칙

인증서의 기본 영역에 사용되는 명칭과 해석 규칙은 X.500 표준 및 ASN.1 구문을 준수한다.

3.1.5. 인증서 DN 값의 유일성

인증서의 DN은 도메인 이름을 포함하고 있으며, 도메인 이름의 유일성은 국제인터넷주소관리기구(ICANN)에 의해 관리된다. 소유자 대체 이름(Subject Alternative Name) 내 기입되는 전체 도메인 이름(Fully Qualified

Domain Name, FQDN)은 3.2.2.4 (도메인 인증 여부 또는 접근 권한 확인) 항목에 따라 검증되고, 가입자 인증서의 일련번호는 유일하게 부여되며 재사용 되지 않는다.

3.1.6. 인증서 상표(Trade marks)의 사용

해당 사항 없음

3.2. 최초 신원확인

3.2.1. 개인 키 소유 증명 방법

최상위 인증기관은 행정안전부 장관이 고시한 인증기관에만 인증기관 인증서를 발급한다. 인증기관 인증서는 인증서 서명 요청(CSR, Certificate Signing Request) 파일의 공개 키를 확인한 후 발급한다.

신청기관은 인증기관에게 PKCS#10 형식의 인증서 서명 요청(CSR) 또는 이와 암호학적으로 동등한 수준의 증거를 제공하여 개인 키의 소유권을 증명해야 한다.

3.2.2. 조직 및 도메인의 초기 신원확인

인증기관은 하기의 경우에 신청기관 및 인증서에 명시된 모든 담당자, 객체, 장치 및 도메인을 식별하고 검증한다.

- 인증서 신청 시
- 인증서 재발급 신청 시

본 인증업무준칙(CPS)에서 정의하는 범위 내에서 폐지를 요청할 수 있는 권한을 보장하기 위해 신청자의 적절한 검증이 수행되어야 한다. 인증서에 포함될 모든 소유자(Subject) 정보는 본 인증업무준칙(CPS)의 요구사항을 충족하고 본 인증업무준칙(CPS)의 절차에 따라 검증되어야 한다. 검증 프로세스는 다음을 목적으로 한다.

- 인증서를 신청하는 신청기관과 신청자의 신원확인
- 신청기관의 기관명 및 존재 여부 확인
- 신청기관의 물리적 위치(주소) 확인
- 인증서에 포함할 도메인 이름의 소유권 확인
- 신청기관이 인증서를 요청할 수 있는 권한이 있는지 확인

3.2.2.1. 신원확인

인증기관은 조직 유효성 검사(OV) 인증서 신청 시 다음 중 하나 이상을 통해 제공되는 문서를 이용하거나 의사소통을 통해 신원과 주소를 확인한다.

- 신청기관의 설립, 존속 또는 공인 여부를 관할하는 정부 기관
- 정기적으로 업데이트되고 신뢰성이 인정되는 제3자 데이터베이스
- 인증기관에 의한 사이트 현장 방문

일반적으로 인증서 신청서는 온라인으로 제출된다. 신청기관이 웹사이트에 온라인 양식을 작성하여 제출하면 인증기관은 다음 사항을 확인한다.

- 신청기관 및 신청자의 신원
- 신청기관의 주소

신원확인 대상	신원확인 방법
신 청 자	·신청서 제출 이전 및 신청 진행 시점의 신청기관을 대표하는 신청자 정보(성명, 연락처, 소속, 고용상태, 신청 자격) 수집
신청기관	·인증기관에 증명할 수 있는 정보 제출(예: 홈택스에서 3개월 이내 발급한 영문 사업자등록증명원 서류) ·신청기관이 제출한 정보를 신뢰할 수 있는 제3자 데이터베이스에서 조회 및 검증(예: 국세청 홈택스 웹사이트에서 검증) · 신뢰할 수 있는 제3자 데이터베이스(예: 114.co.kr 등)에서 확인된 대표전화번호로 전화하여 신청기관 및 신청자 정보(성명, 고용상태, 신청 자격 등) 확인
신청기관 주소	조직 유효성 검사(OV) 인증서의 소유자(Subject) 필드에 확인된 지리적 주소 정보만 포함할 수 있다. 신청기관이 제출한 정보를 신뢰할 수 있는 제3자 데이터베이스와 비교하고 검증한다. 주소에 국제표준이나 정부 공식표준이 있으면 우선하여 준수한다. 인증기관이 인증서의 소유자(Subject) 필드에 포함된 주소를 결정하는 일반적인 기준은 다음과 같다. • 국가 이름(Country Name, C): ISO 3166-1 Alpha-2에 따른 두 글자의 국가 코드 사용(국가 이름 필드가 있는 경우, 인증기관은 신청자가 실제 위치한 국가 이외의 다른 국가에 할당된 IP주소에서의 인증서 신청을 방지하기 위해 프록시 서버를 차단한다) • 주 또는 지방(State or Province, S): ISO 3166-2에 따른 주 또는 지방(예: 특별시, 광역시, 도)의 약어가 아닌 공식 명칭 사용 • 지역 또는 도시(Locality or City, L): Locality 필드는 도시 또는 마을의 공식 영어 이름 사용 단, 신청기관 신원확인 과정에서 확인된 주소 정보와 신청서에 작성되어있는 주소 정보가 동일한 경우 신청기관 주소 검증 단계는 완료된 것으로 간주한다.

인증기관은 특별한 경우 현장 방문 및 대면 방식으로 신청기관 및 신청자의 신원을 확인할 수 있다.

3.2.2.2. 상호/상표

해당 사항 없음

3.2.2.3. 국가 확인

해당 사항은 3.2.2.1 (신원확인) 항목 참조

3.2.2.4. 도메인 인증 여부 또는 접근 권한 확인

검증 방법	상세 내용
도메인 담당자에게 이메일, 팩스, SMS, 우편 중 한 가지 발송	이메일, 팩스, SMS, 우편 중 한 가지 방식을 통해 전체 도메인 이름(FQDN, Fully-Qualified Domain Name)(이하 “FQDN”)에 대한 신청기관의 접근 권한을 확인하고 임의값(Random Value)을 이용해 확인된 응답을 수신한다. 임의값(Random Value)은 인증기관에서 생성하고, 생성 후 최대 30일까지 유효하다. (CA/Browser Forum 기준 3.2.2.4.2 항목 참조)
도메인 담당자에게 이메일 발송	(i) ’admin’, ’administrator’, ’webmaster’, ’hostmaster’, ’postmaster’ 중 한 가지로 로컬파트가 구성된 하나 이상의 이메일 주소로 이메일을 보낸다. 이메일 주소는 로컬파트, @, 인증받은 도메인 순서로 구성된다. (ii) 이때 이메일에 임의값(Random Value)을 포함한다. (iii) 임의값(Random Value)을 이용해 확인된 응답을 수신한다. 임의값(Random Value)은 인증기관에서 생성하고, 생성 후 최대 30일까지 유효하다. (CA/Browser Forum 기준 3.2.2.4.4 항목 참조)

3.2.2.5. IP주소 인증

해당 사항 없음

3.2.2.6. 와일드카드 도메인 검증

해당 사항 없음

3.2.2.7. 데이터 소스 정확성 및 유효기간

모든 데이터 소스는 식별 및 인증(I&A: Identification and Authentication) 용도로 사용되기 전에 신뢰성, 정확성 및 위조로부터의 안정성 여부를 위해 검증되어야 한다. 데이터 소스의 정확성과 신뢰성을 CA/Browser Forum 기준(Baseline Requirements) 3.2.2.7 항목에 준거하여 평가한다.

데이터 소스의 재검증 유효기간은 다음과 같다.

- 신청기관의 법적 존재 및 신원확인 : 397일 이내

3.2.2.8. CAA 기록

4.2.4 (인증기관 승인 기록) 항목 참조

3.2.3. 개인 인증서의 초기 신원확인

인증기관은 개인에게 인증서를 발급하지 않는다.

3.2.4. 검증되지 않은 가입자 정보

인증서에는 검증된 정보만 포함되며, 인증서 소유자(Subject) 필드 내 선택적 하위 필드(Optional subfields)는 검증된 정보를 포함하거나 공란으로 두어야 한다.

3.2.5. 권한 검증

인증기관은 '신뢰할 수 있는 커뮤니케이션 방법'을 활용해 신청자의 인증서 요청의 진위를 검증한다. 인증기관은 신뢰할 수 있는 커뮤니케이션 방법으로 3.2.2.1 (신원확인) 항목에 나열된 방법을 사용한다.

기관을 대표하여 인증서를 요청하는 신청인의 권한은 3.2.2.1 (신원확인) 항목에 따라 확인한다. 인증기관은 신뢰할 수 있는 방법으로 검증된 신청자의 인증서 발급 신청만을 접수한다.

3.2.6. 상호 운용 기준

해당 사항 없음

3.3. 키 교체 요청에 대한 신원확인 및 인증

인증기관은 인증서 키 교체를 제공하지 않는다. 키 교체 요청에 대해 인증기관은 3.2 (초기 신원확인) 항목과 동일한 신청 및 검증 절차를 수행한다.

3.3.1. 키 교체에 대한 신원확인 및 인증

3.2.2 항목 참조

3.3.2. 폐지 후 키 교체에 대한 신원확인 및 인증

해당 사항 없음

3.4. 폐지 신청에 대한 신원확인 및 인증

가입자는 사용하지 않거나, 키 쌍 훼손이 의심되는 경우, 아이디/패스워드 등을 이용하여 인증기관 웹사이트에서 인증서 폐지를 신청할 수 있다. 또한 관련 웹브라우저사에서도 손상을 의심할 수 있는 증거를 가지고 있다면

인증서 폐지를 요청할 수 있다.

인증기관 또는 가입자의 키 쌍이 훼손되었거나 훼손이 의심되면 본 인증업무준칙(CPS) 4.9.1 (인증서 폐지 기준) 항목에 따라 관계된 인증기관 또는 가입자 인증서를 폐지할 수 있다. 인증기관은 폐지 대상 가입자에게 인증서 폐지에 대해 공지한다.

4. 인증서 생명주기 운영 요구사항

본 항목에서는 인증서 신청 절차, 인증서의 생명주기와 관련하여 가입자 및 기타 참여자에게 요구되는 사항들을 설명한다.

인증서 생명주기는 아래와 같이 분류된다.

- 인증서 신청
- 인증서 신청처리 절차
- 인증서 발급
- 인증서 수령
- 키 쌍 및 인증서 사용
- 인증서 재발급
- 인증서 폐지 및 효력 정지
- 인증서 상태 서비스
- 인증 서비스 해지 및 종료
- 키 위탁 및 복구

4.1. 인증서 신청

4.1.1. 인증서 신청 기준

인증기관 인증서 발급은 PKCS#10 인증서 서명 요청(CSR) 형식으로 인증기관 공개 키를 제출해야 한다. 인증기관 인증서는 전자정부법 시행령 제89조 제1항에 따라 행정안전부 장관이 인증업무를 위탁한 기관만이 발급받을 수 있다.

가입자 인증서는 신청서를 인증기관 공식 웹사이트에서 온라인 양식으로 작성하여 제출해야 한다. 신청기관은 가입자 인증서를 신청할 수 있는 전자정부법 제2조 제9호에 해당하는 행정기관 또는 공공기관이다. 신청자는 WHOIS의 AC(Administrative Contact) 필드에 등록되고 신청기관으로부터 적법한 권한을 부여받는 신청기관 고용인 또는 위임자로서 인증기관 공식 웹사이트 가입 시 이용약관에 동의하여야 한다.

- 인증서 신청 정보에 인증서 소유자(Subject)에 포함될 도메인 명칭이

포함되어야 한다. 인증기관은 해당 도메인 명칭이 WHOIS 또는 허용·신뢰할 수 있는 데이터베이스에 포함되었는지 확인한다.

- 인증서 신청 정보에 인증서 SAN(Subject Alternative Name)에 포함될 도메인 명칭이 포함되어야 한다.
- 피싱이나 사기가 의심되어 폐지된 인증서 또는 발급 거부된 신청 정보는 인증기관 내부 데이터베이스에 저장되며 해당 정보를 사용하여 의심스러운 발급요청 식별에 사용할 수 있다.

4.1.2. 인증서 신청 절차 및 책임

최상위 인증기관은 인증기관의 신청서 및 신청 절차 완료를 확인해야 하며 인증기관은 신청내용의 신뢰성에 대해 책임을 진다.

인증기관은 인증서 발급 전에 신청기관이 아래 신청 절차를 완료했음을 확인해야 한다.

- 인증서 신청서 제출
- 이용약관 동의
- 신청서에 명시된 증빙 서류 제출
- 안전한 툴을 이용한 키 쌍 및 인증서 서명 요청(CSR) 생성
- 공개 키가 포함된 인증서 서명 요청(CSR) 제출

4.2. 인증서 신청처리

인증기관은 신청기관이 제출한 정보가 정확한지 검증한다. 신청기관은 PKCS#10 인증서 서명 요청(CSR) 형식으로 공개 키를 인증기관에 제출한다.

4.2.1. 신원확인 및 인증

3.2 항목에 명시된 절차대로 신청기관이 제출한 정보의 식별 및 신원 확인을 수행한다.

4.2.2. 신청에 대한 승인 및 거절

인증기관은 신청 정보의 유효성 검증 완료 시 인증서 요청을 승인하여, 하기의 경우 신청을 거절한다. 신청 정보가 유효성이 검증되지 않거나, 신청이 CPS에 부합하지 않는 경우 인증서 신청을 거절한다.

- 신청 정보 유효성이 검증되지 않는 경우
- 신청이 CPS에 부합하지 않는 경우
- 공개 키가 CA/Browser Forum 기준 6.1.5, 6.1.6을 충족하지 못하는 경우

- 취약한 개인 키(예시: Debian weak key)

4.2.3. 신청처리 소요시간

기타 계약서에 명시되지 않는 한 인증서 신청처리에 관련된 규정된 소요시간은 없으며, 신청기관의 신청서 및 제출서류 검증이 정상적으로 처리된 경우 인증기관 인증서 및 가입자 인증서는 신청 후 30일 이내 인증서를 발급한다.

4.2.4. 인증기관 승인 기록

인증기관은 RFC 8659에 기술된 절차에 따라, 발급될 인증서의 subjectAltName 확장 필드의 각 dNSName에 대한 CAA 기록을 검토한다. CAA ‘issue’ 또는 ‘issuewild’ 기록에 아래 발급자 도메인 이름이 있을 때 인증기관이 인증서를 발급할 수 있는 것으로 인정된다.

- ssl.gpki.go.kr

인증기관은 차후 CA/Browser Forum에서 피드백 요청 시 제공할 수 있도록 CAA 기록 검증에 따라 발급이 제한된 신청에 관한 내용을 상세히 문서화 한다.

4.3. 인증서 발급

인증기관이 발급하는 인증서는 CA/Browser Forum 기준에 의하여 다음 각호의 사항을 포함한다.

- 도메인을 구분하는 명칭
- 인증서 검증 키(공개 키)
- 인증서의 일련번호 :모든 인증서에는 최소 64bit의 CSPRNG 숫자를 포함하여 0보다 큰 일련번호가 포함되어야 한다.
- 인증서의 유효기간 : 397일 이내
- 인증서의 이용 범위 또는 용도를 제한하는 경우 이에 관한 사항

인증기관은 가입자 인증서를 발급하기 전에 CA/Browser Forum 기준(Baseline Requirements) 9.6.3 항목에 따라 가입자 계약서 또는 이용약관을 입수한다.

4.3.1. 인증서 발급 절차

최상위 인증기관의 CA 인증서 발급 시, 인가된 CA 인원이 커맨드를 이용하여 인증서 서명을 수행하여야 한다.

가입자 인증서는 인증서 발급을 위한 신원확인 및 검증 절차가 완료

되면 인증서가 생성되고 키 사용 확장 필드가 추가된다.

인증기관은 사전인증서를 포함하여 인증서 발행 시 인증서 전자서명 처리 이전에 Lint 테스트를 수행하고, 규격오류 발견 시 인증서 발행을 거절하고, 로그를 기록한다.

가입자 인증서는 RFC 6962 표준인 인증서 투명성을 지원하기 위해 3개 이상의 CT 로그에 인증서를 제출하고 서명된 인증서 타임스탬프(SCT)를 수신하여 인증서의 확장 필드에 포함한다.

4.3.2. 인증서 발급 통지

인증기관은 인증서 발급 후 합리적인 시간 내에 인증서를 전달한다. 가입자 인증서는 발급되는 즉시 신청자에게 메시지가 발송된다. 가입자에게 발송되는 메시지는 이메일을 사용한다.

4.4. 인증서 수령

4.4.1. 인증서 수령 절차

인증기관 인증서는 보안 매체에 저장하여 인증기관이 수령하며 특별한 사유가 없는 한 거부할 수 없다.

가입자 인증서는 신청자 본인이 공식 인증기관 웹사이트를 이용하여 인증서를 다운로드 한다.

4.4.2. 인증서 게시

인증기관은 최상위 인증기관 및 인증기관 인증서를 저장소에 게시·공개한다.

4.4.3. 타 주체에 대한 CA에 의한 인증서 발급 통보

해당 사항 없음

4.5. 키 쌍 및 인증서 용도

4.5.1. 인증서 생성 키(개인 키) 사용 용도

인증서의 개인 키는 검증된 가입자의 웹사이트와 접속브라우저 간 전송정보의 암호화에 한정하여 사용한다.

인증기관은 가입자가 약관 9.6.3. (가입자 진술 및 보증) 항목의 2 (개

인 키 보호), 4 (인증서 사용) 항목을 준수하도록 요구하여야 한다.

4.5.2. 신뢰당사자 인증서 검증 키(공개 키)와 사용 용도

해당 사항 없음

4.6. 인증서 갱신

4.6.1. 인증서 갱신 기준

인증서 갱신이란 동일한 키 쌍 및 인증서 소유자(Subject) 정보를 변경하지 않고, 유효기간이 연장된 새로운 인증서를 발급하는 것을 말한다. 인증기관 인증서는 최상위 인증기관 인증서 유효기간 내에서 갱신할 수 있으며, 가입자 인증서는 갱신을 제공하지 않는다. 따라서, 가입자는 인증서 만료 전 30일 이내에 인증서 재발급을 신청하여야 한다. 가입자는 다음의 사유로 인증기관에게 인증서 재발급 신청을 할 수 있으며, 인증기관은 가입자가 요청한 인증서 재발급을 승인한 후 4.1 (인증서 신청) 항목에 따라 새로운 인증서를 발급한다.

- 인증서 유효기간이 만료된 경우
- 신청자의 인증서 개인 키가 노출, 손상, 분실 또는 변경되었다고 우려되는 인증서를 새로 발급받고자 하는 경우
- 인증서 관련 정보가 변경된 경우

4.6.2. 인증서 갱신 신청기관

해당 사항은 4.1.1 (인증서 신청 기준) 항목 참조

4.6.3. 인증서 갱신 절차

해당 사항은 4.2 (인증서 신청 처리) 항목 참조

4.6.4. 인증서 갱신 통지

해당 사항은 4.3.2 (인증서 발급 통지) 항목 참조

4.6.5. 인증서 갱신 수령

해당 사항은 4.4.1 (인증서 수령 절차) 항목 참조

4.6.6. 인증서 갱신 게시

해당 사항은 4.4.2 (인증서 게시) 항목 참조

4.6.7. 다른 기관에 인증서 갱신 통지

해당 사항 없음

4.7. 인증서 키 교체

4.7.1. 인증서 키 교체 기준

인증서 키 교체는 인증서의 유효기간 등 인증서 정보변경 없이 새로운 공개 키를 가진 인증서를 발급하는 것을 말한다.

인증기관은 인증서 키 교체를 제공하지 않는다. 키 교체가 필요한 경우 신규 발급으로 간주하여 4.1 (인증서 신청) 항목에 따라 신규 신청 절차가 적용된다.

인증기관은 인증기관 인증서의 개인 키 손상 등 재해 발생 시 인증기관 인증서를 폐지하며, 4.1 (인증서 신청) 항목에 따라 새로운 인증기관 인증서를 발급한다.

4.7.2. 인증서 키 교체 신청기관

해당 사항은 4.1.1 (인증서 신청 기준) 항목 참조

4.7.3. 인증서 키 교체 절차

해당 사항은 4.2 (인증서 신청 처리) 항목 참조

4.7.4. 인증서 키 교체 통지

해당 사항은 4.3.2 (인증서 발급 통지) 항목 참조

4.7.5. 인증서 키 교체 수령

해당 사항은 4.4.1 (인증서 수령 절차) 항목 참조

4.7.6. 인증서 키 교체 게시

해당 사항은 4.4.2 (인증서 게시) 항목 참조

4.7.7. 다른 기관에 인증서 키 교체 통지

해당 사항 없음

4.8. 인증서 변경

4.8.1. 인증서 변경 기준

인증기관은 발급된 인증서를 변경하지 않으며, 모든 인증서 변경요청은 인증서 신규 발급절차에 따른다.

4.8.2. 인증서 변경 신청기관

해당 사항은 4.1.1 (인증서 신청 기준) 항목 참조

4.8.3. 인증서 변경 절차

해당 사항은 4.2 (인증서 신청 처리) 항목 참조

4.8.4. 인증서 변경 통지

해당 사항은 4.3.2 (인증서 발급 통지) 항목 참조

4.8.5. 인증서 변경 수령

해당 사항은 4.4.1 (인증서 수령 절차) 항목 참조

4.8.6. 인증서 변경 게시

해당 사항은 4.4.2 (인증서 게시) 항목 참조

4.8.7. 다른 기관에 인증서 변경 통지

해당 사항 없음

4.9. 인증서 폐지 및 정지

인증기관은 인증서 폐지를 지원하되, 인증서의 일시 정지 및 회복은 허용하지 않는다. 인증서가 폐지되면 일련번호가 인증서 폐지 목록(CRL)에 추가되어 폐지된 상태로 표시된다. 인증서의 폐지 요청 및 연관된 문의사항에 대한 대응은 연중무휴로 운영된다.

4.9.1. 인증서 폐지 기준

4.9.1.1. 가입자 인증서 폐지 사유

인증기관은 다음과 같은 사유가 발생하는 경우 24시간 이내에 가입자 인증서를 폐지한다.

- 가입자가 인증기관에서 인증서를 폐지할 것을 서면으로 신청한 경우

- 가입자가 인증서 신청서 원본이 승인되지 않았으며 권한이 소급되지 않았음을 인증기관에 통지한 경우
- 인증서의 공개 키에 해당하는 가입자의 개인 키가 손상되었다는 증거를 입수한 경우
- 인증서의 FQDN 및 IP주소에 대한 도메인 인증 또는 제어의 유효성 검사를 신뢰할 수 없다는 증거를 입수한 경우
- 인증서의 공개 키(예: Debian취약 키 https://wiki.debian.org/SSLkeys 참고)에 해당하는 가입자의 개인 키를 쉽게 계산할 수 있는 입증된 방법을 알게 된 경우

인증기관은 다음과 같은 사유가 발생하는 경우 5일 이내에 가입자 인증서를 폐지한다.

- 인증서가 CA/Browser Forum 요구사항의 6.1.5 및 6.1.6 항목의 요건을 충족하지 않는 경우
- 인증서가 오용되고 있다는 증거를 인증기관에서 입수한 경우
- 가입자 계약서 또는 이용약관에 의해 가입자가 중요 의무를 하나 이상 이행하지 않았음을 인증기관에서 인지한 경우
- 인증서에 사용된 FQDN 또는 IP주소가 절대 법적으로 허용되지 않는다는 징후를 인증기관에서 인지한 경우(예: 법원 또는 중재인에 의해 해당 도메인을 사용할 수 있는 도메인명 등록자의 권리 박탈, 도메인명 등록자와 신청기관 간의 라이선스 또는 서비스 계약 종료 또는 도메인명 등록자에 의해 도메인명 갱신 실패)
- 부정확하거나 오도된 하위기관의 FQDN을 검증하기 위해 와일드카드 인증서가 사용되었다는 점을 인증기관에서 인지한 경우
- 인증서에 포함된 정보의 중요한 변화를 인증기관에서 인지한 경우
- 특정 요건, 인증기관의 인증업무준칙(CPS)에 의해 인증서가 발급되지 않았다는 점을 인증기관에서 인지한 경우
- 인증서에 나타난 정보가 부정확하거나 오도된 것으로 인증기관에서 판단한 경우
- 인증기관이 CRL/OCSP 저장소의 유지보수를 계속하기로 약정한 경우를 제외한, CA/Browser Forum 요구사항에 따라 인증기관의 인증서 발급 권한이 취소 또는 만료되거나 종료되는 경우
- 인증기관의 인증업무준칙(CPS)에 의해 폐지해야 하는 경우
- 가입자의 개인 키를 노출하여 손상시키는 취약점을 인지하거나 개인 키를 생성하는데 특정 결함이 있다는 명백한 증거가 있는 경우

4.9.1.2. 인증기관 인증서 폐지 사유

인증기관은 다음과 같은 사유가 발생하는 경우 7일 이내에 인증기관 인증서를 폐지한다.

- 인증기관이 서면으로 취소를 요청한 경우
- 인증기관이 인증서 신청서 원본이 승인되지 않았으며 권한이 소급되지 않았음을 인증기관에 통지한 경우
- 인증서의 공개 키에 해당하는 인증기관의 개인 키가 손상되었거나 CA/Browser Forum 요구사항의 6.1.5 및 6.1.6 항목의 요건을 더 이상 충족하지 않는 경우
- 인증서가 오용되고 있다는 증거를 인증기관이 입수한 경우
- 인증서가 인증업무준칙(CPS)에 의해 발급되지 않았다는 점을 인증기관이 인지한 경우
- 인증서에 나타난 정보가 부정확하거나 오도된 것으로 인증기관에서 판단한 경우
- 인증기관이 어떠한 이유로 인해 운영이 중단되어, 다른 인증기관이 인증기관 인증서에 대해 폐지 지원을 제공할 수 있도록 준비하지 않은 경우
- 인증기관이 CRL/OCSP 저장소의 유지보수를 계속하기로 약정한 경우를 제외한, CA/Browser Forum 요구사항에 따라 인증기관의 인증서 발급 권한이 취소 또는 만료되거나 종료되는 경우
- 인증업무준칙(CPS)에 의해 폐지해야 하는 경우

4.9.2. 인증서 폐지 신청기관

인증기관 인증서는 행정안전부 장관이 인증업무를 위탁한 기관이 폐지를 신청할 수 있으며, 키 손상을 의심할 수 있는 증거를 가진 관련 웹브라우저사 또한 폐지 신청을 할 수 있다. 가입자 인증서는 4.1.1 (인증서 신청 기준) 항목에 해당하는 신청기관의 업무 담당자가 폐지를 신청할 수 있다.

4.9.3. 인증서 폐지 절차

인증기관은 인증기관 인증서에 대해 4.9.1 (인증서 폐지 기준) 항목에 해당하는 폐지요건 발생 시 아래의 절차에 따라 인증기관 인증서를 폐지 처리한다.

1. 행정안전부, 국가정보원, 유관기관 등에 즉시 보고하고 인증기관 인증서 폐지 신청 공문을 발송한다.
2. 인증기관 인증서 폐지 시 인증기관 인증서 폐지 목록(ARL)을 갱신하고 필요한 때 유관기관에 통보한다.

가입자 인증서는 아래의 절차에 따라 폐지 신청을 처리한다.

1. 3.4 (폐지 신청에 대한 신원확인 및 인증) 항목에 따라 인증서 폐지를 신청했거나 문제를 보고한 신청기관의 신원과 폐지 신청 사유를 기록한다. 인증기관이 판단한 사유도 포함할 수 있다.
2. 해당하면 대역 외 통신수단(예: 전화, 팩스, 이메일 등)을 통해 해당 인증서를 사용하는 관리자에게 폐지 신청 여부 확인을 요청한다.
3. 폐지 신청기관이 인증기관 또는 가입자면 즉시 인증서를 폐지한다.
4. 제 3자의 폐지 요청인 경우 해당 요청을 조사하여 철회가 타당한 경우 접수 후 24시간 이내에 해당 인증서를 폐지한다.
5. 인증기관은 폐지 사유가 합당하다고 판단하면 담당자가 인증서를 폐지하고 인증서 폐지 목록(CRL)을 업데이트한다.

가입자 인증서 폐지 신청 및 문제 보고는 상시 가능하도록 운영한다.

4.9.4. 인증서 폐지 요청 유예 기간

가입자는 아래의 경우에 인증서 생성키(개인키) 및 인증서의 사용을 즉시 중지하고 운영센터에 폐지를 요청하여야 한다.

1. 인증서 생성키(개인키)가 분실・훼손 또는 도난・유출 가능성이 있다고 판단되는 경우
2. 인증서의 정보가 완전하지 않거나 부정확한 경우
3. 인증서가 만료되거나 폐지되었을 경우
4. 인증서 관련정보가 변경된 경우

4.9.5. 인증서 폐지 소요시간

인증기관 인증서 폐지 요청은 접수 후 7일 이내에 처리하고, 인증기관 인증서 폐지 목록(ARL)을 공개된 저장소에 게시한다.

가입자 인증서 폐지 요청은 접수 후 즉시 폐지 절차를 개시한다. 인증서 폐지 이후 폐지 사실의 인증서 폐지 목록(CRL) 반영은 24시간 이상 경과 하지 않아야 한다.

인증기관은 인증서 문제 보고서를 접수한 후 24시간 이내에 보고서와 관련된 사실 및 상황을 조사하고, 그 결과에 대한 예비 보고서를 가입자와 인증서 문제 보고서를 제출한 기관에 제공한다.

사실 및 상황을 검토한 후, 인증기관은 가입자 및 인증서 문제 보고서 또는 기타 폐지를 통지한 기관과 협력하여 인증서 폐지 여부를 확인하고, 폐지할 경우 24시간 이내에 인증서를 폐지할 시점을 설정한다. 인증서 문제 보고서 또는 폐지 관련 통지를 받은 후 인증서 폐지까지 기간은 4.9.1.1 (가입자 인증서 폐지 사유) 항목, 4.9.1.2 (인증기관 인증서 폐지 사유) 항목에 명시된 기간을 초과해서는 안 된다. 폐지 일자는 다음과 같은 기준을 고려한다.

- 제기된 문제의 성격(범위, 상황, 심각도, 규모, 손해 위험)
- 폐지에 따른 영향(가입자 및 신뢰당사자에 대한 직접적 및 부수적 영향)
- 특정 가입자에 대해 접수된 인증서 문제 보고 건수
- 민원 발생(예: 웹사이트가 불법행위를 하고 있다는 법 집행관의 불편 사항은 주문한 물품을 수령하지 않았다는 소비자의 불편 사항보다 우선하여 처리되어야 한다)
- 관련 법률

4.9.6. 신뢰당사자에 의한 인증서 폐지 확인 요건

신뢰당사자는 사용자인증서를 신뢰하기 위해 CRL과 OCSP를 이용하여 인증서 체인 유효성을 검증하여야 한다.

4.9.7. 인증서 폐지 목록(CRL) 발행 빈도

인증기관 인증서 폐지 목록(ARL)은 최소 364일마다 그리고 인증기관 인증서가 폐지된 후 24시간 이내에 갱신 및 재발행하며, 다음 업데이트(nextUpdate) 필드의 값은(thisUpdate) 값으로부터 12개월을 초과하지 않는다.

가입자 인증서 폐지 목록(CRL)은 최소 1일마다 갱신하고, 다음 업데이트(nextUpdate) 필드의 값은 (thisUpdate) 값으로부터 10일을 초과하지 않는다.

4.9.8. 인증서 폐지 목록(CRL) 발급 최대 소요 시간

인증기관 인증서 폐지목록(ARL), 가입자 인증서 폐지 목록(CRL)은 생성 후 1시간 이내에 저장소에 게시된다.

4.9.9. 실시간 인증서 폐지 및 상태 확인

인증기관은 발급하는 인증기관 및 가입자 인증서에 대해 실시간 인증서 상태 검증(OCSP)을 지원한다. 실시간 인증서 상태 검증(OCSP) 주소는 다음과 같다.

- 인증기관 인증서 OCSP : ocsp-rca-ssl.gpki.go.kr
- 가입자 인증서 OCSP : ocsp-ca-ssl.gpki.go.kr

실시간 인증서 상태 검증(OCSP) 응답(response)은 RFC 6960을 준수한다. 인증기관은 실시간 인증서 상태 검증(OCSP) 응답에 서명하기 위한 별도의 인증서를 발급한다. 인증기관에서 서명한 OCSP 인증서에는 RFC 6960에 정의된 대로 id-pkix-ocsp-nocheck 유형의 확장 필드가 포함된다.

4.9.10. 실시간 인증서 폐지 확인 요건

실시간 인증서 상태 검증(OCSP) 응답 메시지의 유효기간 간격은 최소 8시간 이상, 최대 10일 이하여야 한다. 유효기간 간격이 16시간 미만인 경우, 다음 갱신 전에 유효기간의 절반 이전에 정보를 갱신해야 하며, 유효기간 간격이 16시간 이상인 경우, nextUpdate 값 최소 8시간 이전 및 thisUpdate 값 이후 4일 이내에 정보를 갱신한다. 실시간 인증서 상태 검증(OCSP) 응답자(responder)는 OCSP 요청 및 수신에 대해 GET 형식을 사용한다.

인증기관 인증서의 경우 OCSP 응답 메시지를 최소 12개월마다 갱신하여야 하며, 인증기관 인증서를 폐지한 경우 24시간 이내 갱신한다.

4.9.11. 이외 인증서 폐지 알림 수단

해당 사항 없음

4.9.12. 키 손상 관련 특수 요구사항

인증기관 인증서 개인 키가 손상되는 경우, 인증기관은 행정안전부, 국가정보원 등 유관기관에 즉시 통보해야 한다.

가입자 인증서 개인 키가 손상되는 경우, 가입자는 인증서가 손상되었음을 인증기관에 통보해야 한다.

주요 손상은 대표홈페이지 웹사이트에서 보고할 수 있다.
키 손상을 의심할 수 있는 증거를 가진 관련 웹브라우저사는 인증서 폐지를 요청할 수 있다.

4.9.13. 인증서의 정지 기준

해당 사항 없음

4.9.14. 인증서의 효력 정지 신청기관

해당 사항 없음

4.9.15. 인증서의 효력 정지 절차

해당 사항 없음

4.9.16. 인증서의 효력 정지 기간

해당 사항 없음

4.10. 인증서 상태 서비스

4.10.1. 인증서 상태 서비스의 기능적 특징

인증서 폐지 목록(CRL) 또는 실시간 인증서 상태 검증(OCSP)은 10초 안에 응답할 수 있도록 운영하며, 인증서 폐지 목록(CRL) 또는 실시간 인증서 상태 검증(OCSP) 응답에 대한 폐지 항목은 폐지된 인증서의 유효기간이 만료된 후에야 삭제될 수 있다.

4.10.2. 서비스 가용성

유지보수 또는 서비스 장애로 인해 일시적으로 사용할 수 없는 경우를 제외하고 인증기관에서 발급한 만료되지 않은 모든 인증서의 현재 상태를 온라인으로 확인할 수 있도록 인증서 폐지 목록(CRL) 및 실시간 인증서 상태 검증(OCSP) 서비스는 연중무휴(24/7)로 제공한다.

4.10.3. 운영 기능

해당 사항 없음

4.11. 인증 서비스 해지

인증기관은 행정안전부 장관의 변경 고시에 의해 인증 서비스가 종료되고 인증기관 인증서가 해지된다.

가입자는 다음을 통해 인증서를 해지할 수 있다.

- 가입자가 웹사이트에 방문하여 인증서 폐지를 신청하면 인증서 서비스를 해지할 수 있다.
- 인증서 만료 후 신규 발급 또는 재발급하지 않으면 인증서 서비스가

해지된다.

4.12. 키 위탁 및 복구

해당 사항 없음

4.12.1. 키 위탁, 복구 정책 및 절차

해당 사항 없음

4.12.2. 세션 키 캡슐화, 복구 정책 및 절차

해당 사항 없음

5. 시설 관리 및 운영 보호조치

5.1. 물리적 보호조치

인증시스템이 설치된 장소는 외부인의 침입이나 불법적 접근 등의 물리적 위협으로부터 보호된다. 중요한 인증시스템 작업은 최소 4단계의 보안 계층이 있는 물리적으로 안전한 장소에서 수행되며, 인가된 직원만 접근할 수 있도록 다른 시스템과 물리적으로 분리된다.

5.1.1. 위치 및 시설

인증시스템은 국가가 지정한 주요정보통신기반시설에 위치하고 있으며, 국가의 관리 규정에 따라 물리적인 접근 통제를 수행한다. 최상위 인증기관과 관련된 시스템 운영(예: 인증기관 인증서의 키 생성 및 인증)에 따른 전자파를 차단하기 위한 물리적 장벽(예: 3.0T 이상 강철 등)이 설치되어 있다.

5.1.2. 물리적 접근

출입통제시스템을 운영하고 신원확인 카드와 생체인증(지문인증, 정맥인식 등)을 결합하여 통제구역에 대한 접근을 통제하며 출입에 대한 접근권한을 주기적으로 검토한다. 인증시스템실 출입 시에는 감사 추적성을 위해 출입 일시를 작성하며, 인증시스템실 내에서의 활동들은 CCTV에 의해 모니터링된다.

5.1.3. 전원 및 공조시설

인증시스템은 정전 및 기타 전기 이상 현상으로부터 보호하기 위해 무정전 전원 공급 장치(UPS)를 설치 운영한다. 인증시스템 시설 내의 전원 및 통신, 데이터 전송 또는 인증기관의 서비스를 지원하는 케이블들이 차단 또는 손상되지 않도록 보호한다.

온도 및 습도를 일정하게 유지하기 위해 공기조절 시스템을 설치 및 운영한다.

5.1.4. 침수 대비

인증시스템은 침수 방지시설을 갖춘다.

5.1.5. 화재 예방 및 보호

인증기관은 소방 규정을 준수하여 화재 탐지기, 휴대용 소화기 및 자동 소화설비 등이 갖춰진 장소에서 운영된다.

5.1.6. 매체 저장

인증 서비스에 사용되는 저장 및 기록 매체를 내화금고에 저장하여 물리적 접근을 통제한다. 저장 매체(고정 및 이동식 디스크)가 들어있는 모든 장비는 폐기 전에 중요한 데이터가 포함되어 있지 않은지 확인한다. 중요한 데이터가 포함된 저장 매체는 폐기 또는 재사용 전에 물리적으로 파괴하거나 복구되지 않는 방법을 이용하여 기존 데이터를 덮어쓴다.

5.1.7. 폐기물 처리

키, 활성화 데이터 또는 중요 파일을 보관하는 모든 매체를 폐기할 때 내부 절차에 따라 처리하거나 완전히 파기한다.

5.1.8. 원격지 백업

인증 서비스를 위한 원격지 백업을 수행한다. 백업 장소는 주요 설비가 설치된 장소와 동등한 보안 단계 및 통제 수준을 유지한다.

5.2. 절차적 보호조치

5.2.1. 신뢰 역할(Trusted Roles)

운영책임자는 최소 권한의 원칙을 기반으로 신뢰할 수 있는 역할

(Trusted Roles)을 지정하고 승인한다. 지정된 신뢰할 수 있는 역할(Trusted Roles)의 목록은 연 1회 이상 검토되고 현행화되어야 한다. 인증시스템 운영의 보안성과 신뢰도를 위해 아래 나열된 역할을 분담하여야 하며 수행 인력별 이해 상충 관계가 있어서는 안 된다. 신뢰할 수 있는 역할(Trusted Roles)은 아래와 같이 정의한다.

- 관리책임자 : 인증업무 총괄 및 정책 승인
- 정책관리자 : 정책 제 · 개정 및 교육 수행
- 보안 관리자 : 인증시스템 보안 관리
- 내부 감사자 : 감사 로그 검토 수행
- 키 관리자 : 키 생성/이관/파기 절차 수행
- 키 쉐어홀더 : 키 생성/이관/파기 절차에 따른 업무 이행시 M of N 절차 수행
- 내화금고 관리자 : HSM 및 백업 보관 관리, 소산 백업 보관 관리
- 인증시스템 관리자 : 인증서 관리(CA), 인증서 발급/재발급/폐지 관리, 인증서 폐지 목록(CRL) 발급, 관리자 인증서 발급/관리
- 인증시스템 운영자 : 서버/DB/네트워크 관리
- 가입자 신청 검증 : 신청자에 대한 신청서 및 신원확인 문서 수령 및 검증, 도메인 검증
- 인증시스템 개발자 : 개발환경에서 소스코드 유지관리

5.2.2. 주요 업무별 수행인력

인증기관 키 생성, 백업, 저장, 복구를 위한 키 활성화에는 최소 3인 이상이 수행한다.

5.2.3. 업무 담당자 신원확인 및 인증

인증기관은 신뢰할 수 있는 역할(Trusted Role)의 각 개인이 인증시스템을 통해 신원이 확인될 수 있도록 고유한 자격증명을 사용한다. 보안 구역 혹은 높은 수준의 보안 구역 출입 시에 사용되는 인증은 다중 인증(Multi-Factor)으로 구현한다.

5.2.4. 직무 분리가 필요한 역할

인증기관의 신뢰할 수 있는 역할(Trusted Roles) 담당자에게 할당된 책임 및 업무를 문서화해야 한다. 또한, 신뢰할 수 있는 역할(Trusted Roles) 담당자가 맡은 의무를 보안 관점에서 기능이 수행되도록 분리해야 한다.

보안 및 내부 감사자는 다른 신뢰할 수 있는 역할(Trusted Roles)을 맡을 수 없다. 관리책임자 및 정책관리자는 인증시스템 운영, 인증서 관리 또는 등록 관리 역할을 수행하지 않는다.

5.3. 인력 관리

신뢰할 수 있는 역할(Trusted Roles)에 할당된 책임과 업무를 문서화하고, 수행할 기능의 보안 관련 우려에 기초하여 신뢰할 수 있는 역할(Trusted Roles)에 대한 직무 분리를 구현한다.

5.3.1. 자격 요건

운영인력은 국가가 인정한 정보통신 관련 자격을 취득하거나 이에 준하는 업무 경력을 보유하여야 한다.

인증서 관리 프로세스에 참여하는 모든 사람이 임직원, 대리인 또는 독립적인 계약자로서 참여하기 전에 인증기관은 해당 사용자의 신원 및 신뢰성을 확인해야 한다. 인증기관은 신뢰할 수 있는 역할(Trusted Roles)에 할당된 수행 인력을 평가해야 하며, 수행 인력은 직무요건을 충족해야 한다.

5.3.2. 신원확인

정부 웹보안인증서인증체계의 운영인력은 국가의 신원확인 결과 결격사유가 없어야 한다. 모든 직원은 식별 가능한 신분증을 패용하여야 한다.

5.3.3. 교육 및 훈련

인증업무 수행 인력은 업무수행에 필요한 보안규정, 내부 관리 절차 및 기술교육을 이수한다. 교육 및 훈련내용은 아래와 같다.

- 정보보안(법, 규정, 매뉴얼 등) 및 개인정보보호 교육 등
- 인증업무처리 절차 및 담당자별 역할, 책임 등
- 정부 웹보안인증서 기반 기술 및 최신 인증 동향 교육 등
- 신원확인 담당자의 신원확인 절차 및 수행 방법 등에 대한 교육

5.3.4. 재교육 빈도 및 요구사항

인증업무 수행 인력은 매년 보안 및 관련 기술교육을 이수한다.

5.3.5. 직무 이동 및 순환

해당 사항 없음

5.3.6. 비인가 행위 처벌

허가되지 않은 행위를 한 인력에 대해서는 관련 규정 및 법에 따라 징계한다.

5.3.7. 독립적 계약자 요건

해당 사항 없음

5.3.8. 직원 문서 열람

인증업무를 수행하는 인력은 업무에 필요한 내부 자료를 열람할 수 있다.

5.4. 감사 로깅(Audit logging) 절차

감사 로깅은 인증기관이나 신뢰된 제3의 위임자의 통제에 따른 보안 지원 시스템은 인증서 시스템의 보안과 관련된 구성 변화를 모니터링, 감지 및 보고하기 위해 시행된다.

5.4.1. 로그(Log)의 유형

인증기관은 인증시스템 및 응용프로그램에 발생한 아래와 같은 사건을 기록하고 내부 감사 절차에 따라 수집된 데이터로부터 인증서 관리 로그를 생성하고 기록한다.

1. 인증기관 및 키 수명 주기 관리 기록
   - 키 생성, 백업, 스토리지 복구, 이관, 전송, 보관 및 폐기
   - 인증서 요청, 갱신, 폐지
   - 인증서 요청 승인 및 거부
   - 암호화 장치 수명 주기 관리 기록
   - CRL 및 OCSP 항목 생성
   - 신규 인증서 프로파일 생성 및 인증서 프로파일 폐기

2. 가입자 인증서 수명 주기 관리 기록
   - 인증서 요청, 폐지
   - CA/Browser Forum 요구사항 및 인증기관 인증업무준칙(CPS)에 명시된 모든 검증 활동

- 인증서 요청 승인 및 거부
- 인증서 발급
- CRL 및 OCSP 항목 생성

3. 보안 기록
- 인증시스템 액세스 시도 성공 및 실패
- 인증시스템 및 보안시스템 관련 작업 기록
- 보안 설정 변경
- 인증시스템에 대한 소프트웨어 설치, 업데이트 및 제거
- 시스템 충돌, 하드웨어 고장 및 기타 이상 징후
- 방화벽 및 라우터 로그
- 인증기관 출입 기록

4. 모든 로그 기록에는 다음 항목이 포함된다.
- 로그 날짜 및 시간
- 로그를 생성하는 주체 ID
- 로그에 대한 설명

5.4.2. 로그(Log)의 검토 주기

로그(Log)는 로그 감사자에 의해 월 1회 검토하며, 인증기관 키 생명주기 관련 로그는 분기별 검토한다.

5.4.3. 로그(Log)의 보관 기간

로그(Log)의 보관 기간은 저장 공간의 가용성과 관리의 효율성을 고려하여 유형에 따라 2년간 보관한다.

5.4.4. 로그(Log)의 보호

인증기관은 감사 로그 보존 기간이 만료되기 전 보관되고 있는 데이터를 비인가자로부터의 위·변조 또는 로그의 무결성 손상 등의 위험으로부터 안전하게 보호하는 절차를 구현하여야 한다.
- 인가자만 로그의 Read-Only 권한 부여
- 감사 로그의 수정 또는 삭제는 허용하지 않음

5.4.5. 로그(Log)의 백업

인증기관 관련 로그는 실시간으로 백업이 되고 로그의 복사본을 안전한 오프 사이트에 보관하여야 한다.

5.4.6. 로그(Log) 수집 시스템

인증기관이 감사 로그 수집 시스템을 직접 운영한다.

5.4.7. 로그(Log) 대상에 대한 통지

담당자에게 중요 보안 이벤트를 알리기 위해 로그 분석 및 이벤트 알림 등 자동화된 모니터링 방법을 구성하여야 한다.

5.4.8. 취약점 평가

인증기관은 지속해서 외부 및 내부 취약성을 모니터링하며, 취약점 평가 대상 범위를 식별하여 최소 매년마다 정기적으로 다음과 같은 위험을 평가 수행하여야 한다. 인증시스템 및 인프라에 대해 정기적인 취약점 평가 및 침투 테스트 수행 시에는 독립성과 객관성을 위해 외부 인력을 고용하여 수행하여야 한다.

- 인증서 데이터 또는 인증서 관리 프로세스의 무단 액세스, 공개, 오용, 변경 또는 파괴를 초래할 수 있는 예측 가능한 내부 및 외부 위협 식별
- 이러한 위협에 대응하기 위해 인증기관이 마련한 정책, 절차, 정보 시스템, 기술 등의 적절성 평가

인증시스템에서 사용하는 공인 및 사설 IP주소에 대해서는 다음과 같이 취약점 점검(Vulnerability Scan)을 수행하여야 한다.

- 최소 3개월마다
- CA/Browser Forum으로부터 요청을 받은 후 1주일 이내
- 인증기관의 중요하다고 판단한 시스템 또는 네트워크 변경 시

인증기관은 발견된 취약점에 대하여 위험도가 높은 중요 취약점은 96시간 내로 조치 수행하여야 하며, 96시간 내 조치가 불가능한 경우 조치 계획 및 보호 대책을 수립하여 취약점을 관리하여야 한다.

5.5. 기록(Records)의 보관

5.5.1. 기록(Records)의 종류

보존할 기록 대상은 5.4.1 (로그(Log)의 유형) 항목에서 명시한 사항을 참조한다.

5.5.2. 기록(Records)의 보관 기간

인증기관은 인증서가 유효하지 않거나 폐지된 이후 인증서 요청양식 및 인증서 발급 및 폐지에 관련된 모든 문서를 최소 2년간 보관한다.

5.5.3. 백업된 정보(Archive)의 보호

인증기관은 비인가 된 변경, 유출, 파괴 등으로부터 정보를 보호하기 위해 백업된 정보는 원격지에 저장 관리한다.

5.5.4. 백업된 정보의 처리 절차

백업된 정보는 정보의 소실 및 훼손 시에 백업/복구 절차에 따라 복구에 사용된다.

5.5.5. 기록(Records)의 시점 확인(Time-Stamping) 요건

인증기관은 보관된 모든 기록에 대해 NTP(Network Time Protocol) 시각 정보를 활용하여 타임스탬프를 기록한다.

5.5.6. 기록(Records) 수집 시스템

해당 사항 없음

5.5.7. 보존 기록 확보 및 검증 절차

인증시스템과 관련된 정보는 인증기관과 사전협의 후 요청기관 명의의 공문을 통해 요청한다. 인증기관은 공문으로 접수된 요청에 대해서 공문으로 회신한다.

5.6. 키 변경

인증기관 키 유효기간이 만료 또는 키 손상 등이 발생한 경우, 인증기관

키를 변경한다. 키 변경 절차는 CA 인증서 신규 발급 절차와 동일하다.

5.7. 재해 복구

5.7.1. 장애 보고 및 대응 절차

인증기관은 장애 보고 및 대응 절차를 통해 보안 장애 및 오작동으로 인한 피해를 최소화할 수 있음을 합리적 수준에서 검증할 수 있는 통제를 유지해야 한다.

인증기관은 재해, 보안 장애 또는 비즈니스 장애 발생 시, 영향을 받는 가입자 및 신뢰당사자에게 해당 사실을 통지하고 합리적으로 보호하기 위해 업무 연속성 유지 및 재해 복구 절차를 문서화해야 하며, 관련 보관 기록을 책임자에게 이전하기 위한 절차를 마련한다. 업무 연속성 계획은 외부 공개 대상에 해당하지 않으며, 인증기관 감사관이 요청 시 업무 연속성 유지 및 보안 계획을 확인할 수 있다. 인증기관은 업무 연속성 계획을 매년 검토 및 업데이트하며, 업무 연속성 계획에 따른 재해 복구 모의훈련을 매년 수행한다.

업무 연속성 계획에 포함되어야 할 사항은 다음과 같다.

1. 계획 활성화(activating) 조건
2. 비상 상황 발생 시 대응 절차
3. 대비(fallback) 절차
4. 재개 절차
5. 업무 연속성 계획 유지관리 일정
6. 인식 제고 및 교육 요건
7. 개인별 역할 및 책임
8. 재해 복구 목표 시간(RTO)
9. 비상계획의 정기적인 테스트(재해 복구 모의훈련)
10. 중요 비즈니스 프로세스 중단 또는 오류 발생 시, 비즈니스 운영을 적시에 유지 또는 복원할 수 있는 계획
11. 중요 암호화 장비(예: 암호화 장비 및 활성화 장비)를 다른 위치에 저장하기 위한 요건
12. 허용 가능한 시스템 중단 시간 및 복구 시간 구성에 필요한 요소
13. 필수 비즈니스 정보 및 소프트웨어 백업 주기

14. 인증기관 주 사이트와 복구 시설까지의 거리
15. 재해 발생 후 기존 또는 원격사이트에서 안전한 운영환경을 복원에 앞서 가능한 범위 내에서 시설을 보호하기 위한 절차

5.7.2. 정보시스템 자원의 손상된 경우의 절차

인증기관은 인증시스템의 주요 데이터가 훼손되거나 파괴되었을 때 아카이브 된 자료를 이용하여 복구한다.

5.7.3. 키 손상에 대한 복구 절차

인증기관은 인증 서비스에 사용되는 개인 키가 안전하지 않다는 사실을 인지한 경우 공개 키를 포함하는 인증서를 폐지하고 신규 키 쌍을 생성하여 인증서를 재발급한다. 인증기관은 최상위 인증기관, 인증기관의 개인 키 손상으로 인해 영향을 받는 가입자, 신뢰당사자에게 인증서 폐지 사실과 새로운 인증서를 재발급받을 것을 통보한다.

최상위 인증기관 개인 키가 손상된 경우, 인증기관은 브라우저 벤더로 손상 사실과 최근 접한 추정 손상 일자를 통보한다.

5.7.4. 업무 연속성 확보

인증기관은 국가의 연속성 계획지침에 따라 인증서 발급, 갱신, 폐지 등 인증서 생명주기 업무와 인증기관 시설이 장애, 테러, 정전, 지진, 화재, 풍수해 등으로 업무가 중단되지 않도록 업무 연속성 계획을 수립하고 이행한다.

5.8. 인증기관 또는 등록기관 종료

최상위 인증기관은 인증기관의 운영 종료 시 이를 공지하고 종료에 따른 영향을 최소화하기 위한 하기의 조치를 취한다.

- 인계할 인증기관이 지정된 경우, 서비스와 운영 관련 기록을 인계
- 본 인증업무준칙(CPS)에서 요구되는 기록을 최소 1년 동안 보존
- 인증기관 위임종료 이전에 모든 가입자 인증서를 폐지

6. 기술적 보호조치

6.1. 키 쌍 생성 및 설치

6.1.1. 키 쌍 생성

인증기관 키 생성은 FIPS 140-2 레벨 3에 준하는 하드웨어 보안 모듈(HSM) 내부에서 생성된다. 생성된 개인 키는 인증기관이 허용한 용도를 제외하고는 하드웨어 보안 모듈(HSM) 외부로 추출할 수 없다. 가입자 키 쌍은 가입자에 의해 생성된다. 본 문서 6.1.5 (키 길이) 항목과 6.1.6 (공개 키 매개변수 생성 및 품질 검사) 항목을 미충족하거나, 개인 키의 보안성이 약한 개인 키를 가진 키 생성 요청은 거절한다. 최상위인증기관 또는 인증기관 키 쌍 생성 시 지정된 인원 중 최소 3인이 참여하고 내부 또는 외부 감사자 입회하에 작업을 수행한다.

6.1.2. 개인 키 전달

인증기관은 가입자 키 쌍을 생성하지 않는다.

6.1.3. 인증서 발급자에게 공개 키 전달

인증기관 인증서 발급 시 인증기관은 PKCS#10 형식의 인증서 서명 요청(CSR)을 최상위 인증기관에 제출한다.

가입자는 SSL 인증서가 적용된 웹사이트를 통해 PKCS#10 형식의 인증서 서명 요청(CSR)을 인증기관에 제출한다.

6.1.4. 신뢰당사자에게 공개 키 제공 절차

인증기관 공개 키는 최상위 인증기관이 전자 서명한다. 인증기관은 웹사이트에 최상위 인증기관 및 인증기관 인증서를 게시하여 가입자 인증서의 체인 검증 절차를 제공한다.

6.1.5. 키 길이

인증서 알고리즘 유형 및 키 길이에 대해 인증서는 다음의 요건을 충족해야 한다.

최상위 인증기관 인증서, 하위 인증기관 인증서, 가입자 인증서는 모두 동일한 요건을 충족해야 한다.

- 다이제스트 알고리즘 : SHA-256, SHA-384 또는 SHA-512
- 최소 RSA 모듈 크기(단위: 비트)
  - 최상위 인증기관 인증서 : 4096
  - 인증기관 인증서 : 3072
  - 가입자 인증서 : 2048

6.1.6. 공개 키 매개변수 생성 및 품질 검사

RSA 키의 경우, 인증기관은 RSA 키의 공개지수 값(value of the public exponent)이 3 이상의 홀수임을 확인한다.

6.1.7. 키 사용 용도

최상위 인증기관 개인 키가 인증서 서명에 사용되는 경우는 다음과 같다.

- 최상위 인증기관임을 자체 보증하기 위한 자체 서명 인증서
- 인증기관 인증서
- 인프라 인증서(예: 관리자용 인증서, 내부 인증기관 운영 장비용 인증서 등)
- OCSP 응답 검증용 인증서

6.2. 개인 키 보호 및 암호화 모듈

6.2.1. 암호화 모듈의 기준

최상위 인증기관 및 인증기관 개인 키 키 쌍은 FIPS 140-2 레벨 3 이상인 하드웨어 보안 모듈(HSM)에 보관하여 운영한다.

6.2.2. 개인 키에 대한 다중 통제

최상위 인증기관 및 인증기관은 내부 키 생성 절차에 의해 인증기관 키 쌍 생성을 수행한다. 키 쌍 생성 시 지정된 인원(5) 중 최소 3인이 참여한다.

6.2.3. 개인 키 위탁

인증기관은 인증기관 키 쌍을 제3자에게 위탁하지 않는다.

6.2.4. 개인 키 백업

최상위 인증기관 개인 키와 인증기관 개인 키는 백업 절차에 따라 안전한 위치에 보관된다. 백업된 개인 키는 금고 내의 하드웨어 보안 모듈(HSM)에 저장된다.

6.2.5. 개인 키 보관

최상위 인증기관 개인 키와 인증기관 개인 키는 별도 매체에 복제(archiving)하지 않는다.

6.2.6. 개인 키 추출

최상위 인증기관 및 인증기관 개인 키는 백업 및 복구 목적으로 인증기관 승인하에 하드웨어 보안 모듈(HSM) 공급업체가 지정한 안전한

절차에 따라 개인 키를 추출할 수 있다.

6.2.7. 개인 키 저장

인증기관 개인 키는 본 인증업무준칙(CPS) 6.2.1 (암호화 모듈의 기준) 항목의 요건을 충족하는 하드웨어 보안 모듈(HSM)에서 생성되고 저장된다.

6.2.8. 개인 키 활성화

하드웨어 보안 모듈(HSM)에 저장된 최상위 인증기관 개인 키와 인증기관 개인 키는 인증기관 승인하에 다중 통제에 의해 보안 모듈(HSM) 공급업체에서 지정한 절차에 따라 활성화된다.

6.2.9. 개인 키 비활성화

하드웨어 보안 모듈(HSM)에 저장된 최상위 인증기관 개인 키와 인증기관 개인 키는 인증기관 승인하에 다중 통제에 의해 보안 모듈(HSM) 공급 업체에서 지정한 절차에 따라 비활성화할 수 있다.

6.2.10. 개인 키 삭제 및 파기

인증기관은 다음과 같은 사유로 최상위 인증기관 및 인증기관 개인 키를 파기할 수 있다.

- 최상위 인증기관 및 인증기관 인증서 유효기간 만료
- 최상위 인증기관 및 인증기관 개인 키가 훼손, 유출 및 손상 가능성이 있는 경우

인증기관은 HSM에 저장된 개인 키를 삭제하여 파기할 수 있다. 또한, 인증기관은 하드웨어 보안 모듈(HSM) 사양에 따라 장비 및 관련 백업 토큰을 제로화(zeroize)하여 파기할 수 있다. 제로화 또는 초기화가 실패하는 경우 개인 키를 추출하지 못하도록 물리적인 방법으로 장비를 파괴한다.

6.2.11. 암호화 모듈 등급

6.2.1 (암호화 모듈의 기준) 항목 요건을 충족하는 하드웨어 보안 모듈(HSM)을 사용한다.

6.3. 키 쌍 관리

6.3.1. 공개 키 보관

인증기관, 가입자 인증서는 백업 절차에 따라 보관된다.

6.3.2. 인증서 운영 기간 및 사용 기간

인증서 유효기간은 인증서 필드에 명시된 유효기간 종료 시점에 만료된다. 가입자 인증서 최대 유효기간은 397일이다.

6.4. 활성화 데이터

HSM 활성화 키는 하드웨어 보안 모듈(HSM)에 저장되며 인증기관이 허가한 키 관리자만 사용할 수 있다. 물리적인 접근 통제 장비로 구현된 다중 통제 절차에 따라 하드웨어 보안 모듈(HSM) 내 키 쌍 사용을 위한 모듈 활성화가 수행된다.

6.4.1. 활성화 데이터 생성

활성화 데이터는 하드웨어 보안 모듈(HSM)의 사양에 따라 생성된다. 보안모듈(HSM)은 FIPS 140-2 레벨 3 인증이 되어야 한다.

6.4.2. 활성화 데이터 보호

하드웨어 보안 모듈(HSM) 데이터를 활성화하기 위해 사용되는 절차는 하드웨어 보안 모듈(HSM) 키 패드(PED)와 접근 인증용 키(Key)에 의존한다. 접근 인증용 키(Key)는 지정된 다중 통제 절차에 의해 관리되며, 키 패드(PED)는 키 관리자에 의해 관리된다.

6.4.3. 활성화 데이터 추가 고려사항

해당 사항 없음

6.5. 컴퓨터 보안

6.5.1. 특정 컴퓨터 보안 요구사항

인증기관 시스템 정보는 서버 및 OS 통제, 물리적 통제 및 네트워크 통제에 의해 보호된다. 네트워크 보안 통제는 6.7 (네트워크 보안) 항목에 명시되어 있다.

인증시스템에서 발급된 인증서 생명주기 관리 업무에 사용되는 모든 계정은 다중 인증(Multi-Factor Authentication)을 적용한다.

- 신뢰할 수 있는 인가된 인원에게 인증시스템에 대한 관리 권한을 부여하고 인증시스템의 보안에 대한 책임을 요구한다.
- 모든 시스템 내 계정은 최소한 3개월마다 재검토를 수행하고 운영에 더 이상 필요하지 않은 계정은 비활성화하여야 한다.
- 인증시스템에 대한 접근 시도가 5회 이상 실패하는 경우 일정 시간 동안 접근을 제한하여야 한다.
- 직무 변경 또는 외부업체와 계약 관계가 만료되면 24시간 이내로 해당 사용자의 인증시스템에 대한 권한은 회수된다.
- 보안 구역에서 접근할 수 있는 모든 인증시스템(제3의 위임자에게 동일하게 적용되는 인증서의 발급을 승인하는 계정 포함)에 대해 다중 인증(MFA: Multi-Factor Authentication)을 적용한다.
- 인증시스템 관련 관리자, 운영자, 담당자가 업무 PC를 더 이상 사용하지 않을 시 로그아웃 또는 세션 타임아웃을 적용한다.
- 보안 패치가 보안 패치 적용의 이점보다 더 큰 추가 취약성 또는 불안정성을 발생시킨다는 검토 문서가 없는 한, 보안 패치 제공 후 6개월 이내에 권장 보안 패치 인증시스템에 적용하여야 한다.

6.5.2. 컴퓨터 보안 등급

해당 사항 없음

6.6. 생명주기 보안

6.6.1. 시스템 개발 통제

인증시스템의 기능 변경, 성능 개선 시 주관기관의 승인 하에 실시된다.

6.6.2. 보안관리 통제

인증시스템에 접근하는 모든 컴퓨터에 대하여 적절한 업무 분담과 최소 권한 원칙을 적용한다. 인증시스템 접근을 위해서는 인증기관의 승인이 필요하며, 업무 변경 즉시 권한을 회수한다.

6.6.3. 생명주기 보안 통제

해당 사항 없음

6.7. 네트워크 보안

인증시스템은 네트워크 관리 정책에 따라 침입 탐지 시스템 및 침입 차단 시스템에 의해 보호되며 하드웨어 방화벽 장비를 통해 인증기관 및 가입자 인증서를 발급하고 검증하는데 사용되는 특정 포트를 통제한다. 인증기관은 CA/Browser Forum의 Network and Certificate System Security Requirements를 준용한다.

1. 인증시스템을 기능적, 논리적, 물리적 관계에 따라 네트워크 또는 영역으로 세분화
2. 인증시스템과 동일한 구역에 위치한 모든 시스템에 동일한 보안 통제 적용
3. 최상위 인증기관 시스템은 높은 보안 수준과 오프라인 상태 또는 다른 네트워크와 에어 갭 상태로 유지관리
4. 최소한 보안 구역 내에서는 인증시스템, 발급시스템, 보안 지원 시스템을 유지관리 및 보호를 시행한다.
5. 보안 구역-상급 보안구역 간 통신 및 (보안 구역과) 해당 구역 외 비인증 시스템, 퍼블릭 네트워크 간의 통신 및 시스템을 보호하는 보안시스템을 구현한다.
6. 인증시스템 운영에 필요하다고 판단된 서비스, 프로토콜, 포트 및 통신만 지원하는 규칙을 사용하여 네트워크 통신 제어(방화벽, 스위치, 라우터 및 게이트웨이)를 구성한다.
7. 인증기관에서 사용되지 않는 모든 계정, 애플리케이션, 서비스, 프로토콜 및 포트를 제거하거나 사용하지 않도록 설정하고, 인증기관으로부터 인가된 계정, 애플리케이션, 서비스, 프로토콜 및 포트만 허용한다.
8. 인증기관의 보안 정책이 문서화, 승인 및 검토의 원칙에 따라 변경관리 절차를 포함하도록 하고, 해당 변경관리 절차에 따른 변경사항을 관리한다.
9. 관리자 접속은 신뢰 역할이 부여된 인원에게 허용하고, 인증시스템 보안 책임을 부여한다.
10. MFA(다중 인증)는 인증시스템(MFA를 지원하는) 각 컴포넌트에 적용한다.
11. 인증시스템에서 접근할 수 있는 사용자의 권한이 변경되거나 취소되는 경우 인증시스템의 권한 있는 계정 또는 서비스 계정에 대한 인증키 또는 암호를 변경한다.
12. 보안 패치가 보안 패치 적용의 이점보다 더 큰 추가 취약성 또는 불안정성을 발생시킨다는 검토 문서가 없는 한, 보안 패치 제공 후 6개월 이내에 권장 보안 패치 인증시스템에 적용하여야 한다.

6.8. 시점 확인

인증서, 인증서 폐지 목록(CRL), 기타 인증서 생명주기에서 생성되는 감사 로그는 시간 정보를 포함한다. 인증기관은 시스템 시간을 NTP(Network Time Protocol)를 사용하여 최소 8시간마다 시각을 동기화하도록 업데이트하고 있으며, 모든 시각은 UTC 시각으로 업데이트된다.

7. 인증서, CRL 및 OCSP 프로파일

7.1. 인증서 프로파일 규격

인증기관이 발급하는 인증서는 RFC 5280과 CA/Browser Forum의 기준(Baseline Requirements)의 요건을 모두 충족한다.
RFC 5280과 CA/Browser Forum 기준(Baseline Requirements)이 다른 경우에는 CA/Browser Forum 기준을 우선으로 준수한다.

7.1.1. 인증서 버전

인증기관이 발급하는 인증기관 및 가입자 인증서는 X.509 Version 3 버전을 발급한다.

7.1.2. 인증서 확장

인증기관이 발급되는 인증서는 “별첨. 인증서 프로파일”에 명시된 인증서 확장 필드를 사용하고, CA/Browser Forum 기준 (Baseline Requirements) 7.1.2 및 RFC 5280을 준수한다.

7.1.3. 알고리즘 개체 식별자

인증서 알고리즘 OID는 “별첨. 인증서 프로파일”에 명시된 OID를 사용한다.

7.1.4. 명칭 양식

7.1.4.1. 명칭 인코딩

최상위 인증기관 인증서를 제외한 모든 인증서의 발급자(Issuer) DN 필드의 인코딩된 값은 해당 인증서를 발급한 인증기관 인증서의 소유자(Subject) DN 필드의 인코딩된 값과 일치해야 한다.

7.1.4.2. 소유자(Subject) 정보 - 가입자 인증서

인증기관은 인증서를 발급함으로써 인증서 발급일 기준 모든 소유자(Subject) 정보가 정확한지 확인하기 위해 인증업무준칙(CPS)에 명시된 절차를 따랐음을 진술한다. 인증기관은 인증서 요청 정보를 신뢰할 수 있는 데이터베이스(WHOIS)와 비교하여 검증한다. 인증서는 3.2.2.4 (도메인 인증 여부 또는 소유권 확인) 항목에 명시된 경우를 제외하고 소유자(Subject) 필드에 도메인 이름을 포함하지 않는다.

가입자 인증서는 3.2(최초 신원확인)에 따라 확인된 정보만 포함 할 수 있으며, 확인되지 않은 정보는 포함하지 않는다.
subject:organizationName, subject:localityName 및 subject:countryName 속성은 3.2.2.1 (신원확인)에 따라 확인한다.

소유자(Subject) 속성은 '.', '-' 및 ' ' (즉, 공백) 문자와 같은 메타데이터를 단독적으로 사용할 수 없으며, 값이 없거나 불완전하거나 해당 사항이 없는 것일 경우 기타 표시도 사용될 수 없다.

subjectAlternativeName 필드 또는 subject:commonName 속성에 예약된 IP주소 또는 내부 이름이 포함된 인증서를 발급하지 않는다.

dNSName의 항목은 RFC 5280에 지정된 "기본 이름 구문(preferred name syntax)" 에 있어야 하므로 밑줄 문자('_')를 포함할 수 없다.

7.1.4.3. 소유자(Subject) 정보 - 인증기관 인증서

인증기관은 인증서 발급일 기준 모든 소유자(Subject) 정보가 정확한지 확인하기 위해 인증업무준칙(CPS)과 CA/Browser Forum 기준(Baseline Requirements)을 준수한다.

subject:commonName 속성은 인증기관 인증서의 식별자로 사용될 수 있다. 인증기관이 발급한 인증기관 인증서의 subject:commonName 속성은 고유하여야 한다.

인증기관은 subject:organizationName 속성에 인증기관 명칭을 포함한다. 현지에서 허용되는 약어인 경우, 검증된 이름과 일반적인 변형 또는 약어와 같이 다소 상이한 정보를 포함할 수 있다. 예를 들어 공식 명칭이 "Company Name Incorporated"로 표시되면 인증기관은 "Company Name Inc." 또는 "Company Name" 이라고 사용할 수 있다.

subject:countryName 속성은 3.2.2.1 (신원확인) 항목에 따라 확인된

ISO3166-1 국가 코드를 포함한다.

7.1.5. 명칭 제한

해당 사항 없음

7.1.6. 인증서 정책 객체 식별자

인증기관이 발급한 인증서는 인증업무준칙(CPS)을 인증서 정책으로 사용하며 관련 정책 식별자는 아래와 같다.

- 가입자 조직 유효성 검사(OV) 인증서: 1.2.410.100001.100.1.2.2
- OCSP 인증서: 1.2.410.100001.100.1.3.2

CA/Browser Forum에서 할당된 다음 정책 식별자도 가입자 인증서에 사용된다.

- 조직 유효성 검사(OV) 인증서: {joint-iso-itu-t(2) international-organizations (23) ca-browser-forum(140) certificate-policies(1) baseline- requirements(2) organization-validated(2)} (2.23.140.1.2.2)

7.1.7. 정책 제한 확장의 사용

해당 사항 없음

7.1.8. 정책 한정자 구문 및 의미

해당 사항 없음

7.1.9. 주요 인증서 정책 확장에 대한 의미 처리

해당 사항 없음

7.2. 인증서 폐지 목록(CRL) 프로파일 규격

인증기관이 발급하는 인증서 폐지 목록(CRL)은 RFC 5280 표준을 준수한다.

7.2.1. 버전

인증서 폐지목록은 X.509 V2로 발급된다.

7.2.2. CRL 확장 필드

- CRL 숫자 : 반복적인 단순 증가 패턴 사용
- 기관 키 식별자(Authority Key Identifier) : 인증서에 열거된 기관 키 식별자와 동일
- 유효기간 만료 일자: UTC 형식의 날짜(선택)
- 원인 코드 : 인증서 폐지 신청 사유(선택)
  - keyCompromise(1)
  - affiliationChanged(3)
  - superseded(4)
  - cessationOfOperation(5)
  - privilegeWithdrawn(9)

7.3. 실시간 인증서 상태 검증 프로파일 규격

실시간 인증서 상태 검증(OCSP) 응답은 RFC 6960 표준을 준수한다. 인증기관 정보 액세스(Authority Information Access)에 실시간 인증서 상태 검증(OCSP) 응답자 URL을 통해 실시간 인증서 상태 검증(OCSP) 신청에 대한 응답을 제공한다. CA/Browser Forum 기준(Baseline Requirements)에 따라 발급되지 않은 인증서에 대해 Good 응답을 제공하지 않는다.

실시간 인증서 상태 검증(OCSP) 응답은 다음과 같은 인증기관 또는 실시간 인증서 상태 검증(OCSP) 응답자가 서명한다.

- 폐지 상태를 검사하는 인증서를 발급한 인증기관
- 폐지 상태를 검사하는 인증서를 발급한 인증기관에 의해 서명된 인증서를 가진 OCSP 응답자(OCSP 서명 인증서는 RFC 6960에 정의된 id-pkix-ocsp-nocheck 유형의 확장 필드가 포함되어야 한다.)

교차 인증서를 포함하여, Root CA, CA 인증서에 대한 OCSP응답 시, 인증서가 폐지된 경우, CertStatus의 RevokedInfo 내에 revocationReason 필드가 반드시 존재하여야 한다.

7.3.1. 버전

실시간 인증서 상태 검증(OCSP) 응답자는 RFC 6960에 정의된 버전 1을 준수한다. 구체적으로 실시간 인증서 상태 검증(OCSP) 응답자는 요청에 난수가 포함되어 있더라도 응답에는 포함하지 않을 수 있다.

7.3.2. OCSP 확장 필드

해당 사항 없음

8. 감사 준수 및 기타 평가

정부 웹보안인증서 인증체계의 적합성을 평가하기 위해 독립적인 외부 감사자가 정기 감사를 수행한다. 감사 보고서는 CA/Browser Forum 기준(Baseline Requirements) 8.6 항목을 충족하여야 한다.

8.1. 평가 빈도 및 환경

인증기관이 운영 및 관리하는 인증 서비스에 대한 감사는 최소 연 1회 실시한다.

8.2. 평가 주체 및 자격

정부 웹보안인증서 인증체계 감사는 다음과 같은 자격 및 기술을 보유한 법인이 수행하여야 한다.

- 피감사 대상자와의 독립성이 위배 되지 않는 자
- 웹트러스트(WebTrust) 또는 이에 준하는 국제 인증 감사 기준을 처리하고 감사하는 역량 및 경험 보유자
- 공개 키 기반구조, 암호학 등 인증 서비스에 대한 전문적인 지식 소유자
- 웹트러스트 감사(WebTrust Audit)인 경우, WebTrust.org로부터 허가된 감사인(Webtrust Practitioner)
- 법률, 정부 규정 또는 직업윤리 강령에 속하는 자
- 내부 정부 감사 기관의 경우를 제외하고, 보험적용 범위 내에서 최소 100만 달러의 정책 한도로 전문 직업 책임 보험(Professional Liability/Errors & Omissions insurance)을 유지하고 있는 감사 기관

8.3. 피감사 대상에 대한 평가자의 관계

감사자는 피감사 대상자와 재정 및 사업적 이해관계가 없어야 한다.

8.4. 평가 범위

연간 감사는 웹트러스트 감사 기준(WebTrust Audit Criteria) 및 CA/Browser Forum 기준(Baseline Requirements)을 기반으로 인증기관의 인증 서비스가 적절하게 수행하는지 확인한다.

8.5. 평가 결과 조치

감사보고서상의 발견사항에 대한 관리적, 기술적 조치를 취한다.

8.6. 평가 결과 공표

감사 보고서는 인증기관이 발급한 인증서와 관련 시스템, 정책 및 절차에 관한 내용이 포함된다. 인증기관은 감사 보고서를 웹사이트를 통해 공개한다. 인증기관은 전반적인 감사 의견에 영향을 미치지 않는 일반적인 감사 결과는 공개하지 않아도 무방하다.

감사 보고서에는 최소한 다음과 같은 명확한 라벨이 부착된 정보가 포함되어 있다.

- 감사를 받는 기관의 명칭
- 감사를 수행하는 조직의 이름 및 주소
- 교차 인증서를 포함한 모든 최상위 인증기관 및 하위 인증기관 인증서의 SHA-256 지문(Fingerprint)
- 각 인증서 및 관련 키를 감사하는데 사용된 감사 기준(버전 포함)
- 감사 수행 시 참조되는 정책 문서 목록(버전 포함)
- 감사가 특정 기간 또는 특정 시점에 대한 평가인지 여부
- 일정 기간을 포함하는 감사 기간의 시작일 및 종료일
- 특정 시점에 대한 시점 일자
- 보고서가 발행된 일자(반드시 감사 종료일 또는 지정 시점일 이후)

8.7. 자체 감사

인증기관은 인증업무준칙(CPS)과 CA/Browser Forum 기준(Baseline Requirements) 준수 여부에 대해 분기별 1회 이상 자체 감사를 시행한다. 직전의 자체 감사 이후 발급된 인증서 중 최소 3%의 인증서 샘플을 무작위로

선택하여 자체적으로 감사한다.

9. 기타 업무상 및 법적 사항

9.1. 요금

9.1.1. 인증서 발급 및 갱신 요금

정부 웹보안인증서 인증체계는 국가가 운영하는 정보 보호 기반 인프라로서 인증서의 발급, 재발급, 갱신의 비용과 기타 요금을 가입자에 청구하지 않는다.

9.1.2. 인증서 접근 요금

별도 비용을 부과하지 않는다.

9.1.3. 폐지 또는 상태정보 확인 요금

별도 비용을 부과하지 않는다.

9.1.4. 기타 서비스 요금

별도 비용을 부과하지 않는다.

9.1.5. 환불 정책

해당 사항 없음

9.2. 재무적 책임

9.2.1. 보험적용 범위

인증기관은 발급하는 인증서와 관련하여 발생한 문제에 대해서 금전적 배상을 하지 않는다.

9.2.2. 기타 자산

해당 사항 없음

9.2.3. 보험 또는 보증 범위

해당 사항 없음

9.3. 기밀 정보 보호

인증기관은 관련 법령 및 인증업무준칙(CPS) 9.4.1 (개인정보보호 계획) 항목에 따라 기밀로 간주되는 개인정보 보호에 관한 해당 규칙을 준수한다.

9.3.1. 기밀 정보의 범위

인증기관은 다음과 같은 유형의 정보를 기밀로 유지하고 신뢰할 수 없는 직원에게 이러한 기록이 노출되는 것을 방지하기 위해 합리적인 통제를 유지한다. 아래 정보는 기밀로 간주되며 합리적인 통제를 구현하여 안전하게 보호하여야 한다.

- 인증서를 지원하기 위해 제출된 인증서 신청 기록 및 문서 (승인 또는 거절 여부와 무관)
- 웹트러스트 감사보고서(WebTrust Audit Report)를 제외한 외부 또는 내부 감사 추적 기록 및 보고서
- 비상계획 및 재해 복구 계획
- 개인 키
- 개인 키 활성화 데이터
- 감사 로그 및 보관 기록
- 개인정보

9.3.2. 기밀 정보의 범위를 벗어난 정보

본 인증업무준칙(CPS) 9.3.1 (기밀 정보의 범위) 항목에서 명시된 항목을 기밀 정보로 간주하며, 이외 정보는 공개 정보로 간주한다. 단, 등록된 인증서 및 폐지 정보는 기밀 정보로 간주 되지 않는다. 가입자는 인증기관에 의해 발급된 모든 인증서의 폐지 데이터가 공개 정보이며 24시간마다 게시된다는 것을 인정한다. 인증서 신청 정보의 일부로 제출된 관련 가입자 이용약관 또는 인증서 요청양식에서 “공개”로 표시된 가입자 신청 정보는 발급된 인증서 내에 게시되므로 이러한 정보는 기밀 정보의 범위에 속하지 않는다.

9.3.3. 기밀 정보 보호의 책임

정부 웹보안인증서 인증체계의 기밀 정보는 안전하게 보관되고 인가된 인력에 의해 관리된다. 인증기관의 임직원, 외주 및 계약업체는 기밀

정보를 보호할 책임이 있으며 계약상의 의무도 있다. 이러한 인력 모두 기밀 정보 처리 관련 교육을 이수하여야 한다.

9.4. 개인정보보호

9.4.1. 개인정보보호 계획

인증기관은 개인정보처리 시 웹사이트에 게시된 개인정보처리방침을 따른다. 개인정보공개는 법률상 공개가 요구되거나 개인정보의 주체가 요청할 때만 공개된다.

9.4.2. 개인정보처리

웹사이트에 게시된 개인정보처리 방침에 따라 개인정보를 수집・보유한다.

9.4.3. 개인정보가 아닌 정보

인증서, CRL 또는 OCSP에 공개된 정보는 개인정보로 간주 되지 않는다.

9.4.4. 개인정보보호 의무

인증기관은 개인정보보호법 등 관련 법・규정을 준수하며 웹사이트에 게시된 개인정보처리방침에 따라 개인정보를 수집・보유・처리한다.

9.4.5. 개인정보 사용에 대한 통지 및 동의

인증기관은 개인정보보호법 등 관계 법・규정을 준수하며 웹사이트와 신청서를 통해 개인정보 사용에 대한 고지 및 정보 주체의 동의를 득한다.

9.4.6. 사법 또는 행정 절차에 따른 공개

정부 SSL 인증서 발급시스템은 정보주체의 개인정보를 9.4.2 (개인정보처리) 항목에서 명시한 범위 내에서만 처리하며, 정보주체의 동의, 법률의 특별한 규정 등 「개인정보 보호법」 제17조 및 제18조에 해당하는 경우에만 개인정보를 제3자에게 제공합니다.

9.4.7. 기타 정보공개 기준

해당 사항 없음

9.5. 지적 재산권

정부 웹보안인증서 인증체계로부터 발생한 모든 지적 권한은 행정안

전부에 있다.

9.5.1. 인증서 및 폐지 정보에 대한 재산권

행정안전부는 언제든지 인증서를 폐지할 수 있는 권리를 보유하며, 폐지 정보를 유지할 책임이 있다.

9.5.2. 계약상의 재산권

정부 웹보안인증서서비스 참여자는 행정안전부가 본 인증업무준칙(CPS)에 대한 모든 지적 재산권을 보유함을 인정한다.

9.5.3. 명의 재산권

가입자는 가입자 인증서에 포함되는 기관명, 도메인 등 DN 정보에 대한 모든 권리를 보유한다.

9.5.4. 키 쌍의 재산권

가입자는 가입자 개인 키, 공개 키에 대한 모든 권리를 보유한다.

9.6. 진술 및 보증

9.6.1. 인증기관 진술 및 보증

인증기관은 본 인증업무준칙(CPS) 또는 가입자와의 별도 약관에 명시된 경우를 제외하고 제공하는 인증 서비스에 대해 어떠한 진술이나 보증도 하지 않는다. 인증기관은 본 인증업무준칙(CPS)에 지정된 범위 내에서 아래 사항에 대해 진술한다.

- 국내외 관련 법, 법령, 시행규칙 및 준칙 준수
- CRL 및 OCSP 응답의 정기적인 게시 및 업데이트
- 본 인증업무준칙(CPS) 및 CA/Browser Forum 기준(Baseline Requirements)에 언급된 최소 요건 준수
- 웹사이트에 저장소 유지

9.6.2. 등록기관 진술 및 보증

해당 사항 없음

9.6.3. 가입자 진술 및 보증

인증기관은 가입자 계약서 또는 이용약관 일부로 인증기관 및 인증서 수령인의 이익을 위해 신청자가 본 항목의 약정 및 보증을 하도록 요구

한다.

인증기관은 인증서 발급 전에 인증기관 및 인증서 수령인의 명시적 이익을 위해 다음 중 하나를 수집한다.

- 가입자 계약서에 대한 신청기관의 동의
- 이용약관에 대한 신청기관의 승인

인증기관은 가입자 계약서 또는 이용약관이 신청기관에 법적으로 적용 가능한지 확인하는 절차를 시행한다. 두 경우 모두, 동의는 인증서 요청에 따라 발급되는 인증서에 적용된다. 인증기관이 가입자에게 발급하는 각 인증서가 가입자 계약서 또는 이용약관의 적용을 명확히 받는 한, 각 인증서 요청에 대해 별도의 동의를 받거나 여러 개의 인증서 요청 및 결과에 대해 단일 동의를 받아서 처리할 수 있다.

가입자 계약서 또는 이용약관에는 신청기관 본인에게 다음과 같은 의무와 보증을 부과하는 조항이 포함되어 있다.

- 정보의 정확성 : 인증서 요청 및 인증기관이 제공할 인증서 발급 관련하여 인증기관이 요청한 대로 항상 정확하고 완전한 정보를 CA에 제공해야 하는 의무 및 보증
- 개인 키 보호 : 신청기관이 요청한 인증서에 포함될 공개 키에 해당하는 개인 키를 단독 제어, 기밀 유지 및 항상 적절하게 보호하기 위해 모든 합리적인 조치를 취해야 할 의무 및 보증
- 인증서 수령 : 가입자가 인증서 내용을 정확하게 검토하고 확인하는 의무 및 보증
- 인증서 사용 : 인증서에 포함된 subjectAltName을 통해서만 접근할 수 있는 서버에만 인증서를 설치하고, 모든 관련 법률 및 가입자 계약서 또는 이용약관에 따라 인증서를 사용해야 하는 의무 및 보증
- 보고 및 폐지 : 1) 인증서에 포함된 공개 키와 관련하여 가입자의 개인 키가 실제로 잘못 사용 및 손상된 경우, 잘못 사용 및 손상이 의심되는 경우 즉시 인증서 폐지를 요청하고 인증서 및 관련 개인 키 사용을 중지해야 하는 의무 및 보증. 2) 인증서의 정보가 정확하지 않거나 부정확한 경우 즉시 인증서의 폐지를 요청하고 사용을 중지해야 하는 의무 및 보증
- 인증서 사용 종료 : 키 손상을 사유로 인증서가 폐지될 때 인증서에 포함된 공개 키에 해당하는 모든 개인 키의 사용을 즉시 중단해야 하는 의무 및 보증

- 대응력 : 키 손상 또는 인증서 오용에 대한 인증기관의 지침에 지정된 기간 내에 응답해야 하는 의무
- 인정 및 수락 : 신청기관이 가입자 계약서 또는 이용약관을 위반하거나 인증기관이 발급한 인증서가 피싱 공격, 사기 또는 악성 프로그램 배포와 같은 범죄 활동을 가능하게 하는 데 사용되는 것을 발견한 경우 인증기관이 해당 인증서를 즉시 폐지할 수 있는 자격이 있다는 것에 대한 인정 및 수락

9.6.4. 신뢰당사자 보증

해당 사항 없음

9.6.5. 기타 참여자의 진술 및 보증

해당 사항 없음

9.7. 보증 면책사항

본 CPS에 명시된 것을 제외하고, 모든 인증서 및 관련 소프트웨어 및 서비스는 “있는 그대로(AS IS)” 와 “사용 가능한 대로(AS AVAILABLE)” 제공된다. CRL 및 모든 참여자 또는 제3자의 참여자(키 쌍, 인증서, CRL 또는 행정안전부가 참여자에게 제공하는 기타 상품 또는 서비스의 사용 포함)에 대해 상품성에 대한 묵시적인 보증, 특정 목적의 적합성에 대한 보증 및 인증서 발급과 관련하여 제공되는 정보의 정확성에 대한 보증을 포함하여 모든 명시적 및 묵시적 보증을 부인한다.

본 인증업무준칙(CPS) 9.6.1 (인증기관 진술 및 보증) 항목에 명시된 경우를 제외하고, 인증기관은 서비스 또는 제품이 모든 기대를 충족시키거나 인증서에 대한 접근이 시기적절하거나 오류가 없을 것이라고 보증하지 않는다.

인증기관은 제품 또는 서비스의 가용성을 보장하지 않으며, 언제든지 제품 또는 서비스 제공을 변경하거나 중단할 수 있다. 법인이 정부 웹보안 인증서 서비스를 이용한다고 해서 수탁 의무가 생기는 것은 아니다.

9.8. 책임 제한

인증기관이 발급하는 가입자 인증서는 전자정부법 및 같은 법 시행령에 따라 발급 및 운영되므로, 가입자 인증서 사용과 관련하여 발생 되는 이슈에 대해 인증기관은 책임지지 않는다.

9.9. 배상

해당 사항 없음

9.10. 유효기간 및 종료

9.10.1. 유효기간

인증업무준칙(CPS)은 저장소에 게시된 즉시 효력이 발생한다.

9.10.2. 종료

인증업무준칙(CPS) 및 관련된 정책 문서는 신규 버전으로 개정되기 전까지 효력을 유지한다.

9.10.3. 종료 및 보존 기간

본 인증업무준칙(CPS)에 따라 발급된 인증서에 대한 인증업무준칙(CPS)의 종료 후에도 다음과 같은 권한, 책임 및 의무가 있다.

- 본 인증업무준칙(CPS)의 9.3 (기밀 정보 보호) 항목을 포함한 기밀 정보와 관련된 모든 책임 및 의무
- 본 인증업무준칙(CPS)의 9.4.4(개인정보보호 의무)에 명시된 것을 포함하여 개인정보를 보호하기 위한 모든 책임 및 의무
- 본 인증업무준칙(CPS)의 9.6(진술 및 보증)에 명시된 내용을 포함한 모든 진술 및 보증
- 본 인증업무준칙(CPS)의 9.8(책임 제한)에 규정된 모든 책임 제한

본 인증업무준칙(CPS)이 종료되더라도 인증서가 취소되거나 만료될 때까지 모든 가입자 계약서 또는 이용약관은 유효하다.

9.11. 의사소통 및 통지

인증기관은 이메일로 본 인증업무준칙(CPS)과 관련된 의사소통 및 통지를 수락한다. 인증기관으로부터 이메일 회신을 받았을 경우 해당 통지는 유효한 것으로 간주 된다. 발송인은 5일 이내에 해당 이메일 회신을 받지 못하였을 경우에는 다음 명시된 주소로 서면 통지서를 재발송하여야 한다.

- 한국지역정보개발원 GSSL 운영센터
- 주소: (03923) 서울 마포구 성암로 301, 한국지역정보개발원
- 이메일: gssl@klid.or.kr

9.12. 개정

행정안전부 정책의 중대한 변경 발생 시, 인증업무준칙(CPS)의 최신 버전이 인증기관 저장소(ssl.gpki.go.kr/legal/cps)에 새로운 버전 번호를 사용하여 공개된다. 본 인증업무준칙(CPS)은 최소 연 1회 이상 업데이트 되어야 한다.

사용자 및 인증서 등에 영향을 미치지 않는 사소한 변경 또는 오류 정정의 경우 인증업무준칙(CPS) 사용자에게 통지하지 않고 기존 인증업무준칙(CPS)의 버전 번호를 유지하여 수정할 수 있다.

9.12.1. 개정 절차

본 인증업무준칙(CPS)에 대한 수정은 행정안전부의 승인 하에 이루어진다. 행정안전부는 본 인증업무준칙(CPS)의 수정 사항을 승인하고, 인증기관은 수정 사항을 저장소에 게시한다. 수정 내용은 이 인증업무준칙(CPS)에 대한 업데이트, 수정, 변경될 수 있으며, 상세한 내용은 인증업무준칙(CPS)에 설명되어 있다. 인증업무준칙(CPS)의 정책과 무관한 사소한 변경이나 오류 정정 등의 사유가 있는 경우 사전 승인 없이 수정할 수 있다.

9.12.2. 개정 공지

정부 웹보안인증서 인증체계의 인증업무준칙(CPS)에 대한 수정 사항을 웹사이트 저장소에 게시하여 사용자에게 통지한다.

9.12.3. 인증체계 객체 식별자 변경 기준

행정안전부는 인증업무준칙(CPS) 개정에 의해 인증서 정책의 객체 식

별자(OID, Object Identifier) 변경을 결정할 수 있는 유일한 권한을 보유한다.

9.13. 분쟁 해결

적용 법률이 허용하는 범위 내에서, 가입자 계약서 또는 이용약관에는 분쟁 해결 조항이 포함되어야 한다. 정부 웹보안인증서 인증체계와 관련하여 발생하는 분쟁은 행정안전부 장관의 결정에 따른다.

9.14. 준거법

본 인증업무준칙(CPS)은 대한민국 법률에 따라 관리되고 해석된다. 이러한 특정 관할권의 법률 선택은 정부 웹보안인증서의 위치, 사용처, 기타 상품 및 서비스와 관계없이 본 인증업무준칙(CPS)에 대한 일괄적인 해석을 보장하기 위함으로 인증서 및 서비스와 관련하여 암시적 또는 명시적으로 적용하거나 인용할 수 있는 모든 계약적 관계에서 제공자, 공급업체, 수익자 수취인 또는 기타 계약 관계에도 동일하게 대한민국 법률이 적용된다.

9.15. 관련 법률의 준수

본 인증업무준칙(CPS)은 전자정부법 및 관련 법령을 준수한다.

9.16. 부칙

9.16.1. 완전 합의

해당 사항 없음

9.16.2. 양도

해당 사항 없음

9.16.3. 분리 조항

해당 사항 없음

9.16.4. 집행 (변호사 비용 및 권리 포기)

해당 사항 없음

9.16.5. 불가항력

해당 사항 없음

9.17. 기타 조항

해당 사항 없음

별첨. 인증서 프로파일

1. 최상위 인증기관 인증서

필드명		요구사항	값	
기본 필드	Version (버전)	(0x2)	3 (0x2)	
	Serial Number (일련번호)	8바이트 이상 CSPRNG 난수	(필수)	
	Signature Algorithm (서명 알고리즘)	SHA256 RSA	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
	Issuer (발급자)	Subject 값과 동일	commonName = MOIS SSL Root CA ogranizationName = Ministry of the Interior and Safety countryName = KR	
	Validity (유효기간)	20년	(필수)	
	Subject (소유자)	필수 속성 값 CN, O, C	commonName = MOIS SSL Root CA ogranizationName = Ministry of the Interior and Safety countryName = KR	
	Subject Public Key Info (소유자 공개 키 정보)	RSA 4096 bit	Public Key Algorithm : rsaEncryption RSA Public-Key : (4096 bit)	
확장 필드	Subject Key Identifier (소유자 키 식별자)	공개 키 Hash 20바이트	non-critical	(필수)
	Key Usage (키 사용)	(0x06)	critical	keyCertSign, cRLSign (0x06)
	Basic Constraints (기본 제한)	고정값	critical	Subject Type = CA Path Length Constraint = None

2. 인증기관 인증서

필드명		요구사항	값
기본 필드	Version (버전)	(0x2)	3 (0x2)
	Serial Number (일련번호)	8바이트 이상 CSPRNG 난수	(필수)
	Signature Algorithm (서명 알고리즘)	SHA256 RSA	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
	Issuer (발급자)	최상위 인증기관 Subject 값	commonName = MOIS SSL Root CA ogranizationName = Ministry of the Interior and Safety countryName = KR
	Validity (유효기간)	10년	(필수)
	Subject (소유자)	필수 속성 값 CN, O, C	commonName = MOIS SSL Server CA ogranizationName = Ministry of the Interior and Safety countryName = KR

	Subject Public Key Info **(소유자 공개 키 정보)**	RSA 3072 bit	Public Key Algorithm : rsaEncryption RSA Public-Key : (3072 bit)	
확장 필드	**Authority Key Identifier** **(기관 키 식별자)**	최상위 인증기관 SKI 값	non-critical	(필수)
	Subject Key Identifier **(소유자 키 식별자)**	공개 키 Hash 20바이트	non-critical	(필수)
	Key Usage **(키 사용)**	(0x86)	critical	keyCertSign, cRLSign, digitalSignature (0x86)
	Basic Constraints **(기본 제한)**	고정값	critical	Subject Type = CA Path Length Constraint = 0
	Certificate Policy **(인증서 정책)**	CPS OID 및 URL(HTTP)	non-critical	[1]Certificate Policy: Policy Identifier=anyPolicy [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://ssl.gpki.go.kr/legal/cps
	Extended Key Usage **(확장 키 사용)**	고정값	non-critical	서버 인증 (1.3.6.1.5.5.7.3.1) 클라이언트 인증 (1.3.6.1.5.5.7.3.2)
	CRL Distribution Points **(CRL 배포 지점)**	CRL URL (HTTP)	non-critical	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ssl.gpki.go.kr/arl/SSL-RootCA.crl
	Authority Information Access **(기관 정보 접근)**	최상위 인증기관 인증서 및 OCSP URL (HTTP)	non-critical	[1]Authority Info Access Access Method=인증기관 발급자 (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ssl.gpki.go.kr/certs/ssl-rootca.cer [2]Authority Info Access Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp-rca-ssl.gpki.go.kr

3. 가입자 조직 유효성 검증(OV) 인증서

필드명		요구사항	값
기본 필드	**Version** **(버전)**	(0x2)	3 (0x2)
	Serial Number **(일련번호)**	8바이트 이상 CSPRNG 난수	(필수)
	Signature Algorithm **(서명 알고리즘)**	SHA256 RSA	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
	Issuer **(발급자)**	인증기관 Subject 값	commonName = MOIS SSL Server CA ogranizationName = Ministry of the Interior and Safety countryName = KR

	Validity **(유효기간)**	최대 397일	(필수)	
	Subject **(소유자)**	속성값 CN, O, L, S, C	commonName = (웹사이트 URL 필수) ogranizationName = (영문 기관명 필수) locality = (영문 시명 선택) stateOrProvince = (영문 시도명 필수) countryName = KR	
	Subject Public Key Info **(소유자 공개 키 정보)**	RSA 2048 bit	Public Key Algorithm : rsaEncryption RSA Public-Key : (2048 bit)	
확장 필드	**Authority Key Identifier** **(기관 키 식별자)**	인증기관 SKI 값	non-critical	(필수)
	Subject Key Identifier **(소유자 키 식별자)**	공개 키 Hash 20바이트	non-critical	(필수)
	Key Usage **(키 사용)**	(0xA0)	critical	digitalSignature, keyEncipherment (0xA0)
	Basic Constraints **(기본 제한)**	고정값	critical	Subject Type = End Entity Path Length Constraint = None
	Certificate Policy **(인증서 정책)**	CPS OID 및 URL(HTTP)	non-critical	[1]Certificate Policy: Policy Identifier=1.2.410.100001.100.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://ssl.gpki.go.kr/legal/cps [2]Certificate Policy: Policy Identifier=2.23.140.1.2.2
	Subject Alternative Name **(소유자 대체 이름)**	대체 도메인 주소(FQDN)	non-critical	(단일 도메인 일 경우) DNS Name = Domain Name 1 또는 (복수 도메인 일 경우) DNS Name = Domain Name 1 DNS Name = Domain Name 2 DNS Name = Domain Name 3 ...
	Extended Key Usage **(확장 키 사용)**	고정값	non-critical	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
	CRL Distribution Points **(CRL 배포 지점)**	CRL URL (HTTP)	non-critical	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ssl.gpki.go.kr/crl/ca/Crl#1p#2Dp#3.crl
	Authority Information Access **(기관 정보 접근)**	인증기관 인증서 및 OCSP URL (HTTP)	non-critical	[1]Authority Info Access Access Method=인증기관 발급자 (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ssl.gpki.go.kr/certs/ssl-ca.cer [2]Authority Info Access Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) Alternative Name:

				URL=http://ocsp-ca-ssl.gpki.go.kr
	SCT List (서명된 인증서 타임스탬프 목록)	CT 로그 3개 이상	non-critical	(필수)

4. OCSP 응답자(Responder) 인증서

- 인증기관 인증서 OCSP URL : http://ocsp-rca-ssl.gpki.go.kr
- 가입자 인증서 OCSP URL : http://ocsp-ca-ssl.gpki.go.kr

필드		요구사항	값	
기본필드	Version (버전)	(0x02)	V3 (0x02)	
	Serial Number (일련번호)	8바이트 이상 CSPRNG 난수	(필수)	
	Signature Algorithm (서명 알고리즘)	SHA256 RSA	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
	Issuer (발급자)	발급자 Subject 값	(필수)	
	Validity (유효 기간)	최대 3년	(필수)	
	Subject (소유자)	필수 속성 값 CN, O, C	(인증기관 인증서 OCSP) commonName = MOIS SSL CA OCSP Responder #(n) (n = 1, 2, 3, ...) ogranizationName = Ministry of the Interior and Safety countryName = KR 또는 (가입자 인증서 OCSP) commonName = MOIS SSL Subscriber CA OCSP Responder #(n) (n = 1, 2, 3, ...) ogranizationName = Ministry of the Interior and Safety countryName = KR	
	Subject Public Key Info (소유자 공개 키 정보)	RSA 2048 bit	Public Key Algorithm : rsaEncryption RSA Public-Key : (2048 bit)	
확장필드	Basic Constraints (기본 제한)	고정값	critical	Subject Type=End Entity Path Length Constraint=None
	Subject Key Identifier (소유자 키 식별자)	공개 키 Hash 20바이트	non-critical	(필수)
	Authority Key Identifier (기관 키 식별자)	발급자 SKI 값	non-critical	(필수)
	Key Usage (키 사용)	(0x80)	critical	Digital Signature (80)

	Extended Key Usage (확장 키 사용)	고정값	non-critical	OCSP Signing (1.3.6.1.5.5.7.3.9)
	Authority Information Access (기관 정보 접근)	OCSP URL(HTTP)	non-critical	**(인증기관 인증서 OCSP)** [1]Authority Info Access Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp-rca-ssl.gpki.go.kr **또는** **(가입자 인증서 OCSP)** [1]Authority Info Access Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp-ca-ssl.gpki.go.kr
	OCSP No Revocation Checking (OCSP 폐지 확인)	고정값	non-critical	id-pkix-ocsp-nocheck (1.3.6.1.5.5.7.48.1.5)