AutoCrypt V2X PKI Root CA

인증업무준칙

(Root CA CPS)

V1.1

2022.09.08

아우토크립트㈜

<개정 이력>

버전	개정 내용	작성자	제•개정일
V1.0	신규 작성	김명현	2022/06/29
V1.1	▪ 공통 (오타 수정, 외래어 표기 수정) ▪ 1.5.4. 인증업무준칙 승인 절차(누락된 1.5.4. 항목 추가) ▪ 2.3. 공고 주기(폐지목록 유효기간 수정) ▪ 5.4.2. 감사로그 검토 주기(감사로그 검토주기 수정) ▪ 5.5.4. 기록의 백업 절차(백업 주기 수정)	김명현	2022/09/08

<목 차>

1. 개요

아우토크립트의 V2X 보안 인증체계는 안전한 자율협력주행 환경에서 차량과 노변기지국, V2X 인증체계 기관에 인증서를 발급, 폐지 등의 관리를 제공하는 공개키 기반의 인증체계이다.

본 인증업무준칙에서는 아우토크립트 V2X 보안인증시스템을 Root CA(최상위 인증기관)라고 하며 하위 기관들에게 인증업무를 수행할 수 있도록 인증서의 발급, 배포, 폐기 등의 관리하는 기술, 법률 및 비즈니스 요구사항을 설정한다

Root CA는 CAMP(The Crash Avoidance Metrics Partnership LLC.)의 SCMS(Security Credential Management System) 아키텍처와 IEEE 1609.2의 기술규격을 따른다. V2X 인증서는 IEEE 1609.2 인증서 포맷을 사용한다.

1.1. 소개

본 문서는 V2X 통신망을 이용하여 처리되는 공개 키 기반구조(PKI)를 가진 차량 간(V2V), 차량과 노변 인프라간(V2I) 메시지의 인증과 무결성 등의 내용을 RFC 3647 기준으로 작성하였으며, 아우토크립트에서 운영하는 CA의 인증서 정책, 인증서 발급/관리, 보안 통제, 기타 운영 정책/절차 등 V2X 보안인증체계와 관련된 업무에 필요한 사항 및 인증기관 등의 책임·의무에 관한 인증업무준칙을 다룬다.

1.2. 문서명 및 식별

본 문서의 명칭은 「AutoCrypt V2X PKI Root CA 인증업무준칙」이라고 한다.

1.3. 전자서명인증체계 관련자

1.3.1. 인증기관

인증기관은 AutoCrypt V2X PKI Root CA(이하 V2X PKI)를 지칭한다. 이는 등록, 식별, 인증 및 발행을 포함한 인증서 관리를 책임지며, V2X 보안인증체계에 따라 발급된 인증서와 관련된 인증기관 서비스 및 인증기관 운영의 모든 측면이 해당 요건, 진술 및 보증서에 따라 수행되도록 책임을 가진다.

인증기관은 CAMP SCMS 아키텍처 및 IEEE 1609.2 프로필 사양과 일치하는 보안 요구 사항을 갖춘 독립 환경이다. 아우토크립트에서는 최상위 인증기관(Root CA)을 운영하며, 업무는 다음과 같

다.

- 안전한 Root CA 시스템 구축 및 운영
- 관리자의 승인에 따라 인증업무 수행
  - Root CA의 인증서 발급/폐지
  - 하위 기관의 인증서 발급/폐지
- 하위 인증기관 검사 및 안전운영 지원

1.3.2. 등록기관

아우토크립트는 하위 기관들의 인증서를 관리하는 업무를 하고 있으며, 이 업무를 위탁하거나 대행하는 별도의 등록기관을 두지 않고 인증기관에서 직접 처리한다.

1.3.3. 가입자

인증서를 신청하게 되는 하위기관이 가입자가 되며 IEEE 1609.2 기술규격과 SCMS 아키텍처를 만족하고 별도의 계약을 체결한 인증 받은 V2X 보안인증체계의 일원 중 하나이다.

- 중계 인증기관(Intermediate Certificate Authority) : V2X 보안인증체계의 신뢰기관 중 Root CA 하단에 존재하며 다른 구성요소에 인증서를 발급하는 기관
- 이상행위 관리기관(Misbehavior Authority) : 단말로부터 전송된 이상 행위 보고서를 통하여 이상 행위 단말을 판별하고 인증서를 폐지하는 기관
- 정책 관리기관(Policy Generator) : Root CA의 요청에 따라 정책 배포를 하기 위해 정책파일과 체인인증서를 생성하고 관리하는 기관
- 인증서폐기목록 관리기관(Certificate Revocation List Generator) : V2X 보안인증체계의 인증서 폐지 목록(CRL)을 관리하는 기관

1.3.4. 신뢰당사자

신뢰 당사자는 발급된 Root CA 인증서를 신뢰하고 V2X 보안 메시지의 신뢰성을 검증하기 위해 인증기관에서 발급한 종단 실체 인증서의 유효성에 의존하므로 인증기관의 가입자가 신뢰 당사자이다.

1.4. 인증서 종류

1.4.1. 인증서 용도

이 인증업무준칙에 따라 발급된 인증서는 V2X 통신을 위한 전자 서명 사실 확인과 유효성을 검사하고 CAMP SCMS 아키텍처 및 IEEE 1609.2 사양에 따라 인증서의 수명 주기를 관리하며, 이 외의 용도로는 사용하지 않는다.

1.4.2. 인증서 용도 제한

Root CA가 발급한 Root CA 인증서와 가입자 기관에게 발급한 V2X 인증서는 발급 시의 이용범위 또는 용도 내에서만 이용되어야 한다. 인증서를 이용범위 또는 용도 외에 이용할 수 없다.

1.5. 준칙의 관리

1.5.1. 인증업무준칙 제정 및 개정 기관

이 인증업무준칙의 작성과 운영은 아우토크립트의 V2X PKI Root CA Policy Authority (PA)에 의해 관리된다. PA의 역할은 다음과 같다.

- 현재 및 미래의 인증업무준칙 버전의 승인
- 인증기관 승인 절차의 정의, 결정 및 공표를 포함한 승인 관리
- 인증기관의 CPS 준수와 게시된 신뢰 서비스 원칙에 따른 운영의 준수를 승인
- 인증기관의 인증업무 및 운영절차 지침에 대한 승인 관리

1.5.2. 인증업무준칙 담당

인증업무준칙 담당에 관련된 연락처는 다음과 같다.

- 업무담당 : AutoCrypt V2X PKI Root CA 보안인증센터
- 전화번호 : (02) 2125-4020
- 조직주소 : 서울특별시 영등포구 여의공원로 115 세우빌딩 6층
- 메일주소 : rootca@autocrypt.io

1.5.3. 인증업무준칙 책임

V2X PKI PA는 인증업무준칙의 적합성 및 개정, 절차를 승인한다.

- V2X PKI CA 인증업무준칙은 V2X PKI PA의 승인하에 최소 1년에 한번 이상 인증업무준칙과 운영 상태를 검토하고 이해 관계자 및 하위 기관과 협의한다.
- 이해 관계자 및 하위 기관에 영향을 미치는 주요한 변경사항에 대해서는 최소 2주간 검토가 허용되며, 개정된 변경사항은 인증업무준칙에 반영한다.
- 개정된 사항이 이해 관계자 및 하위 기관에 미치는 영향이 없더라도 인증업무준칙은 개정하고 반영된다.
- 제·개정된 인증업무준칙은 신고한 날로부터 시행한다

1.5.4. 인증업무준칙 승인 절차

제안 및 변경 사항의 영향에 따라 이해 관계자 및 하위 기관은 검토 및 피드백을 위해 제안된 변경사항에 대한 통지를 받을 수 있다

개정된 인증업무준칙을 센터 홈페이지에 공고하고 개별적으로 이해 관계자 및 하위 기관에 통보하여 이해 관계자 및 하위 기관이 동의 여부를 표시하거나 규정에 따른 준하는 방법으로 의사표시를 한다.

1.6. 정의 및 약어

1.6.1. 정의

CA	인증서와 관련된 CA 서비스, 운영 및 인프라의 모든 측면이 명시된 정책과 관행에 따라 수행하도록 보장하면서, 인증서의 발급 및 관리에 대한 모든 측면을 책임지는 기관
CRL	인증서 폐기 목록. 현재 사용중인 인증서가 만료/정상 유무를 판단할 수 있는 신뢰할 수 있는 인증서 폐기 목록
CRLG	V2X 보안인증체계의 인증서 폐지 목록(CRL)을 관리하는 요소
CSR	인증서를 발급받기 위해서 인증서비스를 사용할 시스템의 비대칭키 정보를 포함시켜 인증 기관으로 보내어 인증서를 발급받기 위한 일종의 신청서
ICA	V2X 보안인증체계의 신뢰 기관 중 Root CA 하단에 존재하며 다른 구성요소에 인증서를 발급하는 기관
MA	단말로부터 전송된 이상 행위 보고서를 통하여 이상 행위 단말을 판별하고 인증서를 폐지하는 기관
PCA	단말의 익명, 식별, 응용 인증서를 발급하고 관리하는 기관
PG	SCMS Manager 의 요청에 따라 정책 배포를 하기 위해 GPF 와 GCCF 를 생성하고 관리
Root CA	V2X 보안인증체계의 신뢰 관계에서 최상위 기관으로 하위 관계의 모든 인증서와 서명을 신뢰할 수 있도록 하는 요소
SCMS	Security Credential Management System(보안인증관리시스템). 미국의 V2X 보안인증체계에서 사용하는 PKI 기반의 기관, 장치, 체계를 이루는 시스템
V2X 보안인증체계	안전한 V2X 통신서비스 제공을 위한 V2X 인증서의 발급 및 인증 관련 기록의 관리 등 인증 업무를 제공하기 위한 체계
개인키	비대칭 암호 알고리즘에서 한 대상이 소유하는 키 쌍 중 공개되지 않고 비밀리에 사용하는 키
공개키	비대칭 암호 알고리즘에서 한 대상이 소유하는 키 쌍 중 공개되는 키
만료	인증용으로 사용하는 인증서가 상위 기관에게 인증 받을 수 있는 최대 기간이 종료된 상태
기관	정책관리, 인증서 발행, 이상 행위 탐지 등 각 맡은 역할을 수행하는 독립적인 조직(단체, 모임)
기관 인증서	V2X 보안인증체계가 운영되기 위해 구성된 기관들이 상호간에 암호화된 데이터와 인증을 통해 안전한 통신을 하기 위해 사용하는 인증서
사용 기간	V2X 보안인증체계의 각 기관들이 그 역할의 특성에 따라 사용되어지는 인증서의 사용 기간으로 사용 기간은 유효 기간 보다 작거나 같다
신뢰 요소	인증서의 안전한 발급 및 관리를 위해 의존하는 Root CA, ICA, CRLG, PG, MA 시스템과 관련 인프라

신청자	가입자가 되기 위해 CA 에 인증서 서비스를 신청하는 법적 기업 또는 그의 공인 대리자
유효 기간	인증용으로 사용하는 인증서가 인증 받을 수 있는 최대 기간
이상 행위	인증관리체계 또는 교통체계를 위협할 수 있는 인증관리체계 내 단말의 오동작 및 유해 행위
인증 기관	보안 적격 여부 및 메시지 암호화를 위한 공개 키의 발급과 관리를 담당하는 신뢰성이 보장된 온라인상 하위기관을 인증해 주는 기관
인증서	공개 키와 ID 를 연결하기 위해 디지털 서명을 사용하는 레코드. 「V2X 인증서 프로파일」을 준수하는 형태
인증서 갱신	인증서의 유효기간을 연장하는 행위
인증서 재발급	인증서를 분실/유출 등의 이유로 다시 발급받는 행위
저장소	인증기관 정보의 저장 위치를 정의한다. 이 정보에는 인증서, 인증서 해지 목록, 인증서 정책 또는 인증서 사용 설명서가 포함될 수 있음
최상위 인증서	V2X 보안인증체계의 신뢰 관계에서 가장 상단에 위치한 최상위 기관의 인증서
키 쌍	비대칭키는 암호화할 때와 복호화 할 때의 키를 별도로 사용하며, 차례로 공개키와 개인키라고 불리우는데 이를 키쌍이라고 한다
폐기	기관이 더 이상 기관의 역할을 수행하지 못해 영구적으로 해체되거나 일시적으로 해체되는 상태
폐지	관리자 또는 인증기관이 하위 기관 및 단말들의 인증서를 폐지 규칙에 부합할 경우 그 인증서를 더 이상 사용하지 못하도록 효력을 중단시키는 행위
하위 기관	각 맡은 역할을 수행하는 독립적인 조직 중 상위 기관에 소속되어서 단말과 중간 소통 역할을 하는 조직

1.6.2. 약어

CA	Certification Authority
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CRLG	CRL Generator
DCM	Device Configuration Manager
EA	Enrolment Authority
EC	Enrolment Credential
EE	End Entity
ICA	Intermediate certificate authority
LA	Linkage Authority

MA	Misbehavior Authority
OBE/OBU	Onboard Equipment / Onboard Unit
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OID	Object Identifier
PA	Policy Authority
PC	Pseudonym Certificate
PCA	Pseudonym Certification Authority
PG	Policy Generator
PKI	Public Key Infrastructure
RA	Registration Authority
RP	Relying Party
RSE/RSU	Roadside Equipment / Roadside Unit
SCMS	Security Credential Management System
Sub-CA	Subordinate CA
V2I	Vehicle to Infra
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
V2X PKI	AutoCrypt V2X PKI Root CA

2. 전자서명인증업무 관련 정보의 공고

2.1. 공고 설비

아우토크립트는 공개 가능한 저장소를 운영하며, V2X PKI 인증업무준칙 및 관련 인증서를 게시한다.

2.2. 공고 방법

저장소에 포함되는 내용과 공고 위치는 다음과 같다.

- V2X PKI 인증업무준칙
    - Root CA 인증서와 발급된 하위기관 인증서
- 인증서 폐기 목록(CRL) 정보를 얻기 위한 CRL 저장소 위치
- (https://autocrypt.co.kr/V2X-PKI-CA)
- 인증서 신청서 서식
- 인증업무담당 정보

2.3. 공고 주기

개정된 인증업무준칙은 PA의 승인 후 신고한 날로부터 10일 이내에 센터 홈페이지에 게시한다. 갱신된 Root CA 인증서는 인증서 사용 전에 인증서를 전파할 수 있도록 유효일 5일 전에 발행하여 즉시 게시한다. 폐지된 인증서 목록의 유효기간은 최대 90일이며, 폐지가 발생되면 1일 이내에 게시한다.

2.4. 공고된 정보에 대한 책임

아우토크립트는 인증업무준칙과 인증서 발급 및 관리 등에 관련된 정보를 누구든지 그 사실을 확인할 수 있도록 홈페이지에 게시하고 홈페이지와 통신 되는 구간은 HTTPS의 보안 통신을 하도록 구현한다.

Root CA는 안전하고 제한된 곳에 운영하며, 최상위 기관에 준하는 접근통제를 구현해야 한다. 시스템 운영자를 제외하고 Root CA 접근은 제한하고 접근 권한을 가진 자의 추가, 수정, 삭제 등의 작업도 통제를 받아야한다. 그 외에 모든 PKI 참가자 및 키 관리자 등 관련하여 출입부터 시스템 접근까지 통제를 구현하여 보호한다.

3. 신원확인

3.1. 가입자 이름 표시 방법

3.1.1. 이름 유형

Root CA에서 발급하는 V2X 인증서의 id 필드에는 IEEE 1609.2 인증서 프로파일 규격에 따라 다음 내용이 포함된다.

- 연결 값
- 호스트이름
- 이진 식별자(binary)

3.1.2. 이름 의미

CAMP 및 IEEE 1609.2의 명명 규칙을 준수하여 외부에서 액세스 가능한 정규화된 도메인 이름(FQDN)을 사용한다.

V2X 인증체계 Root CA에서 발급한 인증서 경우 DN명은 cn=인증체계 기관 호스트 구분자+인증체계명, c=io 체계를 준수하며 다음과 같은 호스트로 식별하게 된다.

- Root CA : Root CA
- ICA : ica
- CRLG : crlg

3.1.3. 신청인을 식별할 수 없는 익명의 인증서 발급

Root CA는 익명인증서를 발급하지 않는다.

3.1.4. 인증서 DN 규칙

다양한 명칭 형태 해석 규칙은 '3.1.2 이름 의미'를 참조한다.

3.1.5. 인증서 DN값의 유일성

Root CA에서 발급하는 인증서는 호스트 이름(hostName)을 부여하여 유일한 값을 가지게 한다.

3.1.6. 상표(Trademarks)의 사용

Root CA는 다른 사람의 상표를 침해하거나 상표 분쟁이 발생할 소지가 있는 인증서는 발급하지 않는다.

3.2. 인증서 신규 발급 시 신원 확인

Root CA는 인증서 신청자의 신원을 확인하기 위해서만 사용하며, 어떤 이유로든 인증서 신청자의 요청에 따라 인증 요청을 거부할 수 있다

3.2.1. 개인 키 소유 증명 방법

Root CA 인증서 신청자는 인증서 요청양식을 아우토크립트 Root CA에 직접 방문하여 제출하고 CSR파일에 기재되어 있는 공개 키에 대응하는 개인 키를 올바르게 보유하고 있음을 확인한다

3.2.2. 기관용 인증서의 초기 신원 확인

조직 인증은 제출한 기관 지정서, 사업자등록증 및 법인등기부등본을 통하여 당해 인증된 기관임을 확인하며 국가기관·지방자치단체의 경우 이에 상응하는 서류를 통해 당해 인증된 기관임을 확인한다

- 인증서 신청인의 신원과 신청 권한 확인
- 해당 기관의 존재 여부 신원 확인
- 해당 기관의 위치, 주소, 법적 등록 정보, 사업 여부를 확인
- 발급받을 인증서 도메인의 소유권 확인
- 발급받을 인증서에 포함될 장치와 소유권 및 통제 주체 확인

3.2.3. 개인용 인증서의 초기 신원 확인

Root CA는 인증서를 신청하는 조직의 개인이나 대리인의 신원을 아래와 같이 검증한다.

- 개인의 이름, 직함, 회사 이름, 이메일 주소, 연락처 검증
- 개인이 소속된 기관의 소속 직원임을 확인할 수 있는 서류 검증
- 개인이 신청기관의 신청 대리 권한을 지녔는지 서면 또는 승인 메일 검증

3.2.4. 신원이 확인되지 않은 인증서의 발급

신청인의 신원이 확인되지 않은 신청은 인증서를 발급하지 않는다.

3.2.5. 권한의 발효

모든 가입자는 인증서 발급, 갱신 및 폐지에 대한 요청을 책임지는 대표자 또는 담당자를 정의한다. 아우토크립트 Root CA는 V2X 인증서 신청인을 직접 대면하여 다음 방법에 의하여 신원을 확인한다.

- 신청인은 가입자 기관의 소속 직원임을 확인할 수 있는 서류로 신원을 확인하며, 신청인이 신청기관의 신청 권한을 지녔는지 검증
- 신청기관은 아우토크립트의 인증서를 발급받아 이용하는 가입자로서 사전 계약이 체결되어 있어야 하며, 이를 확인할 수 있는 계약서 등의 서류로 검증

3.2.6. 상호 운용 기준

Root CA는 IEEE 1609.2 기술규격의 통신 메커니즘 준용하므로 최상위 인증기관으로서 일방적으로 인증기관 및 가입자 기관을 인증한다.

3.3. 인증서 갱신발급, 재발급 및 변경 시, 신원확인

3.3.1. 반복적인 재발급에 대한 신원 확인 및 검증

인증서 재발급은 신청인의 기존 인증서가 유효한 상태일 때 가능하다. 그러므로 인증서의 재발급이 필요한 경우 유효기간이 만료되기 전에 재발급을 요구해야 한다. 키 재생성을 위한 식별 및 인증 방법은 '3.2.2 기관용 인증서의 초기 신원 확인'에 설명한 바와 같이 신규 인증서 발급과 신원확인 절차로 동일하게 따른다.

인증서 재발급 신청 시 신청인의 기존 등록정보가 변경된 경우 신청인 및 등록대행, 기관에게 변

경정보에 대한 증빙자료를 요구할 수 있다.

3.3.2. 폐지 후 재발급에 대한 신원 확인 및 검증

기관이 인증서 재발급을 신청하면 인증서의 분실/훼손 또는 도난/유출과 동일하게 유효기간 만료 여부와 관계없이 폐지하고 신규 발급 신청에 준하는 절차로 신원을 확인한다.

3.4. 인증서 효력정지, 효력회복, 폐지 시, 신원확인

발급된 인증서는 아우토크립트 보안인증센터 담당자가 접수를 받아 Root CA의 승인으로 취소할 수 있다. 폐지 요청에는 폐지 상황 및 폐지될 인증서가 폐지되지 않은 상태로 유지되는 기간이 포함되어야 한다.

인증서 폐지 요청은 공인된 신청인이 서명한 서면으로 이루어져야 하며, 신원 확인, 권한 검증은 '3.2.5 권한의 발효' 항목을 참조하여 검증한다.

PA는 신청인의 폐지 결정에 대해 다음을 확인한다.

- 인증서 폐지 결정 확인서
- 이해관계자의 합의 내용 및 폐지 사유

4. 인증서 관리

4.1. 인증서 발급 신청

Root CA는 하위 기관의 인증서 발급 요청을 PA의 승인에 따라 처리한다. 인증서 발급 및 관리 등에 관련된 정보를 V2X 보안인증체계에 의하여 누구든지 그 사실을 항상 확인할 수 있도록 게시한다.

4.1.1. 인증서 신청 기준

Root CA 인증서는 계약 사항에 따라 V2X 보안인증체계 기술규격을 준수하고 라이선스가 부여되어 인증된 PG, MA, ICA, CRLG 기관이 인증서를 신청할 수 있다.

4.1.2. 인증서 신청 절차 및 책임

인증서를 신청하는 기관은 V2X PKI 보안인증센터에 연락하여 신청 양식을 이메일로 전송 받아 필요한 사항을 작성한 후 Root CA에 신청한다.

신청인은 Root CA에 인증서 발급신청 시, 인증서 발급 요청문(Certificate Signing Request; CSR) 형식으로 가입자 기관의 공개키를 직접 제출하여야 한다.

Root CA는 신청인 또는 기관의 개인키를 생성하거나 보관하지 않는다.

4.2. 인증서 발급 신청 처리

4.2.1. 신원 확인 및 인증

Root CA는 해당 인증업무준칙에 문서화된 바와 같이 각 신청자의 신원 및 권한을 검증하고 인증해야 한다. 인증서 신청인 또는 신청 대리인을 직접 대면하여 '3.신원확인'을 참조하여 인증서 신청 및 승인 절차에 따라 인증 신청에 대한 승인 또는 거절을 한다.

4.2.2. 신청에 대한 승인 및 거절

Root CA는 인증서를 받고자 하는 기관의 인증 신청서와 PA의 승인을 확인하고 1609.2 및 SCMS 요건에 적합한 올바른 형식 및 검증된 인증서 규격을 검토하여 문제가 없는 경우 처리하게 된다.

다음 어느 하나에 해당하는 경우에 Root CA는 인증서 발급을 거절한다.

- 정확하지 않은 정보 포함
- 불분명한 내용 기재
- 신원 확인과정 <V2X 보안 인증서 신청서> 내용이 허위로 기재
- 신청자 또는 기관의 대표 자격이 없다고 판단
- 인증 업무 또는 기술적 지장이 있다고 판단

4.2.3. 신청 처리 소요 시간

Root CA는 신청서 접수를 받을 시 신청자에게 발행시간에 영향을 미칠 수 있는 요소를 인지시킨

다. 인증서의 유효한 신청을 받은 후 영업일 기준 5일 이내에 발급하고 발행기간을 준수한다.

4.3. 인증서 발급 절차 및 보호조치

4.3.1. 인증서 발급 절차

Root CA는 인증서를 신규 발급하기 전에 인증업무준칙에서 설명하는 방식으로 인증서 신청 출처를 확인하고 다음의 인증서 신규발급 신청 절차를 통해 발급한다

- 인증서 신청인이 제출한 공개키의 유일성 확인
- 인증서 신청인이 제출한 공개키와 소유한 개인키에 합치하는지 여부의 확인 (개인키 소유 증명 확인)
- 인증서 신청인이 제출한 요청 정보의 ID 유일성과 필요한 인증서 요청 정보 필드 평가
- CAMP SCMS에 명시된 흐름과 프로토콜에 따라 신청인에게 인증서를 제공

4.3.2. 인증서 발급 통지

인증서 신청기관 인증서의 발급 통지는 이메일로 전달하고 이메일 수신이 어려운 경우 우편과 신청 담당자의 연락처를 통해 해당 기관에 통지한다.

4.4. 인증서 수령

4.4.1. 인증서 수령 절차

V2X PKI 보안인증센터 홈페이지 저장소에 게시된 인증서를 다운로드한다. 신청인 기관 대표자 또는 대리인은 인증서 수령 후 발급된 인증서에 대한 수락 여부를 센터에 제출한다

구독자가 인증서 통지 후 5영업일 이내에 인증서를 설치하거나 인증서 문제를 보고하고 취소를 요청하지 않는 한 인증서는 승인된 것으로 간주된다. 신청인 또는 기관은 올바르게 확인되지 않은 모든 인증서를 폐기하고 Root CA에 통보한 후 새 요청을 보내야 한다.

4.4.2. 인증서 게시

발급된 기관 인증서는 2.1에서 식별된 저장소에 게시한다.

4.4.3. 인증서 발급 공지

Root CA의 새로운 인증서를 발급한 경우 신뢰당사자가 해당 사실을 알 수 있도록 발급된 Root CA 인증서를 V2X 보안인증센터 홈페이지에 게시하고 필요시 영향에 따라 유관기관에 인증서 신청 담당자의 이메일 또는 연락처로 별도 통보한다.

4.5. 인증서 이용

4.5.1. 개인 키 사용 용도

인증서를 제공받은 기관은 Root CA로부터 받은 공개키에 합치하는 개인키를 사용해야 한다. 인증서를 제공받은 기관은 개인키를 안전한 방법으로 생성 및 보관하고 시설 및 장비 등에 관한 규정의 기술규격을 만족하는 하드웨어 보안 모듈(HSM)을 이용하여 개인키가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리하여야 한다.

개인키와 인증서는 전자서명 및 암호화 통신 등 V2X 인증업무 수행을 위해서만 사용한다.

4.5.2. 공개 키 사용 용도

인증서를 제공받은 기관은 SCMS 규격 및 IEEE 1609.2 표준을 준수하여 인증서의 사용 및 검증 방법을 숙지한 후 V2X PKI 보안인증센터 홈페이지로부터 인증서 폐지 목록, 인증서 정보 및 저장소와 유효성, 인증서의 유효기간 등을 먼저 확인해야 한다. 공개키와 인증서는 전자서명 및 암호화 통신 등 V2X 인증업무 수행을 위해서만 사용한다.

4.6. 인증서 갱신발급

V2X 보안인증체계의 Root CA 인증서 발급 정책에서는 가입자가 제공받은 인증서를 갱신하지 않고 신규 발급으로 갱신 발급을 대체 처리한다.

4.6.1. 인증서 갱신 기준

해당사항 없음

4.6.2. 인증서 갱신 신청자

해당사항 없음

4.6.3. 인증서 갱신 절차

해당사항 없음

4.6.4. 인증서 갱신 통지

해당사항 없음

4.6.5. 인증서 갱신 승인

해당사항 없음

4.6.6. 인증서 갱신 게시

해당사항 없음

4.6.7. 인증서 갱신 공지

해당사항 없음

4.7. 인증서 재발급

인증서 재발급의 경우 아우토크립트 Root CA 인증서 발급 정책에 따라 재발급 업무는 신규 발급 처리와 동일한 절차를 따른다.

4.7.1. 인증서 재발급 기준

인증서 재발급의 경우 아우토크립트 Root CA 인증서 발급 정책에 따라 재발급 업무는 신규 발급 처리와 동일한 절차를 따른다.

4.7.2. 인증서 재발급 신청자

인증서 재발급의 경우 아우토크립트 Root CA 인증서 발급 정책에 따라 재발급 업무는 신규 발급 처리와 동일한 절차를 따른다.

4.7.3. 인증서 재발급 절차

인증서 재발급의 경우 아우토크립트 Root CA 인증서 발급 정책에 따라 재발급 업무는 신규 발급 처리와 동일한 절차를 따른다.

4.7.4. 인증서 재발급 통지

인증서 재발급의 경우 아우토크립트 Root CA 인증서 발급 정책에 따라 재발급 업무는 신규 발급 처리와 동일한 절차를 따른다.

4.7.5. 인증서 재발급 승인

인증서 재발급의 경우 아우토크립트 Root CA 인증서 발급 정책에 따라 재발급 업무는 신규 발급 처리와 동일한 절차를 따른다.

4.7.6. 인증서 재발급 게시

인증서 재발급의 경우 아우토크립트 Root CA 인증서 발급 정책에 따라 재발급 업무는 신규 발급 처리와 동일한 절차를 따른다.

4.7.7. 인증서 재발급 공지

인증서 재발급의 경우 아우토크립트 Root CA 인증서 발급 정책에 따라 재발급 업무는 신규 발급

처리와 동일한 절차를 따른다.

4.8. 인증서 변경

4.8.1. 인증서 변경 기준

인증서 변경이 발생한 경우 기존 인증서는 폐지하고 신규로 인증서를 발행하는 방법 및 절차와 동일하게 처리한다.

4.8.2. 인증서 변경 신청자

인증서 변경이 발생한 경우 기존 인증서는 폐지하고 신규로 인증서를 발행하는 방법 및 절차와 동일하게 처리한다.

4.8.3. 인증서 변경 절차

인증서 변경이 발생한 경우 기존 인증서는 폐지하고 신규로 인증서를 발행하는 방법 및 절차와 동일하게 처리한다.

4.8.4. 인증서 발급 통지

인증서 변경이 발생한 경우 기존 인증서는 폐지하고 신규로 인증서를 발행하는 방법 및 절차와 동일하게 처리한다.

4.8.5. 인증서 변경 승인 절차

인증서 변경이 발생한 경우 기존 인증서는 폐지하고 신규로 인증서를 발행하는 방법 및 절차와 동일하게 처리한다.

4.8.6. 인증서 변경 게시

인증서 변경이 발생한 경우 기존 인증서는 폐지하고 신규로 인증서를 발행하는 방법 및 절차와 동일하게 처리한다.

4.8.7. 변경된 인증서 발급 공지

인증서 변경이 발생한 경우 기존 인증서는 폐지하고 신규로 인증서를 발행하는 방법 및 절차와 동일하게 처리한다.

4.9. 인증서 효력정지, 효력회복, 폐지

Root CA는 키 손상, 유출이나 인증서 조기 사용종료 등의 이유로 무결성을 보호하기 위해 키 또는 인증서를 교체하여 자체 인증서를 폐지하거나 발급된 하위기관의 인증서를 폐지할 수 있다.

4.9.1. 인증서 폐지 기준

Root CA는 V2X 보안인증체계 기술규격에 의하여 다음과 같은 사유가 발생하거나 Root CA의 무결성이 의심이 되는 경우 발행된 기관 인증서를 폐지한다.

- 기관이 인증서 폐지를 신청한 경우
- 기관이 실수 또는 고의, 기타 부정한 방법으로 인증서를 발급받은 사실을 인지한 경우
- 기관의 해산 사실을 인지한 경우
- 기관의 개인키가 분실/훼손 또는 도난/유출된 사실을 인지한 경우
- 기관이 준칙의 주요 의무나 주요 사항을 준수하지 않을 경우
- 보안 체계의 보안 유지 및 향상을 위하여 필요한 경우
- 상위 인증서가 폐지된 경우

4.9.2. 인증서 폐지 신청자

신원이 확인된 인증서 폐지 신청인 또는 기관의 대표자는 취소 이유를 상세히 기술하는 인가된 인증서 폐지 요청을 제출함으로써 기관 자체 요구로 Root CA에게 인증서 취소를 요청할 수 있다.

4.9.3. 인증서 폐지 절차

V2X PKI 보안인증센터에서 인증서 취소 신청서를 다음과 같은 절차로 처리한다.

- 인증서 폐지 신청인의 권한 및 신원 확인
- 인증서 폐지 신청서 무결성 확인
- 인증서 폐지 신청서의 폐지 날짜. 폐지 사유 등 유효성 확인
- 인증서 폐지 신청 내용 검토 후 Root CA에 폐지 명령
- 인증서 폐지 결과 게시

4.9.4. 인증서 폐지 요청 유예 기간

Root CA 또는 신청 기관의 인증서 폐지 이유와 보안 위험이 확인되면 지체없이 V2X PKI 보안인증센터에게 폐지를 요청을 하고 신청 후 24시간 이내 폐지 처리를 한다. 유예 기간이 Root CA의 무결성 또는 보안을 손상시키지 않을 경우라면 최대 30영업일의 유예 기간을 제공한다.

4.9.5. 인증서 폐지 요청 처리 시간

V2X PKI 보안인증센터는 기관의 인증서 폐지 사유가 발생한 경우 지체없이 Root CA에게 폐지 요청을 해야 하며 최대 3일을 넘기지 않고 처리한다. 보안상 사고 및 무결성에 영향이 있다면, 폐지 신청 후 24시간 이내 폐지 처리한다.

4.9.6. 인증서 폐지 확인 요구사항

신뢰당사자는 IEEE 1609.2 규격에 명시된 신뢰 경로 인증 체계를 적절하게 처리할 수 있는 소프트웨어를 사용하거나 V2X 보안인증센터 홈페이지의 인증서 폐지 목록(CRL) 및 인증 경로를 확인해야 한다.

4.9.7. 인증서 폐지 목록 발행 빈도

'2.3 공고 주기'에 폐지된 인증 갱신과 공고 내용에 따른다.

4.9.8. 인증서 폐지 목록 발행 최대 소요 시간

Root CA는 폐지 처리 후 지체 없이 CRL을 발행해야 하며, 폐지 후 1영업일 이내에 공고해야 한

다.

4.9.9. 실시간 인증서 폐지 및 상태 확인 유효성

Root CA는 온라인 인증서 상태 확인 서비스를 지원하지 않는다.

4.9.10. 실시간 인증서 폐지 확인 요구사항

Root CA는 온라인 인증서 상태 확인 서비스를 지원하지 않는다.

4.9.11. 인증서 폐지 정보 유효성 검증의 다른 방법

해당사항 없음

4.9.12. 키 교체 또는 키 손상의 특수 요구사항

인증서 발급받은 기관은 자신의 개인키가 분실/훼손 또는 도난/유출 등 안전하지 않다는 사실을 인지한 경우 V2X PKI 보안인증센터에 지체없이 통보하여 안전성과 신뢰성 확보 대책을 강구해야 하며, 손상된 인증서는 즉시 폐지 요청한다.

4.9.13. 인증서 효력 정지 기준

해당사항 없음

4.9.14. 인증서 효력 정지 대상

해당사항 없음

4.9.15. 인증서 효력 정지 절차

해당사항 없음

4.9.16. 인증서 효력 정지 기간

해당사항 없음

4.10. 인증서 유효성 확인 서비스

4.10.1. 인증서 상태 서비스의 기능적 특징

Root CA에서 발급하는 CRL은 IEEE 1609.2 규격에 설명된 방법을 이용하여 신뢰당사자에게 배포하거나 안전하고 신뢰할 수 있는 저장소에 폐지 목록을 발급하고 게시한다.

4.10.2. 인증서 상태 서비스 가용성

V2X PKI 보안인증센터는 인증서 폐지 목록이 갱신된 사실을 언제, 누구든지 확인할 수 있도록 게시한다.

4.10.3. 인증서 상태 서비스 선택적 기능

해당사항 없음

4.11. 서비스 가입 철회

'4.11 서비스 가입 철회'는 인증서의 인증 서비스 중단으로 간주하여 인증서 폐지 절차인 '4.9 인증서 효력정지·효력회복·폐지'의 인증서 폐지 절차를 준용한다.

4.12. 기타 부가 서비스

해당사항 없음

4.12.1. 키 위탁 및 복구 정책 실행

해당사항 없음

4.12.2. 세션 키 캡슐화, 복구 정책 및 절차

해당사항 없음

5. 시설 및 운영 관리

Root CA 인증 시스템은 전력, 전자기기, 장치, 통제 등의 기능과 용량을 충족하는 규격으로 설계하였으며, 인증 서비스를 유지하기 위한 가용성과 연속성을 만족하기 위해 보안, 조직, 관리체계를 구축하여 정기적으로 분석, 평가되도록 관리한다.

5.1. 물리적 보호조치

인증 시스템은 외부인의 침입이나 불법적 접근 등의 물리적 위협으로부터 인증 시스템이 설치된 장소를 보호한다

5.1.1. 위치 및 시설

V2X PKI 보안인증센터의 Root CA 인증 시스템은 다른 시스템과 물리적으로 분리되어 별도의 통제 구역 내 설치되어 철저한 물리적 접근통제와 안전한 오프라인 방식으로 운영된다.

해당 시설은 다단계 보호되도록 설계되었으며 다음과 같은 체계를 포함하고 있다.

- 시설과 시스템실 통제
- 신원확인 및 다중 접근통제
- 통제구역내 담당자 동행
- 출입 내역 기록 및 감사
- 이상 행위/상황 알람
- 내/외부 전자파 도감청 차단

5.1.2. 물리적 접근

인증시스템은 외부인의 침입이나 불법적 접근 등 물리적 위협으로부터 보호하기 위해 접근통제를 실시하고 강제적 침투로부터 보호하기의 외벽을 구축한다.

- Root CA 인증시스템은 격리된 방에 안에 구축하고 출입문과 통제로 보호
- Root CA 실에 출입하기 위해 사전 출입 신청으로 방문자를 식별
- Root CA 실 출입 전 출입내역을 기록하고 정기적으로 검토되고 인가된 방문자는 권한을 가진 담당자와 동행
- V2X PKI 보안인증센터 시설 이상 행위/상황 발생 시 관제/순찰 보안 요원이 통제를 적용

5.1.3. 전원 및 공조시설

Root CA 시스템은 정전 및 변압의 위험에 대비하여 무정전 전원 장치를 이용해 안정적인 전원을 공급하고 냉난방 공조 설비가 설치되어 있어 온도와 습도를 적정한 범위 내로 유지하여 전기적 이상으로부터 시스템을 보호한다.

5.1.4. 침수 대비

침수로부터 시스템을 보호하기 위해 바닥으로부터 최소 30cm 이상의 위치에 설치하고 누수가 발생하더라도 물이 배수되도록 Root CA실 바닥에 배수구와 배수관을 설치한다.

5.1.5. 화재 예방 및 보호

화재 예방을 위해 화염 또는 연기 발생 시 탐지하여 자동 분사 분말소화 장치와 휴대용 소화기를 설치한다.

5.1.6. 매체 저장

Root CA 내 모든 자산을 목록으로 관리하고 주요 저장/기록 매체와 인증서 및 백업 데이터들은 제한된 장소의 금고에 보관하여 손실, 파손으로부터 보호한다.

5.1.7. 폐기물 처리

Root CA 인증업무에서 발생하는 기밀/개인정보가 포함된 모든 형태의 데이터는 외부로 공개를 금지하며, 해당 데이터(폐기물)가 복구될 수 없는 폐기 절차를 마련한다. 물리적 미디어는 완전 파괴하고 전자적 데이터는 해당 미디어에서 적합한 방법으로 폐기처리 한다.

5.1.8. 원격지 백업

시스템 장애 및 재해로부터 복구되기 위해서 정기적인 백업과 원격지 백업을 한다.

주 인증센터 금고에는 복사본과 재해로부터 보호될 수 있도록 10km 이상 떨어진 원격지 DR센터에 백업본을 보관을 한다. 아래는 백업해야 할 대상과 방법이다.

- '5.4.3 감사로그 보관 기간'에 의해 Root CA의 키와 시스템에서 발급한 인증서, 인증서 폐지목록, HSM 감사로그를 효력이 종료된 날부터 10년간 금고와 원격지 DR센터에 각각 보관하고 그 내용을 기록한다.
- 필수 인증업무 정보와 소프트웨어의 백업과 사본은 변경이 발생하면 금고와 원격지 DR센터에 각각 보관하고 그 내용을 기록한다.
- 개별 시스템 정보의 백업과 사본은 정기적으로 금고와 원격지 DR센터에 각각 보관하고 그 내용을 기록한다.

5.2. 절차적 보호조치

5.2.1. 신뢰된 역할

인증서 발급 및 관리하거나 HSM 접근 및 사용 권한을 보유하고 시스템을 운영하는 담당자는 주요업무 담당자로서 신뢰 역할을 수행하려는 자의 업무를 아래와 같이 정의하여 수행한다.

Root CA는 인증업무의 안전성과 신뢰성을 확보하기 위하여 각 역할별 직무를 분리한다.

1) 인증업무총괄책임자

- 인증서의 생성, 철회, 정지에 대한 승인

2) 인증업무관리자

- 인증업무준칙 (CPS) 승인과 최상위 인증기관(Root CA) 전반적인 책임

3) 보안감사자

- 인증기관 시스템 및 인증서비스에 대한 보안 관리
- 연간 재해복구 훈련 및 키 검증 테스트 수행

4) 내부감사자

- 인증서 발급과 시스템 감사로그에 대한 정기적인 내부감사 수행

5) 인증정책관리자

- 인증업무준칙 (CPS) 초안 작성 , 검토
- 재해복구계획 및 관련된 테스트 시나리오 작성, 검토

6) 키업무관리자

- 인증기관 키 생성 보관 운반 마이그레이션 파기 수행 절차 및 세부규정 준수
- 암호화 모듈 장비(HSM) 키 관리

7) 인증시설담당자

- 인증센터 시설, 시스템 운영 및 유지보수

8) 웹사이트관리자

- 인증기관 (Root CA) 웹사이트 운영과 인증업무준칙(CPS)의 웹사이트 게시 및

관리

- 웹사이트를 저장소(Repository)로 콘텐츠 게시 및 관리

5.2.2. 주요 업무별 수행 인력

키 생성은 3인 이상 공동으로 키생성을 한다. 그 외에 인증 업무는 2인이 공동으로 인증 받아 출입하고 2인이 수행한다.

5.2.3. 업무 담당자 신원 확인 및 인증

V2X PKI 보안인증센터의 모든 업무 담당자는 사전에 모두 신원을 확인하고 역할을 부여한다. 담당자들은 신원카드와 지문을 등록하고 절차에 따라 접근 권한과 일시를 신청한다. 신원확인카드 및 지문인식을 통하여 V2X PKI Root CA 보안인증센터 출입을 통제하고 Root CA실 접근 시 다자 인증 및 MFA로 통제된다.

5.2.4. 직무 분리 필요한 역할

민감한 영역에 대한 접근, 키 생성, 키 활성화 등 동일한 개인이 수행할 수 없으며, 아래와 같은 업무는 직무 분리되어 2명이상 수행해야 한다.

- 인증서 생성, 관리, 폐지
- 인증기관 키 생성, 관리, 파기

5.3. 인적 보안

5.3.1. 자격 요건

V2X PKI 보안인증센터의 운영 및 관리 자격은 인증업무 경력 등 자격 요건을 갖추어야 하며 연간 인증 업무와 보안 교육을 이수해야 한다.

5.3.2. 신원 확인

V2X PKI 보안인증센터의 업무 담당자는 직무 기능 및 서비스에 필요한 지식, 경험 및 적절한 자

격을 갖추어야 하며, 인터뷰 및 평가로 업무 수행 능력 및 경험을 확인 받아야 한다.

- 직무 책임 수행에 필수적인 배경 증명, 자격, 경력 증명 확인
- 신원 확인서 제출
- 보안 경력 및 보안교육 수준 확인
- 신뢰받는 지위를 보유하는 직원에 대한 신원 정기적 심사

5.3.3. 교육 및 훈련

인증업무를 담당하는 모든 직원은 업무수행에 필요한 인증업무 규정, 정책 및 인증업무 관리 교육을 이수한다. 교육 프로그램을 정기적으로 시행하고 평가하여 능력을 강화한다.

- 기본 PKI 개념과 업무 플로우
- 기본 IT 지식
- 직무 범위와 책임
- 보안 및 운영 정책과 절차
- 사용 중인 하드웨어 및 소프트웨어 버전 정보
- 위반 처리/보고
- 재난 복구 및 사업 계속 절차

5.3.4. 재교육 및 훈련

인증업무 수행 직원이 직무 책임 숙련도를 유지하기위해 연 1회 이상 업무수행에 필요한 인증업무, 규정/정책 및 인증업무 교육을 이수하고 개인의 수준을 고려하여 범위와 훈련 내용을 업데이트 한다.

5.3.5. 직무 이동 및 순환

5.2.4 직무 분리 필요한 역할'에서 직무의 변화가 시스템의 보안에 영향을 미치지 않는 범위 내에서 변경한다.

5.3.6. 비인가 행위 처벌

비인가된 행위로 인하여 시스템 또는 인증업무에 심각한 결과가 발생했을 경우 역할 할당 및 해당 권한을 철회하고 인사규정 또는 법 규정 등에 따라 해당 직원을 징계한다.

5.3.7. 독립 계약자 요건

독립적 계약 당사자는 신뢰 역할 담당자와 동일한 기능과 보안기준을 갖는 것으로 간주한다. 그러므로 자격요건, 신원확인, 교육, 역할, 비인가 행위, 보안관리, 처벌 등의 인적 보안 통제를 모두 동일하게 적용 받고 Root CA실 출입은 신뢰 역할 담당자와 동반하거나 감독하에 접근할 수 있다.

- 독립적 계약 당사자 : 아우토크립트 소속이 아닌 인증기관에서 인증업무 관련을 수행하기 위해 업무를 수탁 받은 제3자

5.3.8. 직원의 문서 공개

V2X PKI 보안인증센터는 주요 인증업무에 대한 내부문서 및 교육 자료는 역할과 권한에 따라 해당 직원들에게 제공한다.

5.4. 감사 기록

모든 입력 기록은 다음 사항을 포함한다

- 입력 날짜와 시간
- 입력 일련(serial/sequence) 번호 (자동 분개)
- 입력의 종류
- 입력 출처 (예: 터미널, 포트, 장소, 가입자 등)
- 입력을 하는 기관의 신원

5.4.1. 감사로그의 유형

V2X PKI 보안인증센터 운영과 인증업무에서 발생하는 키관리, 인증서 발급/폐지 등 아래 목록을 관리한다.

[기록 목록]

- 물리적 시설 접근 기록
- 인증 업무 담당자 권한 부여 기록
- Root CA 시스템과 Application 접근 기록
- Root CA 키 생명주기 관련 기록
- Root CA 인증서와 하위 기관 인증서 생명주기 관련 기록
- HSM 관리 기록

[기록 제한 목록]

- Root CA의 개인키와 개인키를 유추할 수 있는 모든 형태
- 그 외 개인과 기관의 불이익이나 피해를 줄 수 있다고 판단되는 정보

5.4.2. 감사로그 검토 주기

감사로그는 신뢰 역할 담당자인 내부 감사자가 정기적으로 감사로그의 전체 항목을 검토한다.

- 무결성 검토
- 비인가 활동 및 이상 행위
- 경고 로그와 불규칙성이 보이는 로그

5.4.3. 감사로그 보관 기간

인증 시스템의 감사로그는 발생일로부터 10년동안 보관한다.

5.4.4. 감사로그의 보호

인증 시스템의 감사로그는 내부 감사자가 총괄 관리하고 각 업무관리자는 감사기록을 조회만 할 수 있다. 내부 감사자라 할지라도 감사기록을 수정, 삭제할 수 없으며 무결성을 유지하도록 관리해야 한다.

5.4.5. 감사로그의 백업 절차

Root CA 시스템은 인증서를 생성/폐기/폐기목록생성 등 인증 업무를 수행할 때 외에는 시스템을 끄게 되며 Root CA 시스템 전원이 켜지고 인증업무를 수행할 때마다 생성된 감사로그를 백업한다. 그 외에도 인증업무를 수행하면서 파생되는 '5.4.1 감사로그의 유형'에 명시된 로그를 아래와 같은 절차에 따라 백업한다.

- 인증서 생성관리자는 Root CA 시스템에서 인증서 생성/폐기/폐기목록생성 업무 수행
- 내부 감사자는 업무가 종료되면 감사로그를 백업하고 시스템 내에 복사본을 보관
- 시스템 운영자는 인증시스템과 그와 관련된 시스템 전원 종료
- HSM 관리자는 백업한 감사로그를 4Layer에 보관
- 시스템 운영자는 감사로그 복사본을 DR센터에 동기화

5.4.6. 감사로그 취합 시스템

감사기록은 내부 시스템에서 생성되고 취합되며, 내부 감사자는 Root CA실에 출입하여 감사로그를 분석/검토하고 관리한다.

5.4.7. 감사로그 대상에 대한 통지

감사 로그가 발생한 시스템에서 경보 또는 비정상적인 이벤트가 확인되는 경우 담당 업무 관리자에게 지체없이 통보한다.

5.4.8. 취약점 측정

인증 업무에 포함된 시스템의 보안을 담당하는 내부감사자와 시스템운영자는 감사로그를 검토하고 설명해야 한다. 검토에는 변조, 손실, 불규칙성, 비정상적인 상태의 모든 로그를 검사하고 기록되어져야 한다. 취약성을 측정해야 하는 항목은 다음과 같다.

- 먼저 대상을 식별하고 대상 별 취약성 확인, 검토 후 대응 및 조치를 할 수

있는 프로세서를 문서화한다.

- 의심스러운 행위와 악성 코드로부터 인증 시스템을 보호하기 위해 조직과 기술적 관리적 통제를 구현한다.
- 취약점 점검은 1년에 한번 이상 수행하며, 구성요소와 네트워크, 설정이 변경되었다면 추가로 취약점 점검을 수행할 수 있다.

5.5. 기록 보존

5.5.1. 기록의 유형

'5.4.1 감사기록 대상' 포함 Root CA 인증업무의 상세한 기록은 모두 보관되어야 한다.

- 인증업무와 관련하여 생성된 감사 데이터
- 인증서 신청관련 정보와 문서
- 인증서 발급 및 관리 등 업무
- 인증서 폐기 관련 업무
- 인증에 필요한 관련 시스템의 운영 업무

5.5.2. 기록 보관 기간

모든 기록은 발생일로부터 10년 동안 보관하고 유지 관리되어야 한다.

5.5.3. 기록 보호

보존 기록들은 자신의 업무 범위 내의 보존기록만 조회 가능하며 위/변조 및 훼손 등을 방지하기 위하여 다음과 같이 보존기록을 보호한다.

- 전자문서는 안전하게 저장한 후 금고에 보관
- 일반문서는 금고 안쪽의 문서 박스에 보관

5.5.4. 기록의 백업 절차

인증업무를 마치거나 변경이 발생하면 아래 주기와 대상에 대해서 백업 하고, 백업한 파일은 10km 이상의 원격지 금고에 보관한다.

- 백업주기 : 변경이 발생한 경우(키 생성, 인증서 생성, 인증서 폐지, CRL 업데이트 등 Root CA 업무 수행 시)
- 백업대상 : Root CA의 개인 키, Root CA의 인증서, Root CA가 발급한 인증서, Root CA의 감사로그, CRL(인증서 폐지 목록), HSM 감사로그

5.5.5. 기록의 시점 보유 요건

Root CA의 시간 소스와 안전하게 동기화 되어야 하므로 Root CA를 작동시키기 전에 신뢰할 수 있는 통신사의 시간을 확인하고 30초 이상 차이가 있을 경우 수동으로 조정한다.

5.5.6. 기록 취합 시스템

보존기록은 시스템 내부에서 생성되고 취합된다.

5.5.7. 정보의 청구 절차

인증시스템 운영자 또는 내부감사자만 보존기록에 접근 가능하다. 기록 요청은 관리대장에 기록되어야 하며 담당자 서명을 득해야 한다. 기록이 청구되면 청구한 자가 수령하기 전 기록의 무결성을 검토해야 한다.

5.6. 전자서명인증사업자의 전자서명생성정보 갱신

Root CA는 현재 인증서의 사용 기간이 만료되기 전에 새 키 쌍에 대한 새 인증서를 생성해야 한다.

새 인증서의 유효기간은 현재 개인 키의 예정된 비활성화 전에 시작된다. Root CA는 새 인증서가 유효기간이 시작되기 전에 인증서 발급받은 기관과 신뢰 당사자에게 배포되도록 한다. 새 Root CA 인증서가 유효해지면 이전 Root CA 개인 키를 비활성화하고 인증서 발급에 사용하지 않는다.

다음과 같은 사유로 키는 변경될 수 있다.

- Root CA가 인증서 폐지를 신청한 경우
- Root CA가 사기나 위조, 기타 부정한 방법으로 키를 생성하거나 인증서 발급 사실을 인지한 경우
- Root CA의 개인키가 분실/훼손 또는 도난/유출된 사실을 인지한 경우
- Root CA 업무준칙의 주요 의무나 주요 사항을 준수하지 않아 중대한 피해가 발생한 경우
- 보안 체계의 보안 유지 및 향상을 위하여 필요한 경우

5.7. 장애 및 재난 복구

아우토크립트는 다음과 같은 하위 절에서 설명한 바와 같이, 치명적인 고장 발생 시 서비스 수준 계약에 따라 Root CA를 재구성하기 위한 복구 절차를 수립한다.

5.7.1. 정보시스템 재해 복구 절차

Root CA 운영기관은 시스템 자원 및 소프트웨어 등에 장애가 발생한 경우에 장애의 성격과 정도, 완화계획을 결정하기 위한 조사를 수행하고, 이중으로 설치한 시스템 자원 및 소프트웨어를 이용하여 복구한다.

관련성이 있는 경우, Root CA는 해당 이해관계자에게 자체 사고 관리 계획을 활성화할 수 있도록 경고해야 한다.

5.7.2. 정보시스템 자원 손상된 경우 절차

Root CA 운영기관은 인증서 등의 주요 데이터에 훼손·멸실이 발생하였을 경우에 기록 보존된 자료를 이용하여 복구한다.

5.7.3. 키 소실에 대한 복구 절차

아우토크립트 Root CA는 인증업무에 이용하고 있는 개인키가 손상, 분실, 파괴 또는 손상된 것으로 의심되는 경우 다음을 수행한다.

- 운영을 중단
- 위태로운 상황을 초래한 문제를 조사하고 인증서 폐지 실행
- 인증서를 발급받은 기관 및 모든 이해관계자에게 통보 및 경고

5.7.4. 업무 연속성 확보

아우토크립트 Root CA는 인증서 발급, 갱신, 폐지 등 인증관리 업무, 개인키 등 관리업무, 인증기관 심사 및 점검 업무와 전자서명 인증기술 등 핵심/주요 업무가 정보자산 및 설비자산 장애, 테러, 정전, 지진, 화재, 풍수해 등으로 업무가 중단되지 않도록 업무 연속성 계획을 수립한다.

업무 연속성 계획을 수립함으로써 인적·물적 자원의 피해가 발생한 시점에 가장 효율적인 업무 연속성 유지 방법을 제시하여, 인증시스템 운영기관의 운영업무와 전자서명인증 관리 핵심업무 중단기간을 최소화하고, 10km 이상 떨어진 DR센터를 통해 정상 업무로의 복원을 효과적으로 수행하여 인증시스템 운영기관의 정보자산 인프라의 회복력을 향상시키고, 업무중단으로 인한 운영상의 영향을 최소화한다.

5.8. 업무 휴지, 폐지, 종료

아우토크립트 Root CA는 최상위인증기관으로서 인증기관의 업무 종료는 V2X PKI PA와 관련 이해관계자와의 협의를 통하여 결정할 수 있다.

아우토크립트 Root CA 운영기관의 업무 양도 시, 가입자에게 계약 양도를 최소 90일전에 통지하여야 하며, 양도에 따른 계약을 별도로 진행하여야 한다. 업무를 양도받는 운영기관은 새로운 Root CA 추가와 동일한 절차로 심사를 받아야 하며, 기존 Root CA 업무의 관련 중요 데이터는 안전하게 이관 받아야 한다.

아우토크립트 Root CA 운영기관의 서비스 종료 시, 가입자에게 최소 180일 전에 통지해야 한다. Root CA 운영기관의 종료가 V2X 보안인증체계의 신뢰성을 보장할 수 없을 경우 서비스를 종료할 수 없다.

V2X 보안인증체계의 신뢰성을 보장할 수 없는 상태에서 Root CA 운영기관의 인증업무 또는 인증을 중단할 경우 이에 대한 민-형사상의 책임을 져야 한다.

6. 기술적 보호 조치

6.1. 전자서명생성정보 보호

6.1.1. 키쌍 생성 절차

아우토크립트 Root CA는 키쌍 생성 절차를 문서화하였으며, 다음 요건을 충족한다

- 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 통제 시스템이 갖추어 있는 안전한 공간에서 생성한다.
- 개인 키는 V2X 보안인증체계 기술규격을 만족하고, FIPS 140-2 레벨 3 표준에 따라 NIST가 인증한 하드웨어 보안 모듈(HSM) 내에서 생성 및 보호된다.
- 공개 키 및 관련 매개변수가 가입자 기관에 배포될 때 무결성과 신뢰성을 유지한다.
- 인가된 자만이 개인키를 생성할 수 있도록 하며, 개인키 생성 시 3명 이상의 다중 통제 아래 키 생성 절차서에 따라 수행한다.

6.1.2. 개인 키 전달 절차

아우토크립트 Root CA는 가입자 기관 개인키를 생성하거나 전달하지 않는다.

6.1.3. 공개 키 전달 절차

가입자 기관이 되고자 신청한 기관이 생성한 공개 키는 CAMP 및 IEEE 1609.2 지정 프로토콜을 사용하여 아우토크립트 Root CA로 안전하게 전달(또는 보안 이메일 전송)되어 개인 키의 소유권을 검증할 수 있도록 해야 한다.

가입자 기관의 공개키는 개인키를 이용한 전자서명을 포함하여 인증서 발급요청문(CSR) 형태로 아우토크립트 Root CA에 전달되어야 한다.

6.1.4. 관련자에게 공개 키 제공 절차

공개키를 포함한 인증서는 '2.2 공고방법'에 따라 제공된다.

인증업무와 관련한 홈페이지에 게시되는 항목은 다음과 같다.

– 발급된 (현재 유효한) Root CA 인증서

6.1.5. 키 길이

아우토크립트는 IEEE 1609.2 FIPS 186-4에 명시된 NIST P-256/SHA-256 및 원곡선 디지털 서명 알고리즘 ECDSA(Elliptic Curve Digital Signature Algorithm)를 지원하며, 「전자서명 알고리즘 규격」에서 명시된 서명 알고리즘을 사용한다. 비밀키의 길이는 256bit이다.

6.1.6. 공개 키 매개 변수 생성 및 품질 검사

공개키 매개변수는 미국 국립표준기술연구소(NIST : National Institute of Standards and Technology) FIPS 186-4 기술규격에 따라 생성 및 유효성을 검사한다.

6.1.7. 키 사용 용도

아우토크립트 Root CA의 개인키는 인증서 서명, 인증폐지목록 서명에 사용되며 해당키 사용 용도는 인증서 권한 필드에 명시되어 있다.

가입자 기관이 인증 업무를 제공함에 있어서 아우토크립트 Root CA로부터 인증을 받은 공개키에 합치하는 개인키를 사용하여야 한다.

6.2. 전자서명생성정보 보호조치

6.2.1. 암호화 모듈의 기준

인증기관은 개인키를 안전하게 저장하기 위하여 V2X 보안인증체계 기술규격 및 FIPS 140-2 레벨3을 만족하는 보안 모듈을 이용하여 개인키가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리하여야 한다.

6.2.2. 다중 통제

아우토크립트 Root CA의 개인키는 한 사람이 서명 프로세스를 호출하거나 암호화 모듈에 접근할 수 없으며, 2명 이상의 운영자에 의한 다중 통제 아래 생성되고 관리된다.

6.2.3. 개인 키 위탁

아우토크립트 Root CA는 가입자 기관의 개인키를 위탁하지 않는다.

6.2.4. 개인 키 백업

아우토크립트는 개인키의 훼손에 대비하여 다중통제(2인 이상)를 통해 개인키를 백업하고 금고에 저장하며 키 생성과 동일한 보안 모듈(FIPS 140-2 레벨 3 검증된 HSM)을 사용하여 암호화된 백업 키를 관리한다.

또한 개인키의 훼손에 대비하여 개인키를 백업하여 전자서명인증관리 원격지 DR센터에 보관한다.

보관된 개인키는 센터 내에서 사용되는 동일한 모듈을 사용하여 암호화된 백업키를 관리한다.

6.2.5. 개인 키 보관

Root CA의 개인키는 안전하게 보관하기 위하여 암호화된 개인키가 담긴 이동 저장 매체에 봉인하여 복사본은 보안인증센터 금고에 보관하고 백업본은 DR센터 금고에 보관한다.

6.2.6. 개인 키 추출

아우토크립트 Root CA는 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되는 안전한 키 생성시스템 또는 V2X 보안인증체계 기술규격을 만족하는 보안 모듈에서 개인키를 생성한다.

HSM 내부에 보관된 개인키를 다시 활성화하기 위해서는 다중통제 또는 암호 모듈 제조업체에서 지정한 기술을 통해 안전한 암호화 모듈을 사용한다.

6.2.7. 개인 키 저장

아우토크립트 Root CA는 내부 및 외부의 정보통신망과 연결되지 않고 물리적 침해 등으로부터 보호되는 안전한 키 생성시스템 또는 V2X 보안인증체계 기술규격을 만족하는 보안 모듈에서 개인키를 생성한다.

HSM 내부에 보관된 개인키를 다시 활성화하기 위해서는 다중통제 또는 암호 모듈 제조업체에서

지정한 기술을 통해 안전한 암호화 모듈을 사용한다.

6.2.8. 개인 키 활성화

암호화 모듈에 저장된 개인키는 활성화 토큰을 사용해 최소 2명 이상의 운영자에 의해 다중 통제되고 이용된다

6.2.9. 개인 키 비활성화

암호화 모듈에 저장된 개인키를 비 활성화 토큰을 사용하여 최소 2명 이상의 운영자에 의해 비활성화 할 수 있다.

6.2.10. 개인 키 삭제 및 파괴

인증서 또는 개인키 유효기간이 만료되거나 개인키가 훼손·유출되었을 경우에는 V2X PKI PA의 승인하에 해당 개인키 저장매체를 물리적으로 완전히 파기하거나, V2X 보안인증체계 기술규격에 따라 개인키를 삭제한다.

HSM에 저장된 Root CA 및 ICA 개인 키는 암호화 모듈에서 제공하는 방법을 사용하여 파괴되며 개인 키의 모든 백업도 마찬가지로 파괴한다.

6.2.11. 암호화 모듈 등급

6.2.1 암호화 모듈의 기준'에 명시된 암호화 모듈 등급을 준수한다. FIPS 140-2 레벨 3에 검증된 암호화 모듈을 사용한다.

개인키를 안전하게 저장하기 위하여 공인인증 기관의 시설 및 장비 등에 관한 규정의 기술규격 및 FIPS 140-2 레벨3을 만족하는 보안 모듈을 이용하여 개인키가 분실·훼손 또는 도난·유출되지 않도록 안전하게 관리한다.

6.3. 전자서명생성정보 및 전자서명검증정보의 관리

아우토크립트 Root CA가 발급한 인증서는 Root CA 또는 기관에서 소유하고 있는 개인키에 합치한다는 사실을 확인 및 증명하기 위하여 사용된다.

6.3.1. 공개 키 보관

5.4.3 감사로그 보관 기간'의 기준으로 인증서가 유효하지 않게 된 후 최소 10년 동안 기록 보존 절차에 따라 모든 인증기관 및 가입자 기관의 공개키(Public Keys) 사본을 보관한다.

아우토크립트 Root CA는 '5.5 기록 보존'에 따라 공개키(Public key)를 보관한다.

전자서명정보를 원격지에 보관한다.

6.3.2. 인증서 운영 기간 및 사용 기간

모든 인증서 및 해당 키는 IEEE 1609.2 사양에서 권장하는 유효성을 초과하지 않으며, 인증서의 이용범위 및 용도, 이용된 기술의 안전성과 신뢰성 등을 고려하여 인증서의 유효기간을 정한다.

가입자 기관 개인 키는 유효기간 만료 최소 30일 전에 인증서 재 키(Re-Keying) 및 배포를 해야 한다.

각 가입자 기관은 유효기간 만료전에 최상위 인증기관과 협의하여 새로운 인증서로 갱신하거나 기존 인증서의 유효기간을 연장할 수 있다.

- Root CA의 인증서 유효기간은 17년으로 한다.
- Root CA가 발급하는 가입자 기관의 인증서 유효기간은 다음과 같다.

PG	4년+1주
MA	4년+1주
CRLG	4년+1주
ICA	13년

5.4.3 감사로그 보관 기간'에 의해 아우토크립트는 Root CA가 발급한 인증서, 인증서 폐지목록 등을 물리적으로 격리된 원격지에 백업하여 당해 인증서의 효력이 소멸된 날부터 10년간 보관한다.

6.4. 데이터 보호 조치

6.4.1. 활성화 데이터 생성

활성화 데이터는 하드웨어 보안 모듈(HSM)의 기술사양에 따라 생성한다.

활성화 데이터는 PIN, 암호문과 키 분할 체계 등이 있으며, 이 하드웨어의 등급은 '6.2.11 암호화

모듈 등급'에 따른다.

6.4.2. 활성화 데이터 보호

활성화 데이터를 보호하기 위해 사용되는 절차는 데이터가 PIN번호와 접근 인증용 키에 의존한다. 접근 인증용 키는 지정된 관리자에 의해 유지되며 PIN번호는 아우토크립트 암호화 정책에 따라 암호화하여 저장된다.

6.4.3. 활성화 데이터 추가 고려사항

해당사항 없음

6.5. 시스템 보안 통제

관련 시스템에 대해 기술적 관리적 물리적 보안방안을 준수하며 보안점검 활동을 수행하여 안전하게 관리한다.

인증시스템(하드웨어, 운영 체제, 응용 프로그램 소프트웨어) 등 논리적 접근 시 접근 승인 결재 시스템을 통하거나 기안을 받아 절차를 거쳐 사전에 승인을 받아야 하며, 승인받은 신뢰된 역할자라 할지라도 접근 권한은 정기적인 주기로 검토되고 갱신한다.

6.5.1. 특정 컴퓨터 보안 요건

아우토크립트는 인증시스템의 운영체제, 서버, 하드웨어, 소프트웨어에 대한 보안체계를 수립하고 보안정책과 지침, 절차에 따라 인증시스템을 운영한다. 인증시스템 및 보조 시스템은 보안인증 또는 그에 준하는 승인된 하드웨어 및 소프트웨어를 사용한다. 특정 컴퓨터 보안 요건 세부사항은 다음과 같다.

- 인증된 로그인 기능
- 보안 감사 기능
- 인증 서비스에 대한 액세스 제어 제한
- 역할에 대한 의무의 분리를 시행
- 역할 및 관련 ID의 식별 및 인증 필요
- 데이터베이스 보안 및 외부 세션 통신에 암호화 사용
- Root CA 기록 및 감사 데이터

6.5.2. 컴퓨터 보안 등급

Root CA실을 출입하기 위해서 단계별 인증을 거쳐야 하며 Root CA실 입장 시 2명이 Multi Factor 인증을 수행해야한다. 시스템의 논리적 접근 시에도 Multi Factor 인증을 진행하며 시스템에 접근하는 매체는 Root CA실에서만 사용된다.

6.6. 시스템 운영 관리

6.6.1. 시스템 개발 통제

아우토크립트 인증관리시스템의 운영체제 설치, 기능 변경, 성능 개선, 장비 설치 시 인증센터 최고책임자의 승인하에 실시되며,

인증관리시스템 개발 통제 사항은 다음과 같다.

- 문서화된 개발 프로세스를 사용하여 제안된 환경에서 개발을 수행
- 하드웨어 및 소프트웨어는 구성요소 변조방지를 위해 초기화 상태로 설치
- 암호화 모듈은 설치 전에 초기화하여 설치
- 운영체제는 서버 설치 시 정품 O/S를 사용하여 설치
- 타사 구성 요소, 업데이트 및 관련 보안 패치는 진위 여부 검증 후 적용

6.6.2. 보안 관리 통제

시스템 구성 및 변경, V2X 소프트웨어 설치에 대한 보안관리 통제 절차는 문서화된 운영정책을 따른다.

아우토크립트는 인증관리시스템에 접근하는 모든 컴퓨터(서버)에 대하여 적절한 업무분장이 되어 있으며, 접근 권한을 최소화하여 운영한다.

아우토크립트 Root CA에 접근을 위해서는 인증센터, PA의 승인이 필요하며, 접근 인력의 업무변경 시 주기적으로 권한변경을 한다.

6.6.3. 생명 주기 보안 통제

아우토크립트는 인증시스템 소프트웨어, 특히 외부 네트워크에 노출된 모든 신뢰 요소의 잠재적인 취약점에 대해 주기적으로 점검하고 필요에 따라 보안 패치를 적용한다.

오프라인 인증시스템에 대한 취약성 평가는 매년 수행하며, 분기별 패치 계획을 수립하여 정기적으로 수행한다.

6.7. 네트워크 보호조치

아우토크립트 Root CA는 오프라인으로 운영되며, 필요시 네트워크 보안을 위하여 침입탐지시스템 및 침입차단시스템을 사용한다.

6.8. 시점확인서비스 보호조치

아우토크립트 Root CA의 시간은 신뢰할 수 있는 통신사 네트워크를 참조하여 시스템 시간을 수동으로 조정한다.

7. 인증서 형식

7.1. 인증서 형식

아우토크립트 Root CA가 발급하는 인증서의 프로파일은 IEEE 1609.2 인증서의 규격 및 V2X 보안

인증체계 기술 규격을 준수한다.

Root CA 인증서에는 발급과 CRL 발급 권한이 포함된다.

Root CA 인증서는 서명할 수 있는 인증서, 메시지 또는 데이터 유형에 대한 권한을 표시해야 한다.

7.1.1. 인증서 버전

아우토크립트 Root CA는 IEEE 1609.2 V3 인증서를 발급한다. (버전 필드 값은 숫자 3으로 지정)

7.1.2. 인증서 확장

아우토크립트 Root CA에서 발급되는 인증서는 Root CA 인증서 프로파일에 명시된 인증서 확장 필드를 사용한다.

7.1.3. 알고리즘 개체 식별자

인증서 알고리즘 개체 식별자(OID : Object Identifier)는 Root CA 인증서 프로파일에 명시된 체계를 준수한다.

7.1.4. 이름 양식

발급자 DN과 주체 DN은 Root CA 인증서 프로파일에 명시된 체계를 준수한다.

7.1.5. 이름 제한

해당사항 없음

7.1.6. 인증서 정책 개체 식별자

인증서 정책 개체 식별자는 Root CA 인증서 프로파일 체계를 준수한다.

7.1.7. 정책 제한 확장의 사용

인증서 정책 개체 식별자는 Root CA 인증서 프로파일 체계를 준수한다.

7.1.8. 정책 한정자 구문 및 의미

해당사항 없음

7.1.9. 주요 인증서 정책 확장에 대한 의미 처리

인증서 정책 개체 식별자는 Root CA 인증서 프로파일 체계를 준수한다.

7.2. 인증서 유효성 확인 정보 형식

인증서 소유자의 조직정보가 변경되거나 개인키의 신뢰가 손상되었을 때 인증서를 폐지할 필요가 있다.

IEEE 1609.2 및 V2X 보안인증체계 기술 규격을 준수하는 인증서 폐지 목록(CRL)을 발급한다.

7.2.1. 버전

아우토크립트 Root CA는 IEEE 1609.2 V3를 발급한다.

7.2.2. 확장 필드

인증서 폐지목록의 확장필드는 V2X PKI 인증서 프로파일 체계를 준수한다.

7.3. 인증서 유효성 확인 서비스 형식

아우토크립트 Root CA는 인증서 폐지 목록을 센터 홈페이지에 게시한다.

7.3.1. 버전

해당사항 없음

7.3.2. 실시간 인증서 상태 검증 필드

해당사항 없음

8. 감사 및 평가

8.1. 감사 및 평가 현황

인증관리센터 업무를 수행함에 있어서 효율적인 보안 관리를 위하여 정기적으로 감사 또는 평가를 실시한다.

감사는 최대 1년을 넘지 않는다.

- 운영 개시 후 매년
- 심각한 보안 위반 또는 중대한 감사 문제로 인해 운영이 중단된 후 PA의 지시가 있을 경우

8.2. 평가자의 신원, 자격

매년 1회 이상 웹트러스트 감사 또는 이에 준하는 감사를 수행한다

감사기관은 다음과 같은 자격을 갖추어야 한다.

- 피감사대상자로부터 독립적인 자
- 국내·외 법·제도 및 관련 기술표준에 대한 충분한 지식이 있는 자
- PKI 기술, 정보통신기술 및 정보시스템 감사관련 전문가
- 관련 국제 자격 WebTrust, ETSI 또는 그에 준하는 자격이 있는 자

8.3. 평가 대상과 평가자의 관계

감사자(감사기관)는 피감사 대상자와 금전적으로나 사업적으로 이해관계가 없는 대외 감사기관을 선정해야 한다.

8.4. 평가 목적 및 내용

감사 범위는 아우토크립트 Root CA의 CPS 준수여부, 인증기관 키 관리, 인증서 관리 및 최상위 인증기관(Root CA) 시스템 관리를 포함한다.

감사 범위에 대한 세부 사항은 인증정책에 명시한다.

본 인증업무준칙을 참조하는 CA 라이선스에 따라 PCA를 운영하는 고객은 자체적으로 년 1회 감사를 받아야 하며, 부정행위와 이를 해결하기 위해 취한 조치를 PA에 보고해야 한다.

8.5. 부적합 사항에 대한 조치

감사에서 본 문서에 기술된 서비스와 관련하여 해당 법률, 본 CPS 또는 계약상 의무를 준수하지 않는다고 보고한 경우, Root CA 등 인증체계를 법적으로 안전하게 할 의무가 있는 관련와 제3자의 승인에 따라 그러한 비 준수 내용을 시정하기 위한 계획을 개발하여야 한다.

감사를 통해 발견된 미비점과 특이점은 보고서에 포함되며, 감사결과에 따라 정책적, 기술적으로 조치를 취하게 되며, 범위는 영향도 등에 따라 결정한다. 조치는 시정계획에 따라 합리적인 기간 내에 실행되며 적절한 조치를 취하지 못한 경우 수정조치를 취하거나 정책을 완화할 때까지 인증서를 취소하고, CA를 일시 중지하도록 지시할 수 있다.

8.6. 결과 보고

모든 평가결과는 PA에 보고한다. 필요에 따라 일부 평가결과는 이해관계자들에게 제공될 수 있다.

그 외의 모든 감사 정보는 9.3에 따라 기밀 사업 정보로 간주된다.

9. 전자서명인증업무 보증 등 기타사항

9.1. 수수료

9.1.1. 인증서 발급 및 갱신 요금

인증서 발급 및 인증서 서비스에 대한 모든 수수료는 아우토크립트 Root CA와 인증서비스 계약

자 간의 업무 협약(계약)을 따른다.

9.1.2. 인증서 접근 요금

인증서를 열람·확인하는 신뢰당사자에게 수수료를 부과하지 않는다.

9.1.3. 인증서폐지목록 정보 확인 요금

인증서 효력정지 및 폐지목록에 접근하는 신뢰 당사자에게 수수료를 부과하지 않는다

9.1.4. 기타 서비스 요금

필요할 경우 기타 서비스에 대한 수수료는 부과할 수 있다.

9.1.5. 환불 정책

인증서 발급 신청 철회 등에 따른 환불은 인증서 발급 수수료를 부과한 경우에 한해 환불한다.

9.2. 배상

아우토크립트 Root CA는 관련 법, 시행령, 시행규칙 또는 Root CA의 인증업무준칙의 각 규정에서 정한 사항 이외에 사유로 인한 손해 또는 전쟁, 천재지변 등 불가항력적인 사유로 인한 인증업무의 처리지연 또는 처리 불능으로 인한 손해에 대하여는 책임을 지지 않는다.

아우토크립트 Root CA와 인증서비스 계약자간의 재정적 책임은 업무 협약(계약)을 따른다.

9.2.1. 보험 적용 범위

해당사항 없음

9.2.2. 기타 자산

해당사항 없음

9.2.3. 보험 또는 보증 범위

해당사항 없음

9.3. 영업비밀

9.3.1. 기밀 정보의 범위

아우토크립트 Root CA는 비즈니스 정보와 보안에 민감한 내부 정보를 회사 기밀로 분류하고 사내 보안정책을 준수하여 기밀정보를 보호한다.

공공 또는 허가되지 않은 직원에게 기밀정보가 노출되는 것을 방지하기 위해 정보의 민감도와 관련한 보안 통제를 실시한다.

상황에 따라 일부 정보는 비밀유지계약(NDA, Non-Disclosure Agreement)에서 계약자와 공유될 수 있으며, 기밀정보 범위는 다음과 같다.

- 모든 비즈니스 연속성 사고 대응, 비상 사태 및 재해 복구 계획
- 정보의 기밀성, 무결성 또는 가용성을 보호하는 데 사용되는 기타 보안 관행, 조치, 메커니즘, 계획 또는 절차
- 아우토크립트에서 보유한 모든 정보는 9.4항에 따라 개인정보로 유지
- 5.4항 또는 5.5항에 확인된 모든 거래, 감사 기록 및 아카이브 저장 기록
- 인증서 신청서를 지원하기 위해 제출된 인증서 신청서 및 문서
- 거래, 재무 감사, 외부 또는 내부 감사 추적 기록 및 자세한 감사 보고서

9.3.2. 기밀 정보의 범위를 벗어난 정보

가입자 기관에 발급한 인증서, 인증서 폐지 등 상태 정보, 최상위인증기관의 업무와 관련하여 공고하는 정보는 기밀정보로 간주하지 않으며, 외부 감사자의 감사보고서 요약 서신(e-Mail) 또한 기밀로 간주되지 않는다.

인증업무의 안전성 및 신뢰성에 영향이 없는 정보에 대해서는 공개한다.

9.3.3. 기밀 정보 보호의 책임

아우토크립트 Root CA와 인증업무 협약(계약)을 체결한 모든 사용자(기관, 단체, 조직)는 아우토크립트 개인정보보호정책(9.4절 참조)이 기밀로 간주하는 개인 데이터의 보호에 관한 규정을 준수하며 기밀을 유지할 의무와 책임이 있다.

9.4. 개인정보 보호

아우토크립트 Root CA는 인증업무 수행과 관련한 개인정보의 보호를 위해 개인정보보호 관련 법 및 규정에 따라 안전하게 관리한다.

9.4.1. 개인정보보호 계획

아우토크립트 Root CA는 인증업무 수행과 관련한 개인정보의 보호를 위해 개인정보보호 관련 법률 및 규정을 준수하며 홈페이지에 게시된 개인정보처리방침에 따라 개인정보를 수집·보유·처리한다.

9.4.2. 개인정보로 간주되는 정보

인증서 신청인 연락처 정보, 비즈니스 용어, 고객 인증서 볼륨 및 최종 사용자 가명인증서 링크는 비공개가 필요한 개인정보로 간주된다.

9.4.3. 개인정보로 간주되지 않는 정보

인증서, CRL 및 해당 정보에 표시되는 개인 또는 회사 정보는 비공개를 해야하는 개인정보로 간주되지 않는다.

9.4.4. 개인정보보호 의무

V2X PKI 보안인증센터 및 기관은 적절한 보호 조치를 사용하여 개인 정보의 무단 공개를 방지하기 위해 합리적인 예방 조치를 취해야 한다. 개인정보보호에 관한 법률 및 규정을 준수한다.

9.4.5. 개인정보 사용에 대한 통지 및 동의

아우토크립트 Root CA 는 개인정보 주체의 명시적 서면 동의 또는 해당 법률 또는 법원 명령에 따라 개인정보를 사용할 수 있으며, 개인정보 수집 및 이용 그리고 제3자 제공에 대한 고지와 동의를 득한 후 개인정보를 사용한다.

9.4.6. 사법 또는 행정 절차에 따른 공개

아우토크립트 Root CA는 법률에 의해 개인정보 또는 기밀정보 공개를 요구하는 경우를 제외하고, 승인된 당사자의 합리적이고 구체적인 요청이 없이는 기밀정보를 공개하지 않는다.

- 정보를 기밀로 유지해야 할 의무가 있는 당사자
- 당사자가 이러한 정보를 요청하는 경우
- 유효하고 집행 가능하고 논쟁의 여지가 없는 법원 명령이 있는 경우

9.4.7. 기타 정보 공개 기준

아우토크립트 모든 직원은 개인 데이터 보호와 기밀정보 보호와 관련된 대한민국의 관련 법률의 요구사항을 포함하여 모든 정보를 엄격하게 준수한다.

9.5. 지식재산권

인증서 발급 및 개인키와 관련한 지적재산권은 저작권법 및 기타 관련 법률에 따라 아우토크립트 Root CA에 귀속된다.

아우토크립트 Root CA는 자사의 상표를 보호하고 타사(타인)의 상표를 존중하며, 웹사이트 또는 다른 서비스(포탈, 언론매체, 소셜미디어 등)에서 다른 회사 상표를 홍보하기 전에 상표 소유자의 허가를 사전에 구한다.

가입자 기관에 발급한 인증서는 아우토크립트 Root CA의 독점 재산이며, 아우토크립트 Root CA는 비즈니스 계약에 따라 인증서를 복제하고 배포할 수 있는 권한을 가입자 기관에 부여한다.

아우토크립트 Root CA는 언제든지 단독 재량에 따라 발급한 인증서를 해지할 권리가 있다.

- 아우토크립트 Root CA가 개발한 소프트웨어 및 하드웨어
- 아우토크립트 Root CA의 인증업무준칙
- 아우토크립트 Root CA의 명칭
- 아우토크립트 Root CA가 생성한 전자서명성생정보 등

9.6. 보증

9.6.1. 인증기관 보증

아우토크립트 Root CA는 인증서와 관련하여 다음의 내용을 보증한다.

- 발급된 인증서에 포함된 내용이 틀림없다는 사실
- 관련법의 규정에 의하여 인증서가 발급되었다는 사실
- 인증서 폐지에 대한 내용이 틀림없다는 사실

9.6.2. 등록기관 보증

해당사항 없음

9.6.3. 사용자 보증

해당사항 없음

9.6.4. 신뢰 당사자 보증

해당사항 없음

9.6.5. 기타 참가자 보증

해당사항 없음

9.7. 보증 예외 사항

본 인증서 정책에서 진술 및 보증하거나 해당 업무 협약(계약)에 명시된 경우를 제외하고, 아우토크립트 Root CA는 명시적이거나 묵시적인 모든 보증을 부인한다.

9.8. 보험의 보상 범위

아우토크립트 Root CA는 인증 업무와 관련하여 관련 법, 동법 시행령 및 시행규칙 또는 인증업무준칙의 각 규정에서 정한 사항 이외에 사유로 인한 손해 또는 전쟁, 천재지변 등 불가항력적인 사유로 인한 인증 업무의 처리지연 또는 처리 불능으로 인한 손해에 대하여는 책임을 지지 않는다.

9.9. 배상 한계

아우토크립트 Root CA는 인증 업무와 관련하여 동법, 동법 시행령 및 시행규칙 또는 인증업무준칙의 각 규정에서 정한 사항 이외에 사유로 인한 손해 또는 전쟁, 천재지변 등 불가항력적인 사유로 인한 인증업무의 처리지연 또는 처리 불능으로 인한 손해에 대하여는 책임을 지지 않는다.

9.10. 준칙의 효력

9.10.1. 유효 기간

발급된 인증서 정책과 인증서 유효기간은 아우토크립트 Root CA 인증정책을 따르며 그 내용은 아우토크립트 홈페이지에 게시된 후 효력이 발생한다.

9.10.2. 종료

본 문서의 개정 내용은 저장소에 게시된 후 발효되며, 새로운 버전으로 대체가 되거나 종료될 때까지 계속 유효한다. 본 CPS를 갱신하는 과정과 계약자에게 영향을 미칠 수 있는 변경사항은 '1.5.4 인증업무준칙 승인 절차'에 설명한 대로 이해관계자에게 전달된다.

9.10.3. 종료 후 효력

인증서 해지 및 존속에 관한 사항은 업무 협약(계약)을 따른다.

V2X PKI 인증업무준칙이 개정되는 경우에도 중요정보에 대한 책임은 유효하다.

9.11. 통지 및 의사소통

알림 또는 문의를 위한 연락처는 다음과 같다.

- 업무담당 : AutoCrypt V2X PKI Root CA 보안인증센터
- 전화번호 : (02) 2125-4020
- 조직주소 : 서울특별시 영등포구 여의공원로 115 세우빌딩 6층
- 메일주소 : rootca@autocrypt.io

9.12. 이력 관리

9.12.1. 개정 절차

1.5.4 인증업무준칙 승인 절차'의 인증 수행 절차 및 승인 프로세스 참고

9.12.2. 개정 공지

1.5.4 인증업무준칙 승인 절차'의 인증 수행 절차 및 승인 프로세스 참고

인증업무준칙(CPS)의 변경이 발생한 경우 V2X PKI 보안인증센터 홈페이지에 게시한다.

9.12.3. 인증체계식별명의 변경사항

인증서 정책 OID는 IEEE 1609.2 인증서에 적용되지 않는다.

9.13. 분쟁 해결

인증업무와 관련하여 분쟁이 발생한 경우, 관계법령과 계약에 따라 해결한다.

9.14. 관할법원

본 인증업무준칙은 대한민국의 관계 법령에 따라서 해석되고 적용되며 상충될 경우 상위법을 따

른다.

인증 업무와 관련한 법적 사항은 업무 협약(계약)에 명시한다.

9.15. 관련 법률 준수

아우토크립트 Root CA는 인증, 인증서의 발급・관리 및 폐지 등 인증 서비스를 제공하는 관련된 모든 해당 법률 및 규정을 준수하는 것을 목표로 한다.

9.16. 기타 규정

기타 규정은 적용 가능한 업무 협약(계약)에서 확인할 수 있다.

9.16.1. 완전 합의

해당사항 없음

9.16.2. 양도

해당사항 없음

9.16.3. 분리 조항

해당사항 없음

9.16.4. 집행 (변호사 비용 및 권리 포기)

해당사항 없음

9.16.5. 불가항력

전쟁, 테러, 자연재해, 인터넷 또는 기타 인프라 장애 등 본 인증업무준칙의 당사자의 합리적 통제를 벗어난 사건으로 인한 준칙 미이행 사항은 불가항력으로 판단한다.

9.17. 기타 조항

계약 범위, 계약의 완전성, 계약 집행 및 불가항력과 같은 기타 조항은 해당 업무 협약(계약)의 적용을 받는다.