AutoCrypt V2X PKI Root CA

Certificate Practices Statement

(Root CA CPS)

V1.1

2022.09.08

<Enactment / Amendment History>

버전	Category	Name	Date
V1.0	Enacted	Myunghyun Kim	2022/06/29
V1.1	Corrected typos and foreign language notation ▪ 1.5.4. Certification Practices Statement Approval Procedure(Added clause 1.5.4.) ▪ 2.3. Announcement Cycle (Amended the validity period of the CRL) ▪ 5.4.2. Audit Log Review Cycle (Amended Audit Log Review Cycle) ▪ 5.5.4. Backup Procedure of Records (Amended Backup Cycle)	Myunghyun Kim	2022/09/08

Table of Contents

1. Overview

AutoCrypt's V2X security certification system is a public key-based certification system that provides management such as issuing and revoking certificates to vehicles, roadside equipment, and V2X certification system organizations in a safe autonomous cooperative driving environment.

This Certification Practices Statement describes AutoCrypt V2X security certification system as Root CA (top-level certification authority), and it establishes technical, legal, and business requirements for managing certificate issuance, distribution, and revocation so that sub-authorities can perform certification tasks.

Root CA follows the SCMS (Security Credential Management System) architecture of CAMP (The Crash Avoidance Metrics Partnership LLC.) and the technical standard of IEEE 1609.2. V2X certificate uses IEEE 1609.2 certificate format.

1.1. Introduction

This document is based on RFC 3647 for certification and integrity of vehicle-to-vehicle (V2V) and vehicle-to-roadside infrastructure (V2I) messages with public key infrastructure (PKI) processed using V2X communication networks, and it deals with Certification Practices Statement regarding the V2X security certification system-related tasks such as the CA's certificate policy, certificate issuance/management, security control, and other operational policies/procedures operated by AutoCrypt, and the responsibilities and duties of the certification authority.

1.2. Document Title and Identification

This document is called 「AutoCrypt V2X PKI Root CA Certification Practice Statement」.

1.3. Those Related to the Electronic Signature Certification System

1.3.1. Certification Authority

The certification authority refers to AutoCrypt V2X PKI Root CA (hereinafter referred to as V2X PKI). It is responsible for certificate management, including registration, identification, certification and issuance, and for all aspects of certificate authority service and certificate authority operation related to certificates issued under the V2X Security Certification System to be performed in accordance with the requirements, statements and warranties.

The CA is an independent environment with security requirements consistent with the CAMP SCMS architecture and IEEE 1609.2 profile specifications. AutoCrypt operates a top-level certification authority (Root CA), and its tasks are as follows.

- Establishment and operation of a secure Root CA system
- Conduct certification tasks according to the manager's approval
  - Issuance/Revocation of certificate of Root CA
  - Issuance/Revocation of certificates from sub-authorities
- Inspection and safety operation support of subordinate certification authorities

1.3.2. Registration Authority

AutoCrypt is responsible for managing certificates of subordinate authorities, and it is handled directly by the certification authority without having a separate registration authority entrusted or acting on behalf of the subordinate authorities.

1.3.3. Subscriber

The sub-authority applying for the certificate becomes the subscriber, and it is one of the certified V2X security certification system members that satisfy the IEEE 1609.2 technical standard and SCMS architecture and conclude a separate contract.

- Intermediate Certificate Authority: An authority that exists below the Root CA among trusted authorities of the V2X security certification system and issues certificates to other components.
- Misbehavior Authority: An authority that identifies a terminal with a misbehavior through the report of misbehavior transmitted from the terminal and revokes the certificate.
- Policy Generator: An authority that creates and manages policy files and chain certificates to distribute policies according to the request of the Root CA.
- Certificate Revocation List Generator: An authority that manages the Certificate Revocation List (CRL) of the V2X security certification system.

1.3.4. Relying Party

The relying party trusts the issued Root CA certificate and depends on the validity of the end-entity certificate issued by the certification authority to verify the reliability of the V2X security message, so the subscriber of the certification authority is the relying party.

1.4. Type of Certificate

1.4.1. Purpose of Certificate

The certificate issued in accordance with Certification Practices Statement checks the digital signature fact and validity for V2X communication, manages the life cycle of the certificate according to the CAMP SCMS

architecture and IEEE 1609.2 specifications, and is not used for any other purpose.

1.4.2. Restriction on the Use of Certificate

The Root CA certificate issued by the Root CA and the V2X certificate issued to the subscriber authority should be used only within the scope of use or purpose at the time of issuance. The certificate cannot be used outside the scope or purpose of use.

1.5. Management of Certification Practice Statement

1.5.1. Authorities Establishing and Revising Certification Practice Statement

AutoCrypt's V2X PKI Root CA Policy Authority (PA) manages the preparation and operation of Certification Practices Statement. The roles of the PA are as follows:

- Approval of current and future versions of Certification Practice Statement
- Approval management, including definition, determination and publication of the certification authority approval process
- Approving the certification authority's compliance with the CPS and its operation in accordance with the published Trusted Service Principles.
- Approval management of the certification authority's certification tasks and operating procedure guidelines

1.5.2. Contact Information

The contact information related to Certification Practices Statement is as follows:

- Department: AutoCrypt V2X PKI Root CA Security Certification Center
- Phone Number: +82-2-2125-4020
- Address: (07241) 6F Sewoo Building, 115 Yeouigongwon-ro, Yeongdeungpo-gu, Seoul, South Korea
- E-mail: rootca@autocrypt.io

1.5.3. Responsibilities for Certification Practice Statement

The V2X PKI PA approves the conformity, revision, and procedure of Certification Practice Statement.

- The V2X PKI CA Certification Practices Statement is reviewed by the V2X PKI PA at least once a year and the operational status is reviewed and discussed with stakeholders and sub-authorities.
- A review of at least two weeks is allowed for major changes affecting stakeholders and

sub-authorities, and the revised changes are reflected in Certification Practice Statement.

- Even if the amended matters do not have an impact on stakeholders and sub-authorities, Certification Practices Statement is revised and reflected.

- The established and revised Certification Practices Statement shall be implemented from the date of report.

1.5.4. Certification Practices Statement Approval Procedure

The V2X PKI PA may notify stakeholders or sub-authorities of the proposed changes for review and feedback, depending on the impact of the suggestions and changes.

The V2X PKI PA announces the revised Certification Practices Statement on the Center's website and notifies stakeholders or sub-authorities individually, and stakeholders indicate their agreement or express their will under regulations.

1.6. Definitions and Abbreviations

1.6.1. Definitions

CA	Certification Authority. The authority responsible for all aspects of the issuance and management of certificates, ensuring that all aspects of CA services, operations and infrastructure related to certificates are carried out in accordance with stated policies and practices
CRL	Certificate Revocation List. Trusted certificate revocation list that can determine whether the certificate currently in use is expired/normal
CRLG	Certificate Revocation List Generator. Element that manages the certificate revocation list (CRL) of the V2X security certification system
CSR	Certificate Signing Request. A kind of application for issuing a certificate by sending the asymmetric key information of the system that will use the certification service to receive a certificate and sending it to the certificate authority
ICA	Intermediate Certification Authority. Among the trusted authorities of the V2X security certification system, the authority that exists below the Root CA and issues certificates to other components.
MA	Misbehavior Authority. An authority that identifies abnormal terminals and revokes certificates through the abnormal behavior report sent from the terminal
PCA	Pseudonym Certification Authority. An organization that issues and manages anonymity, identification, and application certificates for devices
PG	Policy Generator. Create and manage GPF and GCCF for policy distribution according to SCMS Manager's request
Root CA	Root Certification Authority. As the top-level authority in the trust relationship of the V2X security certification system, it is an element that allows all certificates and signatures of subordinate relationships to be trusted.
SCMS	Security Credential Management System. A system that constitutes PKI-based authorities, devices, and systems used by the V2X security certification system in the United States
V2X Security Certification System	A system for providing certification services such as issuance of V2X certificates and management of certification-related records to provide secure V2X communication services

Private Key	A key used in secret and undisclosed among key pairs owned by a target, in an asymmetric password algorithm.
Public Key	A key that is disclosed among key pairs owned by one target in an asymmetric password algorithm
Expired	The maximum period that can be certificated by the higher authority of the certificate has expired
Authority	Independent organizations (institutes, associations) that perform their respective roles, including policy management, certificate issuance, and detection of abnormal behavior
Authority Certificate	A certificate used by the authorities configured to operate the V2X security certification system for secure communication through mutually encrypted data and certification
Period of Use	The period of use of the certificate, which is used by each authority of the V2X security certification system according to the nature of its role, is less than or equal to the validity period.
Trust Factor	Root CA, ICA, CRLG, PG, MA systems and related infrastructure that depend on secure issuance and management of certificates
Applicant	A legal entity or its authorized representative applying for certificate services to a CA to become a subscriber
Validity Period	Maximum time period during which certificates used for certification can be certificated
Abnormal Behavior	Malfunctions and harmful behaviors of terminals within the certification management system that may threaten the certification management system or the traffic system
Certification Authority	A authority that certifies trustworthy online subordinate authority responsible for issuing and managing public keys for security eligibility and message encryption
Certificate	A record that uses a digital signature to associate an identity with a public key. A form that complies with「V2X Certificate Profile」
Certificate Renewal	Extending the validity period of the certificate
Certificate Re-issuance	The act of reissuing the certificate due to loss/leakage, etc.
Storage	Defines the storage location of certification authority information. This information may include certificates, certificate revocation lists, certificate policies, or certificate user guides.
Top-level Certificate	Certificate of the highest authority located at the top of the trust relationship of the V2X security certification system
A Pair of Keys	An asymmetric key uses separate keys for encryption and decryption, and is called a public key and a private key in turn, which is called a pair of keys.
Disposal	The condition in which an authority is permanently disbanded or temporarily disbanded because it is no longer able to fulfill its role
Revocation	If the administrator or certification authority complies with the rules for revocation, it suspends the validity of the certificate from its subordinate authorities and terminals
Subordinate Authority	An authority that belongs to a higher level authority among independent authorities that perform each role and plays an intermediate communication role with the terminal

1.6.2. Abbreviations

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 Certification 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 Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
V2X PKI	AutoCrypt V2X PKI Root CA

2. Announcement of Information Related to Digital Signature Certification Service

2.1. Announcement Facility

AutoCrypt operates a publicly available repository and publishes V2X PKI Certification Practices Statement and related certificates.

2.2. Method of Public Announcement

The contents included in the storage and the location of the announcement are as follows.

- V2X PKI Certification Practice Statement
  - Root CA certificate and issued subordinate authority certificate
- CRL storage location for obtaining Certificate Discard List (CRL) information
  - https://autocrypt.io/services/v2x-pki-ca
- Certificate Application Form
- Certification Task Information

2.3. Announcement Cycle

The revised Certification Practices Statement will be posted on the center website within 10 days from the date of report after approval by the PA. Renewed Root CA certificates are issued 5 days before the effective date and published immediately so that certificates can be propagated before use of the certificate. The validity period of the CRL is up to 90 days and shall be posted within 1 day if the revocation occurs.

2.4. Responsibility for Published Information

AutoCrypt publishes information related to Certification Practices Statement and certificate issuance and management on the homepage so that anyone can check the fact, and the section communicating with the homepage implements HTTPS secure communication.

Root CA operates in a safe and restricted place, and must implement access control comparable to the highest level. Except for the system operator, access to the Root CA should be restricted, and operations such as addition, modification, and deletion of those with access permissions should be controlled. In addition, it implements and protects controls from access to system access in relation to all PKI participants and key administrators.

3. Identification

3.1. How To Display Subscriber Name

3.1.1. Name Type

The id field of the V2X certificate issued by the Root CA includes the following contents according to the IEEE 1609.2 certificate profile standard.

- Connection Value
- Host Name
- Binary Identifier

3.1.2. Meaning of Name

Use an externally accessible fully qualified domain name (FQDN) that conforms to the naming conventions of CAMP and IEEE 1609.2.

In the case of a certificate issued by the V2X certification system Root CA, the DN name complies with the cn=certification system host identifier + certification system name, c=io system, and is identified as the following hosts:

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

3.1.3. Issuing an Anonymous Certificate That Cannot Identify the Applicant

Root CA does not issue anonymous certificates.

3.1.4. Certificate DN Rules

Refer to '3.1.2 Meaning of name' for various name form interpretation rules.

3.1.5. Uniqueness of Certificate DN value

The certificate issued by the Root CA is given a host name (hostName) to have a unique value.

3.1.6. Use of Trademarks

Root CA does not issue certificates that may infringe other people's trademarks or cause trademark disputes.

3.2. Identification When Issuing a New Certificate

The Root CA is used only to verify the identity of the certificate applicant, and may reject the certificate request at the request of the certificate applicant for any reason.

3.2.1. How To Prove Ownership of a Private Key

The Root CA certificate applicant directly visits AutoCrypt Root CA and submits the certificate request form and confirms that he/she has the private key corresponding to the public key written in the CSR file.

3.2.2. Initial Identification of Certificates for Authority

Authority certification confirms that the authority is certified through the submitted authority designation, business registration certificate, and a certified copy of corporate registration, and for the national authority or

a local government, it should be confirmed that it is an accredited authority through the corresponding document.

- Confirm the identity of the certificate applicant and the permission to apply
- Identify of the existence of the authority
- Verify the location, address, legal registration information and business status of the authority
- Confirm ownership of the certificate domain to be issued
- Identify the devices and who owns and controls them to be included in the certificate to be issued

3.2.3. Initial Identification of a Personal Certificate

Root CA verifies the identity of an individual or agent of an organization applying for a certificate as follows:

- Verification of personal name, title, company name, email address, and contact information
- Verification of documents that can confirm that the individual is an employee of the authority to which he/she belongs
- Verification of written or approved mail that the individual has the authority to represent the application of the applicant authority

3.2.4. Issuance of Unidentified Certificates

An application whose identity of the applicant is not verified will not be issued a certificate.

3.2.5. Enforcement of Permission

All subscribers define a representative or contact person responsible for requests for issuing, renewing and abolishing certificates. AutoCrypt Root CA checks the identity of the V2X certificate applicant face-to-face.

- The applicant is identified by documents confirming that he/she is an employee of the subscriber authority, and whether the applicant has the authority to apply for the application of the applicant authority
- As a subscriber who receives and uses AutoCrypt's certificate, the applicant organization must have a prior contract, and verify it with documents such as a contract that can be verified.

3.2.6. Inter-Operational Criteria

Root CA unilaterally certifies certification authority and subscriber bodies as top-level certification authorities because they apply mutatis mutandis to communication mechanisms in the IEEE 1609.2 technical specifications.

3.3. Identity Verification When Updating, Reissuing and Changing Certificates

3.3.1. Identification and Verification for Repeated Reissuance

Certificate reissuance is possible only when the applicant's existing certificate is valid. Therefore, if reissuance of the certificate is required, it must be requested before the expiration of the validity period. Identification and certification methods for key regeneration follow the same procedure for issuing new certificates and verifying identity as described in '3.2.2 Initial Identification of Certificates for Authority'.

If the applicant's existing registration information is changed when applying for reissuance of the certificate, the applicant, registration agent, or authority may request evidence of the changed information.

3.3.2. Identification and Verification of Reissuance After Revocation

When an authority applies for reissuance of a certificate, it is revoked regardless of whether the validity period expires or not, and identity is verified through a procedure similar to the application for a new issuance in the same way as loss/damage or theft/leakage of a certificate.

3.4. Identification for Certificate Suspension, Restoration of Validity, Abolition

The issued certificate can be revoked with the approval of the Root CA after being received by the person in charge of AutoCrypt Security Certification Center. The revocation request shall include the circumstances of the revocation and how long the certificate to be revoked will remain unrevoked.

Certificate revocation request must be made in writing signed by an authorized applicant, and verification of identity and permission is verified by referring to '3.2.5 Enforcement of Permission'.

PA confirms the following with respect to the applicant's decision to revoke.

- Certificate revocation decision confirmation
- Contents of stakeholder agreement and reasons for revocation

4. Certificate Management

4.1. Application for Certificate Issuance

The Root CA processes the certificate issuance request of the subordinate authority according to the PA's approval. Information related to certificate issuance and management is posted so that anyone can always check the fact according to the V2X security certification system.

4.1.1. Criteria for Applying for a Certificate

The Root CA certificate complies with the technical specifications of the V2X security certification system according to the contract, and PG, MA, ICA, and CRLG organizations that are licensed and certified can apply for the certificate.

4.1.2. Certificate Application Process and Responsibilities

The authority applying for the certificate contacts the V2X PKI Security Certification Center, receives the application form by e-mail, fills out the necessary information, and applies to the Root CA.

When applying for issuance of a certificate to the Root CA, the applicant must directly submit the public key of the subscriber authority in the form of a Certificate Signing Request (CSR).

The Root CA does not generate or store the private key of the applicant or authority.

4.2. Processing of Certificate Issuance Application

4.2.1. Identification and Certification

The Root CA shall verify and certify the identity and authority of each applicant as documented in the applicable Certification Practice Statement. After face-to-face with the certificate applicant or application agent, refer to '3. Identification' and approve or reject the certificate application according to the certificate application and approval procedure.

4.2.2. Approval and Rejection of Applications

Root CA shall check the certification application and PA approval of the authority that wants to receive the certificate, review the correct format suitable for 1609.2 and SCMS requirements, and the verified certificate specification, and process it if there are no problems.

In any of the following cases, the Root CA refuses to issue a certificate:

- Contains inaccurate information
- Writes unclear content
- False entry of <V2X Security Certificate Application> in the identification process
- Judged that the applicant or authority is not qualified as a representative
- Judged that there is a problem with certification work or technical difficulties

4.2.3. Application Processing Time

When the Root CA receives an application, it informs the applicant of factors that may affect the issuance time. After receiving a valid application for a certificate, issue it within 5 business days and comply with the issuance

period.

4.3. Certificate Issuance Procedures and Protective Measures

4.3.1. Certificate Issuance Procedure

Before issuing a new certificate, the Root CA checks the source of the certificate application in the manner described in Certification Practices Statement and issues it through the following certificate issuance application procedure.

- Confirm the uniqueness of the public key submitted by the certificate applicant
- Check whether the public key submitted by the certificate applicant matches the private key owned by the certificate applicant (checking the proof of ownership of the private key)
- Evaluate the ID uniqueness of the request information submitted by the certificate applicant and the required certificate request information fields
- Provide a certificate to the applicant in accordance with the flow and protocol specified in CAMP SCMS

4.3.2. Certificate Issuance Notification

The issuance notice of the certificate application authority certificate is delivered by e-mail, and if it is difficult to receive an e-mail, the relevant authority is notified through the mail and the contact information of the applicant.

4.4. Receipt of Certificate

4.4.1. Certificate Receiving Procedure

Download the certificate posted on the V2X PKI Security Certification Center website storage. The representative or agent of the applicant authority submits to the center whether or not to accept the issued certificate after receiving the certificate.

A Certificate is considered approved unless the Subscriber installs the certificate or reports a certificate issue and requests revocation within 5 business days of notification of the certificate. Applicants or authorities must revoke all certificates that are not properly verified and send a new request after notifying the Root CA.

4.4.2. Publishing Certificate

Issued authority certificates are published in the repository identified in 2.1.

4.4.3. Certificate Issuance Notice

If a new certificate of Root CA is issued, post the issued Root CA certificate on the V2X Security Certification

Center website so that the trust party can know about it, and notify the relevant authority separately by email or contact information if necessary.

4.5. Using Certificates

4.5.1. Private Key Usage Purpose

The authority receiving the certificate must use the private key that matches the public key received from the Root CA. The authority receiving the certificate should create and store the private key in a secure way, and use hardware security module (HSM) that satisfies the technical specifications of the regulations on facilities and equipment, etc. to safely manage the private key so that it is not lost, damaged, stolen, or leaked.

The private key and certificate are used only for performing V2X certification tasks such as digital signature and encrypted communication.

4.5.2. Public Key Usage Purpose

After being familiar with the use and verification methods of certificates in compliance with the SCMS standard and IEEE 1609.2 standard, the authority that received the certificate should check the certificate revocation list, certificate information and storage and validity, and the validity period of the certificate from the V2X PKI Security Certification Center website. The public key and certificate are used only for performing V2X certification tasks such as digital signature and encrypted communication.

4.6. Certificate Renewal

In the Root CA certificate issuance policy of the V2X security certification system, the renewal issuance is replaced by a new issuance without renewing the certificate provided by the subscriber.

4.6.1. Certificate Renewal Criteria

Not applicable

4.6.2. Certificate Renewal Applicant

Not applicable

4.6.3. Certificate Renewal Procedure

Not applicable

4.6.4. Certificate Renewal Notification

Not applicable

4.6.5. Certificate Renewal Approval

Not applicable

4.6.6. Publishing Certificate Renewal

Not applicable

4.6.7. Certificate Renewal Announcement

Not applicable

4.7. Certificate Re-Issuance

In the case of certificate reissuance, in accordance with AutoCrypt Root CA certificate issuance policy, the reissuance task follows the same procedure as the new issuance process.

4.7.1. Criteria for Certificate Reissuance

In the case of certificate reissuance, in accordance with AutoCrypt Root CA certificate issuance policy, the reissuance task follows the same procedure as the new issuance process.

4.7.2. Applicant for Certificate Reissuance

In the case of certificate reissuance, in accordance with AutoCrypt Root CA certificate issuance policy, the reissuance task follows the same procedure as the new issuance process.

4.7.3. Certificate Reissuance Procedure

In the case of certificate reissuance, in accordance with AutoCrypt Root CA certificate issuance policy, the reissuance task follows the same procedure as the new issuance process.

4.7.4. Certificate Reissuance Notification

In the case of certificate reissuance, in accordance with AutoCrypt Root CA certificate issuance policy, the reissuance task follows the same procedure as the new issuance process.

4.7.5. Approval of Certificate Reissuance

In the case of certificate reissuance, in accordance with AutoCrypt Root CA certificate issuance policy, the reissuance task follows the same procedure as the new issuance process.

4.7.6. Publish Certificate Reissuance

In the case of certificate reissuance, in accordance with AutoCrypt Root CA certificate issuance policy, the reissuance task follows the same procedure as the new issuance process.

4.7.7. Certificate Reissuance Notice

In the case of certificate reissuance, in accordance with AutoCrypt Root CA certificate issuance policy, the reissuance task follows the same procedure as the new issuance process.

4.8. Change the Certificate

4.8.1. Certificate Change Criteria

In the event of a certificate change, the existing certificate is abolished and processed in the same manner as the method and procedure for issuing a new certificate.

4.8.2. Certificate Change Applicant

In the event of a certificate change, the existing certificate is abolished and processed in the same manner as the method and procedure for issuing a new certificate.

4.8.3. Procedure for Changing Certificates

In the event of a certificate change, the existing certificate is abolished and processed in the same manner as the method and procedure for issuing a new certificate.

4.8.4. Certificate Issuance Notification

In the event of a certificate change, the existing certificate is abolished and processed in the same manner as the method and procedure for issuing a new certificate.

4.8.5. Certificate Change Approval Procedure

In the event of a certificate change, the existing certificate is abolished and processed in the same manner as the method and procedure for issuing a new certificate.

4.8.6. Publishing Certificate Changes

In the event of a certificate change, the existing certificate is abolished and processed in the same manner as the method and procedure for issuing a new certificate.

4.8.7. Notice of Issuance of Changed Certificates

In the event of a certificate change, the existing certificate is abolished and processed in the same manner as the method and procedure for issuing a new certificate.

4.9. Suspension, Reinstatement and Revocation of Certificate

Root CA can revoke its own certificate by replacing the key or certificate to protect the integrity due to key corruption, leakage, or early termination of use of the certificate, or revoke the certificate of an issued subordinate authority.

4.9.1. Criteria for Certificate Revocation

The Root CA revokes the issued authority certificate when the following reasons occur or the integrity of the Root CA is questioned according to the V2X security certification system technical standard.

- If the authority has applied for revocation of the certificate
- When the authority recognizes that the certificate was issued by mistake, intentional, or other fraudulent means
- When the dissolution of the authority is recognized
- When it is recognized that the private key of the authority has been lost/damaged or stolen/leaked
- If an authority does not comply with its main obligations or key points in the statements
- When necessary to maintain and improve the security of the security system
- When the parent certificate is revoked

4.9.2. Applicant for Certificate Revocation

An identified certificate revocation applicant or representative of an authority may request revocation of a certificate from the Root CA at the authority's own request by submitting an authorized certificate revocation request detailing the reasons for the revocation.

4.9.3. Certificate Revocation Procedure

In the V2X PKI Security Certification Center, the certificate revocation application is processed as follows.

- Verification of authority and identity of certificate revocation applicant
- Check the integrity of the certificate revocation application
- The revocation date of the certificate revocation application. Validation of reasons for revocation, etc.
- After reviewing the certificate revocation application, order revocation to the Root CA
- Publish certificate revocation results

4.9.4. Grace Period for Requesting Certificate Revocation

If the reason for revocation of the certificate of the Root CA or the applying authority and the security risk are confirmed, request the revocation to the V2X PKI Security Certification Center without delay and revocation is processed within 24 hours after application. If the grace period does not impair the integrity or security of the Root CA, a grace period of up to 30 business days is provided.

4.9.5. Processing Time for Certificate Revocation Requests

The V2X PKI Security Certification Center must request revocation to the Root CA without delay when the cause of the authority's certificate revocation occurs, and it is processed within a maximum of 3 days. If there is an impact on security accidents and integrity, revocation is processed within 24 hours after application for revocation.

4.9.6. Requirements for Certificate Revocation Verification

The relying party must use software that can properly process the trust path certification scheme specified in the IEEE 1609.2 standard or check the certificate revocation list (CRL) and certification path on the V2X Security Certification Center website.

4.9.7. Frequency of Certificate Revocation List Issued

Follow the abolished certification renewal and announcement in ‘2.3 Announcement Cycle’.

4.9.8. Maximum Time Required To Issue a Certificate Revocation List

Root CA must issue a CRL without delay after revocation processing, and must notify within 1 business day after revocation.

4.9.9. Real-Time Certificate Revocation and Status Validation

Root CA does not support online certificate status check service.

4.9.10. Requirements for Real-Time Certificate Revocation Verification

Root CA does not support online certificate status check service.

4.9.11. Alternative Methods of Validating Certificate Revocation Information

Not applicable

4.9.12. Special Requirements for Key Replacement or Key Damage

If the authority that has issued the certificate recognizes that its private key is not secure, such as lost/damaged or stolen/leaked, it must notify the V2X PKI Security Certification Center without delay to take measures to secure safety and reliability, and request for immediate revocation of damaged certificates.

4.9.13. Criteria for Certificate Suspension

Not applicable

4.9.14. Subject to Certificate Suspension

Not applicable

4.9.15. Certificate Suspension Procedure

Not applicable

4.9.16. Certificate Suspension Period

Not applicable

4.10. Certificate Validation Service

4.10.1. Functional Features of Certificate Status Service

The CRL issued by the Root CA is distributed to the relying party using the method described in the IEEE 1609.2 standard, or a revocation list is issued and published in a secure and trusted repository.

4.10.2. Certificate Status Service Availability

The V2X PKI Security Certification Center publishes the fact that the certificate revocation list has been updated so that anyone can check it at any time.

4.10.3. Certificate Status Service Optional Features

Not applicable

4.11. Withdrawal of Service Subscription

'4.11 Withdrawal of Service Subscription' is regarded as cessation of certificate certification service and the certificate revocation procedure of '4.9 Certificate Suspension/Revocation/Revocation', which is the certificate revocation procedure, applies mutatis mutandis.

4.12. Other Supplementary Services

Not applicable

4.12.1. Enforce Key Consignment and Recovery Policies

Not applicable

4.12.2. Session Key Encapsulation, Recovery Policies and Procedures

Not applicable

5. Facility and Operations Management

Root CA certification system is designed to meet functions and capacities such as power, electronic devices, devices, and control, and security, organization, and management system are established to meet availability and continuity to maintain certification services, and is regularly analyzed and evaluated.

5.1. Physical Protection Measures

The certification system protects the place where the certification system is installed from physical threats such as intrusion or illegal access by outsiders.

5.1.1. Location and Facilities

The Root CA certification system of the V2X PKI Security Certification Center is physically separated from other systems and installed in a separate control area, and is operated in a safe offline manner with thorough physical access control.

The facility is designed for multi-level protection and includes the following systems.

- Control of facilities and system rooms
- Identification and multiple access control
- Accompanying the person in charge in the controlled area
- Access history records and audits
- Abnormal behavior/situation alarm
- Block internal/external electromagnetic wave eavesdropping

5.1.2. Physical Access

The certification system implements access control to protect against physical threats such as intrusion or illegal access by outsiders, and builds an outer wall to protect against compulsory intrusion.

- The Root CA certification system is built in an isolated room and protected by access doors and controls.
- Identifies visitors by applying for access in advance to access the Root CA room
- Before entering the Root CA room, the entry and exit details are recorded, and visitors who are regularly reviewed and authorized are accompanied by a person with authority.
- In the event of an abnormal behavior/situation in the V2X PKI security certification center, control/patrol security personnel apply control

5.1.3. Power and Air Conditioning Facilities

The Root CA system supplies stable power by using an uninterruptible power supply in preparation for the risk of power failure and voltage change, and is equipped with air conditioning and heating facilities to maintain temperature and humidity within an appropriate range to protect the system from electrical abnormalities.

5.1.4. Preparation for Flooding

To protect the system from flooding, install at least 30cm from the floor and install a drain hole and drain pipe on the floor of the Root CA room so that water can be drained even if a leak occurs.

5.1.5. Fire Prevention and Protection

To prevent fire, detect the occurrence of flames or smoke and install an automatic spray powder extinguishing device and a portable fire extinguisher.

5.1.6. Media Storage

All assets in the Root CA are managed in a list, and major storage/recording media, certificates, and backup data are stored in a safe in a limited place to protect them from loss and damage.

5.1.7. Waste Disposal

All types of data including confidential/personal information generated in the Root CA certification business are prohibited from being disclosed to the outside, and a disposal procedure in which the data (waste) cannot be recovered shall be prepared. The physical media is completely destroyed, and the electronic data is disposed of in an appropriate way on the media.

5.1.8. Remote Backup

In order to recover from system failures and disasters, regular and remote backups are performed.

In the vault of the main certification center, a copy and a backup copy are stored at a remote DR center more than 10km away to be protected from disasters. Below are the destinations and methods to back up.

- According to '5.4.3 Audit Log Retention Period', the key of the Root CA, the certificate issued by the system, the certificate revocation list, and the HSM audit log are stored in the safe and remote DR center for 10 years from the date of expiration, respectively, and the contents are recorded.
- Backups and copies of essential certification information and software are stored in safes and remote DR centers, respectively, and the contents are recorded when changes occur.
- Backups and copies of individual system information are regularly stored in safes and remote DR centers, respectively, and the contents are recorded.

5.2. Procedural Protection Measures

5.2.1. Trusted Role

The person in charge of issuing and managing the certificate or who has the HSM access and use authority and operates the system defines and performs the duties of the person who wants to perform the role of trust as the person in charge of the main task as follows.

The Root CA separates the duties of each role in order to secure the safety and reliability of the certification work.

1) General Manager of Certification

- Approving the generation, withdrawal, or suspension of a certificate

2) Certification Task Manager

- Approval of Certification Practices Statement (CPS) and overall responsibility of the top

certification authority (Root CA)

3) Security Auditor

- Security management of the certification authority system and certification service
- Conduct annual disaster recovery training and key validation testing

4) Internal Auditor

- Regular internal audit of certificate issuance and system audit log

5) Authentication Policy Manager

- Draft Certificate Policy (CP) and Certification Practices Statement (CPS) and Review
- Create and review disaster recovery plans and related test scenarios

6) Key Business Manager

- Compliance with procedures and detailed regulations for generating, storing, transporting, migrating, and destroying the certification authority key
- Manage Hardware Security Module (HSM) key

7) Certification Facility Manager

- Operate and maintain certification center facilities and systems

8) Website Manager

- Certification authority (Root CA) website operation and website posting and management of certificate policy (CP) and Certification Practices Statement (CPS)
- Publishing and managing content on the website as a repository

5.2.2. Personnel Performing Each Major Task

Key generation is performed jointly by 3 or more people. In addition, the certification work is jointly certified by two people and is performed by two people.

5.2.3. Identification and Authentication of Business Personnel

All personnel in charge of V2X PKI Security Certification Center check their identities in advance and assign roles. Persons in charge register identity cards and fingerprints, and apply for access rights and date and time according to the procedure. Access to the V2X PKI Root CA security certification center is controlled through identification card and fingerprint recognition, and access to the Root CA room is controlled by multi-party certification and MFA.

5.2.4. Roles Required for Job Separation

Access to sensitive areas, key generation, key activation, etc. cannot be performed by the same individual, and the following tasks must be performed by two or more people separated from their duties.

- Generate, manage, and revoke certificates
- Generate, manage, and destroy certificate authority keys

5.3. Human Security

5.3.1. Qualifications

For the operation and management qualification of the V2X PKI Security Certification Center, qualifications such as experience in certification work must be met, and annual certification work and security training must be completed.

5.3.2. Identification

The person in charge of the V2X PKI Security Certification Center must have the knowledge, experience, and appropriate qualifications necessary for job functions and services, and must have his/her job performance and experience confirmed by interview and evaluation.

- Identify background, qualifications, and career credentials required to perform job responsibilities
- Submit identification
- Check security experience and security training level
- Regularly screening of identities for employees who hold positions of trust

5.3.3. Education and Training

All employees in charge of certification work must complete certification business regulations, policies, and certification business management training necessary for the performance of their duties. Implement and evaluate training programs on a regular basis to strengthen competence.

- Basic PKI concepts and workflows
- Basic IT knowledge
- Scope of duties and responsibilities
- Security and operations policies and procedures
- Information on hardware and software version being used
- Handling/Reporting violations
- Disaster recovery and business continuity procedures

5.3.4. Re-Education and Training

In order to maintain the mastery of job responsibilities, certification service employees must complete certification work, regulations/policy, and certification work training required for work performance at least once a year, and update the scope and training contents in consideration of the individual's level.

5.3.5. Job Shift and Rotation

In '5.2.4 Role Required for Job Separation', changes are made to the extent that job changes do not affect the security of the system.

5.3.6. Punishment for Unauthorized Conduct

In the event of serious consequences to the system or certification work due to unauthorized actions, the role assignment and relevant authority shall be revoked, and the relevant employee will be disciplined according to the personnel regulations or legal regulations.

5.3.7. Independent Contractor Requirements

Independent contracting parties are considered to have the same functions and security standards as those in the trust role. Therefore, all human security controls such as qualification requirements, identification, education, roles, unauthorized actions, security management, and punishment are applied equally, and access to the Root CA room can be accessed with or under the supervision of a trusted role manager.

- Independent Contracting Party: A third party entrusted with the work to perform certification work in a certification body that is not affiliated with AutoCrypt

5.3.8. Disclosure of Documents to Employees

The V2X PKI Security Certification Center provides internal documents and training materials for key certification tasks to the employees according to their roles and authority.

5.4. Audit Records

All input records include the followings.

- Input date and time
- Input serial/sequence number (automatic journal entry)
- Type of input
- Input source (e.g. terminal, port, location, subscriber, etc.)
- The identity of the authority making the input

5.4.1. Type of Audit Log

The following list is managed, such as key management and certificate issuance/discontinuance occurring in the operation of the V2X PKI Security Certification Center and certification work.

[List of records]

- Physical facility access records
- Authorization record for certification operations personnel
- Root CA system and application access record
- Root CA key lifecycle related records
- Records related to the life cycle of Root CA certificates and subordinate authority certificates
- HSM management records

[List of record restrictions]

- Root CA's private key and any form that can infer the private key
- Information that is judged to cause disadvantage or damage to other individuals and authorities

5.4.2. Audit Log Review Cycle

In the audit log, the internal auditor, who is in charge of the trust role, reviews all items regularly in the audit log.

- Integrity review
- Unauthorized activities and abnormal behavior
- Warning log and log showing irregularities

5.4.3. Retention Period of Audit Log

The audit log of the certification system is kept for 10 years from the date of occurrence.

5.4.4. Protection of Audit Logs

The audit log of the certification system is managed in general by the internal auditor, and each business manager can only inquire the audit record. Even internal auditors cannot modify or delete audit records and must manage them to maintain integrity.

5.4.5. Backup Procedure for Audit Logs

The Root CA system turns off the system except when performing certification tasks such as certificate generation/revocation/revocation list creation, and backs up the generated audit log whenever the Root CA system is powered on and performs certification tasks. In addition, back up the logs specified in '5.4.1 Types of Audit Logs', which are derived while performing certification tasks, according to the procedure below.

- The certificate generating manager performs the certificate generation / revocation / revocation list generation task in the Root CA system.
- The internal auditor backs up the audit log when the work is over and keeps a copy in the system.
- The system operator shuts down the certification system and related system power.
- HSM administrator keeps backed up audit logs in 4 Layers
- The system operator synchronizes the audit log copy to the DR center.

5.4.6. Audit Log Collection System

Audit records are created and collected in the internal system, and the internal auditor enters the Root CA room to analyze/review and manage audit logs.

5.4.7. Notification of Audit Log Target

If an alarm or abnormal event is identified in the system where the audit log is generated, the manager in charge is notified without delay.

5.4.8. Vulnerability Measurement

Internal auditors and system operators in charge of the security of the system involved in the certification task should review and explain the audit log. The review shall examine and record all logs of tampering, loss, irregularity, and abnormal conditions. Items to measure vulnerability are as follows.

- Identify the target and document the process for identifying, reviewing, and responding to vulnerabilities by target.
- Implement organizational and technical and administrative controls to protect certification systems from suspicious behavior and malicious code.
- Perform a vulnerability checks at least once a year, and additional vulnerability checks can be performed if components, networks, and settings have been changed.

5.5. Record Keeping

5.5.1. Type of Record

All detailed records of Root CA certification work including '5.4.1 Audit Record Subject' should be kept.

- Audit data generated in relation to certification work
- Information and documents related to certificate application
- Work such as certificate issuance and management
- Work related to certificate revocation
- Operational work of related systems required for certification

5.5.2. Record Retention Period

All records must be kept and maintained for a period of 10 years from the date of occurrence.

5.5.3. Record Protection

Only archived records within the scope of one's work can be viewed, and the archived records are protected as follows to prevent forgery/falsification and damage.

- Save electronic documents safely and store them in a safe
- Store general documents in a document box inside the safe

5.5.4. Backup Procedure of Records

When certification is completed or changes occur, back up the following cycles and targets, and store the backed-up files in a safe at a remote location more than 10km away.

- Backup cycle: When changes occur (when performing Root CA tasks such as key generation, certificate generation, certificate revocation, CRL update, etc.)

- Backup subject: Root CA's private key, Root CA's certificate, Root CA issued certificate, Root CA's audit log, CRL (certificate revocation list), HSM audit log

5.5.5. Point of Record Retention Requirements

Since it must be securely synchronized with the time source of the Root CA, check the time of a trusted carrier before operating the Root CA, and adjust manually if there is a difference of more than 30 seconds.

5.5.6. Record Collection System

Retention records are generated and collected inside the system.

5.5.7. Information Claim Process

Only the certification system operator or internal auditor has access to the archived records. Record requests must be recorded in the management ledger and must be signed by the person in charge. When records are claimed, the integrity of the records must be reviewed prior to receipt by the claimant.

5.6. Renewal of Digital Signature Creation Information of Digital Signature Certification Service Providers

The Root CA must generate a new certificate for the new key pair before the current certificate's validity period expires.

The validity period of the new certificate begins before the scheduled deactivation of the current private key. The Root CA ensures that new certificates are distributed to the issuing authorities and relying parties before their validity period begins. When the new Root CA certificate becomes valid, the old Root CA private key is deactivated and is not used for certificate issuance.

The key may be changed for the following reasons.

- When the Root CA applied for certificate revocation

- When the Root CA is aware of the fact that the key is generated or issued by fraud, forgery, or other illegal means

- When it is recognized that the private key of the Root CA has been lost/damaged or stolen/leaked

- In case significant damage occurs due to non-compliance with the main obligations or main matters of the Root CA practice statements

- When necessary to maintain and improve the security of the security system

5.7. Recovery of Errors and Disasters

As described in the following subsection, AutoCrypt establishes a recovery procedure to reconfigure the Root CA according to the service level agreement in the event of a catastrophic failure.

5.7.1. Disaster Recovery Procedure of Information System

When a failure occurs in system resources and software, the Root CA operating authority conducts an investigation to determine the nature and extent of the failure and a mitigation plan, and restores it using the dually installed system resources and software.

Where relevant, the Root CA should alert its stakeholders so that they can activate their own incident management plan.

5.7.2. Procedures in Case of Information System Resource Damage

In case of damage or loss of key data such as certificates, the Root CA operating authority restores them using the recorded data.

5.7.3. Recovery Procedure for Lost Key

AutoCrypt Root CA performs the following when it is suspected that the private key used for certification is damaged, lost, destroyed or damaged.

- Discontinue operations
- Investigate the issue that caused the compromise and enforce certificate revocation
- Notify and alert the authorities and all stakeholders who have issued the certificates

5.7.4. Securing Business Continuity

AutoCrypt Root CA establishes a business continuity plan so that key/main tasks such as certificate issuance, renewal, and revocation such as certificate issuance, renewal, and revocation, management tasks such as private keys, certification authority review and inspection tasks, and key/major tasks such as digital signature certification technology are not interrupted by information assets and facility asset failures, terrorism, power outages, earthquakes, fires, flood damage, etc.

By establishing a business continuity plan, the most efficient way to maintain business continuity at the time when human and material resource damage occurs, minimizes the period of interruption in the operation of the certification system operating authority and the core business of digital signature certification management, and through a DR center that is more than 10 km away, it is necessary to effectively restore to normal operation, improve the resilience of the information asset infrastructure of the certification system operating authority, and minimize the operational impact caused by business interruption.

5.8. Suspension, Abolition, and Termination of Business

AutoCrypt Root CA is the highest level certification authority, and the termination of the certification authority's work can be decided through consultation with the V2X PKI PA and related stakeholders.

When transferring the work of AutoCrypt Root CA operating authority, the subscriber must be notified of the transfer of the contract at least 90 days in advance, and the contract according to the transfer must be carried out separately. The operating authority to which the work is transferred must undergo the same procedure as adding a new Root CA, and important data related to the existing Root CA work must be transferred safely.

When the service of AutoCrypt Root CA operating authority is terminated, subscribers must be notified at least 180 days in advance. If the termination of the Root CA operating authority cannot guarantee the reliability of the V2X security certification system, the service cannot be terminated.

If the certification work or certification of the Root CA operating authority is suspended in a state where the reliability of the V2X security certification system cannot be guaranteed, civil and criminal responsibilities shall be taken for this.

6. Technical Protection Measures

6.1. Protection of Digital Signature Generation Information

6.1.1. Key Pair Generation Procedure

AutoCrypt Root CA has documented the key pair generation process and meets the following requirements.

- It is created in a safe space equipped with a physical intrusion control system without being connected to internal and external information and communication networks.
- The private key satisfies the V2X security certification system technical standard, and is generated and protected in a hardware security module (HSM) certified by NIST according to the FIPS 140-2 level 3 standard.
- It maintains integrity and authenticity when public keys and related parameters are distributed to subscriber organizations.
- Only authorized persons are allowed to generate the private key, and when generating the private key, it is performed according to the key generation procedure under the control of three or more people.

6.1.2. Private Key Forwarding Procedure

AutoCrypt Root CA does not generate or transmit the subscriber authority private key.

6.1.3. Public Key Forwarding Procedure

The public key generated by the authority applying to become a subscriber authority must be securely delivered (or sent via secure email) to AutoCrypt Root CA using CAMP and IEEE 1609.2 specified protocols to verify ownership of the private key.

The public key of the subscriber authority must be delivered to AutoCrypt Root CA in the form of a certificate issuance request (CSR) including a digital signature using the private key.

6.1.4. Procedure for Providing Public Key to Relevant Parties

The certificate including the public key is provided according to '2.2 Announcement Method'.

Items posted on the website related to certification work are as follows.

- Issued (currently valid) Root CA certificate

6.1.5. Length of key

AutoCrypt supports NIST P-256/SHA-256 and ECDSA (Elliptic Curve Digital Signature Algorithm) specified in IEEE 1609.2 FIPS 186-4, and uses the signature algorithm specified in「Digital Signature Algorithm Specification」. The length of the secret key is 256 bits.

6.1.6. Generate Public Key Parameters and Check Quality

Public key parameters are generated and validated according to the National Institute of Standards and Technology (NIST) FIPS 186-4 technical specification.

6.1.7. Key Usage

The private key of AutoCrypt Root CA is used to sign the certificate and the certificate revocation list, and the purpose of using the key is specified in the certificate permission field.

When a subscriber authority provides certification services, a private key matching the public key certified by AutoCrypt Root CA must be used.

6.2. Digital Signature Creation Information Protection Measures

6.2.1. Criteria for Encryption Module

In order to safely store the private key, the certification authority shall use a security module that satisfies the V2X security certification system technical specification and FIPS 140-2 Level 3 to safely manage the private key so that it is not lost, damaged, stolen, or leaked.

6.2.2. Multiple Control

AutoCrypt Root CA's private key is created and managed under multi-control by two or more operators, with no single person invoking the signing process or accessing the encryption module.

6.2.3. Consignment of Private Keys

AutoCrypt Root CA does not entrust the private key of the subscriber authority.

6.2.4. Private Key Backup

AutoCrypt backs up the private key through multiple control (two or more people) in preparation for damage to the private key and stores it in a safe, and manages encrypted backup keys using the same security module (FIPS 140-2 Level 3 verified HSM) as the key generation.

In addition, in case the private key is damaged, the private key is backed up and stored in a remote DR center for digital signature certification management.

The stored private key manages the encrypted backup key using the same module used within the center.

6.2.5. Storing Private Key

The private key of the Root CA is sealed in a mobile storage medium containing the encrypted private key for safe storage, a copy is stored in the security certification center vault, and a backup copy is stored in the DR center vault.

6.2.6. Private Key Extraction

AutoCrypt Root CA generates a private key in a secure key generation system that is not connected to internal and external information and communications networks and is protected from physical infringement, or in a security module that satisfies the technical specifications of the V2X security certification system.

In order to reactivate the private key stored inside the HSM, a secure encryption module is used through multi-control or technology specified by the encryption module manufacturer.

6.2.7. Storing Private Key

AutoCrypt Root CA generates a private key in a secure key generation system that is not connected to internal and external information and communications networks and is protected from physical infringement, or in a security module that satisfies the technical specifications of the V2X security certification system.

In order to reactivate the private key stored inside the HSM, a secure encryption module is used through multi-control or technology specified by the encryption module manufacturer.

6.2.8. Activate Private Key

The private key stored in the cryptographic module is multi-controlled and used by at least two operators using activation tokens.

6.2.9. Disable Private Key

The private key stored in the encryption module can be deactivated by at least two operators using the deactivation token.

6.2.10. Deleting and Destroying Private Keys

When the validity period of the certificate or private key expires or the private key is damaged or leaked, the

private key storage medium is physically completely destroyed with the approval of the V2X PKI PA, or the private key is deleted according to the technical specifications of the V2X security certification system.

The Root CA and ICA private keys stored in the HSM are destroyed using the method provided by the encryption module, and all backups of the private keys are also destroyed.

6.2.11. Encryption Module Rating

Complies with the encryption module rating specified in '6.2.1 Standards of encryption module'. Uses cryptographic modules validated to FIPS 140-2 level 3.

In order to store the private key safely, the private key is safely managed so that it is not lost, damaged, stolen, or leaked using a security module that meets FIPS 140-2 Level 3 and technical specifications of facilities and equipment of the authorized certification authority.

6.3. Management of Digital Signature Creation Information and Digital Signature Verification Information

The certificate issued by AutoCrypt Root CA is used to confirm and prove that it matches the private key owned by the Root CA or the authority.

6.3.1. Storing Public Key

According to the '5.4.3 Audit Log Retention Period', after the certificate becomes invalid, copies of the public keys of all certification authorities and subscriber authorities are kept according to the record retention procedure for at least 10 years.

AutoCrypt Root CA stores the public key according to '5.5 Record Retention'.

Electronic signature information is stored in a remote location.

6.3.2. Certificate Operation Period and Usage Period

All certificates and their keys do not exceed the validity recommended in the IEEE 1609.2 specification, and the validity period of the certificate is determined in consideration of the scope and use of the certificate, the safety and reliability of the technology used.

The subscriber organization private key must be re-keyed and distributed at least 30 days before the expiration of the validity period.

Each subscriber authority may renew a new certificate or extend the validity of an existing certificate in consultation with the highest certification authority before the expiration of the validity period.

- The validity period of the root CA certificate is 17 years.
- The validity period of the certificate of the subscriber authority issued by the Root CA is as follows.

PG	4 years + 1 week
MA	4 years + 1 week
CRLG	4 years + 1 week
ICA	13 years

By ‘5.4.3 Audit log retention period', AutoCrypt backs up certificates issued by the Root CA, certificate revocation lists, etc. to a physically isolated remote location and stores them for 10 years from the date the certificate expires.

6.4. Data Protection Measures

6.4.1. Generate Activation Data

Activation data is generated according to the technical specifications of the hardware security module (HSM).

Activation data includes PIN, cipher text, and key division system, and the grade of this hardware follows '6.2.11 Encryption Module Rating'.

6.4.2. Activation Data Protection

The procedure used to protect the activation data relies on the data being a PIN number and a key for certification of access. The key for access certification is maintained by a designated administrator, and the PIN number is encrypted and stored according to AutoCrypt encryption policy.

6.4.3. Additional Considerations for Activation Data

Not applicable

6.5. System Security Control

It is managed safely by complying with technical, administrative and physical security measures for related systems and performing security check activities.

In case of logical access such as certification system (hardware, operating system, application software), approval must be obtained in advance through the access approval system or through a draft procedure, and even for authorized trusted parties, access rights are reviewed and updated on a regular basis.

6.5.1. Specific Computer Security Requirements

AutoCrypt establishes a security system for the operating system, server, hardware, and software of the

certification system, and operates the certification system according to security policies, guidelines, and procedures. The certification system and auxiliary system use security certification or equivalent approved hardware and software. The specific computer security requirements details are as follows.

- Certified login function
- Security audit function
- Restricting access control to certification services
- Enforce separation of duties for roles
- Requires identification and certification of roles and associated identities
- Using encryption for database security and external session communication
- Root CA history and audit data

6.5.2. Computer Security Ratings

In order to enter the Root CA room, step-by-step certification is required, and when entering the Root CA room, 2 people must perform multi-factor certification. Multi-factor certification is performed even when logically accessing the system, and the medium to access the system is used only in the Root CA room.

6.6. System Operation Management

6.6.1. System Development Control

When installing the operating system of AutoCrypt certification management system, changing functions, improving performance, and installing equipment, it is carried out under the approval of the chief executive officer of the certification center,

The certification management system development controls are as follows.

- Conduct development in the proposed environment using a documented development process
- Hardware and software are installed in the initial state to prevent tampering with components
- Encryption module is initialized before installation
- The operating system is installed using genuine O/S when installing the server.
- Third-party components, updates and related security patches are applied after verification of authenticity

6.6.2. Security Management Control

Security management control procedures for system configuration and change and V2X software installation follow documented operating policies.

AutoCrypt has appropriate division of duties for all computers (servers) accessing the certification management system, and operates with minimal access rights.

In order to access AutoCrypt Root CA, approval of the certification center and PA is required, and when the work of the accessing personnel changes, the authority is periodically changed.

6.6.3. Lifecycle Security Controls

AutoCrypt periodically checks for potential vulnerabilities in the certification system software, especially all trusted elements exposed to external networks, and applies security patches as necessary.

Vulnerability evaluation of the offline certification system is performed annually, and a quarterly patch plan is established and performed regularly.

6.7. Network Protection Measures

AutoCrypt Root CA operates offline, and if necessary, an intrusion detection system and intrusion prevention system are used for network security.

6.8. Timestamp Service Protection Measures

The time of AutoCrypt Root CA is manually adjusted by referring to the trusted carrier network.

7. Certificate Format

7.1. Certificate Format

The profile of the certificate issued by AutoCrypt Root CA complies with IEEE 1609.2 certificate standard and V2X security certification system technical standard.

The root CA certificate includes the authority to issue and issue CRLs.

The Root CA certificate must indicate authority for a certificate, message, or data type that can be signed.

7.1.1. Certificate Version

AutoCrypt Root CA issues IEEE 1609.2 V3 certificates. (Specify the value of the version field as the number 3)

7.1.2. Certificate Extension

Certificates issued by AutoCrypt Root CA use the certificate extension fields specified in the Root CA certificate profile.

7.1.3. Algorithm Object Identifier

Certificate Algorithm Object Identifier (OID) conforms to the scheme specified in the Root CA certificate profile.

7.1.4. Name Format

Issuer DN and subject DN conform to the scheme specified in the Root CA certificate profile.

7.1.5. Name Restriction

Not applicable

7.1.6. Certificate Policy Object Identifier

The certificate policy object identifier conforms to the Root CA certificate profile scheme.

7.1.7. Use of Policy Restrictions Extensions

The certificate policy object identifier conforms to the Root CA certificate profile scheme.

7.1.8. Policy Qualifier Syntax and Meaning

Not applicable

7.1.9. Handling Semantics for Major Certificate Policy Extensions

The certificate policy object identifier conforms to the Root CA certificate profile scheme.

7.2. Certificate Validation Information Format

It is necessary to revoke the certificate when the organizational information of the certificate holder is changed or the trust of the private key is compromised.

Issues a certificate revocation list (CRL) that complies with IEEE 1609.2 and V2X security certification system technical standards.

7.2.1. Version

AutoCrypt Root CA issues IEEE 1609.2 V3.

7.2.2. Extension Fields

The extension field of the certificate revocation list complies with the V2X PKI certificate profile system.

7.3. Certificate Validation Service Format

AutoCrypt Root CA publishes the certificate revocation list on the center homepage.

7.3.1. Version

Not applicable

7.3.2. Real-Time Certificate Status Validation Field

Not applicable

8. Audit and Evaluation

8.1. Audit and Evaluation Status

Regular audits or evaluations are carried out for efficient security management in the performance of the certification management center.

The audit may not exceed a maximum of one year.

- Every year after the start of operation
- At the direction of the PA after an operation has been disrupted due to a serious security breach or significant audit issue.

8.2. Assessor's Identity and Qualifications

Conduct a web trust audit or equivalent audit at least once a year

The audit body shall have the following qualifications.

- A person who is independent of the audited person
- A person who has sufficient knowledge of domestic and foreign laws and systems and related technical standards
- PKI technology, information communication technology and information system audit

related experts

- Relevant International Qualifications WebTrust, ETSI or equivalent

8.3. Relationship Between the Subject of Evaluation and the Evaluator

The auditor (audit authority) shall select an external audit authority that has no financial or business interest with the subject to be audited.

8.4. Purpose and Content of the Evaluation

The scope of auditing includes CPS compliance of AutoCrypt Root CA, certificate authority key management, certificate management, and root CA system management.

The details of the audit scope are specified in the certification policy.

Customers operating a PCA under a CA license that refers to Certification Practices Statement shall undergo an annual self-audit and report any misconduct and actions taken to address it to the PA.

8.5. Actions on Nonconformities

If the audit reports non-compliance with applicable law, this CPS or contractual obligations with respect to the services described herein, a plan to correct such non-compliance should be developed according to the approval of the relevant and third parties that are legally obligated to secure the certification system, such as the Root CA.

Deficiencies and singularities discovered through the audit are included in the report, and policy and technical measures are taken according to the audit results, and the scope is determined according to the degree of impact. Actions are executed within a reasonable time in accordance with the remedial plan, and if appropriate action is not taken, the certificate may be revoked and the CA may be instructed to suspend until corrective action is taken or policy relaxed.

8.6. Report of Results

All evaluation results are reported to the PA. If necessary, some evaluation results may be provided to stakeholders.

All other audit information is considered confidential business information in accordance with 9.3.

9. Other Matters Such As Guarantee of Digital Signature Certification Service

9.1. Fee

9.1.1. Certificate Issuance and Renewal Fees

All fees for certificate issuance and certificate service follow the business agreement (contract) between AutoCrypt Root CA and the certificate service contractor.

9.1.2. Certificate Access Charges

No fee is charged to the trusted party who reads and verifies the certificate.

9.1.3. Verification Fee for Certificate Revocation List Information

No fee is charged to the trust party accessing the certificate suspension and revocation list

9.1.4. Other Service Charges

Fees for other services may be charged if necessary.

9.1.5. Refund Policy

Refunds due to withdrawal of the certificate issuance application will be refunded only if a certificate issuance fee is charged.

9.2. Compensation

AutoCrypt Root CA is not responsible for damage, war, delay in the processing of certification work due to force majeure, such as natural disasters, or inability to process due to reasons other than those stipulated in the relevant Act, the Enforcement Decree of the relevant Act, the Enforcement Rules or Certification Practices Statement of Root CA in relation to the certification work.

The financial responsibility between AutoCrypt Root CA and the certification service contractor follows the business agreement (contract).

9.2.1. Insurance Coverage

Not applicable

9.2.2. Other Assets

Not applicable

9.2.3. Insurance or Warranty Coverage

Not applicable

9.3. Trade Secret

9.3.1. Scope of Confidential Information

AutoCrypt Root CA classifies business information and security-sensitive internal information as company confidential and protects confidential information by complying with internal security policies.

Implement security controls related to the sensitivity of information to prevent disclosure of confidential information to the public or unauthorized personnel.

Depending on the circumstances, some information may be shared with the contractor in a Non-Disclosure Agreement (NDA), and the scope of confidential information is as follows.

- All business continuity incident response, emergency and disaster recovery plans
- Other security practices, measures, mechanisms, plans or procedures used to protect the confidentiality, integrity or availability of information
- All information held by AutoCrypt Co., Ltd. is kept as personal information in accordance with Section 9.4
- All transactions, audit records and archive storage records identified in Section 5.4 or 5.5
- Certificate application and documents submitted to support the certificate application
- Transaction, financial audit, external or internal audit trail records and detailed audit reports

9.3.2. Information Outside the Scope of Confidential Information

Certificates issued to subscriber organizations, status information such as certificate revocation, and information announced in relation to the work of the top certification authority are not considered confidential information, and the external auditor's audit report summary letter (E-mail) is also not considered confidential.

Information that does not affect the safety and reliability of certification work is disclosed.

9.3.3. Responsibilities for Protecting Confidential Information

All users (authorities, organizations, and institutes) who have entered into a certification business agreement (contract) with AutoCrypt Root CA shall comply with the provisions of AutoCrypt Privacy Policy (refer to Section 9.4) regarding the protection of personal data considered confidential, and have the duty and responsibility to maintain confidentiality.

9.4. Privacy Protection

AutoCrypt Root CA safely manages personal information related to certification work in accordance with laws and regulations related to personal information protection.

9.4.1. Privacy Protection Plan

AutoCrypt Root CA complies with laws and regulations related to personal information protection for the protection of personal information related to certification work, and collects, retains, and processes personal information in accordance with the privacy policy posted on the website.

9.4.2. Information That is Considered Personal Information

Certificate applicant contact information, business terms, customer certificate volume, and end-user pseudonymous certificate links are considered personal information that requires non-disclosure.

9.4.3. Information That is Not Considered Personal Information

Personal or company information displayed in certificates, CRLs and such information is not considered personal information that is subject to non-disclosure.

9.4.4. Privacy Protection Obligation

V2X PKI security certification centers and authorities shall take reasonable precautions to prevent unauthorized disclosure of personal information by using appropriate protective measures. Comply with laws and regulations on the protection of personal information.

9.4.5. Notice and Consent to Use of Personal Information

AutoCrypt Root CA may use personal information in accordance with the express written consent of the personal information subject or in accordance with applicable laws or court orders, and use personal information after obtaining notice and consent for the collection and use of personal information and provision to third parties.

9.4.6. Disclosure in Accordance With Judicial or Administrative Procedures

AutoCrypt Root CA will not disclose confidential information without a reasonable and specific request from an authorized party, except where disclosure of personal or confidential information is required by law.

- Parties obligated to keep information confidential
- When a party requests such information
- Where there is a valid, enforceable and undisputed court order

9.4.7. Other Information Disclosure Standards

All AutoCrypt employees strictly comply with all information, including the requirements of the relevant laws of the Republic of Korea related to the protection of personal data and confidential information.

9.5. Intellectual Property Rights

Intellectual property rights related to certificate issuance and private keys belong to AutoCrypt Root CA in accordance with the Copyright Act and other relevant laws.

AutoCrypt Root CA protects its own trademarks and respects the trademarks of others (others), and seeks the permission of the trademark owner in advance before promoting another company's trademark on the website or other services (portal, media, social media, etc.).

Certificates issued to Subscriber Authorities are the exclusive property of AutoCrypt Root CA, which authorizes Subscriber Authorities to replicate and distribute certificates in accordance with business agreements.

AutoCrypt Root CA reserves the right to revoke certificates it has issued at any time in its sole discretion.

- Software and hardware developed by AutoCrypt Root CA
- AutoCrypt Root CA Certification Practice Statement
- Name of AutoCrypt Root CA
- Digital signature generation information generated by AutoCrypt Root CA, etc.

9.6. Guarantee

9.6.1. Certification Authority Guarantee

AutoCrypt Root CA guarantees the following regarding certificates.

- The fact that it must be included in the issued certificate
- The fact that the certificate was issued in accordance with the provisions of relevant laws
- The fact that there is no doubt about the revocation of the certificate

9.6.2. Registrar Guarantee

Not applicable

9.6.3. User Warranty

Not applicable

9.6.4. Relying Party Guarantee

Not applicable

9.6.5. Other Participant Guarantee

Not applicable

9.7. Warranty Exclusions

Except as otherwise expressly stated and warranted in this Certificate Policy or as specified in the applicable Business Agreement (Contract), AutoCrypt Root CA disclaims any warranties expressed or implied.

9.8. Coverage of Insurance

AutoCrypt Root CA is not responsible for damage, war, delay in the processing of certification work due to force majeure, such as natural disasters, or inability to process due to reasons other than those stipulated in the relevant Act, the Enforcement Decree of the relevant Act, the Enforcement Rules or Certification Practices Statement in relation to the certification work.

9.9. Limitations of Liability

AutoCrypt Root CA is not responsible for damage, war, delay in the processing of certification work due to force majeure, such as natural disasters, or inability to process due to reasons other than those stipulated in the relevant Act, the Enforcement Decree of the relevant Act, the Enforcement Rules or Certification Practices Statement in relation to the certification work.

9.10. Effect of Statements

9.10.1. Validity period

The issued certificate policy and certificate validity period follow AutoCrypt Root CA certification policy, and the contents take effect after being posted on AutoCrypt website.

9.10.2. Termination

Amendments to this document become effective after being posted to the repository, and remain in effect until superseded or terminated by a new version. The process of renewing this CPS and any changes that may affect contractors are communicated to stakeholders as described in '1.5.4 Certification Practices Statement Approval Procedure'.

9.10.3. Effect After Termination

Matters related to certificate revocation and continuation are subject to the business agreement (contract).

Even if V2X PKI Certification Practices Statement is revised, the responsibility for important information remains valid.

9.11. Notice and Communication

The contact information for notifications or inquiries is as follows.

- Department: AutoCrypt V2X PKI Root CA Security Certification Center
- Phone Number: +82-2-2125-4020
- Address: (07241) 6F Sewoo Building, 115 Yeouigongwon-ro, Yeongdeungpo-gu, Seoul, South Korea
- E-mail: rootca@autocrypt.io

9.12. History Management

9.12.1. Revision Procedure

Refer to the certification process and approval process in '1.5.4 Certification Practices Statement Approval Procedure'.

9.12.2. Announcement of Revision

Refer to the certification process and approval process in '1.5.4 Certification Practices Statement Approval Procedure'.

If there is a change in Certification Practice Statement, it will be posted on the V2X PKI Security Certification Center website.

- Certification Practices Statement URL: https://autocrypt.io/services/v2x-pki-ca

9.12.3. Changes in the Certification Scheme Identification Name

Certificate Policy OIDs do not apply to IEEE 1609.2 certificates.

9.13. Settlement of Disputes

If a dispute arises in relation to the certification work, it shall be resolved in accordance with relevant laws and contracts.

9.14. Competent Court

This Certification Practices Statement shall be interpreted and applied in accordance with the relevant laws and regulations of the Republic of Korea, and in case of conflict, the higher law shall prevail.

Legal matters related to certification are specified in the business agreement (contract).

9.15. Compliance With Applicable Laws

AutoCrypt Root CA aims to comply with all relevant laws and regulations that provide certification services such as certification, issuance, management, and revocation of certificates.

9.16. Other Regulations

Other regulations can be found in the applicable business agreement (contract).

9.16.1. Complete Agreement

Not applicable

9.16.2. Conveyance

Not applicable

9.16.3. Separated Clause

Not applicable

9.16.4. Enforcement (Attorney Fees and Waiver)

Not applicable

9.16.5. Irresistible Force

Failure to comply with the statements due to events beyond the reasonable control of the parties to Certification Practice Statement, such as war, terrorism, natural disasters, the Internet or other infrastructure failures, shall be judged to be force majeure.

9.17. Other Provisions

Other provisions such as the scope of the contract, the completeness of the contract, the execution of the contract and force majeure shall be governed by the applicable business agreement (contract).